МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Государственное образовательное учреждение высшего профессионального образования

Ивановский государственный энергетический университет имени В.И.Ленина

УТВЕРЖДАЮ

Декан ИВТФ

_____ Кокин В.М.

« ___ »_____ 2011 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«ЗАЩИТА ИНФОРМАЦИИ»

(Б.3.2.5)

Направление подготовки 230100 «Информатика и вычислительная техника»

Квалификация выпускника бакалавр
(бакалавр, магистр)

Профиль подготовки «Высокопроизводительные вычислительные системы на базе больших ЭВМ»

Форма обучения очная
(очная, заочная и др.)

Выпускающая кафедра Кафедра высокопроизводительных вычислительных систем

Кафедра-разработчик Программного обеспечения компьютерных систем

Семестр	Трудоём-кость, з.е. / час	Лек-ций, час	Практич. занятий, час	Лаборат. работ, час	Курсовое проекти-рование, час	СРС, час	Форма промежуточного контроля
8	4 / 144	34	-	22	-	88	экзамен

Иваново 2011

Рабочая программа дисциплины (РПД) составлена в соответствии с требованиями ФГОС ВПО по направлению подготовки 230100 «Информатика и вычислительная техника» с учетом рекомендаций ПрООП по профилю подготовки «Высокопроизводительные вычислительные системы на базе больших ЭВМ»

Программу составил:
кафедра Программного обеспечения компьютерных систем (ПОКС)

Игнатьев Е.Б., к.т.н., доцент

Рецензент:

_____

_____

Программа одобрена на заседании кафедры высокопроизводительных вычислительных систем (ВВС)
(протокол № от « ___ » _____ 2011 г.)

Заведующий кафедрой ВВС:

Сидоров С.Г., к.т.н., доцент

Председатель цикловой методической комиссии:

Ратманова И.Д., д.т.н., профессор

СОДЕРЖАНИЕ

1. Цели освоения дисциплины
2. Место дисциплины в структуре ООП ВПО
3. Структура и содержание дисциплины
4. Формы контроля освоения дисциплины
5. Учебно-методическое и информационное обеспечение дисциплины
6. Материально-техническое обеспечение дисциплины

Приложение 1. Аннотация рабочей программы
Приложение 2. Технологии и формы преподавания
Приложение 3. Технологии и формы обучения
Приложение 4. Оценочные средства и методики их применения

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является достижение следующих результатов обучения (РО):

- знания:
  - на уровне представлений: о современных средствах защиты информации и тенденциях их развития;
  - на уровне воспроизведения: методов защиты компьютерной информации;
  - на уровне понимания: стандартов, регламентирующих создание и функционирование систем защиты информации;
- умения: обеспечить информационную безопасность при проектировании компьютерных систем;
- навыки: владения методами и средствами защиты информации в ВС, локальных и глобальных сетях.

Перечисленные РО являются основой для формирования следующих компетенций:

общекультурных:

ОК-1 (владение культурой мышления, способность к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения);

ОК-12 (навыки работы с компьютером как средством управления информацией);

ОК-13 (способность работать с информацией в глобальных компьютерных сетях);

профессиональных:

ПК-2 (освоение методики использования программных средств для решения практических задач);

ПК-5 (разработка компонентов программных комплексов и баз данных, использование современных инструментальных средств и технологий программирования).

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВПО

Дисциплина «Защита информации» является вариативной (профильной) частью профессионального цикла дисциплин.

Необходимыми условиями для освоения дисциплины являются: знание основ программирования, умение применять основы информатики и программирования к проектированию, конструированию и тестированию программ, владение языком программирования высокого уровня.

В таблице приведены предшествующие дисциплины, направленные на формирование компетенций, заявленных в разделе «Цели освоения дисциплины».

