Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Новгородский государственный университет имени Ярослава Мудрого»
Институт электронных и информационных систем
Кафедра информационных технологий и систем

УТВЕРЖДАЮ
Директор ИЭИС, профессор
_____ С.Г.Гаврилов
«__» _____ 2017 г.

СОВРЕМЕННЫЕ WEB-ТЕХНОЛОГИИ И МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Учебный модуль по направлению подготовки
44.03.05.-Педагогическое образование (с двумя профилями подготовки)
Технология и Информатика Математика и Информатика, Физика и Информатика
Рабочая программа

СОГЛАСОВАНО:
Начальник учебного отдела
_____ О.Б.Широколобова
«30» 05 2017г

Разработал
Доцент кафедры ИТИС
_____ Г.Ю.Соколова

Принято на заседании кафедры ИТИС
Протокол № 28 от 05 2017
2017г
Заведующий кафедрой ИТИС
_____ А.Л.Гавриков

Модуль «Современные web-технологии и методы и средства защиты информации» состоит из двух разделов:

Раздел 1 Современные WEB-технологии

Раздел 2 Методы и средства защиты информации

1 Цели и задачи учебного модуля

Цели учебного модуля (УМ) «Современные web-технологии и методы и средства защиты информации»:

– формирование у будущих бакалавров компетенций, необходимых для овладения базовыми теоретическими знаниями и практическими навыками по разработки программного обеспечения.

Задачи УМ «Современные web-технологии и методы и средства защиты информации»:

– изучение основных положений технологии разработки программного обеспечения, формулировка практических рекомендаций по организации работы коллективов программистов, руководства такими коллективами;

формирование у студентов знаний по дисциплине, связанных с процессом разработки программного обеспечения, включая связи с предметной областью, реализацию, организацию производства, контроль сроков исполнения и качеством;

– ознакомление с техническими программными и технологическими решениями, используемыми при разработке ПО;

– приобретение практических навыков работы в коллективе программистов, умения находить правильные технологические решения по выбору структуры программного проекта, методов тестирования;

– ознакомление с основными технологиями разработки ПО.

2 Место учебного модуля «Современные web-технологии и методы и средства защиты информации» в структуре ОП направления подготовки:

Модуль «Современные web-технологии и методы и средства защиты информации» входит в вариативную часть.

Освоение УМ «Современные web-технологии и методы и средства защиты информации» базируется на знаниях и умениях, приобретённых при изучении дисциплин: «Теоретические основы информатики», «Информационные технологии», «Математическая логика и теория алгоритмов», «Программирование», «Алгоритмические языки», «Базы данных».

Знания и умения, полученные при изучении УМ «Современные web-технологии и методы и средства защиты информации», являются необходимым для последующего освоения модуля «Мультимедиа технологии в образовании и технологии дистанционного обучения, для успешного прохождения практик, для выполнения научно-исследовательской работы, при написании выпускной квалификационной работы и дальнейшем обучении в магистратуре.

3 Требования к результатам освоения учебного «Современные web-технологии и методы и средства защиты информации»:

Процесс изучения УМ направлен на формирование компетенций:.

– Способность использовать современные методы и технологии обучения и диагностики (ПК-2)

– Способность демонстрировать знания, умения и навыки в области математики и информатики и применять их в научно-исследовательской и педагогической деятельности (СК-1)

- Способность использовать методологии программирования и современные компьютерные технологии для обработки информации, решения практических задач и разработки программного обеспечения (СКИ-1)

- Готовность применять современные информационные и коммуникационные технологии для проектирования информационной образовательной среды и разработки электронных образовательных ресурсов (СКИ-3)

В результате освоения УМ студент должен знать, уметь и владеть:

Код Компе-тенции	Уровень Освоения Компетен-ции	Знать	Уметь	Владеть
ПК-2	базовый	– различные подходы к индивидуализации обучения и воспитания	– выбирать, применять и разрабатывать методики и технологии обучения с учетом возрастных и индивидуальных особенностей обучающихся	– использованием результатов диагностирования достижений обучающихся
СК-1	базовый	– математические методы и методы информатики	– применять конкретные математические методы и методы информатики	– решением типовых задачи и применять его к стандартным ситуациям.
СКИ-1	базовый	- современные компьютерные технологии для обработки информации	- использовать основы работы с компьютером как средством управления информацией	- программированием и обработкой информации
СКИ-3	базовый	-современные информационные и коммуникационные технологии для разработки электронных образовательных ресурсов	- использовать современные информационные и коммуникационные технологии разработки электронных образовательных ресурсов	- возможностями информационных и коммуникационных технологий для разработки электронных образовательных ресурсов

4 Структура и содержание модуля

Учебная работа (УР)	Распределение по семестрам 8 семестр Всего:	Раздел1 Современные web-технологии	Раздел 2 Методы и средства защиты информации	Коды формир. компетенций
Трудоемкость модуля в зачетных единицах (ЗЕ)	**6**	3	3	**МиИ ФиИ ПК-2.СК-1 ТиИ СКИ-1,СКИ-3**
Распределение трудоемкости по видам УР в академических часах (АЧ):	**216**	108	108	
- лекции	**36**	18	18	
- лабораторные занятия	**54**	36	18	
- аудиторная СРС	**18**	9	9	
- внеаудиторная СРС	**90**	54	36	

Аттестация: экзамен	**36**		36	

4.2 Организация изучения УМ

Методические рекомендации по организации изучения УМ с учетом использования в учебном процессе активных и интерактивных форм проведения учебных занятий даются в Приложении А

5 Контроль и оценка качества УМ

Контроль качества освоения студентами УМ и его составляющих осуществляется непрерывно в течение всего периода обучения с использованием балльно-рейтинговой системы (БРС), являющейся обязательной к использованию всеми структурными подразделениями университета.

Для оценки качества освоения модуля используются формы контроля: текущий – регулярно в течение всего семестра. Форма текущего контроля: собеседование (защита лабораторных работ), домашние задания. Проверка знаний, полученных при изучении материала раздела1 «Современные web-технологии» проводится на 7-ой неделе по вопросам, представленным в Приложении А. Оценка знаний, полученных при изучении материала раздела2 «Методы и средства защиты информации» проводится после окончания изучения УМ в виде экзамена по вопросам, представленным в Приложении А. Итоговая оценка за экзамен выставляется с учетом баллов за собеседование по вопросам раздела1.

К итоговой аттестации допускаются студенты, выполнившие и защитившие все лабораторные работы, СРС, успешно прошедшие собеседование после изучения материала раздела1.

Оценка качества освоения модуля осуществляется с использованием фонда оценочных средств, разработанного для данного модуля, по всем формам контроля в соответствии с положением СМК УД 3.1.-00-02.17-13 Положениями «Об организации учебного процесса по образовательным программам высшего образования» и «О фонде оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации студентов и итоговой аттестации выпускников».

Содержание видов контроля и их график отражены в технологической карте учебного модуля (Приложение Б).

Формы текущего контроля

Форма проведения	«удовлетворительно»	«хорошо»	«отлично»
Раздел 1. Современные WEB-технологии			
Собеседование (защита) по ЛР	5 –6 баллов – испытывает трудности при демонстрации знаний; испытывает трудности в определении терминов и описании алгоритмов действий	7 – 8 баллов – допускает неточности при демонстрации знаний; недостаточно четко объясняет значение терминов и описании алгоритмов действий	9 – 10 баллов – имеет целостное представление материала; четко объясняет значение всех терминов, четко и безошибочно описывает алгоритмы действий
Собеседование по задачам из ДЗ	5 – 6 баллов – испытывает трудности при демонстрации знаний; испытывает трудности в	7 – 8 баллов – допускает неточности при демонстрации знаний; недостаточно четко объясняет	9 –10 баллов – имеет целостное представление материала; четко объясняет значение

	определении терминов и описании алгоритмов действий	значение терминов и описании алгоритмов действий	всех терминов, четко и безошибочно описывает алгоритмы действий.
Собеседование по вопросам к разделу1. (тест)	15 – 15,6 баллов – испытывает трудности при демонстрации знаний	15,7 – 20,3 баллов – допускает неточности при демонстрации знаний;	20,4 – 30 баллов – имеет целостное представление материала;
Раздел 2. Методы и средства защиты информации			
Собеседование ауд.СРС (защита ДЗ)	2 – 2,6 испытывает трудности при демонстрации знаний; испытывает трудности в определении терминов и описании алгоритмов действий	2,7– 3,3 допускает неточности при демонстрации знаний; недостаточно четко объясняет значение терминов и описании алгоритмов действий	3,4 – 4.0 имеет целостное представление материала; четко объясняет значение всех терминов, четко и безошибочно описывает алгоритмы действий
Собеседование – Защита по ЛР	2 – 2,6 испытывает трудности при демонстрации знаний; испытывает трудности в определении терминов и описании алгоритмов действий	2,7– 3,3 допускает неточности при демонстрации знаний; недостаточно четко объясняет значение терминов и описании алгоритмов действий	3,4 – 4.0 имеет целостное представление материала; четко объясняет значение всех терминов, четко и безошибочно описывает алгоритмы действий
Экзамен по УМ	25 – 30 баллов – выполнено заданий 50-74%	31 – 40 баллов – выполнено заданий 75-89%	41 – 50 баллов – выполнено заданий 90-100%

6 Учебно-методическое и информационное обеспечение

Учебно-методическое и информационное обеспечение учебного модуля представлено Картой учебно-методического обеспечения (Приложение В).

7 Материально-техническое обеспечение учебного модуля

Для осуществления образовательного процесса по дисциплине необходимы:

– для проведения лекций, а также практических занятий – аудитория, оборудованная мультимедийным оборудованием;

– для проведения лабораторных занятий – компьютерные классы с современными ПК и установленным на них лицензионным программным обеспечением. На персональных компьютерах должны быть установлены: ОС Windows 7 (Windows XP), VisualBasic 6.0.

Приложения (обязательные):

А – Методические рекомендации по организации изучения учебного модуля

Б – Технологическая карта

В - Карта учебно-методического обеспечения УМ

ПРИЛОЖЕНИЕ А
Методические рекомендации по организации изучения учебного модуля «Современные web-технологии и методы и средства защиты информации»

А.1 Методические рекомендации по теоретической части учебного модуля

Теоретическая часть модуля направлена на формирование системы знаний в области теории информатики и информационных технологий. Основное содержание теоретической части излагается преподавателем на лекционных занятиях, а также усваивается студентом при знакомстве с дополнительной литературой, которая предназначена для более глубокого овладения знаниями основных дидактических единиц соответствующего раздела и указана в таблице А.

