Предисловие

Тематика учебного пособия «Межсетевые экраны» относится к области «Информационная технология», раздел «Сетевые технологии», подраздел «Сетевая безопасность». Объектом рассмотрения являются межсетевые экраны (МЭ) как наиболее часто используемые программные или программно-аппаратные комплексы при построении систем обработки информации в защищенном исполнении (например, информационные системы). В учебном пособии предметом рассмотрения являются технологии, реализуемые МЭ как средство обеспечения сетевой безопасности, в том числе их практическое использование.

При подготовке данного Учебного пособия авторы исходили из того, что профессионалы в области сетевой безопасности должны обладать современными профессиональными компетенциями (ПК), необходимыми для решения конкретных профессиональных задач и реализации конкретных трудовых функций.

Формирование ПК относится к задачам, решаемым существующей системой образования, нормативной базой которого является комплекс Федеральных государственных образовательных стандартов (ФГОС) высшего образования (ВО). В данном случае речь идет о ФГОС ВО, относящихся к Укрупненной группе специальностей и направлений подготовки (УГСНП) 10.00.00 «Информационная безопасность». При разработки ФГОС последнего поколения (ФГОС++) были сформулированы общепрофессиональные компетенции (ОПК) выпускников, прошедших обучение в рамках определенного ФГОС [П1].

Эти ПК можно связать с положениями действующих в настоящее время профессиональных стандартов (ПС), относящихся к группе занятий (профессий) «Специалисты в области информационной безопасности» [П2].

Анализ указанных выше ФГОС и ПС позволил установить связь объекта и предмета рассмотрения учебным пособием с определенными образовательными и профессиональными стандартами:

- ФГОС ВО по направлению подготовки 10.04.01 «Информационная безопасность» (уровень магистратура);
- ПС 06.032. Специалист по безопасности компьютерных систем и сетей (вид профессиональной деятельности: защита информации в компьютерных системах и сетях);

- ПС 06.033. Специалист по защите информации в автоматизированных системах (АС) (вид профессиональной деятельности: обеспечение безопасности информации в АС).

Содержание учебного пособия непосредственно соответствует ОПК, сформулированным в ФГОС 10.04.01. Конкретная программа магистратуры, реализуемая в рамках данного образовательного стандарта, должна устанавливать следующие ОПК. Выпускник должен быть способен:

- обосновывать требования к системе обеспечения информационной безопасности (ИБ) и разрабатывать проект технического задания на ее создание (ОПК-1);
- разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения ИБ (ОПК-2).

Программа магистратуры должна обеспечивать реализацию дисциплин, обозначенных в ФГОС 10.04.01 как базовые дисциплины профессионального модуля. Среди них можно выделить дисциплину, которой соответствует тематика учебного пособия: «Технологии обеспечения информационной безопасности» (ТОИБ).

Проект примерной основной образовательной программы магистратуры по ФГОС ВО 10.04.01 устанавливает связь между дисциплиной ТОИБ и ОПК-1 и ОПК-2 путем формулирования индикаторов достижения (ИД) ОПК [П3].

ИД ОПК-1 и ОПК-2 приведены в табл. П1 для дисциплины ТОИБ (индикаторы скорректированы по отношению к индикаторам, приведенным в [П3]).

Приведенные выше ИД ОПК с привязкой к дисциплине ТОИБ могут быть сопоставлены с обобщенными трудовыми функциями (ОТФ) и связанными с ними трудовыми функциями (ТФ), при-

Таблица П1

ИД ОПК-1 и ОПК-2 для дисциплины ТОИБ

Код ИД	Индикаторы достижения ОПК-1
ОПК-1.1.1	Знать основы отечественных и зарубежных стандартов в области обеспечения ИБ
ОПК-1.2.1	Уметь проектировать техническое задание на создание системы обеспечения ИБ
ОПК-1.3.1	Владеть навыками участия в разработке системы обеспечения ИБ
Код ИД	Индикаторы достижения ОПК-2
ОПК-2.1.1	Знать методы концептуального проектирования технологий обеспечения ИБ
ОПК-2.2.1	Уметь выбирать и обосновывать применение методов решения задач обеспечения ИБ
ОПК-2.3.1	Владеть навыками выполнения работы при разработке и эксплуатации систем и средств обеспечения ИБ

веденными в профессиональных стандартах ПС 06.032 и ПС 06.033. При этом выделены только те ОТФ и ТФ, которые имеют отношение к тематике учебного пособия.

Для дисциплины ТОИБ:

ПС-06-032. Специалист по безопасности компьютерных систем и сетей.