№ п/п	Наименование компетенции	Предшествующие дисциплины	Последующие дисциплины (группы дисциплин)
Общекультурные компетенции			
ОК-1	владение культурой мышления, способность к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения		
ОК-12	навыки работы с компьютером как средством управления информацией		
ОК-13	способность работать с информацией в глобальных компьютерных сетях		
Профессиональные компетенции			
ПК-2	освоение методики использования программных средств для решения практических задач		
ПК-5	разработка компонентов программных комплексов и баз данных, использование современных инструментальных средств и технологий программирования		

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 4 зачётных единицы, 144 часа.

№ раздела	Наименование раздела дисциплины	Объем часов по видам учебной нагрузки					
		Лекции	Практические занятия (ПЗ)	Лабораторные работы (ЛР)	Курсовое Проектирование (КП)	Самостоятельная работа студента (СРС)	Всего
1	Основные положения. Стандарты	6				2	8
2	Основы криптографии	14		12		28	54
3	Защита информации в сетях	8		6		14	28
4	Подсистема безопасности в ОС	6		4		8	18
5	Подготовка к экзамену					36	36
	Итого:	34		22		88	144

3.1. Лекции

№ зан.	№ раздела дисциплины	Тема лекции	Объем часов
1	1	Основные понятия и определения	2
2		Стандарты безопасности. Оранжевая книга	2
3		Стандарты безопасности. Классы безопасности.	2
4	2	Типы алгоритмов шифрования.	2
5		Симметричные криптосистемы	2
6		Хеширование	2
7		Криптосистемы с открытым ключом	2
8		Системы электронной подписи	2
9		Криптосистемы на эллиптических кривых	2
10		Управление ключами	2

11	3	Протоколы распределения ключей и аутентификации	2
12		Сетевая безопасность	2
13		Экранирование	2
14		Защита электронной почты	2
15	4	Подсистема безопасности защищенных версий ОС MS Windows	2
16		Дискреционное управление доступом в MS Windows	2
17		Защита информации в ОС семейства Unix	2
		Итого:	34

3.2. Лабораторные работы

№ зан.	№ раздела дисциплины	Наименование лабораторной работы	Наименование лаборатории	Объем часов
1	1, 2	ЛР № 1. Шифрование простой подстановкой и перестановкой. Генераторы псевдослучайных чисел, гаммирование	КК*	2
2		ЛР № 2. Дешифровка, частотный анализ. Маскировка длины символа	КК	2
3		ЛР № 3. Симметричные криптосистемы. Блочные шифры	КК	2
4		ПК1	КК	2
5		ЛР № 4. Хеширование	КК	2
6		ЛР № 5. Криптосистемы с открытым ключом	КК	2
7	3	ЛР № 6. Получение и применение сертификата открытого ключа	КК	2
8		ЛР № 7. Возможности утилиты MS BaseLineSecuriyAnalizer	КК	2
9		ПК2	КК	2
10	4	ЛР № 8. Электронные ключи HASP	КК	2
11		ЛР № 9. Защита файлов в Windows	КК	2
			Итого:	22

*КК - компьютерный класс.

3.3. Самостоятельная работа студента

№ п/п	№ раздела дисциплины	Вид СРС	Объем часов
1	1	Подготовка к ПК1	2
2	2	Выполнение задания ЛР № 1	4
3		Выполнение задания ЛР № 2	4
4		Выполнение задания ЛР № 3	6
5		Подготовка к ПК1	4
6		Выполнение задания ЛР № 4	4
7		Выполнение задания ЛР № 5	6
8	3	Выполнение задания ЛР № 6	4
9		Выполнение задания ЛР № 7	4
11		Подготовка к ПК2	6
12	4	Выполнение задания ЛР № 8	4
13		Выполнение задания ЛР № 9	4
14	5	Подготовка к экзамену	36
		Итого:	88

4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль освоения дисциплины производится в соответствии с ПОЛОЖЕНИЕМ о системе РИТМ в ИГЭУ.