А.2 Содержание и структура разделов учебного модуля

РАЗДЕЛ 1. «Современные web-технологии»

1.Введение. Структура и принципы Веб

Понятие Интернет. Роль стандартизации в Интернет. Система доменных имен DNS. Структура и принципы WWW. Сайты и страницы, сервисы, порталы. Веб-браузеры. Прокси-серверы. Протоколы Интернет прикладного уровня. Клиент-серверные технологии Веб. Протокол HTTP. Структура IP адреса.

2. Язык гипертекстовой разметки HTML, XHTML

Развитие стандартов HTML. Стандарты кодирования XHTML. Типы тегов XHTML. Структурирование содержимого страницы. Теги и атрибуты. Заголовки. Списки. Списки определений. Соединение страниц. Вывод изображений. Таблицы**.**

3. Каскадные таблицы стилей CSS

Линейные таблицы стилей. Встроенные таблицы стилей. Внешние таблицы стилей. Применение таблиц стилей. Основные свойства.

4. Системы управления контентом CMS

Объектная модель CMS. Сетевая модель CMS. Модульная модель CMS. Основные функции CMS. Обзор популярных CMS.

5. Синтаксис языка PHP

Соединение XHTML и PHP. Вывод данных. Терминатор инструкции. Комментарии в коде. Переменные. Выражения. Функции.

6. Формы. Обработка форм

Элементы форм. Передача данных с помощью форм. Трансляция полей формы. Трансляция переменных окружения. Обработка списков с множественным выбором. Обработка массивов. Особенности обработки независимых переключателей

7. Регулярные выражения. Работа с файлами в PHP

Регулярные выражения. Модификаторы регулярных выражений. Работа с файлами. Обзор обработки файлов. Проблемы, возникающие при открытии файлов. Блокирование файлов

8. Взаимодействие PHP и MySQL

Доступ к базам данных. Выполнение запросов к базе данных через Web. Освобождение ресурсов. Создание и удаление баз данных. Другие интерфейсы PHP-баз данных. Технологии применения.

9. Сессии и cookie в PHP

Сессии (сеансы) в PHP. Открытие сессии. Регистрация переменных сессии. Закрытие сессии. Кукисы (cookies). Установка cookies. Удаление cookie. Проблемы безопасности, связанные с cookies.

РАЗДЕЛ 2. «Методы и средства защиты информации»

В структуре раздела «Методы и средства защиты информации» выделены следующие учебные элементы модуля (УЭМ) в качестве самостоятельных разделов:

– УЭМ1 Средства защиты от несанкционированного доступа;

– УЭМ2 Криптографические средства.

УЭМ1. Средства защиты от несанкционированного доступа

1.1 Информационная безопасность
1.2 Средства защиты от несанкционированного доступа
1.3 Системы обнаружения и предотвращения вторжений
1.4 Системы мониторинга сетей
1.5 Антивирусные средства
1.6 Межсетевые экраны
1.7 Технические средства защиты авторских прав
1.8 Запутывание кода программ
1.9 Управление ключами. Электронная цифровая подпись

УЭМ 2. Криптографические средства

2.1 Криптографические средства
2.2 Криптографические алгоритмы. Симметричное шифрование
2.3 Алгоритм шифрования«РЕЙНДОЛ» (AES)
2.4 Алгоритм шифрования ГОСТ 28147-89
2.5 Алгоритм шифрования DES
2.6 Шифры РИВЕСТА
2.7 Алгоритм шифрования «БЛОУФИШ»
2.8 Алгоритм шифрования «ТУФИШ»
2.9 Алгоритм шифрования «ИДЕА»
2.10 Алгоритмы шифрования «ХУФУ» И «ХАФРЕ»
2.11 Потоковый алгоритм шифрования «RC4»
2.12 Асимметричный алгоритм шифрования RSA
2.13 Криптоанализ

Методические рекомендации по организации изучения данного раздела 2.

Для УЭМ1 – Средства защиты от несанкционированного доступа

Тема 1.1 Информационная безопасность

Цель: изучить основные понятия защиты информации.

Ключевые понятия

Защита информации, информационная безопасность,уровни безопасности, Общие критерии оценки защищённости ИТ, сервисы безопасности, Требования гарантии безопасности.

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Подготовить ответы на дополнительные вопросыД.З.1. - Д.З.4.

Тема 1.2Средства защиты от несанкционированного доступа

Цель: изучить основные средства защиты от несанкционированного доступа.

Ключевые понятия

Предотвращения утечек информации, DLP системы, средства ограничения физического доступа, межсетевое экранирование,системы аутентификации.
Технологии и формы организации
Информационная лекция.
Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.
Задания для самостоятельной работы
Выполнить и сдать на проверку заданияаудиторной СРС 1.
Подготовить ответы на дополнительные вопросыД.З.5. - Д.З.8.

Тема 1.3 Системы обнаружения и предотвращения вторжений

Цель: изучить системы обнаружения и предотвращения вторжений (IDS/IPS) и системы предотвращения утечек конфиденциальной информации (DLP-системы).
Ключевые понятия
Сетевая COBNetwork-based IDS (NIDS), основанная на протоколе COB (PIDS), основанная на прикладных протоколах COB (APIDS), узловая COBHost-based IDS (HIDS), гибридная COBHybrid IDS, классификация систем предотвращения вторжений, спуфинг, Виды DoSатак, эксплойт, ботнет, межсетевой экран.
Технологии и формы организации
Информационная лекция.
Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.
Задания для самостоятельной работы
Подготовить ответы на дополнительные вопросыД.З.9. - Д.З.14.

Тема 1.4 Системы мониторинга сетей

Цель: изучить системы мониторинга сетей, анализаторы протоколов.
Ключевые понятия
Сниффер, способы перехвата трафика, взлом беспроводных сетей, «Рыбалка» со спутника, средства снижения угрозы сниффинга.
Технологии и формы организации
Информационная лекция.
Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.
Задания для самостоятельной работы
Выполнить и сдать на проверку задания аудиторной СРС 2.
Подготовить ответы на дополнительные вопросыД.З.15. - Д.З.19.

Тема 1.5 Антивирусные средства

Цель: изучить программы для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления зараженных (модифицированных) такими программами файлов, а также для профилактику заражения (модификации) файлов или операционной системы вредоносным кодом.
Ключевые понятия
Классификация антивирусов, сигнатурный метод обнаружения, проактивная защита, полиморфизм компьютерного вируса, эмуляция кода, технология песочницы, виртуализация рабочего окружения, лжеантивирусы.
Технологии и формы организации
Информационная лекция.
Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.
Задания для самостоятельной работы

Подготовить ответы на дополнительные вопросыД.З.20. - Д.З.24.

Тема 1.6 Межсетевые экраны

Цель: изучить возможности межсетевых экранов и проблемы, нерешаемые межсетевым экраном.
Ключевые понятия
Классификация межсетевых экранов по характеристикам, Бэкдор.
Технологии и формы организации
Информационная лекция.
Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.
Задания для самостоятельной работы
Выполнить и сдать на проверку задания аудиторной СРС 3.
Подготовить ответы на дополнительные вопросы Д.З.25. - Д.З.27.

Тема 1.7 Технические средства защиты авторских прав

Цель: изучить технические средства защиты авторских прав или DRM (Digital rights management), программные или программно-аппаратные средства, которые намеренно ограничивают либо затрудняют какие-либо действия с данными в электронной форме (копирование, модификацию, просмотр ит.п.), либо позволяют отследить такие действия.
Ключевые понятия
Эффективность и правовая основа DRM.Современные технологии DRM
Технологии и формы организации
Информационная лекция.
Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.
Задания для самостоятельной работы
Подготовить ответы на дополнительные вопросыД.З.28. - Д.З.30.

Тема 1.8 Запутывание кода программ

Цель: изучить способы запутывания кода программ, для предотвращения нарушения авторских прав.
Ключевые понятия
Анализ программного обеспечения,Байт-код шифрование, обфускация имени, стринг шифрование, запутывание потока, антидекомпиляторы, популярные обфускаторы.
Технологии и формы организации
Информационная лекция.
Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.
Задания для самостоятельной работы
Выполнить и сдать на проверку задания аудиторной СРС 4.
Подготовить ответы на дополнительные вопросы Д.З.31. - Д.З.32.

Тема 1.9. Управление ключами. Электронная цифровая подпись

Цель: изучить роль управления ключами в криптографии, цели управления ключами.
Ключевые понятия
Закрытый ключ. Электронная цифровая подпись. Виды ЭП в РФ. Алгоритмы получения ЭП. Использование хэш-функций. Симметричная и асимметричная схема. Взлом подписей. Подделка документа (коллизия первого рода). Получение двух документов с одинаковой подписью (коллизия второго рода). Социальные атаки. Слепая подпись.

Управление открытыми ключами. Хранение закрытого ключа. Политика безопасности. Жизненный цикл ключей

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Подготовить ответы на дополнительные вопросыД.З.33. - Д.З.34.

Для УЭМ2 – «Криптографические средства»

Тема 2.1. Криптографические средства

Цель: изучить методы обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации.

Ключевые понятия

Криптография, принцип Керкгоффса, криптостойкость, шифр Вернама, криптодоказующие программы, устойчивость к брутфорс-атаке, хеширование паролей, атака нахождения прообраза, коллизии криптографических хеш-функции, средства взлома,уязвимость протокола WPS.

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Выполнить и сдать на проверку задания аудиторной СРС 6.

Подготовить ответы на дополнительные вопросы Д.З.35. - Д.З.36.

Тема 2.2. Криптографические алгоритмы. Симметричное шифрование

Цель: изучить открытые алгоритмы шифрования, предполагающие использование вычислительных средств.

Ключевые понятия

Симметричное шифрование, простая перестановка, одиночная перестановка по ключу, перестановка «Магический квадрат», двойная перестановка, требования к симметричным криптосистемам, общая схема симметричных криптосистем, виды симметричных блочных шифров, стандарты шифрования.

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Выполнить и сдать на проверку задания аудиторной СРС 7.

Подготовить ответы на дополнительные вопросы Д.З.37. - Д.З.38.

Тема 2.3. Алгоритм шифрования «РЕЙНДОЛ» (AES)

Цель: изучить симметричный алгоритм блочного шифрования Advanced Encryption Standard (AES), также известный как Рейндол.

Ключевые понятия

Принцип работы, трансформации, процедура SubBytes, процедура ShiftRows, процедура MixColumns, процедура AddRoundKey, алгоритм обработки ключа, алгоритм выбора раундового ключа, криптостойкость AES, XSL-атака, атака по сторонним каналам.

Технологии и формы организации
Информационная лекция.
Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.
Задания для самостоятельной работы
Подготовить ответы на дополнительные вопросы Д.З.39. - Д.З.40.

