S. V. Zapechnikov

Educational and Methodical Maintenance of "Open Information Systems" Discipline

Keywords: information technology, open information systems, information security, specialists training, educational and methodical maintenance

The educational and methodical complex for the "Open Information Systems" discipline has been prepared at the "Cybernetics and Information Security" faculty as part of the teaching curricula upgrade for the transition to the 3-generation educational standards. The main content of the discipline is devoted to the issues of development of information technologies, including model representation and standardization of information systems.

С. В. Запечников

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ «ОТКРЫТЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ»

Дисциплина «Открытые информационные системы» — одна из базовых дисциплин общепрофессионального цикла. Изучение этой дисциплины имеет целью познакомить студентов с важными концепциями, заложенными в основу развития информационных технологий в 1970—1980-е годы, последовательно и строго проводившимися в жизнь международными организациями по стандартизации и крупными фирмами-производителями и позволившими к началу 2000-х годов сформировать глобальную среду открытой распределенной обработки, хранения и передачи данных.

Учебные занятия по дисциплине состоят из лекций и лабораторных работ. Форма итогового контроля успеваемости — зачет.

Курс лекций по дисциплине «Открытые информационные системы» посвящен изучению теоретических и методологических вопросов развития информационных технологий, поддерживающих концепцию открытости, на современном этапе. Часть лекционного курса подана на историческом материале, показывающем эволюцию информационных технологий от первых электронно-вычислительных машин, сконструированных в середине XX в., до современных концепций сред облачных вычислений и технологий обработки «больших данных» (big data).

В таблице 1 приведен календарный план лекционного курса.

Таблица 1. Календарный план лекционных занятий по дисциплине «Открытые информационные системы»

Учебная неделя, кол-во часов, наименование темы	**Содержание занятий**
1 неделя (3 часа). Очерк истории информационных технологий.	Предпосылки возникновения концепции открытых систем. Классификация IT-систем, исторические пути развития вычислительной техники, операционных систем, прикладного ПО, Интернета, распределенных систем. Проблемы обеспечения совместимости IT-систем. Требования к совместимости систем. Переносимость и способность к взаимодействию.

2 неделя (3 часа). Основы стандартизации.	Понятие стандарта. Виды стандартов. Международные организации, занимающиеся стандартизацией информационных технологий. Формы систематизации стандартов. Государственная система технического регулирования и стандартизации в РФ. Метрология как основа стандартизации. Управление качеством. Гармонизация российских и международных стандартов.
3 неделя (3 часа). Модели открытых систем. Системный подход к описанию функциональности.	Составляющие понятия совместимости. Базовая модель информационной системы (ИС). Сервисы, интерфейсы и протоколы. Обеспечение переносимости прикладных программ (ПП), пользователей и данных. Обеспечение способности к взаимодействию. Системный подход к описанию функциональности на базе модельного представления ИС. Сервисы человеко-машинного взаимодействия, сервисы данных, сетевые сервисы, внутренние сервисы платформы.
4 неделя (3 часа). Способы обеспечения переносимости и способности к взаимодействию. Модели открытых систем.	Расширение модели ИС для взаимодействующих систем. Коммуникационные архитектуры. Модели распределенных вычислений. Системообразующие стандарты: модель ISO/OSI, профили взаимосвязи открытых систем ISO/IEC 10000, другие системообразующие стандарты ISO и ITU, модель POSIX/OSE, модель TCP/IP, модель TOGAF.
5 неделя (3 часа). Аппаратное обеспечение открытых информационных систем: средства и системы обработки данных.	Обзор различных классов компьютерных систем: суперкомпьютеры, мейнфреймы, центры обработки данных, компьютеры высокой производительности для крупного и среднего бизнеса, веб-серверы (балансировка нагрузки), серверы локальных сетей, персональные компьютеры, мобильные устройства: планшеты, нетбуки, коммуникаторы. «Всепроникающие вычисления» (Ubiquitous computing, «интернет вещей»). Платформы специального назначения. Встроенные системы (embedded systems).
6 неделя (3 часа). Аппаратное обеспечение открытых информационных систем: средства и системы хранения данных.	Эволюция средств и систем хранения данных. Классификация систем хранения данных: локальные дисковые накопители, RAID-массивы, сети хранения данных (SAN), ленточные библиотеки. Модели управления хранением данных. Международные стандарты.
7 неделя (3 часа). Аппаратное обеспечение открытых информационных систем: коммуникационные средства и архитектуры.	Физические способы передачи сигнала: проводные, оптоволоконные, беспроводные сети. Функции коммуникационных средств. Функциональные уровни. Коммуникационные архитектуры: 7-уровневая модель OSI, модель TCP/IP. Сервисы, интерфейсы и протоколы. Основные типы оборудования: репитеры, свитчи, роутеры, шлюзы. Основные характеристики коммуникационных каналов.