ОТФ-C. Оценивание уровня безопасности компьютерных систем и сетей:

ТФ-C/01.7. Проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации (СЗИ);

ТФ-C/02.7. Разработка требований по защите, формирование политик безопасности компьютерных систем и сетей.

ОТФ-D: Разработка программно-аппаратных СЗИ компьютерных систем и сетей:

ТФ-D/01.8. Разработка требований к программно-аппаратным СЗИ компьютерных систем и сетей;

ТФ-D/02.8. Проектирование программно-аппаратных СЗИ компьютерных систем и сетей;

ТФ-D/03.8. Разработка и тестирование СЗИ компьютерных систем и сетей;

ТФ-D/04.8. Сопровождение разработки СЗИ компьютерных систем и сетей.

ПС-06-033. Специалист по защите информации в автоматизированных системах (АС).

ОТФ-D. Разработка систем защиты информации АС:

ТФ-D/01.7. Тестирование систем защиты информации АС;

ТФ-D/02.7. Разработка проектных решений по защите информации в АС;

ТФ-D/03.7. Разработка эксплуатационной документации на системы защиты информации АС;

ТФ-D/04.7. Разработка программных и программно-аппаратных средств для систем защиты информации АС.

ОТФ-E. Формирование требований к защите информации в АС:

ТФ-E/01.8. Обоснование необходимости защиты информации в АС;

ТФ-E/02.8. Определение угроз безопасности информации, обрабатываемой АС;

ТФ-E/03.8. Разработка архитектуры системы защиты информации АС;

ТФ-Е/04.8. Моделирование защищенных АС с целью анализа их уязвимостей и эффективности средств и способов защиты информации.

На этапе разработки рабочих планов конкретной магистерской программы и рабочих программ конкретных дисциплин должен быть расширен компетентностный подход путем формулирования ПК и соответствующих им ИД.

В Национальном исследовательском ядерном университете «МИФИ» (НИЯУ МИФИ) накоплен обширный опыт подготовки магистров по направлению 10.04.01. В настоящее время в НИЯУ МИФИ реализуются следующие магистерские программы [П4]:

МП-1. Безопасность данных и криптография;

МП-2. Информационно-аналитическое обеспечение финансового мониторинга;

МП-3. Обеспечение безопасности значимых объектов критической информационной инфраструктуры;

МП-4. Обеспечение непрерывности и ИБ бизнеса;

МП-5. Теоретическая и практическая криптография.

Для этих магистерских программ были дополнительно сформулированы ПК, а для каждой магистерской программы дополнительно определены специальные ПК (СПК). Ниже приведем ПК и СПК, имеющие отношения к реализации учебной дисциплины ТОИБ в части учебного модуля «Межсетевые экраны» для всех магистерских программ (ПК) и в качестве примера для магистерской программы МП-4 (СПК). Выпускник должен быть способен:

- принимать участие в разработке систем обеспечения ИБ или информационно-аналитических систем безопасности (ПК-1);
- разрабатывать технические задания на проектирование систем обеспечения ИБ или информационно-аналитических систем безопасности (ПК-2);
- планировать и организовывать предпроектное исследование объектов обеспечения ИБ или объектов информационно-аналитических систем безопасности (ПК-3);
- на практике применять стандарты, относящиеся к обеспечению непрерывности бизнеса и обеспечению ИБ (СПК-1);
- участвовать в проектировании, эксплуатации, контроле и совершенствовании системы обеспечения ИБ объекта и системы обеспечения непрерывности бизнеса организации (СПК-2).

Учебное пособие состоит из введения, пяти разделов, заключения и приложения.

Во введении обосновывается актуальность использования МЭ при построении защищенных вычислительных сетей, а также определяется место МЭ в системе обеспечения ИБ таких объектов.

В первом разделе рассматривается эволюция средств обеспечения сетевой безопасности, которая привела к появлению МЭ. Определяются задачи, решаемые МЭ при защите информационного взаимодействия, организованного с использованием сетевых информационных технологий (ИТ). Вводится определение МЭ и рассматривается нормативная база, относящаяся к вопросам применения МЭ.

Во втором разделе описывается краткая эволюция МЭ, позволяющая проследить усложнение функциональных возможностей МЭ по мере их усовершенствования при обеспечении сетевой безопасности. Отдельно рассматривается основная функция МЭ, связанная с фильтрацией сетевого трафика на различных уровнях эталонной модели взаимодействия открытых систем OSI/ISO (Open System Interaction/International Standard Organization), а также определены типовые функциональные подсистемы МЭ.