Тема 2.4. Алгоритм шифрования ГОСТ 28147-89

Цель: изучить советский и российский стандарт симметричного шифрования, введённый в 1990 году, который также является стандартом СНГ.
Ключевые понятия
Схема работы алгоритма, режим простой замены, гаммирование, режим выработки имитовставки.узлы замены (S-блоки)
Технологии и формы организации
Информационная лекция.
Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.
Задания для самостоятельной работы
Выполнить и сдать на проверку задания аудиторной СРС 8.
Подготовить ответы на дополнительные вопросыД.З.41. - Д.З.42.

Тема 2.5. Алгоритм шифрования DES

Цель: изучитьсимметричный алгоритм шифрования DES (Data Encryption Standard), разработанный фирмой IBM и утвержденный правительством США в 1977 году как официальный стандарт.
Ключевые понятия
Блочный шифр, преобразования Сетью Фейстеля, циклы шифрования, генерация ключей, конечная перестановка, схема расшифрования, слабые ключи, известные атаки на DES
Технологии и формы организации
Информационная лекция.
Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.
Задания для самостоятельной работы
Подготовить ответы на дополнительные вопросы Д.З.43. - Д.З.44.

Тема 2.6. Шифры РИВЕСТА

Цель: изучить блочный шифр (длина блока 64 бита) с переменной длиной ключа RC2 (Ron's Code 2 или Rivest's Cipher 2), разработанный Роном Ривестом в 1987 году на основе сети Фейстеля.
Ключевые понятия
Описание алгоритма RC5, расширение ключа, свойства алгоритма, варианты алгоритма RC5
Технологии и формы организации
Информационная лекция.
Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.
Задания для самостоятельной работы
Выполнить и сдать на проверку задания аудиторной СРС 9.
Подготовить ответы на дополнительные вопросы Д.З.45. - Д.З.46.

Тема 2.7. Алгоритм шифрования «БЛОУФИШ»

Цель: изучить криптографический алгоритм Блоуфиш, реализующий блочноесимметричное шифрование.

Ключевые понятия

Алгоритм Блоуфиш, сравнение с симметричными криптосистемами

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Подготовить ответы на дополнительные вопросы Д.З.47. - Д.З.48.

Тема 2.8. Алгоритм шифрования «ТУФИШ»

Цель: изучитьс имметричный алгоритм блочного шифрования Twofish с размером блока 128 бит и длиной ключа до 256 бит, разработанный группой специалистов во главе сБрюсом Шнайером.

Ключевые понятия

Алгоритм Twofish, алгоритм Отбеливание, криптопреобразование Адамара, циклический сдвиг на 1 бит, генерация ключей

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Выполнить и сдать на проверку задания аудиторной СРС 10.

Подготовить ответы на дополнительные вопросы Д.З.49. - Д.З.50.

Тема 2.9. Алгоритм шифрования «ИДЕА»

Цель: изучить симметричный блочный алгоритм шифрования данных IDEA (англ. International Data Encryption Algorithm, международный алгоритм шифрования данных), запатентованный швейцарской фирмой Ascom.

Ключевые понятия

Алгоритм IDEA, генерация ключей, режимы шифрования, слабые ключи, сравнение с некоторыми блочными алгоритмами

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Подготовить ответы на дополнительные вопросыД.З.51. - Д.З.53.

Тема 2.10. Алгоритм шифрования «ХУФУ» И «ХАФРЕ»

Цель: изучить симметричный блочный криптоалгоритм Khufu, разработанный Ральфом Мерклом в 1990 году в качестве альтернативы DES, исправляющий ряд ее недостатков.

Ключевые понятия

Алгоритм Khufu, Криптоустойчивость Khufu и Khafre

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Выполнить и сдать на проверку задания аудиторной СРС 11.

Подготовить ответы на дополнительные вопросы Д.З.54. - Д.З.56.

Тема 2.11. Потоковый алгоритм шифрования «RC4»

Цель:изучитьпотоковый шифр RC4(также известен какARCFOURилиARC4), широко применяющийся в различных системах защиты информации в компьютерных сетях (например, в протоколахSSLиTLS, алгоритме безопасности беспроводных сетейWEP).

Ключевые понятия

Алгоритм RC4, Криптоустойчивость RC4, ИнициализацияS-блока, Генерация псевдо-случайного словаK, Исследования Руза и восстановление ключа из перестановки, Атака Флурера, Мантина и Шамира, Атака Кляйна, Комбинаторная проблема

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Подготовить ответы на дополнительные вопросы Д.З.57. - Д.З.58.

Тема 2.12. Асимметричный алгоритм шифрования RSA

Цель: изучить криптографический алгоритм с открытым ключом RSA(аббревиатура от фамилий Rivest, Shamir и Adleman), основывающийся на вычислительной сложности задачи фактор изациибольших целых чисел.

Ключевые понятия

Алгоритм RSA, Криптоустойчивость RSA, Создание открытого и секретного ключей, Цифровая подпись, Скорость работы алгоритма RSA, Использование китайской теоремы об остатках для ускорения расшифровки, Атака Винера на RSA, Алгоритм шифрования сеансового ключа

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Подготовить ответы на дополнительные вопросы Д.З.59. - Д.З.60.

Тема 2.13. Криптоанализ

Цель: изучить криптоанализ, как науку о методах расшифровки зашифрованной информации без предназначенного для такой расшифровки ключа.

Ключевые понятия

Криптоанализ. Методы криптоанализа. Атака на основе шифротекста. Атака на основе открытых текстов. Атака на основе подобранного открытого текста. Атака на основе подобранного ключа. Атака «человек посредине». Атака по сторонним каналам. Атака «дней рождений»

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Выполнить и сдать на проверку задания аудиторной СРС 12.

Подготовить ответы на дополнительные вопросы Д.З.61. - Д.З.63.

А3. Лабораторный практикум

РАЗДЕЛ 1. «Современные web-технологии»

Тематика лабораторных работ

№ темы раздела 1	Наименование	Трудоемкость, ак.час
1,2	ЛР№1 Подготовка HTML-документов	4
1,3	ЛР№2 Каскадные таблицы стилей (CSS)	4
1,2,3	ЛР№3 Приемы создания статического web-сайта	2
4	ЛР№4 Конструкторы сайтов. Системы управления контентом.	4
5,6	ЛР№5 Создание простейших PHP скриптов	4
6,7	ЛР№6 Загрузка файлов на сервер.	4
6,7	ЛР№7 Работа с массивами и регулярными выражениями.	4
8	ЛР№8 Создание простейших Web-интерфейсов к БД с помощью PHP	6
9	ЛР№9 Аутентификация пользователей средствами управления сеансом.	4
		36

Вопросы для собеседования лабораторным работам

ЛР№1

1. Структура и основные элементы HTML страниц.
2. Язык гипертекстовой разметки страниц HTML: общая структура документа
3. Что такое тег? Структура тега HTML. Формат записи тега HTML.
4. Привести структуру HTML документа. Описать назначение тегов <HTML>, <HEAD>, <META>, <BODY>.
5. Что такое атрибут тега? Формат записи атрибутов тега HTML.
6. Перечислить теги для представления текстовой информации и дать их описание.
7. Как представляются гиперссылки в HTML документе? Дать пример внутренних и внешних ссылок.
8. Перечислить виды списков, существующих в HTML. Привести теги, представляющие списки в HTML.
9. Что такое вложенные списки в HTML? Привести пример вложенного списка HTML.
10. Web-графика, графические форматы, графический объект как ссылка.
11. Как включаются графические объекты в HTML документы?
12. Куда будет указывать ссылка, если атрибут href оставить пустым (какой-то адрес)?
13. Как будет отображаться страница, если мета-тег charset не будет соответствовать фактической кодировке текста?.
14. Что произойдет, если в странице использовать следующий код:
    <meta http-equiv="refresh" content="0;">

ЛР№2

1. Синтаксис и принцип работы CSS
2. Способы включения CSS в HTML документ
3. CSS Селекторы
4. Как применить один стиль к нескольким селекторам?
5. Селекторы, зависящие от контекста
6. Обзор свойств CSS
7. Сокращённые свойства CSS

8. Приоритеты в каскаде стилей. Что означает !important?
9. Как задать цвет в CSS
10. Как задаются размеры (длина, ширина) в CSS
11. Вставка комментариев в CSS код
12. Классы и псевдоклассы.
13. Блоковая модель.
14. Позиционирование блоков. Плавающие блоки
15. Чем отличаются действия свойств display:none и visiblity:hidden?
16. На веб-странице размещено изображение шириной 200px. Как задать для него обтекание текстом по правой стороне?
17. Как поместить элемент веб-страницы (например, <p>) за видимую область экрана?

ЛР№3

1. Линейная структура многостраничных HTML документов.
2. Нелинейная структура многостраничных HTML документов.
3. Типы web-сайтов. Статические и динамические сайты
4. Информационные сайты и веб-приложения
5. Порталы
6. Виды специализированных сайтов
7. Внутренняя и внешняя структура web-сайта
8. Типовые структуры web-сайтов.
9. Требования к навигации сайта.
10. Типы навигации: перебор страниц, пиктограммы.
11. Способы организации меню сайта.
12. Карта сайта.
13. Хостинг. Бесплатный хостинг. FTP. Размещение Интернет-ресурса на сервере провайдера.

ЛР№4

1. Что такое конструктор сайта?
2. Основные возможности конструктора Ucoz.
3. Что такое система управления контентом?
4. В чем отличия конструктора сайта от cms?
5. Как зарегистрировать нового пользователя в системе uCoz?
6. Какие модули можно использовать в системе uCoz?
7. Как настроить используемые Модули в системе uCoz?
8. Как настроить Дизайн в системе uCoz?
9. Как отредактировать HTML-код модуля uCoz?
10. Какие виды тестов можно использовать в системе uCoz?

ЛР№5

1. Синтаксис php. Встраивание сценариев php в html.
2. Формирование html внутри php-сценария
3. Переменные в PHP
4. Типы данных в PHP
5. Выражения в PHP
6. Основные операторы PHP
7. Управляющие конструкции языка PHP
8. Способы передачи параметров сценарию
9. Обработка параметров запросов
10. Элементы HTML-форм
11. Функции даты и времени
12. Строковые функции

ЛР№6

1. Этапы работы протокола HTTP.

2. Структура URL. Структура запроса клиента/ответа сервера.
3. Протокол HTTP. Основные http-заголовки. Коды ответов сервера.
4. Передача данных методами GET и POST.
5. Переменные окружения. Полный ответ сервера
6. Функции для записи и чтения из файлов
7. Функции для работы с файловой системой
8. Суперглобальный массив FILES. Структура, параметры.
9. Multipart-форма для загрузки файлов на сервер
10. Проверка типа и размера файлов при загрузке

ЛР№7

1. Определение массива
2. Ассоциативные массивы
3. Доступ к элементам массива
4. Обход элементов ассоциативного массива
5. Функция file(), назначение пример использования
6. Функция file(), назначение пример использования
7. Функция explode(), implode(), назначение пример использования
8. Многомерные массивы
9. Операции над массивами
10. Для чего нужны регулярные выражения?
11. Основные шаблоны регулярных выражений.