8 неделя (3 часа). Программное обеспечение открытых информационных систем: операционные системы.	Основные семейства операционных систем, используемых в открытой среде: UNIX-подобные (AIX, Solaris, FreeBSD, Linux, Android, MAC OS X и пр.), Windows, OS X. ПО с открытым кодом и проприетарное ПО.
9 неделя (3 часа). Программное обеспечение открытых информационных систем: системное и прикладное ПО.	Типология и обзор системного ПО: СУБД, мониторы виртуальных машин, middleware и др. Типология и обзор прикладного ПО: CRM, CMS, CAD и др. GRID-системы. Облачные среды.
10 неделя (3 часа). Языки программирования.	Процедурное, объектно-ориентированное и функциональное программирование. Сравнительная характеристика языков программирования C, C++, C#, Java, Python, Perl, PHP и др.
11 неделя (3 часа). Программные платформы (архитектура программного обеспечения).	Понятие программной платформы (software frameworks). Платформы .NET и JavaScript: общая характеристика, эволюция платформ, модули и расширения платформ, интерфейсы прикладного программирования (API), используемые в них языки программирования, обеспечение интероперабельности языков программирования и переносимости программного кода. Другие платформы. Архитектуры прикладного ПО. Архитектуры веб-разработки.
12 неделя (3 часа). Модели и средства разработки ПО. Синтез архитектур корпоративных информационных систем.	Интегрированные среды разработки системного и прикладного ПО для открытой среды: MS Visual Studio, Eclipse, PyCharm и др. Повторное использование кода. Библиотеки разработчика. Шаблоны разработки (design patterns). Современная методология создания корпоративных ИС на примере модели TOGAF: ADM, репозиторий, шаблоны, TRM. Язык UML, шаблоны проектирования. Методы моделирования сложных ИС.
13 неделя (3 часа). Веб-сервисы. Веб-разработка.	Архитектуры ПО на стороне сервера и на стороне клиента. Средства веб-разработки: Joomla, Drupal, WordPress, Django и др. Технические аспекты веб-разработки: хостинг сайтов, поддержка доменных имен. Системы управления контентом.
14 неделя (3 часа). Модели централизованных и распределенных вычислений. Облачные среды.	Модели терминального доступа, «клиент — сервер», облачных вычислений. Модели предоставления облачных сервисов. Отображение моделей облачных сервисов на базовую модель ИС. Документы NIST по обеспечению безопасности облачных технологий. Сервисы, предоставляемые облачными провайдерами для пользователей. API облачных сервисов для разработчиков прикладного ПО (на примере Google App Engine, Amazon, Microsoft Azure, Яндекс API). Поддержка API облачных сервисов и языков программирования в интегрированных средах разработки.

15 неделя (3 часа). Инфраструктура безопасности открытых систем.	Стандарты для разработчиков средств защиты информации (обзор, эволюция стандартов). Архитектура безопасности ISO/OSI. Стандарты ISO/IEC 10181 и производные от них. Стандарты IEEE. Концепция инфраструктуры управления ключами (PKI и KMI). Стандарт ISO/IEC 18033 и другие. Стандарты для владельцев информационных активов (обзор, эволюция стандартов). ISO/IEC 15408. Серия ISO 27000. Серия ISO 31000 и другие.