В третьем разделе представлены классификации МЭ в отношении области применения, исполнения, схемы подключения (размещения), используемой технологии анализа трафика и функционирования на соответствующем уровне модели OSI/ISO.

В четвертом разделе описаны основные виды МЭ по мере усложнения их функционала — это экранирующие концентраторы, пакетные фильтры, шлюзы сеансового и прикладного уровней, МЭ экспертного уровня, а также персональные МЭ, UTM-устройства (Unified Threat Management) и МЭ с DPI (Deep Packet Inspection) и МЭ следующего поколения (Next Generation Firewall — NGFW).

В пятом разделе приводятся заключительные замечания, которые посвящены таким вопросам, как совместное размещение в интранете традиционных МЭ и средств построения виртуальных частных сетей, уязвимости МЭ по базам данных Федеральной службы по техническому и экпортному контролю Российской Федерации (ФСТЭК России), CVE (Common Vulnerabilities and Explosures) и американской базе NVD (National Vulnerability Database), критерии выбора конкретного МЭ для использования в организации (в том числе и требования к сертификации МЭ в России и за рубежом), а также сертифицированные в России и зарубежом МЭ.

В заключении рассмотрены перспективы разработки и использования современных МЭ.

В приложении представлена программа учебного модуля М-МЭ, входящего в учебную программу дисциплин ТОИБ и имеющего от-

ношение к тематике учебного пособия, а также приведены рекомендации по его реализации в учебной дисциплине.

В конце каждого раздела приведены вопросы для самоконтроля.

В результате изучения учебного пособия, а также освоения учебного модуля М-МЭ, входящего в учебную программу дисциплины ТОИБ, у обучаемых должны быть сформированы определенные уровни знаний и умений, которые являются ИД ПК, описанных выше. Обучаемые должны:

знать:

- терминологию, относящуюся к разработке и использованию МЭ;
- основные вехи эволюционного развития средств обеспечения сетевой безопасности и МЭ;
- основные виды сетевых соединений;
- нормативную базу, относящуюся к МЭ;
- профили защиты для МЭ (на основе стандарта ИСО/МЭК 15408-2002 и ФСТЭК России);
- особенности обеспечения сетевой безопасности с применением шлюзов безопасности (на базе международного стандарта ISO/IEC 27033-4:2014);
- особенности обеспечения сетевой безопасности с применением межсетевых экранов (на базе специальной публикации Национального института стандартов и технологий США NIST SP 800-41);
- назначение и основные функции МЭ;
- современные классификации МЭ и их критерии;
- основные виды МЭ и критерии выбора определенных видов МЭ;
- особенности совместного использования традиционных МЭ и средств построения виртуальных частных сетей;
- особенности сертификации МЭ;

уметь:

- применять терминологию, относящуюся к разработке и использованию МЭ;
- использовать нормативную базу и рекомендации национальных и международных стандартов при разработке и использовании МЭ;
- формулировать задачи, решаемые при защите информационного взаимодействия в сетях;
- определять функциональную структуру МЭ;
- классифицировать МЭ по различным критериям;

- проводить сравнение различных видов МЭ по разным критериям;
- обосновано выбирать определенный вид МЭ для конкретной сетевой структуры;
- определять уязвимости конкретных МЭ на основе анализа существующих баз данных (например, ФСТЭК России, CVE или NVD).

Предлагаемое учебное пособие может быть полезным не только в случае подготовки магистров по направлению 10.04.01, но и при разработке и реализации отдельных программ дополнительного образования (повышения квалификации и профессиональной переподготовки).

Использованные источники

П1. Методические материалы XXII Пленума ФУМО ВО ИБ. Проекты ФГОС ВО 3++ УГСНП 10.00.00 «Информационная безопасность» (Краснодар, 2–7 октября 2018 г.) / Разраб.: Е.Б. Белов и др. Краснодар: Издательский дом «Юг», 2018. 140 с.

П2. Научно-методические и нормативные материалы XX пленума ФУМО ВО ИБ. Сборник профессиональных стандартов по группе занятий (профессий) «Специалисты в области информационной безопасности». Москва, 23–28 ноября 2016 г. 198 с.

П3. Методические материалы XXIII Пленума ФУМО ВО ИБ. Часть 1. Проекты примерных основных образовательных программ бакалавриата и магистратуры (по ФГОС ВО 3++) УГСНП 10.00.00 «Информационная безопасность». Ставрополь, 1–5 октября 2019 г. 52 с.

П4. Подготовка магистров по направлению 10.04.01: Рабочие учебные планы и компетентностные модели. URL: http://www.mephi.ru.