ЛР№8

1. Устройство MySQL
2. Поля и их типы в MySQL
3. Создание таблиц. Оператор CREATE
4. Ключи и идексы
5. Добавление данных в таблицу. Оператор INSERT
6. Обновление записей. Оператор UPDATE
7. Выбор записей. Оператор SELECT
8. Функции MIN, MAX, AVG, SUM
9. Группировка записей
10. Функции PHP для соединения с сервером MySQL
11. Функции выполнения запросов к серверу баз данных
12. Функции обработки результатов запроса: mysql_fecth_array(), mysql_fecth_row(), mysql_fetch_assoc()

ЛР№9

1. Что такое авторизация?
2. Что такое аутоинтефикация?
3. Что такое сессия?
4. Что такое куки?
5. Механизмы авторизации через сессии и куки
6. Как задается имя сессии?.
7. Где располагается файл сессии?
8. Как сохранить переменные в сессию?
9. Как можно получить переменные сессии?
10. Функции работы с сессиями.
11. Как можно изменить время существования сессии?
12. Сортировка с помощью окна списка.
13. Ввод данных в динамический массив.

РАЗДЕЛ 2. «Методы и средства защиты информации»

Лабораторный практикум

№ раздела УМ	Наименование лабораторных работ	Трудоемкость, ак.час
1.2	ЛР№1. Применение технологии трансляции сетевых адресов отправителя и получателя в межсетевом экране Netfilter в ОС Linux ([1] 38 с.).	1
1.3	ЛР№2. Использование прокси-сервера SQUID ([1] 58 с.).	1
1.4	ЛР№3. Настройка Zone-Based Policy Firewall ([1] 82 с., [4]).	1
1.5	ЛР№4. Настройка CBAC ([4]).	1
1.6	ЛР№5. Межсетевые экраны CiscoPIX (ASA) ([1] 86 с.).	2
1.7	ЛР№6. Организация защищенного канала на основе протокола IPSec между маршрутизаторами Cisco Systems ([1] 96 с.).	2
1.8	ЛР №7. Использование средств обфускации программ	2
2.1	ЛР№8. Технологии виртуальных частных сетей. Защита данных на сетевом уровне. Организация VPN средствами СКЗИ VipNet. Использование протокола IPSec для защиты сетей [4, пп. 5.6-5.8 (135 – 157с.)].	1
2.2	ЛР№9. Настройка службы динамического распределения сетевых адресов. Динамическое распределение адресов. Роль DHCP-сервера для контроллера домена Windows Server. Интеграция с Active Directory [3, п4 (32-39 с.)].	1
2.3	ЛР№10. Применение технологии терминального доступа для организации многопользовательского режима обработки информации и удаленного администрирования в Microsoft Windows Server [4, 184 с.].	1
2.4	ЛР№11. Организация VPN прикладного уровня на основе ОС Windows и криптопровайдера КриптоПро CSP [4, 179 с.].	1
2.5	ЛР№12. Применение технологии трансляции сетевых адресов отправителя и получателя в межсетевом экране Netfilter в ОС Linux ([1] 38 с.).	2
2.13	ЛР№13. Анализ устойчивости алгоритмов шифрования WEP и WPA-TKIP	2
		18

А4. Задания для аудиторной самостоятельной работы студентов

РАЗДЕЛ 2 «Методы и средства защиты информации»

Аудиторная СРС 1. Необходимо ограничить пользователя «INI» в использовании web-сервиса так, чтобы он мог работать только с сервером «OUT2». Обратите внимание на правильную последовательность определения правил фильтрации.

Аудиторная СРС 2. При начальных условиях предыдущей задачи необходимо предоставить внутренним пользователям возможность использования коман-ды Ping для проверки доступности внешних узлов, но исключить такую воз-можность для внешних узлов при сканировании узлов защищаемой сети

Аудиторная СРС 3. При начальных условиях предыдущей задачи необходимо предоставить всем клиентам внутренней сети FTP-сервис (рис. 2.10). Учтите, что на рис. 2.10 показан типовой обмен клиента и FTP-сервера, а программа E-Serv, установленная на виртуальных компьютерах, инициализирует передачу данных не с порта 20, а с порта >1024.

Аудиторная СРС 4. При начальных условиях предыдущей задачи необходимо ограничить пользователя компьютера «IN1» в использовании FTP-сервиса так, чтобы он мог работать только с сервером «OUT2»

Аудиторная СРС 5. При начальных условиях предыдущей задачи необходимо предоставить пользователю компьютера «IN1» сервис электронной почты. На компьютере «IN1» приложение Outlook Express настроено на почтовый ящик с адресом «U1@mail.ru» на сервере «OUT1». Выемка почто-вой корреспонденции осуществляется по протоколу POP3. Произведите от-правку электронного сообщения от имени пользователя U1 самому себе.

Аудиторная СРС 6. При начальных условиях предыдущей задачи необходимо предоставить пользователю внешнего узла «OUT1» возможность работы с внутренним web-сервером «IN1»

Аудиторная СРС 7. При начальных условиях предыдущей задачи необходимо предоставить пользователю внешнего узла «OUT2» возможность работы с внутренним FTP сервером «IN2»

Аудиторная СРС 8. Разработать политику для web-сервера, на котором разрешен только трафик через порты TCP/80 и TCP/443 из любой точки.

Аудиторная СРС 9. Вирус и антивирус. Готовится несколько файлов, часть из которых содержат некие фразы, которые антивирус должен воспринимать как вредоносный код. Антивирус является сервисом, он остаётся запущенным. При открытии/выполнении файлов, содержащих вредоносный код, антивирус блокирует к ним доступ и оповещает об этом пользователя.

Аудиторная СРС 10. Шифратор/ дешифратор. Пользователь вводит текст, выбирает метод шифрования, при необходимости задаёт ключевое слово и другие параметры (в зависимости от шифра). После нажатия кнопки шифрации он видит шифрованный текст. Затем этот текст может быть дешифрован по нажатию соответствующей кнопки.

Аудиторная СРС 11. Счётчик трафика. Приложение показывает список запущенных процессов, использующих сеть. Также собирает информацию о суммарном количестве входящего трафика по каждому из процессов и всего.

Аудиторная СРС 12. Анализатор трафика. Приложение перехватывает сетевой трафик и анализирует его, отображая в результате следующую информацию: время, IPадрес, порт, протокол, действие.

А4 Задания для внеаудиторная самостоятельная работа студентов

РАЗДЕЛ 1. «Современные web-технологии»

Домашнее задание №1

1. Спроектировать структуру веб-сайта
2. Разработать эскиз оформления веб-сайта
3. Выполнить верстку двух макетов страницы по разработанному эскизу с использованием табличной и блочной верстки.

Домашнее задание №2

1. Создать внешние таблицы стилей (раздельные для устройств screen, print и handheld) для разрабатываемого вами сайта.
2. Подключить созданные стилевые таблицы к макету страницы.

Домашнее задание №3

Разработать программный модуль на PHP, MySql по своему варианту. Программный модуль включить в созданный в заданиях 1,2 сайт

Номера вариантов соответствуют порядковому номеру в списке группы (см. www.novsu.ru)

Порядковый номер в списке группы	Номер варианта
1, 11,21	1
2,12,22	2
3,13,23	3
4,14,24	4
5,15,25	5
6,16,26	6
7,17,27	7
8,18,28	8
9,19,29	9
10,20,30	10

Вывод статических страниц осуществляется с помощью операторов включения include или *require* (см. пример).

Пример. Общий вывод статических страниц.

```
<?
// файл  static.php
// Загружаем, если это необходимо функции и переменные, которые находятся //например в файле function.php
include(“function.php”);
//Выводим верхнюю часть сайта, которая постоянна на всех страницах
include (“header.htm”);
// выводим меню – перечень ссылок
include(“menu.php”);
// Выводим запрашиваемое содержание
include(“$content.htm”);
//Выводим нижнюю постоянную часть сайта
include(“footer.htm”);
?>
```

Для основного сценария достаточно включить в страницу соответствующие ссылки, например:

```
<a href=”static.php?content=project”> Мой курсовой проект </a>
<a href=”static.php?contnt=text1”> Что умеет Яндех</a>
```

и т.д.

Вариант 1
Система Интернет-голосования
Основные функции:
1. Все голосования хранятся в БД (можно иметь много голосований).
2. Количество вопросов каждого голосования варьируется от 3 до 5.
3. По каждому голосованию подводятся результаты (количество проголосовавших, самый популярный ответ - % проголосовавших за него).
4. Каждое голосование должно иметь 2 состояния: активно, пассивно. Принимать участие пользователь может только в активном голосовании, в пассивном – просматривать результаты.
5. Голосование должно быть редактируемо в режиме администратора (вопрос, варианты ответов).

Предусмотреть защиту голосования от накруток. Для этого использовать невозможность проголосовать дважды с одного IP.

Вариант 2
Интернет доска объявлений
Основные функции
1. В БД хранятся тексты объявлений, время их создания, автор и т.д.
2. Пользователи имеют возможность размещения своего объявления.
3. Объявления выводятся по 10 штук на странице отсортированные по дате.
4. Должна быть предусмотрена возможность добавления комментарий для каждого объявления.
5. Должен быть предусмотрен WEB – интерфейс для редактирования объявлений, в том числе удаления администратором.

Вариант 3
Публикация новостей.
Основные функции:
1. Новости хранятся в БД и создаются только пользователем с разрешением их публиковать (автором) Можно ограничится связкой login-password.
2. Новости выводятся по 5 на страницу. Следующие 5 на другую страницу и т.д.
3. Формат вывода новостей:
– дата, краткий заголовок,
– сообщение (с новой строки)
4. Должна быть предусмотрена возможность добавления комментарий для каждой новости.
5. Предусмотреть web-интерфейс для редактирования новостей, в том числе удаления администратором.

Вариант 4
Система электронной рассылки
Основные функции:
1. В БД хранится информация о пользователях, подписавшихся на рассылку по e-mail.
2. Пользователь имеет возможность подписаться и отписаться от рассылки через web-форму. Отписавшийся пользователь удаляется из БД.
3. Рассылка осуществляется администратором через Web-форму, в которой есть поле «Сообщение» и кнопка «Отправить подписавшимся».
4. Предусмотреть web-интерфейс для просмотра и редактирования информации о пользователях для администратора.