4.1. Текущий контроль студентов производится в дискретные временные интервалы (в соответствии с приказом ректора о проведении ТК и ПК по системе РИТМ в ИГЭУ) лектором и преподавателем(ями), ведущими лабораторные работы и практические занятия по дисциплине в следующих формах:

- компьютерное тестирование в электронном учебнике (ПК1 и ПК2);
- выполнение и защита лабораторных работ;
- кроме того, учитывается посещаемость и активность на занятиях.

4.2. Промежуточный контроль по дисциплине проходит в форме экзамена по окончании семестра (включает в себя ответы на теоретические вопросы и решение задач).

На экзамене студент получает экзаменационный билет, содержащий два теоретических вопроса из первой половины лекционного материала и из второй половины.

4.3. Итоговый контроль по окончании восьмого учебного семестра проводится в рамках Междисциплинарного государственного экзамена по направлению.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература

1. Девянин П. Н. Модели безопасности компьютерных систем: [учебное пособие для вузов].— М.: Академия, 2005.—144 с. (66 экз.)
2. Игнатьев Е. Б. Основы криптографии: методические указания к лабораторным работам № 1, 2 по курсу "Методы и средства защиты информации".- Федеральное агентство по образованию, Государственное образовательное учреждение высшего профессионального образования "Ивановский государственный энергетический университет им. В. И. Ленина, Каф. программного обеспечения компьютерных систем; под ред. В. А. Гусева.—Иваново: Б.и., 2004.—28 с. (44 экз.)
3. Игнатьев Е. Б. Основы криптографии: методические указания к лабораторной работе № 3 по курсу «Методы и средства защиты компьютерной информации».- ГОУВПО «Ивановск. гос. энергетич. ун-т им. В.И.Ленина», каф. программного обеспечения компьютерных систем. - Иваново, 2010. - 28 с. (в электронном виде)
4. Игнатьев Е. Б. Основы криптографии: методические указания к лабораторной работе № 4 по курсу «Методы и средства защиты компьютерной информации».- ГОУВПО «Ивановск. гос. энергетич. ун-т им. В.И.Ленина», каф. программного обеспечения компьютерных систем. - Иваново, 2010. - 28 с. (в электронном виде)
5. Игнатьев Е. Б. Основы криптографии: методические указания к лабораторной работе № 5 по курсу «Методы и средства защиты компьютерной информации».- ГОУВПО «Ивановск. гос. энергетич. ун-т им. В.И.Ленина», каф. программного обеспечения компьютерных систем. - Иваново, 2010. - 28 с. (в электронном виде)
6. Игнатьев Е. Б. Основы криптографии: методические указания к лабораторной работе № 6 по курсу «Методы и средства защиты компьютерной информации».- ГОУВПО «Ивановск. гос. энергетич. ун-т им. В.И.Ленина», каф. программного обеспечения компьютерных систем. - Иваново, 2011. - 28 с. (в электронном виде)
7. Игнатьев Е. Б. Основы криптографии: методические указания к лабораторной работе № 7 по курсу «Методы и средства защиты компьютерной информации».- ГОУВПО «Ивановск. гос. энергетич. ун-т им. В.И.Ленина», каф. программного обеспечения компьютерных систем. - Иваново, 2011. - 28 с. (в электронном виде)
8. Игнатьев Е. Б. Основы криптографии: методические указания к лабораторной работе № 8 по курсу «Методы и средства защиты компьютерной информации».- ГОУВПО «Ивановск. гос. энергетич. ун-т им. В.И.Ленина», каф. программного обеспечения компьютерных систем. - Иваново, 2011. - 28 с. (в электронном виде)
9. Игнатьев Е. Б. Основы криптографии: методические указания к лабораторной работе № 9 по курсу «Методы и средства защиты компьютерной информации».- ГОУВПО «Ивановск. гос. энергетич. ун-т им. В.И.Ленина», каф. программного обеспечения компьютерных систем. - Иваново, 2011. - 28 с. (в электронном виде)
10. Хорев Л.Б. Методы и средства защиты информации в компьютерных системах. – М.: Академия, 2005. (5 экз.)
11. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: курс лекций: учеб. пособие: для студентов вузов, обучающихся по специальности 510200 «Приклад. математика и информатика» / под ред. В.А. Сухомлина. – М.: Интернет-Ун-т Информ. Технологий, 2005. – 608 с.

