СТРУКТУРА СОДЕРЖАТЕЛЬНОЙ ЧАСТИ УЧЕБНОЙ ДИСЦИПЛИНЫ “СТАНДАРТИЗАЦИЯ И СЕРТИФИКАЦИЯ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ”

***А.В. Потий**, к.т.н.,*
Харьковский национальный университет радиоэлектроники

Учебная дисциплина “Стандартизация и сертификация в области защиты информации” подготовлена и введена в учебный процесс в соответствии с учебным планом подготовки специалистов по направлению подготовки 0914 “Компьютеризованные системы, автоматика и управление” по специальности 091403 “Защита информации с ограниченным доступом и автоматизация её обработки”.

Одной из многочисленных задач, возникших в процессе подготовки дисциплины, являлась задача информационного наполнения и структурирования содержательной части дисциплины. В данной статье автором предложена структура содержательной части дисциплины. На основе требований нормативных документов в области образования, предлагается блочно-модульная структура дисциплины, дальнейшая декомпозиция которой позволит построить структурно-логическую схему дисциплины. Информационное наполнение блоков и модулей, формулировка знаний и умений, которые должны быть сформированы в ходе освоения каждого блока, осуществлялись на основе разработанных в Харьковском техническом университете радиоэлектроники образовательно-профессиональной программы и образовательно-квалификационной характеристики данного специалиста.

Содержание дисциплины состоит из трех образовательных блоков:

Блок 1. Научно-методические и организационные основы стандартизации.

Блок 2. Стандарты и нормативные документы в области защиты информации.

Блок 3. Сертификация в области защиты информации.

Рассмотрим содержание этих блоков подробнее.

Модуль 1.1. содержит в себе две группы образовательных элементов, которые направлены на раскрытие, соответственно, сущности стандартизации вообще и организации работ по стандартизации в Украине. В процессе обучения изучаются вопросы сущности и содержания стандартизации, категории и виды нормативных документов, порядок их применения и ответственность за нарушение требований нормативных документов.

При рассмотрении вопросов организации работ по стандартизации в Украине особое внимание уделяется правовым основам стандартизации в нашем государстве. Рассматриваются также организационная структура

Государственного комитета по стандартизации Украины, порядок разработки государственных стандартов Украины и организация Государственного надзора за соблюдением обязательных требований нормативных документов.

Основной учебной целью изучения данного модуля является формирование ознакомительно-ориентировочных знаний по вопросам организации работ по стандартизации, а также стройной системы взглядов на процесс стандартизации как научной и практической деятельности государственных органов власти, учреждений, предприятий, научно-технических обществ и других организаций. С практической точки зрения ставится задача сформировать умения работы с нормативными документами и анализа отечественной нормативно-правовой базы, регламентирующей процесс стандартизации в Украине.

Рис. 1. Структура первого образовательного блока

Блок 2. Стандарты и нормативные документы в области защиты информации.

Второй блок образовательных модулей посвящен рассмотрению рекомендаций и требований конкретных нормативных документов и стандартов. Блок включает три образовательных модуля (рис. 2).