Кроме лекционного курса, дисциплина предусматривает выполнение восьми лабораторных работ, связанных с решением расчетных задач, выполнением практических заданий с использованием общедоступного ПО и проведением несложных экспериментов по замеру некоторых параметров распространения информации в Интернете при использовании различных сетевых сервисов. Краткое содержание лабораторного практикума приводится в таблице 2.

Таблица 2. Лабораторный практикум по дисциплине «Открытые информационные системы»

Лабораторная работа	**Содержание занятий**
1. Расчет времени прохождения пакетов по сети линейной топологии.	Решить комплексную расчетную задачу, состоящую из нескольких подзадач. Дана простейшая сеть линейной топологии, состоящая из 2 терминальных хостов и 2 роутеров. Заданы длины 2 пакетов, пропускные способности 3 соединяющих их каналов связи, условия приема и дальнейшей передачи пакетов роутерами. Требуется найти моменты времени, когда роутеры и хосты завершат прием каждого из пакетов, в том числе при изменившейся пропускной способности канала. (Несмотря на кажущуюся простоту постановки задачи, расчеты довольно сложны и приводят к большому количеству ошибок при невнимательности учащихся!)
2. Исследование зависимости времени прохождения пакетов в Интернете от расстояния.	Используя утилиту ping, доступную из командной строки Windows, а также сервиса Google/Карты или Яндекс/Карты, провести замеры времени прохождения пакетов до сайтов ряда университетов, расположенных на различном удалении от Москвы в разных странах мира и на разных континентах. Проведя не менее 7 замеров и повторив каждый из них не менее 3 раз, требуется построить график зависимости времени прохождения пакета от расстояния, а также показать минимальные и максимальные значения времени прохождения пакетов для каждой точки. По полученным данным требуется определить вид функциональной зависимости и предложить объяснение наблюдаемым на графике особенностям.
3. Трассировка маршрутов прохождения пакетов до заданных сайтов в Интернете.	Применяя утилиту tracert, доступную из командной строки Windows (аналогичные утилиты traceroute есть и в ОС семейств Linux и Mac OS), необходимо протрассировать маршруты от компьютера, используемого для выполнения лабораторной работы, до хостов, указанных в выданном варианте задания. По результатам эксперимента для каждого хоста требуется привести распечатку трассировки маршрута и построить (на одном поле) два графика

	прохождения маршрутов до исследуемых хостов. По результатам выполнения задания необходимо ответить на ряд вопросов и объяснить наблюдаемые явления, в том числе, возможно, имеющиеся на графиках аномалии. Завершается работа проверкой полученных результатов с помощью свободно распространяемой программы VisualRoute 2010.
4. Изучение процессов, происходящих при дистанционном доступе к веб-странице с клиентского браузера.	Используя одно из инструментальных средств тестирования скорости загрузки веб-сайтов, доступных на сайтах по адресам: www.webpagetest.org (рекомендуется); http://tools.pingdom.com/fpt/; http://loadimpact.com/, получить отчет о тестировании доступа к веб-странице, загружаемой по умолчанию при обращении к сайту, указанному в выданном варианте задания. По результатам экспериментов для каждого исследованного случая привести диаграммы первого обращения к странице, повторного обращения к странице, структуру содержимого веб-страниц по типу контента. По полученным данным определить время окончания загрузки веб-страницы и время полной загрузки контента при первом обращении к странице и при повторном обращении к странице. По итогам эксперимента требуется письменно ответить на ряд контрольных вопросов.
5. Сравнительный анализ надежности двух вариантов организации системы массово-параллельной обработки данных в Центре обработки данных (ЦОД).	Рассматриваются два варианта организации ЦОД из одного состава оборудования: 2 коммутатора с раздельным выходом в Интернет, 2 мастер-узла и 2 стойки с узлами, собранными в кластер. В одном случае предлагается зарезервировать каждый из элементов ЦОД по отдельности, во втором — ЦОД с полным составом оборудования целиком. Есть статистические сведения о показателях надежности отдельных видов техники в ЦОД. Требуется оценить надежность двух вариантов построения системы обработки данных, а именно для каждого из двух вариантов: 1) изобразить эквивалентную схему последовательно-параллельного соединения элементов системы; 2) вычислить стационарный коэффициент готовности системы; 3) вычислить верхнюю и нижнюю оценки вероятности безотказной работы системы в течение 1 года; 4) вычислить верхнюю и нижнюю оценки среднего времени безотказной работы системы; 5) сравнить показатели надежности для двух вариантов организации системы обработки данных и сделать обоснованный вывод, какой из них более предпочтителен.
6. Сравнительный анализ производительности двух вариантов организации системы массово-параллельной обработки данных.	Рассматриваются два варианта организации потоковой обработки данных в ЦОД с n серверами: с балансировщиком нагрузки и общей очередью к нему (до модернизации), а также с общим шлюзом и раздельными очередями к каждому из серверов (после модернизации ЦОД). Требуется: 1) проверить условия существования финальных вероятностей (условия работоспособности) для первого и для второго случаев и, тем самым, выяснить, сможет ли ЦОД работать, или он будет «забиваться» бесконечно растущей очередью; 2) определить, приведет ли предлагаемая модернизация ЦОД к