5.2. Дополнительная литература

12. Закон Российской Федерации "О правовой охране программ для ЭВМ и баз данных".
13. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. М.: Постмаркет, 2001. – 328 с.
14. Лукацкий А. В. Обнаружение атак. СПб., "БХВ-Петербург". 2001.- 624 с.

15. Петров. А. А. Компьютерная безопасность. Криптографические методы защиты. - М.: ДМК, 2000. - 448 с.
16. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке Си. Серия «Знания и опыт экспертов» Пер.с англ. 2-е издание. - Издательство «Триумф», 2003. - 815 с.
17. Домашев А. В., Попов В. О., Правиков Д. И. и др. Программирование алгоритмов защиты информации. Учебное пособие. М., Нолидж, 2000.- 288 с.
18. Рябко Б.Я., Фионов А.Н. Основы современной криптографии для специалистов в информационных технологиях. – М.: Научный мир, 2004. – 173 с.
19. Проскурин В.Г., Крутов С.В., Мацкевич И.В. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: Учеб. пособие для вузов.- М.: Радио и связь, 2000.- 168 с.

5.3. Программное обеспечение

20. Игнатьев Е.Б., Игнатьева Е.Е. Методы и средства защиты компьютерной информации. Электронный учебник. – Иваново: Ивановский гос. энергетич. ун-т. – 2010.

Функционирует на основе программного комплекса «ГИПЕРТЕСТ», разработанного на каф. ПОКС ИГЭУ. Учебник содержит лекционный материал по разделам дисциплины, систему контроля знаний ПК1 и ПК2.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Лабораторные работы

a) компьютерный класс,
b) среда программирования Microsoft Visual Studio;
c) текстовый редактор Word (Microsoft Office), Writer (OpenOffice.org) или Abi Word (GNOME Office).

6.2. Текущий контроль

Для проведения текущего контроля требуется следующее программное обеспечение:
Операционная система серверов: Windows 2003 Server, Linux.
Операционная система клиентов: Windows XP, Windows Vista.
В качестве web-сервера используется Apache 2.2.6.
Для интерпретации скриптов серверного ПО используется PHP 5.2.1.
В качестве СУБД используется MySQL Server 4.1.
Роль клиентского ПО играет Microsoft Internet Explorer, version 7.0.
Основой электронного учебника служит система ГИПЕРТЕСТ.
Обмен данными между клиентом и сервером происходит по сети Internet/Intranet по протоколу TCP/IP.

Приложение 1
к рабочей программе дисциплины
«Защита информации»

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ «ЗАЩИТА ИНФОРМАЦИИ» (Б.3.2.5)

Дисциплина «Защита информации» является профильной частью профессионального цикла дисциплин подготовки студентов по направлению подготовки 230100 «Информатика и вычислительная техника».

Дисциплина реализуется на факультете информатики и вычислительной техники кафедрой программного обеспечения компьютерных систем.

Дисциплина нацелена на формирование у выпускника следующих компетенций:

общекультурных:

ОК-1 (владение культурой мышления, способность к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения);

ОК-12 (навыки работы с компьютером как средством управления информацией);

ОК-13 (способность работать с информацией в глобальных компьютерных сетях);

профессиональных:

ПК-2 (освоение методики использования программных средств для решения практических задач);

ПК-5 (разработка компонентов программных комплексов и баз данных, использование современных инструментальных средств и технологий программирования).

Содержание дисциплины охватывает круг вопросов, связанных с основами теории информационной безопасности, стандартами безопасности, основами криптографии, симметричными криптосистемами, хешированием, криптосистемами с открытым ключом, управлением ключами, протоколами распределения ключей и аутентификации, сетевой безопасностью, экранированием, защитой электронной почты, подсистемами безопасности ОС Windows и Unix.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы, работа под контролем преподавателя,

самостоятельная работа студента.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости - в форме компьютерных тестов, промежуточный контроль - в форме экзамена, итоговый контроль - в форме Междисциплинарного государственного экзамена по направлению.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа. Программой дисциплины предусмотрены лекционные (34 часа), лабораторные (22 часов) занятия, самостоятельной работы студента (88 часов).