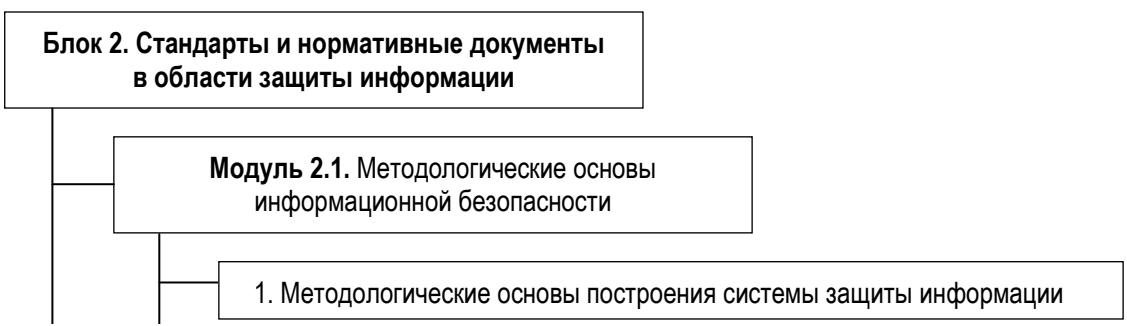

Рис. 2. Структура второго образовательного блока

Содержание элементов модуля 2.1. направлено на изучение методологических основ разработки и построения систем защиты информации. Модуль состоит из четырех групп образовательных элементов. При изучении методологических основ информационной безопасности особое внимание уделяется нормативным документам, определяющим концептуальные вопросы обеспечения безопасности информации и вопросам разработки политики безопасности. При этом в первую очередь делается упор на освещение этих вопросов в отечественной нормативной базе, а также в руководящих документах Гостехкомиссии РФ и рекомендациях ISO.

Анализ рисков и разработка системы управления безопасностью являются важными этапами разработки системы защиты информации. Данные вопросы выделены в отдельную группу образовательных элементов.

Модель анализа рисков, методики их оценки, формирование системы управления безопасности рассматриваются на основе международного стандарта ISO/IEC 13335, а также стандартов Великобритании и Германии, которые признаны лучшими документами в этой области и отличаются высоким качеством проработки.

Третья группа элементов введена для изучения нормативных документов по архитектуре безопасности, а именно стандартов ISO 7498-2 и ISO/IEC10181. Данные стандарты определяют функции и механизмы безопасности.

Наконец, четвертая группа элементов необходима для изучения нового международного документа ISO/IEC 15408 “Общие критерии оценки безопасности информационных технологий”, который, по сути, описывает все функциональные требования к системам защиты информации. Тут же дается сравнительная характеристика соответствующего украинского национального документа НД ТЗИ 2.5-004-99 “Критерии оценки защищенности информации в компьютерных системах от несанкционированного доступа”.

1. Группа образовательных элементов “Механизмы конфиденциальности” направлена на изучение порядка регистрации криптографических алгоритмов в международном реестре, режимов работы блочных шифров, применения существующих стандартов блочного шифрования (ГОСТ 28147-89, DES, Triple DES, IDEA, Skipjack). В модуль введены сведения о новом стандарте блочного шифрования Rijndael, а также о финалистах конкурса NIST – алгоритмах блочного шифрования RC6, MARS, Twofish и Serpent. Также рассматриваются алгоритмы-кандидаты на европейский стандарт блочного и поточного шифрования.

2. Вторая группа образовательных элементов предполагает изучение парольных систем идентификации, правил введения меток и атрибутов безопасности, протоколов идентификации и аутентификации объектов. Основной информационной базой данной группы выступают международный стандарт ISO/IEC 9798, Руководящие документы Гостехкомиссии России и национальные стандарты США (FIPS 112, FIPS 181).

3. Изучению механизмов обеспечения целостности данных и цифровой подписи посвящена третья группа образовательных элементов. Здесь рассматриваются принципы и модели обеспечения целостности данных, методы вычисления и применения MAC-кодов (MAC на основе блочных алгоритмов шифрования, алгоритмы MDC-2, MDC-4, HMAC, MAA) и хеш-кодов (семейство хеш-функций MDx, RIPEMD, SHA-1 и ГОСТ 34.11). Отдельным вопросом является изучение стандартов цифровых подписей. Основой здесь выступают международные стандарты ISO/IEC 9796, ISO/IEC 14888, а также стандарт IEEE 1363, стандарт РФ ГОСТ 34.10 и проект Украинского стандарта цифровой подписи на эллиптической кривой.

4. При решении задач аутентификации, проверки целостности, подтверждения подлинности, непричастности важную роль играет третья

доверительная сторона (ДТС). Условия функционирования, требования к ДТС, их классификация, администрирование, службы рассматриваются в четвертой группе образовательных элементов. Здесь же рассматриваются механизмы неотказуемости, определяемые международным стандартом ISO/IEC 13888.