Вариант 5
Случайное фото.
Основные функции:
1. На сайте (каждый раз при загрузке страницы) публикуется случайным образом фото.
2. Названия файлов фото, информация об их владельце, время добавления и т.д. хранятся в БД. Фото выводится в уменьшенном виде, с возможностью получить просмотр в оригинале по ссылке.
3. Имеется возможность размещения фото любым пользователем.
4. Должна быть предусмотрена возможность добавления комментарий для каждой фотографии.
5. Размер фото ограничен, в случае превышения размера выдается соответствующее сообщение.

Предусмотреть web-интерфейс для просмотра и редактирования информации и пользователях и размещенных на сервере фото в режиме администратора.

Вариант 6
Баннерный показ
Основные функции:
1. На сайте (каждый раз при загрузке страницы) публикуется случайным образом баннер.
2. Названия баннеров, имя файла, URL, информация об их владельце, время показа и т.д. хранятся в БД. Если текущая дата больше даты времени показа, то баннер не показывается.
3. В БД также хранить количество кликов по баннеру и количество его показов. Для определения количества кликов использовать промежуточную страницу на которой организовать переход по ссылке баннера:

```
<?
 header("Location: http://   ");
?>
```

Предусмотреть web-интерфейс для просмотра и редактирования информации в режиме администратора.

Вариант 7
Система тренировочного тестирования по различным курсам
Основные функции:
1. Сами тесты по различным (не менее 3-х) курсам, варианты правильных ответов, информация о зарегистрированных пользователях хранятся в БД.
2. В режиме администратора можно добавлять вопросы для каждого теста и новый тест. Для упрощения задачи принимаются допущения:
3. форма теста – выбор одного варианта из нескольких,
4. порядок вопросов – последовательный от 1 до последнего.
5. При заходе на страницу тестирования пользователь авторизуется, выбирает тест из списка, вводит свои анкетные данные (ФИО), проходит тест, видит количество правильных ответов и сообщение «Тест сдан», если количество правильных ответов превышает 80% от всех вопросов, или «Тест не сдан» в противном случае.
Результаты тестирования не сохраняются.

Вариант 8
Гостевая книга
Основные функции:
1. Обсуждения и сведения о пользователях хранятся в БД.
2. В качестве сведений о пользователе выступают: ник, фотография размером не более 100x100, e-mail.

3. Должна быть предусмотрена возможность добавления комментарий для каждого обсуждения.
4. Предусмотреть web-интерфейс для редактирования собственной гостевой зарегистрированным пользователям.

Вариант 9
Биржа труда
Система, которая предназначена для размещения и поиска вакансий и резюме Основные функции:
1. Регистрация соискателей и работодателей
2. Добавления резюме через web-форму. Резюме не видимо в каталоге, но доступно для отправки на вакансию.
3. Добавление вакансий
4. Отправка резюме на вакансию
5. Просмотр вакансий и уведомление о новых присланных резюме.

Для упрощения задачи принимаются допущения:

Рассматривается только одна категория - Информационные технологии

В категории несколько специальностей – системный администратор, системный программист, WEB-программист и т.д.

Информационые технологии (0)
WEB-программист (0)
Системный программист(2)
Системный администратор (4)

Пример резюме:
Имя:
Фамилия:
Отчество:
Телефон:

Требования к будущей работе

Сфера деятельности	Банковское дело
Должность	банкир
Минимальная зарплата	20 000$
Тип работы	полный рабочий день
Информация о соискателе	
Уровень образования	высшее
Возраст	26
Опыт работы	

Старший помощник оператора торгового зала

Пример вакансии:

Сфера деятельности	Создание сайтов
Должность	Управление проектами
Зарплата	до 1000 руб.
Тип работы	полный рабочий день
Возраст	до 40
Пол	муж.
Семейное положение	Холост/Не замужем
Образование	высшее
Общий стаж	до 3 лет

Функциональные обязанности:

Отправить резюме на эту вакансию

Вариант 10
Файлообменник

Основные функции:
1. Зарегистрированным пользователям предоставляется возможность закачки и временного хранения (12 часов) файлов. Для доступа к файлу сообщается ссылка.
2. Информация о зарегистрированных пользователях, закачанных файлах хранится в БД.
3. Файлы закачиваются только в архивах.
4. Если файл затребован пользователем позднее 12 часов после закачки, то выдается сообщение «Файл недоступен», а файл удаляется.
5. Должно быть предусмотрено программное удаления всех устаревших файлов администратором с помощью специального скрипта.
6. Предусмотреть web-интерфейс для редактирования собственной гостевой зарегистрированным пользователям.

Форма контроля: проверка исходного кода и результатов работы программы.

РАЗДЕЛ 2 «Методы и средства защиты информации»

Д.З.1. Сформулируйте понятие информационной безопасности ИС.

Д.З.2. Объясните понятия целостности, конфиденциальности и доступности информации.

Д.З.3. Укажите отличия санкционированного доступа к информации от несанкционированного.

Д.З.4. Перечислите основные признаки классификации возможных угроз безопасности И С

Д.З.5. Дайте краткую характеристику угрозы безопасности, обозначаемой термином «троянский конь».

Д.З.6. Дай те краткую характеристику угроз безопасности, обозначаемых терминами «вирус» и «червь».

Д.З.7. Назовите и охарактеризуйте наиболее распространенные виды сетевых атак.

Д.З.8. Опишите атаку «человек-в-середине». Какие средства позволяют эффективно бороться с атаками такого типа?

Д.З.9. Опишите атаку типа «отказ в обслуживании» н распределенную атаку «отказ в обслуживании».

Д.З.10. Опишите особенности фишинга н фарминга. Укажите меры противодействия этим атакам.

Д.З.11. Каковы источники нарушений безопасности проводных корпоративных сетей?

Д.З.12.Назовите основные уязвимости и угрозы беспроводных сетей.

Д.З.13. Объясните понятие «политика безопасности организации».

Д.З.14. Какие разделы должна содержать документально оформленная политика безопасности?

Д.З.15. Какие проблемы решает верхний уровень политики безопасности?

Д.З.16. Какие задачи решает средний уровень политики безопасности?

Д.З.17. Каковы особенности нижнего уровня политики безопасности?

Д.З.18. Сформулируйте обязанности руководителей подразделений, администраторов и пользователей при реализации политики безопасности.

Д.З.19. Опишите структуру политики безопасности организации.

Д.3.20. Что представляют собой специализированные политики безопасности?

Д.3.21. Приведите несколько примеров специальных политик безопасности с описанием их особенностей.

Д.3.22. Что представляют собой процедуры безопасности?

Д.3.23.Приведите несколько примеров процедур безопасности с описанием их особенностей,

Д.3.24. Перечислите основные этапы (разработки политики безопасности организации.

Д.3.25. Дайте определение понятий «идентификация», «аутентификация», «авторизация», «администрирование».

Д.3.26. Что понимают под решением задач AAA?

Д.3.27. Какие задачи решает подсистема управления идентификацией и доступом IAM?

Д.3.28. На какие категории можно разделить процессы аутентификации в зависимости от сущностей, предъявляемых пользователем для подтверждения своей подлинности?

Д.3.29. Перечислите основные атаки на протоколы аутентификации.

Д.3.30. Опишите метод аутентификации на основе многоразовых паролей. Каковы его недостатки?

Д.3.31. Опишите метод аутентификации на основе одноразовых паролей. Каковы его достоинства и недостатки?

Д.3.32. Сформулируйте принцип строгой аутентификации. Опишите типы процедур строгой аутентификации.

Д.3.33. Объясните назначение PIN-кода и особенности его использования.

Д.3.34.Объясните принцип работы двухфакторной аутентификации. Какие внешние носители информации используют для двухфакторной аутентификации пользователей? Каковы достоинства этого метода аутентификации?

Д.3.35. Опишите функциональность и характеристики смарт-карт и USB-токе-нов.

Д.3.36. Опишите методы биометрической аутентификации пользователя.

Д.3.37. Сформулируйте главную задачу стандартов информационном безопасности с позиции производителей п потребителей продуктов информационных технологий, а также специалистов но сертификации этих продуктов.

Д.3.38. Назовмте основные международные стандарты информационной безопасности.

Д.3.39. Дайте краткую характеристику международного стандарта ISO/IEC 17799:2000 (BS 7799-1:2000).

Д.3.40. Каковы основные особенности германского стандарта BSI «Руководство но защите информационных технологий для базового уровня защищенности»?

Д.3.41. Опишите содержание и укажите значение международного стандарта ISO 15408 «Общие критерии безопасности информационных технологий».

Д.3.42. Перечислите стандарты для беспроводных сетей п дайте их краткую характеристику.

Д.3.43. Назовите стандарты информационной безопасности для Интернета

Д.3.44. Каковы назначение и особенности функционирования протокола SET?

Д.3.45. Каковы назначение н функциональность протоколов SSL н IPSec? В чем эти протоколы существенно различаются?

Д.3.46. Каковы назначение и функциональность инфраструктуры управления открытыми ключами PKI?

Д.3.47.Перечислите российские стандарты безопасности информационных технологий.

Д.3.48.Каково назначение стандарта ГОСТ Р ИСО/МЭК 15408? Назовите и охарактеризуйте три основных части этого стандарта.

Д.3.49. Дайте определения следующих понятий: криптограмма, крипто алгоритм, криптосистема.

Д.3.50. В чем состоит коренное различие симметричных и асимметричных криптосистем?

Д.3.51. Охарактеризуете четыре основных режима работы блочной) алгоритма.

Д.3.52. Расскажите о способах комбинирования блочных алгоритмов для получения алгоритмов с более длинным ключом, сравните их между собой.

Д.3.53. Каковы основные характеристики и режимы работы отечественного стандарта шифрования данных?

Д.3.54. Сформулируйте концепцию криптосистемы с открытым ключом.

Д.3.55. Дайте определение однонаправленной функции. 11риведите примеры однонаправленных функций.

Д.3.56. Каковы особенности однонаправленных функций с секретом?

Д.3.57. На чем основывается надежность крипто алгоритма шифрования RSA?

Д.3.58. Опишите две основные процедуры, осуществляемые системой электронной цифровой подписи для подтверждения подлинности электронного документа.

Д.3.59. Опишите отечественный стандарт цифровой подписи, укажите его преимущества по сравнению с алгоритмом цифровой подписи DSA.

Д.3.60. Каково назначение хэш-функции и каким требованиям должна удовлетворять качественная хэш-функция?

Д.3.61. Каким образом комбинированный метод шифрования позволяет сочетать достоинства асимметричных п симметричных криптосистем? Опишите протокол реализации комбинированного метода шифрования.