Приложение 2
к рабочей программе дисциплины
«Защита информации»

ТЕХНОЛОГИИ И ФОРМЫ ПРЕПОДАВАНИЯ
Рекомендации по организации и технологиям обучения для преподавателя

I. Образовательные технологии

Преподавание дисциплины ведется с применением следующих видов образовательных информационных технологий:

- использование электронных образовательных ресурсов при выполнении лабораторных работ;
- использование электронного учебника при подготовке к текущему контролю;
- использование электронного учебника для организации автоматизированного текущего контроля знаний студентов.

II. Виды и содержание учебных занятий

Раздел 1. Основные положения. Стандарты

Теоретические занятия (лекции) - 6 часов

Лекция 1. Основные понятия и определения - 2 часа
Информационная лекция
Основные понятия и определения. Информационная безопасность. Основные задачи. Источники, риски и формы атак на информацию. Конфиденциальность, целостность, достоверность, оперативность, юридическая значимость и неотслеживаемость информации.

Лекция 2. Стандарты безопасности. Оранжевая книга - 2 часа
Информационная лекция
Оранжевая книга. Критерии оценки надежных компьютерных систем. Политика безопасности. Добровольное управление доступом. Безопасность повторного использования объектов. Метки безопасности. Принудительное управление доступом.

Лекция 3. Стандарты безопасности. Классы безопасности - 2 часа
Информационная лекция
Классы безопасности. Идентификация и аутентификация. Пароли. Токены. Биометрические устройства. Передача координат. Управление доступом. Протоколирование и аудит.

Управление самостоятельной работой студента – (2 часа)[1]

Консультации по вопросам выполнения лабораторных работ и подготовке к текущему контролю проводятся во время проведения лабораторных работ.

[1] В скобках указано время для студентов

Раздел 2. Основы криптографии

Теоретические занятия (лекции) - 14 часов

Лекция 4. Типы алгоритмов шифрования - 2 часа
Информационная лекция
Типы алгоритмов шифрования. Прямые подстановки. Многоалфавитные подстановки. Гаммирование. Криптографические модели. Классификация алгоритмов.

Лекция 5. Симметричные криптосистемы - 2 часа
Информационная лекция
Симметричные криптосистемы. Требования к блочным шифрам. Сеть Фейштеля. Стандарт шифрования данных ГОСТ 28147-89.

Лекция 6. Хеширование - 2 часа
Информационная лекция
Хеширование. Требования к хеш-функциям. Простые хеш-функции. Алгоритмы MD5, SHA-1, SHA-2, ГОСТ 3411.

Лекция 7. Криптосистемы с открытым ключом - 2 часа
Информационная лекция
Криптосистемы с открытым ключом. Алгоритм RSA. Расширенный алгоритм Евклида.

Лекция 8. Системы электронной подписи - 2 часа
Информационная лекция
Системы электронной подписи. Эффективное шифрование. Электронная подпись на основе алгоритма RSA. Стандарты на электронную (цифровую) подпись. ГОСТ Р34.10-94 и FIPS 186. Алгоритм DSA (Digital Signature Algorithm).

Лекция 9. Криптосистемы на эллиптических кривых - 2 часа
Информационная лекция
Криптосистемы на эллиптических кривых. Цифровая подпись на эллиптической кривой (ГОСТ Р34.10 2001).

Лекция 10. Управление ключами - 2 часа
Информационная лекция
Управление ключами. Генерация ключей. Накопление ключей. Распределение ключей. Обмен ключами по алгоритму Диффи-Хеллмана.