	уменьшению длины очереди запросов, ожидающих обслуживания (сравнить среднюю длину очереди в буфере балансировщика нагрузки n-канальной СМО в первом случае со средней длиной очереди в буфере одного сервера одноканальной СМО во втором случае); 3) определить, уменьшится ли после модернизации ЦОД среднее время ожидания запроса в очереди. Ответы на вопросы должны быть подкреплены расчетами. Исходные данные берутся из таблицы по вариантам. Результаты расчетов рекомендуется проверить с помощью программного средства Java Modelling Tools.
7. Структурно-функциональное описание компьютерной системы.	Необходимо дать описание любой имеющейся в распоряжении учащегося компьютерной системы с установленным на ней программным обеспечением (настольного компьютера, ноутбука, планшетного компьютера, смартфона и пр.) как части среды открытых систем. В описании необходимо: 1) указать основные характеристики платформы: аппаратного обеспечения и системного программного обеспечения; 2) перечислить прикладное ПО, установленное на изучаемой компьютерной системе; 3) описать доступные в момент выполнения задания способы взаимодействия с другими компьютерными системами и сетями; 4) составить максимально полный каталог функций, реализуемых системой при работе с локальными информационными ресурсами (с разбиением их по категориям сервисов согласно п. 43 части VI модели TOGAF v9.1: http://pubs.opengroup.org/architecture/togaf9-doc/arch/, с указанием конкретных программных продуктов, которыми они реализуются; 5) на основе составленного описания построить графическое представление функциональной модели системы. В качестве образца графического представления модели использовать эталонную модель (TRM) TOGAF v9.1: http://pubs.opengroup.org/architecture/togaf9-doc/arch/.
8. Изучение официального текста стандарта (на примере рекомендации из серии RFC) и подготовка аналитической записки об изученном документе.	Пользуясь официальным текстом рекомендаций серии RFC (Request for Comments), опубликованным на сайте www.ietf.org/rfc.html, изучить одну из рекомендаций серии RFC и подготовить аналитическую записку об этом стандарте. Рекомендуемый объем — от 3 до 5 страниц. В записке должны быть отражены: 1) наименование стандарта, обозначение, версия, год принятия, новый или введен взамен ранее действовавшего стандарта; 2) статус стандарта в соответствии с RFC 3700, взаимосвязь с другими стандартами; 3) аннотация; 4) конкретная техническая задача, решению которой посвящен стандарт; 5) методы решения задачи, предлагаемые в стандарте; 6) технические детали и особенности реализации предлагаемых в стандарте методов: 7) примеры продуктов и систем, в которых реализуется данный стандарт.