Д.3.62. Опишите работы алгоритма Диффи-Халлмана. Укажите достоинства этого алгоритма.

Д.3.63. Каково назначение инфраструктуры открытых ключей PKI? Опишите функционирование и инфраструктуры РК1.

Вопросы для собеседования в конце изучения раздела 1 «Современные web-технологии» (9 неделя-тест)

1. По какому адресу доступны документы локального Web-сервера (по умолчанию):

1. http://192.168.0.1;
2. http://127.0.0.1;
3. http://www.localhost.ru;
4. http://localhost;
5. верны варианты 2,4;
6. верны варианты 2,3,4.

2. Для работоспособности http-сервера необходимо:

1. Наличие установленного и настроенного Apache;
2. Наличие доменного имени у нужного компьютера;
3. Наличие возможности подключения к компьютеру из сети интернет;
4. Наличие всех перечисленных моментов.

3. Заданы переменные $a=”A”, $b=”B” , каким образом можно вывести «A+B»?

1. echo ‘$a+$b’;
2. echo $a+’+’+$b;
3. echo $a.+.$b;
4. echo “$a+$b”.

4. Какие методы позволяют вывести все элементы массива $Test?

1. foreach($Test as $tmp) {print “$tmp
”;} ;
2. foreach($Test as $i) {print “$Test[i]
”;};

3. for($i=0;$i<count($Test)-1;$i++) {print “$Test[$i]”;};
4. for($i=count($Test);$i>0;$i++) {print $Test[$i];}.

5. В каких глобальных переменных могут храниться значения, полученные их формы?

1. $GLOBAL;
2. $_POST;
3. $_GET;
4. $HEAD;

6. По каким основным соображениям подключение к базе данных принято выводить во внешний файл и подключать его с помощью функции include():

1. Для экономии дискового пространства;
2. Для экономии времени при формировании кода;
3. Это позволяет быстро изменить настройки взаимодействия с MySQL для всего сайта;
4. Особого смысла в этом подходе нет.

7. Какое утверждение о cookie справедливо?

1. Если пользователь загружает один html документ, то может быть установлено не более одного cookie;
2. Определенные настройки браузера позволяют предупредить об установки cookie;
3. Создание cookie может быть отключено пользователем;
4. В данных cookie принято сохранять имя и пароль пользователя на доступ;
5. Верны варианты 1,4;
6. Верны варианты 2,3.

8. Кто задаёт Web стандарты?

1. Microsoft
2. Mozilla
3. Консорциум Всемирной паутины
4. Google

9. Выберите правильный способ создания ссылки?

1. <a>http://www.w3schools.com
2. W3Schools
3. W3Schools.com
4. W3Schools.com

10. Как задать цвет фона для всех элементов h1?

1. h1.all {background-color:#FFFFFF;}
2. all.h1 {background-color:#FFFFFF;}
3. h1 {background-color:#FFFFFF;}

11.В какой части HTML документа следует подключать таблицы стилей?

1. В секции <body>
2. В секции <head>
3. В начале документа
4. В конце документа

12.Какой HTML атрибут используется для создания встроенных стилей?

1. font
2. style
3. class
4. styles

13.Какие из утверждений о методах POST и GET справедливы?

1. POST запрашивает только заголовок данных;
2. POST используется по умолчанию;
3. GET используют для ввода пароля;
4. GET вставляет запрос в строку адреса;
5. верны варианты 1, 4;

6. верны варианты 2, 3.

14.Заданы переменные $a=”A”, $b=”B” , каким образом можно вывести «A+B»?

1. echo ‘$a+$b’;
2. echo $a+’+’+$b;
3. echo $a.+.$b;
4. echo “$a+$b”.

15.Какими «свободно» распространяемые редакторы могут использоваться для редактирования PHP кода:

1. Microsoft Word;
2. Notepad++ ;
3. Adobe DreamWeaver;
4. Write (из пакета Open Office);
5. верны варианты 2,4

16. html-шаблоны в виде отдельных фалов предназначены для:

1. хранения в них шаблонов используемых таблиц стилей;
2. хранения больших объемов текстовой информации представляемой на сайте;
3. экономии места занимаемого базой данных;
4. хранения макета отдельных разделов сайта;
5. верны ответы 1,2,3;
6. верны ответы 3,4

17. Какие утверждения о функциях по работе с файлами справедливы?

1. fgets() - предназначена для чтения произвольного кол-ва символов;
2. freads() - предназначена для чтения произвольного кол-ва символов;
3. fgetc() - предназначена для чтения отдельных символов;
4. fgets() - предназначена для чтения отдельных символов;

18. По каким основным соображениям подключение к базе данных принято выводить во внешний файл и подключать его с помощью функции include():

1. Для экономии дискового пространства;
2. Для экономии времени при формировании кода;
3. Это позволяет быстро изменить настройки взаимодействия с MySQL для всего сайта;
4. Особого смысла в этом подходе нет.

ВОРОСЫ К ЭКЗАМЕНУ

1. Средства защиты от несанкционированного доступа
2. Информационная безопасность
3. Средства защиты от несанкционированного доступа
4. Системы обнаружения и предотвращения вторжений
5. Системы мониторинга сетей
6. Антивирусные средства
7. Межсетевые экраны
8. Технические средства защиты авторских прав
9. Запутывание кода программ
10. Управление ключами. Электронная цифровая подпись
11. Криптографические средства
12. Криптографические алгоритмы. Симметричное шифрование
13. Алгоритм шифрования «РЕЙНДОЛ» (AES)
14. Алгоритм шифрования ГОСТ 28147-89
15. Алгоритм шифрования DES
16. Шифры РИВЕСТА
17. Алгоритм шифрования «БЛОУФИШ»

18. Алгоритм шифрования «ТУФИШ»
19. Алгоритм шифрования «ИДЕА»
20. Алгоритмы шифрования «ХУФУ» И «ХАФРЕ»
21. Потоковый алгоритм шифрования «RC4»
22. Асимметричный алгоритм шифрования RSA
23. Криптоанализ

Пример экзаменационного билета

БИЛЕТ № 1	
Вопрос 1.	**Средства защиты от несанкционированного доступа**
Вопрос 2.	**Запутывание кода программ**

Таблица А.1 - Организация изучения учебного модуля «Современные web-технологии и методы и средства защиты информации»

Раздел модуля	Технология и форма проведения занятий	Задания на СРС	Дополнительная литература и интернет-ресурсы
РАЗДЕЛ 1 СОВРЕМЕННЫЕ WEB-ТЕХНОЛОГИИ			
1.Введение. Структура и принципы Веб	– информационная лекция	– подготовиться к собеседованию (внеауд. СРС)	1. Аляев Ю. А. Алгоритмизация и языки программирования Pascal, C++, Visual Basic : учеб.-справ. пособие для курсантов военно-учеб. заведений и училищ, техн. вузов и учащихся спец. кл. шк. - М. : Финансы и статистика, 2004. - 318с. 2. Visual Basic для начинающих http://www.codenet.ru/progr/vbasic/bit/
2. Язык гипертекстовой разметки HTML, XHTML	– информационная лекция – выполнение заданий ЛР №1	– подготовиться к собеседованию (внеауд. СРС) – задание 1 из ДЗ (внеауд. СРС)	1. Окулов С.М. Программирование в алгоритмах. - М. : БИНОМ. Лаборатория знаний, 2004. - 341с. 2. В. Л. Быков. Основы программирования на языке Visual Basic 6.0: пособие – Брест: БГТУ, 2002.
3. Каскадные таблицы стилей CSS	– информационная лекция – выполнение заданий ЛР №2,3 – собеседование (защита ЛР№1)	– подготовиться к собеседованию (внеауд. СРС)	1. Краткие описания основных функций и команд VB http://www.codenet.ru/progr/vbasic/listfun.php 2. Окулов С.М. Программирование в алгоритмах. - М. : БИНОМ. Лаборатория знаний, 2004. - 341с.
4. Системы управления контентом CMS	– информационная лекция – выполнение заданий ЛР №4 – собеседование (защита ЛР№2,3)	– подготовиться к собеседованию (внеауд. СРС) – задание 2 из ДЗ (внеауд. СРС)	1. Аляев Ю. А. Алгоритмизация и языки программирования Pascal, C++, Visual Basic : учеб.-справ. пособие для курсантов военно-учеб. заведений и училищ, техн. вузов и учащихся спец. кл. шк. - М. : Финансы и статистика, 2004. - 318с.
5. Синтаксис языка PHP	– лекция-демонстрация – выполнение заданий ЛР №5 – собеседование (защита ЛР№4)	– подготовиться к собеседованию (внеауд. СРС)	1 В. Л. Быков. Основы программирования на языке Visual Basic 6.0: пособие – Брест: БГТУ, 2002 2 Князева М.Д. Алгоритмика: от алгоритма к программе : учеб. пособие для сред. и высш. проф. образования. - М. : Кудиц-Образ, 2006. - 191с..
6. Формы. Обработка	– информационная	– подготовиться к	1. Аляев Ю. А. Алгоритмизация и языки

Раздел модуля	Технология и форма проведения занятий	Задания на СРС	Дополнительная литература и интернет-ресурсы
форм	лекция – выполнение заданий ЛР №6 – собеседование (защита ЛР№5)	собеседованию (внеауд. СРС) – задание 3 из ДЗ (внеауд. СРС)	программирования Pascal, C++, Visual Basic : учеб.-справ. пособие для курсантов военно-учеб. заведений и училищ, техн. вузов и учащихся спец. кл. шк. - М. : Финансы и статистика, 2004. - 318с. 2. Шень А. Программирование:теоремы и задачи. - 2-е изд., испр. и доп. - М. : МЦНМО, 2004. - 294с.
7. Регулярные выражения. Работа с файлами в PHP	– информационная лекция – выполнение заданий ЛР №7 – собеседование (защита ЛР№6)	– подготовиться к собеседованию (внеауд. СРС) – задание 3 из ДЗ (внеауд. СРС)	1. Аляев Ю. А. Алгоритмизация и языки программирования Pascal, C++, Visual Basic : учеб.-справ. пособие для курсантов военно-учеб. заведений и училищ, техн. вузов и учащихся спец. кл. шк. - М. : Финансы и статистика, 2004. - 318с. 2. Шень А. Программирование:теоремы и задачи. - 2-е изд., испр. и доп. - М. : МЦНМО, 2004. - 294с.
8. Взаимодействие PHP и MySQL	– информационная лекция – выполнение заданий ЛР №8 – собеседование (защита ЛР№7)	– подготовиться к собеседованию (внеауд. СРС) – задание 3 из ДЗ (внеауд. СРС)	1 Князева М.Д. Алгоритмика: от алгоритма к программе: учеб. пособие для сред. и высш. проф. образования. - М. : Кудиц-Образ, 2006. - 191с. 2 Сергиевский Г. М. Функциональное и логическое программирование : учеб. пособие для вузов / Г. М. Сергиевксий, Н. Г. Волчёнков. - М. : Академия, 2010. - 317с.
9. Сессии и cookie в PHP	– лекция –демонстрация – выполнение заданий ЛР №9 – собеседование (защита ЛР№8,9)	– подготовиться к собеседованию (внеауд. СРС) – задание 3 из ДЗ (внеауд. СРС)	1 Зарубин В. С.Моделирование : учеб. пособие для вузов / В. С. Зарубин. - М. : Академия, 2013. - 335 с 2 В. Л. Быков. Основы программирования на языке Visual Basic 6.0: пособие – Брест: БГТУ, 2002.