Лабораторные работы - 12 часов, 5 ЛР + ПК1

В рамках лабораторных работ разрабатываются компоненты программного обеспечения, реализующие изученные методы криптографии. Рекомендуемый язык программирования - C++.

Лабораторная работа 1. Шифрование простой подстановкой и перестановкой. Генераторы псевдослучайных чисел, гаммирование - 2 часа
Индивидуальная
Шифрование простой подстановкой и перестановкой. Генераторы псевдослучайных чисел.

Лабораторная работа 2. Дешифровка, частотный анализ. Маскировка длины символа - 2 часа
Индивидуальная
Дешифровка, частотный анализ. Маскировка длины символа

Лабораторная работа 3. Симметричные криптосистемы. Блочные шифры - 2 часа
Индивидуальная
Симметричные криптосистемы. Блочные шифры.

Текущий контроль ПК1
Проведение компьютерного тестирования в электронном учебнике по усвоенному теоретическому материалу

Лабораторная работа 4. Хеширование - 2 часа
Индивидуальная
Хеширование.

Лабораторная работа 5. Криптосистемы с открытым ключом - 2 часа
Индивидуальная
Криптосистемы с открытым ключом.

Управление самостоятельной работой студента – (28 часов)
Консультации по вопросам выполнения ЛР и подготовке к текущему контролю проводятся во время проведения лабораторных работ.

Раздел 3. Защита информации в сетях

Теоретические занятия (лекции) - 8 часов

Лекция 11. Протоколы распределения ключей и аутентификации - 2 часа
Информационная лекция
Протоколы распределения ключей и аутентификации с использованием третьей доверенной стороны.

Лекция 12. Сетевая безопасность - 2 часа
Информационная лекция
Сетевая безопасность. Атакуемые сетевые компоненты. Многоуровневая защита корпоративных сетей. Защита информации в сетях.

Лекция 13. Экранирование - 2 часа
Информационная лекция
Экранирование. Виды экранов. Использование межсетевых экранов для создания VPN. Proxy-серверы. Виды подключения межсетевых экранов. Требования к системам защиты информации.

Лекция 14. Защита электронной почты - 2 часа
Информационная лекция
Защита электронной почты. Почта PEM. Программа PGP. Система защиты в MS Outlook.

Лабораторные работы - 6 часов, 2 ЛР + ПК2

Лабораторная работа 1. Получение и применение сертификата открытого ключа - 2 часа
Индивидуальная
Получение и применение сертификата открытого ключа.

Лабораторная работа 2. Возможности утилиты MS BaseLineSecuriyAnalizer - 2 часа
Индивидуальная
Возможности утилиты MS BaseLineSecuriyAnalizer.

Текущий контроль ПК2 - 2 часа
Проведение компьютерного тестирования в электронном учебнике по усвоенному теоретическому материалу

Управление самостоятельной работой студента – (14 часов)
Консультации по вопросам выполнения ЛР и подготовке к текущему контролю проводятся во время проведения лабораторных работ.

Раздел 4. Подсистема безопасности в ОС

Теоретические занятия (лекции) - 6 часов

Лекция 15. Подсистема безопасности защищенных версий ОС Windows - 2 часа
Информационная лекция
Подсистема безопасности защищенных версий ОС MS Windows. Идентификация, аутентификация и инициализация в MS Windows XP.

Лекция 16. Дискреционное управление доступом в MS Windows - 2 часа
Информационная лекция
Дискреционное управление доступом в MS Windows XP.

Лекция 17. Защита информации в ОС семейства Unix - 2 часа
Информационная лекция
Защита информации в ОС семейства Unix.

Лабораторные работы - 4 часа, 2 ЛР

Лабораторная работа 8. Электронные ключи HASP - 2 часа
Индивидуальная.
Электронные ключи HASP.

Лабораторная работа 9. Защита файлов в Windows - 2 часа
Индивидуальная.
Защита файлов в Windows.

Управление самостоятельной работой студента – (8 часов)
Консультации по вопросам выполнения ЛР проводятся во время проведения лабораторных работ.