В дальнейшем лабораторный практикум планируется расширить путем добавления лабораторных работ, посвященных сетевому планированию и управлению при работе большого

коллектива над проектами по созданию сложных информационных систем (на примере метода PERT — Project Evaluation and Review Technique).

Текущий контроль успеваемости по дисциплине проводится в рейтинговой форме. Среди контрольных мероприятий предусмотрен письменный опрос или тест в аудитории (15—20 мин.) на 8-й учебной неделе, а также письменный опрос или тест в аудитории (20—25 мин.) на 15-й учебной неделе. Для студентов, не набравших в течение семестра рейтинг, достаточный для получения зачета, предоставляется возможность набрать недостающие баллы путем выполнения дополнительных заданий повышенной сложности. Предлагается три типа таких заданий.

Первый тип — подготовить аналитический отчет по одной из предложенных тем и презентацию по теме написанного отчета. Примеры тем заданий этого типа приводятся в таблице 3.

Таблица 3. Список предлагаемых тем аналитических отчетов

№ варианта	**Задание**
1	Российский рынок средств двухфакторной аутентификации.
2	Ведущие мировые провайдеры облачных вычислений.
3	Российский рынок средств защиты информации от НСД по состоянию на 2014 г.
4	Российский рынок средств защиты контента для малого и среднего бизнеса (SMB) по состоянию на 2014 г.
5	Российский рынок интеграторов в области ИБ по состоянию на 2014 г.
6	Российский рынок антивирусных средств по состоянию на 2014 г.
7	Российский рынок систем контентной фильтрации по состоянию на 2014 г.
8	Российский рынок консалтинга в области ИБ по состоянию на 2014 г.
9	Российский рынок аудита ИБ по состоянию на 2014 г.
10	Российский рынок услуг по сертификации продукции по требованиям информационной безопасности по состоянию на 2014 г.
11	Российский рынок услуг по обучению вопросам информационной безопасности по состоянию на 2014 г.
12	Российский рынок систем сбора и корреляции событий (SIEM) по состоянию на 2014 г.
13	Российский рынок систем идентификации и аутентификации (IDM) по состоянию на 2014 г.
14	Мировой рынок средств защиты виртуализации по состоянию на 2014 г.
15	Мировой рынок средств защиты систем управления технологическими процессами (SCADA) по состоянию на 2014 г.
16	Мировой рынок средств управления мобильными устройствами (MDM — Mobile Device Management) по состоянию на 2014 г.
17	Российский рынок услуг в области функционального и нагрузочного тестирования по состоянию на 2014 г.
18	Мировой рынок средств массово-параллельной обработки «больших данных» (big data) по состоянию на 2014 г.
19	Российский рынок геоинформационных систем по состоянию на 2014 г.
20	Российский рынок средств электронной подписи по состоянию на 2014 г.

21	Российский рынок электронных идентификаторов (токенов) по состоянию на 2014 г.
22	Российский рынок смарт-карт по состоянию на 2014 г.
23	Российский рынок продуктов и решений в области PKI по состоянию на 2014 г.
24	Российский рынок средств обеспечения сетевой безопасности по состоянию на 2014 г.
25	Российский рынок инструментальных средств анализа защищенности по состоянию на 2014 г.
26	Российский рынок систем управления взаимоотношениями с клиентами (CRM) по состоянию на 2014 г.

Второй тип заданий — разработать гипертекстовую справочную информационную систему (в виде файла «справки» Windows) по одной из предложенных тем. Средства разработки — *HTML Help Workshop*, *HelpNDoc*, *CHM Builder* (бесплатные программы) либо иные по выбору учащегося. От справочной системы не требуется, чтобы весь содержащийся в ней текст и иллюстрации были написаны или подготовлены лично автором, — оригинальным здесь является само сочетание источников (их номенклатура, отбор материала из них), которое в таком виде больше нигде не встречается. Не менее важны полнота, качество и достоверность используемых источников. Гипертекстовый справочник должен быть привязан к библиографическому списку источников информации. Объем гипертекстового справочника — не менее 50 HTML-страниц, связанных ссылками.