РАЗДЕЛ 2 «МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»

УЭМ1Средства защиты от несанкционированного доступа			
1.1 Информационная безопасность	– информационная лекция	– Д.З.1. - Д.З.4.	– Мельников В. П. Защита информации : учебник : для вузов / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; под ред. В. П. Мельникова. - М. : Академия, 2014
1.2 Средства защиты от	– информационная	– Аудиторная СРС 1.	– Мельников В. П. Защита информации : учебник : для

несанкционированного доступа	лекция – выполнение ЛР№1; – собеседование (защита ЛР№1)	– Д.3.5. - Д.3.8.	вузов / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; под ред. В. П. Мельникова. - М. : Академия, 2014 – Арутюнов В. В. Защита информации : учеб.-метод. пособие. - М. : Либерея-Бибинформ, 2008
1.3. Системы обнаружения и предотвращения вторжений	– информационная лекция – выполнение ЛР№2; – собеседование (защита ЛР№2)	– Д.3.9. - Д.3.14.	– Мельников В. П. Защита информации : учебник : для вузов / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; под ред. В. П. Мельникова. - М. : Академия, 2014 – Арутюнов В. В. Защита информации : учеб.-метод. пособие. - М. : Либерея-Бибинформ, 2008
1.4 Системы мониторинга сетей	– информационная лекция – выполнение ЛР№3; – собеседование (защита ЛР№3)	– Аудиторная СРС 2. – Д.3.15. - Д.3.19.	– Мельников В. П. Защита информации : учебник : для вузов / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; под ред. В. П. Мельникова. - М. : Академия, 2014 – Арутюнов В. В. Защита информации : учеб.-метод. пособие. - М. : Либерея-Бибинформ, 2008
1.5 Антивирусные средства	– информационная лекция – выполнение ЛР№4; – собеседование (защита ЛР№4)	– Д.3.20. - Д.3.24.	– Мельников В. П. Защита информации : учебник : для вузов / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; под ред. В. П. Мельникова. - М. : Академия, 2014 – Арутюнов В. В. Защита информации : учеб.-метод. пособие. - М. : Либерея-Бибинформ, 2008
1.6 Межсетевые экраны	– информационная лекция – выполнение ЛР№5; – собеседование (защита ЛР№5)	– Аудиторная СРС 3. – Д.3.25. - Д.3.27.	– Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: Курс лекций: Учеб.пособие/Под ред.В.А.Сухомлина. - М.: Интернет-Ун-т Информ.Технологий,2005. – Арутюнов В. В. Защита информации : учеб.-метод. пособие. - М. : Либерея-Бибинформ, 2008
1.7 Технические средства защиты авторских прав	– информационная лекция – выполнение ЛР№6; – собеседование (защита ЛР№6)	– Д.3.28. - Д.3.30.	– Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: Курс лекций: Учеб.пособие/Под ред.В.А.Сухомлина. - М.: Интернет-Ун-т Информ.Технологий,2005. – Арутюнов В. В. Защита информации : учеб.-метод. пособие. - М. : Либерея-Бибинформ, 2008
1.8 Запутывание кода программ	– информационная лекция	– Аудиторная СРС 4. – Д.3.31. - Д.3.32.	– Мельников В. П. Защита информации : учебник : для вузов / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ;

	– выполнение ЛР№7; – собеседование (защита ЛР№7)		под ред. В. П. Мельникова. - М. : Академия, 2014. - 295, [2] с. – Арутюнов В. В. Защита информации : учеб.-метод. пособие. - М. : Либерея-Бибинформ, 2008
1.9 Управление ключами. Электронная цифровая подпись	– информационная лекция –	– Д.З.33. - Д.З.34.	– Мельников В. П. Защита информации : учебник : для вузов / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; под ред. В. П. Мельникова. - М. : Академия, 2014. - 295, [2] с.
Рубежный контроль		– выполнить КР(Аудиторная СРС 5.)	
УЭМ2 Криптографические средства			
2.1 Криптографические средства	– информационная лекция – выполнение ЛР№8; – собеседование (защита ЛР№8)	– Аудиторная СРС 6. – Д.З.35. - Д.З.36.	– Смарт Н. Криптография / Пер.с англ.С.А.Кулешова под ред.С.К.Ландо. - М. : Техносфера, 2006. - 525с. – Арутюнов В. В. Защита информации : учеб.-метод. пособие. - М. : Либерея-Бибинформ, 2008
2.2 Криптографические алгоритмы. Симметричное шифрование	– информационная лекция – выполнение ЛР№9; – собеседование (защита ЛР№9)	– Аудиторная СРС 7. – Д.З.37. - Д.З.38.	– Смарт Н. Криптография / Пер.с англ.С.А.Кулешова под ред.С.К.Ландо. - М. : Техносфера, 2006. - 525с. – Арутюнов В. В. Защита информации : учеб.-метод. пособие. - М. : Либерея-Бибинформ, 2008
2.3 Алгоритм шифрования «РЕЙНДОЛ» (AES)	– информационная лекция; – выполнение ЛР№10; – собеседование (защита ЛР№10)	– Д.З.39. - Д.З.40.	– Смарт Н. Криптография / Пер.с англ.С.А.Кулешова под ред.С.К.Ландо. - М. : Техносфера, 2006. - 525с. – Арутюнов В. В. Защита информации : учеб.-метод. пособие. - М. : Либерея-Бибинформ, 2008
2.4 Алгоритм шифрования ГОСТ 28147-89	– информационная лекция – выполнение ЛР№11; – собеседование (защита ЛР№11)	– Аудиторная СРС 8. – Д.З.41. - Д.З.42.	– Смарт Н. Криптография / Пер.с англ.С.А.Кулешова под ред.С.К.Ландо. - М. : Техносфера, 2006. - 525с. – Арутюнов В. В. Защита информации : учеб.-метод. пособие. - М. : Либерея-Бибинформ, 2008
2.5 Алгоритм шифрования DES	– информационная лекция	– Д.З.43. - Д.З.44.	– Торстейнсон Питер. Криптография и безопасность в технологии.NET = .Net security and cryptography / Пер.с

	– выполнение ЛР№12; – собеседование (защита ЛР№12)		англ.В.Д.Хорева под ред.С.М.Молявко. - М. : БИНОМ. Лаборатория знаний, 2007 – Арутюнов В. В. Защита информации : учеб.-метод. пособие. - М. : Либерея-Бибинформ, 2008
2.6 Шифры РИВЕСТА	– информационная лекция	– Аудиторная СРС 9. – Д.З.45. - Д.З.46.	– Торстейнсон Питер. Криптография и безопасность в технологии.NET = .Net security and cryptography / Пер.с англ.В.Д.Хорева под ред.С.М.Молявко. - М. : БИНОМ. Лаборатория знаний, 2007
2.7 Алгоритм шифрования «БЛОУФИШ»	– информационная лекция	– Д.З.47. - Д.З.48.	– Смарт Н. Криптография / Пер.с англ.С.А.Кулешова под ред.С.К.Ландо. - М. : Техносфера, 2006. - 525с.
2.8 Алгоритм шифрования «ТУФИШ»	– информационная лекция	– Аудиторная СРС 10. – Д.З.49. - Д.З.50.	– Мао, Венбо Современная криптография. Теория и практика = Modern cryptography / Пер.с англ.и ред. Д. А .Клюшина. - М.:Вильямс,2005
2.9 Алгоритм шифрования «ИДЕА»	– информационная лекция	– Д.З.51. - Д.З.53.	– Смарт Н. Криптография / Пер.с англ.С.А.Кулешова под ред.С.К.Ландо. - М. : Техносфера, 2006. - 525с.
2.10 Алгоритмы шифрования «ХУФУ» И «ХАФРЕ»	– информационная лекция	– Аудиторная СРС 11. – Д.З.54. - Д.З.56.	– Смарт Н. Криптография / Пер.с англ.С.А.Кулешова под ред.С.К.Ландо. - М. : Техносфера, 2006. - 525с.
2.11 Потоковый алгоритм шифрования «RC4»	– информационная лекция	– Д.З.57. - Д.З.58.	– Мао, Венбо Современная криптография. Теория и практика = Modern cryptography / Пер.с англ.и ред. Д. А .Клюшина. - М.:Вильямс,2005
2.12 Асимметричный алгоритм шифрования RSA	– информационная лекция	– Д.З.59. - Д.З.60.	– Бернет Стив. Криптография.Официальное руководство RSA Security / Пер.с англ.под ред.А.И.Тихонова. - М. : Бином, 2007
2.13 Криптоанализ	– информационная лекция – выполнение ЛР№13; – собеседование (защита ЛР№13)	– Аудиторная СРС 12. – Д.З.61. - Д.З.63.	– Мао, Венбо Современная криптография. Теория и практика = Modern cryptography / Пер.с англ.и ред. Д. А .Клюшина. - М.:Вильямс,2005 – Арутюнов В. В. Защита информации : учеб.-метод. пособие. - М. : Либерея-Бибинформ, 2008

ПРИЛОЖЕНИЕ Б

Технологическая карта
учебного модуля «Современные web-технологии и методы и средства защиты информации»
семестр 8, ЗЕТ 6, вид аттестации Экзамен, акад.часов 216, баллов рейтинга 300