Раздел 5. Подготовка к экзамену

Управление самостоятельной работой студента – 1 час (36 часов)
Консультации по вопросам подготовки к экзамену проводятся на консультации перед экзаменом.

Приложение 3
к рабочей программе дисциплины
«Защита информации»

ТЕХНОЛОГИИ И ФОРМЫ ОБУЧЕНИЯ

Рекомендации по освоению дисциплины для студента

Трудоемкость освоения дисциплины составляет 144 часа, из них 56 часов аудиторных занятий и 88 часов, отведенных на самостоятельную работу студента.

Контроль освоения дисциплины осуществляется в соответствии с ПОЛОЖЕНИЕМ о системе РИТМ в ИГЭУ.

Рекомендации по распределению учебного времени по видам самостоятельной работы и разделам дисциплины приведены в таблице.

Вид работы	Содержание (перечень вопросов)	Трудоемкость, час.	Рекомендации
Раздел № 1. Основные положения. Стандарты			
Подготовка к текущему контролю «ПК1»	Изучение теоретического материала	2	конспект лекций № 1-3;
Итого по разделу:		2	
Раздел № 2. Основы криптографии			
Подготовка к лабораторной работе № 1 и её выполнение	Изучение теоретического материала. Выполнение задания ЛР №1. Подготовка отчёта	4	См. описание лабораторной работы [2]; конспект лекций № 4;
Подготовка к лабораторной работе № 2 и её выполнение	Изучение теоретического материала. Выполнение задания ЛР №2. Подготовка отчёта	4	См. описание лабораторной работы [2]; конспект лекций № 4;
Подготовка к лабораторной работе № 3 и её выполнение	Изучение теоретического материала. Выполнение задания ЛР №3. Подготовка отчёта	6	См. описание лабораторной работы [3]; конспект лекций № 5;
Подготовка к текущему контролю «ПК1»	Изучение теоретического материала	4	конспект лекций № 4,5;
Подготовка к лабораторной работе № 4 и её выполнение	Изучение теоретического материала. Выполнение задания ЛР №4. Подготовка отчёта	4	См. описание лабораторной работы [4]; конспект лекций № 6;
Подготовка к лабораторной работе № 5 и её выполнение	Изучение теоретического материала. Выполнение задания ЛР №5. Подготовка отчёта	6	См. описание лабораторной работы [5]; конспект лекций № 7,8,9;
Итого по разделу:		28	
Раздел № 3. Защита информации в сетях			

Подготовка к лабораторной работе № 6 и её выполнение	Изучение теоретического материала. Выполнение задания ЛР № 6. Подготовка отчёта	4	См. описание лабораторной работы [6]; конспект лекций № 8;
Подготовка к лабораторной работе № 7 и её выполнение	Изучение теоретического материала. Выполнение задания ЛР № 7. Подготовка отчёта	4	См. описание лабораторной работы [7]; конспект лекций № 12;
Подготовка к текущему контролю «ПК2»	Изучение теоретического материала	6	конспект лекций № 6-14;
Итого по разделу:		14	
Раздел № 4. Подсистема безопасности в ОС			
Подготовка к лабораторной работе № 8 и её выполнение	Изучение теоретического материала. Выполнение задания ЛР № 8. Подготовка отчёта	4	См. описание лабораторной работы [8]; См. конспект лекций № 2;
Подготовка к лабораторной работе № 9 и её выполнение	Изучение теоретического материала. Выполнение задания ЛР № 9. Подготовка отчёта	4	См. описание лабораторной работы [9]; См. конспект лекций № 15-17;
Итого по разделу:		8	
Раздел № 5. Подготовка к экзамену			
Подготовка к экзамену	Повторение теоретического материала. Решение задач из домашнего задания для подготовки к ПК1 и ПК2	36	См. конспект лекций № 1-17;
Итого по разделу:		36	
Всего:		88	

* ДЛ – дополнительная литература

Приложение 4
к рабочей программе дисциплины
«Защита информации»

ОЦЕНОЧНЫЕ СРЕДСТВА И МЕТОДИКИ ИХ ПРИМЕНЕНИЯ

Оценивание уровня учебных достижений студента осуществляется в виде текущего и промежуточного контролей в соответствии с ПОЛОЖЕНИЕМ о системе РИТМ в ИГЭУ.