Примеры тем заданий этого типа приводятся в таблице 4.

Таблица 4. Список предлагаемых тем гипертекстовых справочников

№ варианта	**Задание**
1	Системообразующие стандарты ISO по безопасности информационных технологий (по состоянию на 2014 г.)
2	Наиболее важные стандарты IEEE по безопасности информационных технологий (по состоянию на 2014 г.)
3	Системообразующие стандарты ITU по безопасности информационных технологий (по состоянию на 2014 г.)
4	Российские государственные стандарты по безопасности информационных технологий (по состоянию на 2014 г.)
5	Комплекс национальных стандартов США по безопасности информационных технологий (по состоянию на 2014 г.)
6	Комплекс стандартов Европейского Союза по безопасности информационных технологий (по состоянию на 2014 г.)
7	Международные стандарты в области обеспечения безопасности банковских технологий и защиты банковской информации
8	Международные стандарты и проекты стандартов по управлению непрерывностью бизнеса и информационно-телекоммуникационных технологий
9	Отечественные и зарубежные программные средства разработки и внедрения политик безопасности

10	Отечественные и зарубежные программные продукты для анализа, оценки и управления рисками информационной безопасности
11	Отечественные и зарубежные антивирусные программные средства
12	Отечественные и зарубежные средства криптографической защиты файловых систем
13	Современные языки программирования и их основные характеристики

Третий тип заданий — предложить сценарий лабораторного эксперимента, посвященного изучению современных информационных технологий, и разработать методические рекомендации по проведению этого лабораторного эксперимента с приложением необходимых для этого программных средств, если это потребуется. Расчетная продолжительность лабораторного эксперимента должна составлять от 4 до 6 часов. Обязательным условием является связь предлагаемой темы работы или эксперимента (или, по крайней мере, некоторой части рабочего задания, предлагаемого в работе) с задачами обеспечения безопасности информации в компьютерных системах. Предлагаемые эксперименты должны быть воспроизводимы с использованием доступных аппаратных и программных средств (желательно без нарушения авторских прав, то есть с использованием свободно распространяемого ПО или, по крайней мере, пробных версий ПО. Можно подготовить образ виртуальной машины, который будет работать на одном из свободно распространяемых мониторов виртуальных машин: VMware Player, Virtual Box и др.

Примеры сценариев заданий этого типа приводятся в таблице 5.

Таблица 5. Список предлагаемых сценариев лабораторных экспериментов

№ варианта	**Задание**
1	Изучение методологии PERT (Program Evaluation and Review Technique) с использованием программного средства Microsoft Project 2013
2	Решение задач анализа рисков при помощи программных средств ModelRisk и ModelTree [http://www.vosesoftware.com/index.php]
3	Моделирование коммуникационных протоколов при помощи программного средства CPNTools [http://cpntools.org]
4	Расчет показателей производительности (доступности) вычислительных систем (центров обработки данных) при помощи программных средств Java Modelling Tools [http://jmt.sourceforge.net/Download.html] (или других аналогичных)
5	Расчет показателей надежности вычислительных систем (центров обработки данных) при помощи программных средств, представленных на сайте Weibull.com [http://www.weibull.com/itools/index.htm] (или других аналогичных)

Разработанный учебно-методический комплекс внедрен в педагогическую практику. Первый раз курс «Открытые информационные системы» был прочитан в весеннем семестре 2013/2014 уч. г. на факультете «Кибернетика и информационная безопасность» Национального исследовательского ядерного университета «МИФИ» для студентов, обучающихся по специальности 090303 — «Информационная безопасность автоматизированных систем». В дальнейшем планируется регулярное обновление содержания лекционного курса, актуализация лабораторного практикума и заданий для самостоятельной работы в соответствии с актуальным состоянием дел в сфере информационных технологий.