№ и наименование раздела учебного модуля, КП/КР	№ недели сем.	Трудоемкость, ак.час					Форма текущего контроля успев. (в соотв. с паспортом ФОС)	Максим. кол-во баллов рейтинга
		Аудиторные занятия				СРС		
		ЛЕК	ПЗ	ЛР	АСРС			
РАЗДЕЛ 1 «Современные WEB-технологии»		18		36	9	54		
1.Введение. Структура и принципы Веб 2. Язык гипертекстовой разметки HTML, XHTML	1	2 2	-	4	2	6	собеседование (защита ЛР№1, ЛР№2) Задание № 1 из ДЗ	10+10 10
3. Каскадные таблицы стилей CSS	2	2	-	4	1	4	собеседование (защита ЛР№3)	10
							Задание № 2 из ДЗ	10
4. Системы управления контентом CMS	3	2	-	6	1	10	собеседование (защита ЛР№4)	10
5. Синтаксис языка PHP	4	2	-	4	1	10	собеседование (защита ЛР№5)	10
6. Формы. Обработка форм	5	2	-	4	1	8	собеседование (защита ЛР№6)	10
7. Регулярные выражения. Работа с файлами в PHP 8. Взаимодействие PHP и MySQL	6	2 2	-	4 6	2	10	собеседование (защита ЛР№7, ЛР№8)	10+10
9. Сессии и cookie в PHP	7	2	-	4	1	6	собеседование (защита ЛР№9) Задание № 3 из ДЗ	10 10
Собеседование	7						Тест	30
РАЗДЕЛ 2 «Методы и средства защиты информации»		18		18	9	36		
УЭМ1 Средства защиты от несанкционированного доступа:								

1.1 Информационная безопасность 1.2 Средства защиты от несанкционированного доступа 1.3 Системы обнаружения и предотвращения вторжений	8	3,0		3.0	1.0	3,0	собеседование Аудиторная СРС 1. Д.З.1. - Д.З.14. – собеседование Защита ЛР№1, ЛР№2	4 4+4
1.4 Системы мониторинга сетей 1.5 Антивирусные средства	8	2,0		3,0	1.0	3,0	собеседование Аудиторная СРС 2. Д.З.15. - Д.З.24. – собеседование защита ЛР№3, ЛР№4	4 4+4
1.6 Межсетевые экраны 1.7 Технические средства защиты авторских прав	9	2,0		3,0	1.0	3,0	собеседование Аудиторная СРС 3. Д.З.25. - Д.З.30. – собеседование защита ЛР№5, ЛР№6	4 4+4
1.8 Запутывание кода программ	10	1,0		2,0	1,0	3,0	собеседование Аудиторная СРС 4. Д.З.31. - Д.З.32 – собеседование защита ЛР№7	4 4
1.9 Управление ключами. Электронная цифровая подпись	10	1.0			1.0	3.0	собеседование Аудиторная СРС 5 ДЗ.33 – З.34	4
УЭМ2 Криптографические средства:								
2.1 Криптографические средства	11	1,0		1,0	1.0	3,0	собеседование Аудиторная СРС 6. Д.З.35. - Д.З.36. – собеседование защита ЛР№8	4 4
2.2 Криптографические алгоритмы. Симметричное шифрование	11	2,0		2,0	0,5	3,0	собеседование Аудиторная СРС 7.	4

2.3 Алгоритм шифрования «РЕЙНДОЛ» (AES)							– Д.З.37. - Д.З.40. – собеседование защита ЛР№9, ЛР№10	4+4
2.4 Алгоритм шифрования ГОСТ 28147-89 2.5 Алгоритм шифрования DES	12	1.0		2,0	0,5	3,0	собеседование Аудиторная СРС 8. Д.З.41. - Д.З.44. – собеседование защита ЛР№11, ЛР№12	4 4+4
2.6 Шифры РИВЕСТА 2.7 Алгоритм шифрования «БЛОУФИШ»	13	1.0			0,5	3.0	собеседование Аудиторная СРС 9. Д.З.45. - Д.З.48.	4
2.8 Алгоритм шифрования «ТУФИШ» 2.9 Алгоритм шифрования «ИДЕА»	13	1.5			0,5	3,0	собеседование Аудитор. СРС 10. Д.З.49. - Д.З.53.	4
2.10 Алгоритмы шифрования «ХУФУ» И «ХАФРЕ» 2.11 Асимметричный алгоритм шифрования RSA	14	1.5			0,5	3,0	собеседование Аудиторная СРС11 Д.З.54. - Д.З.60.	4
2.13 Криптоанализ	14	1,0		1,0	0,5	3,0	собеседование Аудиторная СРС12 Д.З.61. - Д.З.63. – собеседование –защита ЛР№13	4 4
Аттестация – экзамен								50

Критерии оценки качества освоения студентами дисциплины в соответствии с положениями «Об организации учебного процесса по образовательным программам высшего образования» и «О фонде оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации студентов, итоговой аттестации выпускников»:

- оценка «удовлетворительно – 150-179
- оценка «хорошо» – 180-269
- оценка «отлично» – 270-300

Приложение В

Карта учебно-методического обеспечения

Учебного модуля *Современные web-технологии и методы и средства защиты информации*

Направление (специальность) 44.03.05 - Педагогическое образование
профили – Математика и Информатика, Физика и Информатика
Курс 4 Семестр 8

Часов**:** всего 6 ЗЕ (216), лекций 36, лаб. раб. 54**,** ауд.СРС 18, внеуд. СРС 90
Обеспечивающая кафедра – ИТИС
Формы обучения **очная**

Обеспечение учебного модуля учебными изданиями

Для раздела 1. «Современные WEB-технологии»

Библиографическое описание* издания (автор, наименование, вид, место и год издания, кол. стр.)	Кол. экз. в библ. НовГУ	
Учебники и учебные пособия		
1. Основы web-технологий : учеб. пособие для вузов. - 2-е изд., испр. - М. : Интернет-Университет Информ. Технологий : БИНОМ. Лаборатория знаний, 2007. - 374с.	20	
2. Смелянский Р. Л. Компьютерные сети : учебник : для вузов : в 2 т. Т. 2 : Сети ЭВМ / Р. Л. Смелянский. - М. : Академия, 2011. - 239, [1] с.	2	
3. Кузнецов М.В. PHP 5/6 : Самоучитель. - 3-е изд., перераб. и доп. - СПб. : БХВ-Петербург, 2009. - 651с.	2	
4. Васильев В.В. Практикум по Web-технологиям : Практикум для вузов. - М. : Форум, 2009. - 413,[1]с.	3	
Учебно-методические издания		
1. Интернет-технологии для работников образования : метод. рекомендации. Ч. 4 : Разработка WEB-представлений / авт.-сост. Н. В. Курмышев, Г. Ю. Соколова ; Новгород. гос. ун-т им. Ярослава Мудрого. - Великий Новгород, 2004. - 33с	10	

Для раздела 2. «Методы и средства защиты информации»

Библиографическое описание* издания (автор, наименование, вид, место и год издания, кол. стр.)	Кол. экз. в библ. НовГУ	
Учебники и учебные пособия		
Мельников В. П.Защита информации : учебник : для вузов / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; под ред. В. П. Мельникова. - М. : Академия, 2014. - 295, [2] с.	2	

Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия. Курс лекций Учеб.пособие/Под ред.В.А.Сухомлина.- М.: Интернет-Ун.т Информ.Технологий, 2005.-604с	2	
Смарт Н. Криптография/ Пер.с англ. С.А.Кулешова под ред. С.К. Ландо. – М.: Техносфера. 2006.- 525с	9	
Бернет Стив. Криптография. Официальное руководство RSA Security/Пер.с англ.под ред.А.И.Тихонова.-М.: Бином, 2007.- 381,[1]с.	1	
Мао Венбо. Современная криптография. Теория и практика – Modern cruptography/ Пер.с англ.и ред.Д.А.Клюшина.-М.: Вильямс. 2005.-763с.	3	
Торстейнсон Питер. Криптография и безопасность в технологии. NET=.Net security and cryptography/ Пер.с англ. В.Д.Хорева под ред. С.М.Молявко.- М.: БИНОМ. Лаборатория знаний. 2007.-479с	1	
Учебно-методические издания		
Арутюнов В.В. Защита информации: учеб.-метод.пособие.- М.: Либерия-Бибинформ. 2008.- 55,[1]с.	1	

Информационное обеспечение УМ

Название программного продукта, интернет-ресурса
[Электронный ресурс]: ГОСТ Р 50922-2006 «Защита информации» - Режим доступа: WWW.URL: http://www.altell.ru/legislation/standards/50922-2006/pdf
[Электронный ресурс]: Журнал «Защита информации. Инсайд» - Режим доступа; WWW.URL: http://www/inside-zi/ru/
Национальный Открытый Университет «ИНТУИТ» [Электронный ресурс]: Курс «Введение в NTML и CSS» - Режим доступа: http://www/intuit.ru/studies/courses/1005/276/info
Национальный Открытый Университет «ИНТУИТ» [Электронный ресурс]: Курс «Введение в программирование на PHPS – Режим доступа: http://www/intuit/ru/stuies/courses/1025/166/info
NTML. Справочник [Электронный ресурс]: - Режим доступа: nrrp;//ntmi.manual.ru/
CSS.Справочник [Электронный ресурс]: - Режим доступа: http;//css/manual.ru/
Online Справочник-учебник по языку программирования PHP [Электронный ресурс]: - Режим доступа: nttp://www/php-spavka.ru/

Таблица 3 – Обеспечение УМ дополнительной литературой

Библиографическое описание* издания (автор, наименование, вид, место и год издания, кол. стр.)	Кол. экз. в библ. НовГУ
Аляев Ю. А. Алгоритмизация и языки программирования Pascal, C++, Visual Basic : учеб.-справ. пособие для курсантов военно-учеб. заведений и училищ, техн. вузов и учащихся спец. кл. шк. - М. : Финансы и статистика, 2004. - 318с.	15
Окулов С.М. Программирование в алгоритмах. - М. : БИНОМ. Лаборатория знаний, 2004. - 341с. [2002]	7
Князева М.Д. Алгоритмика: от алгоритма к программе: учеб. пособие для сред. и высш. проф. образования. - М. : Кудиц-Образ, 2006. - 191с.	1
Сергиевский Г. М. Функциональное и логическое программирование : учеб. пособие для вузов / Г. М. Сергиевкский, Н. Г. Волчёнков. - М. : Академия, 2010. - 317с. -2	2
Зарубин В. С.Моделирование : учеб. пособие для вузов / В. С. Зарубин. - М. : Академия, 2013. - 335 с -	1
Проектирование инфраструктуры Active Direktory Microsoft Windows Server 2003 = Designing a Microsoft Windows server 2003 Active Direktory and network infrastructure: экзамен 70-297 MCSE: учеб.курс Microsoft: пер.с англ./ Авт.: Уолтер Гленн при участии Майкла Т.Симпсона.- М.: Русская редакция: Питер. 2006.- 341, [1]с.	1

Действительно на 2017-2020 уч.год

Зав.кафедрой ИТИС: _____ А.Л.Гавриков

СОГЛАСОВАНО:

Новгородский государственный университет им. Ярослава Мудрого
Научная библиотека
Сектор учета

НБ НовГУ: гл. библ. _____ Калинина А.
Должность подпись расшифровка