Фонды оценочных средств

Фонды оценочных средств, позволяющие оценить РО по данной дисциплине, включают в себя:

- варианты тестовых заданий (ПК1, ПК2) размещены в электронном учебнике;
- комплект вопросов к экзамену размещен в УМКД;
- комплект билетов к экзамену размещен в УМКД.

Критерии оценивания

Текущее тестирование

Критерии оценивания ПК1 и ПК2:

Пересчет результатов теста в баллы выполняется следующим образом:

- рейтинг теста меньше 50% – 0 баллов,
- рейтинг теста равен 50% – 2 балла,
- рейтинг теста 100% – 5 баллов,
- рейтинг теста от 50-100% – пересчет по формуле:
  ([рейтинг теста]-50) / 50 * 3 + 2.

Оценка округляется до ближайшей кратной 0,5.

Лабораторные работы

Отчет по лабораторной работе представляется в печатном виде и содержит: титульный лист, исходный текст компонентов ПО, контрольные примеры. Защита отчета проходит в форме демонстрации работы компонентов ПО и ответов на вопросы преподавателя.

В случае если все требования к разрабатываемым компонентам ПО и оформлению отчета выполнены, а студент во время защиты ответил на все вопросы и показал, что хорошо понимает работу компонентов, то он получает максимальное количество баллов – 5.

Основаниями для снижения количества баллов в диапазоне от 5 до 0 являются:

- небрежное выполнение отчета,
- невыполнение всех функциональных требований,
- выполнение и защита работы были после срока,
- при неправильных ответах на вопросы во время защиты,
- ошибках в ПО, выявленных во время защиты,
- плохая ориентация в исходном тексте ПО.

Оценка выставляется кратной 0,5.

Лабораторная работа не принимается и подлежит доработке в случае:

- получена оценка менее 2,5 баллов,
- непонимания студентом основных принципов использованного метода,
- отсутствия отчета,

- некорректной обработки результатов измерений.

Текущий контроль

ТК1. Оценка за ТК1 выставляется по результатам лабораторных работ № 1, 2. Оценка округляется до ближайшей кратной 0,5.

ПК1. Оценка за ПК1 выставляется по результатам лабораторных работ № 1-3 и по результатам тестирования «ПК1» в ЭУ. Оценка вычисляется как среднее арифметическое двух оценок – за лабораторные работы и за тест. Оценка округляется до ближайшей кратной 0,5.

ТК2. Оценка за ТК1 выставляется по результатам лабораторных работ № 1-4. Оценка округляется до ближайшей кратной 0,5.

ПК2. Оценка за ПК2 выставляется по результатам лабораторных работ № 1-5 и по результатам тестирования «ПК2» в ЭУ. Оценка вычисляется как среднее арифметическое двух оценок – за лабораторные работы и за тест. Оценка округляется до ближайшей кратной 0,5.

Промежуточный контроль

Промежуточный контроль по дисциплине проходит в форме экзамена по окончании семестра (включает в себя ответы на теоретические вопросы).

Допуск к экзамену происходит при наличии положительных (2.5 балла и выше) оценок за каждую из 9-ти ЛР и оба теста.

На экзамене студент получает экзаменационный билет, содержащий два теоретических вопроса из первой половины лекционного материала и из второй половины.

Итоговый контроль

По окончании восьмого учебного семестра проводится в рамках Междисциплинарного государственного экзамена по направлению.

Общая оценка за экзамен вычисляется как среднее арифметическое оценок по всем четырём дисциплинам.

Студент, получивший две оценки в 2 балла (по любым двум дисциплинам из четырёх), получает общую оценку за экзамен – «неудовлетворительно».