5. Наконец, пятая группа образовательных элементов посвящена рассмотрению общего механизма безопасности – аудита безопасности. Здесь на основе международных и национальных стандартов излагаются задачи аудита безопасности, рассматриваются вопросы структурного и функционального построения систем аудита, методики, методы и средства проведения аудита безопасности.

В последнее время, в связи с широким использованием несимметричных криптосистем большую важность приобрела задача сертификации ключей. В условиях реального перехода на электронный документооборот построение национальных и корпоративных систем сертификации ключей являются актуальными задачами. Рекомендации нормативных документов по данному вопросу рассматриваются во второй группе образовательных элементов. Здесь рассматриваются рекомендации международного стандарта ISO 11166, стандарта ITU X509v3, рекомендации IETF RFC2459, RFC2510, RFC2527 и других документов по созданию инфраструктуры открытых ключей. Студенты изучают задачи и модели сертификации ключей, основы разработки правил организации сертификации ключей как составляющей части политики безопасности, протоколы управления сертификатами.

Таким образом, содержание блока “Стандарты и нормативные документы в области защиты информации” является основой учебной дисциплины. Главная задача изучения блока – получить знания о совокупности стандартов механизмов безопасности, рекомендованных методах реализации механизмов безопасности, а также приобрести умения по применению требований и рекомендаций нормативных документов при решении практических задач по организации защиты информации.

В данной статье изложен взгляд автора на структуру и информационное наполнение содержательной части дисциплины “Стандартизация и сертификация в области защиты информации”. Анализ каждого блока и модуля дисциплины в конечном итоге облегчает задачу формирования перечня знаний и умений специалиста, который он должен приобрести в ходе изучения всего курса. Опыт двухлетнего изложения данного курса показал, что такое построение является достаточно рациональным. В курсе гармонично сочетаются как специальные вопросы в области криптографической и технической защиты информации, так и общие вопросы организации работ по стандартизации и сертификации в области защиты информации. Основной сложностью как подготовки, так и освоения данного курса является достаточно большой массив изучаемых нормативных документов. При изучении данного курса большая роль отводится самостоятельной работе студентов с нормативными документами, поскольку на лекционных занятиях не имеется возможности излагать содержание

конкретных стандартов. В связи с этим принято решение, что данный курс преподается на пятом, выпускном курсе, непосредственно перед производственной практикой и дипломным проектированием. В этом случае уровень подготовки студентов позволяет самостоятельно изучать отдельные конкретные алгоритмы и реализационные решения, рекомендуемые стандартами.

Усиление роли учебной дисциплины видится в отражении изучаемых вопросов в дипломных работах и проектах. Так, при постановке задачи на исследование в дипломной работе целесообразно требовать сравнительной оценки предлагаемого решения с имеющимися решениями, изложенными в нормативных документах. При выполнении дипломных проектов использование нормативных документов должно быть обязательным.

В перспективе предполагается, что на преддипломную практику студентам будут выдаваться задания, направленные на решение для типовых конфигураций объектов защиты таких задач, как анализ и оценка рисков, разработка системы управления безопасностью, разработка профиля и проекта защиты, проведение аттестации и квалификационного анализа предложенных решений. Причем все эти задачи должны решаться на основе грамотно использованной как отечественной, так и зарубежной и международной нормативной базы.

Данная учебная дисциплина является новой и актуальной. Ее становление и введение в учебный процесс не лишено методических и практических проблем, таких как:

- разработка структурно-логической схемы учебной дисциплины;
- разработка плана и содержания методических указаний и конспектов лекций по изучению блоков и модулей дисциплины;
- разработка согласованной и объективной системы оценки знаний и умений студентов с использованием модульно-рейтинговой системы;
- методическое и информационное обеспечение дисциплины и др.

Подходы к решению этих и других задач будут рассмотрены автором в дальнейших публикациях.

Потий, А.В. Структура содержательной части учебной дисциплины "Стандартизация и сертификация в области защиты информации" [Текст] / А. В. Потий // Проблеми і перспективи розвитку банківської системи України: зб. наук. праць. – Суми: УАБС НБУ 2002. - Т.6.– С. 230-236.