МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ТАДЖИКИСТАН
МЕЖГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКО-ТАДЖИКСКИЙ (СЛАВЯНСКИЙ) УНИВЕРСИТЕТ»

«Утверждаю»
Декан ЕНФ _____
Муродзода Д.С.
«31» 08 2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки - 09.03.03 «Прикладная информатика»
Профиль – Инженерия программного обеспечения
Форма подготовки - очная
Уровень подготовки - бакалавриат

ДУШАНБЕ 2024

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования, утверждённого приказом Министерства образования и науки РФ от 19 сентября 2017 г. № 922

При разработке рабочей программы учитываются

- требования работодателей, профессиональных стандартов по направлению / специальности (при наличии) (для общепрофессиональных и профессиональных дисциплин);
- содержание программ дисциплин, изучаемых на предыдущих и последующих этапах обучения;
- новейшие достижения в данной предметной области.

Рабочая программа обсуждена на заседании кафедры Информатики и ИТ., протокол № 1 от 28 августа 2024 г.

Рабочая программа утверждена УМС естественнонаучного факультета, протокол № 1 от 29 августа 2024 г.

Рабочая программа утверждена Учёным советом естественнонаучного факультета, протокол № 1 от 30 августа 2024г.

Заведующий кафедрой, к.э.н., доцент  Лешукович А.И.

Зам. председателя УМС факультета
к. ф-м.н., доцент  Халимов И.И.

Разработчик, преподаватель  Каримов М.М.

Расписание занятий дисциплины

Ф.И.О. преподавателя	Аудиторные занятия		Приём СРС	Место работы преподавателя
	Лекция	Практические занятия (КСР, лаб.)		
Норкулов Х.О	Пятница 11.30-12.50 Корпус 2: Ауд.214	Пятница 08:00-9:30, 09:40-11:10, 11:20-12:50	Суббота 10:00-12:30	РТСУ, кафедра информатики и ИС, старый корпус, 216 каб.

1. ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

1.1. Цели изучения дисциплины

Заложить методически правильные основы знаний по информационной безопасности (ИБ), необходимые специалистам, занимающимся вопросами проектирования, внедрения и эксплуатации корпоративных вычислительных и информационных систем (ВС/ИС). Дисциплина является важной составной частью теоретической подготовки специалиста по прикладной информатике и занимает существенное место в его будущей практической деятельности. Она обеспечивает возможность эффективной работы специалиста в ИТ-службах предприятий и государственных учреждений.

Преподавание дисциплины «Информационная безопасность» имеет следующие базовые задачи:

- дать будущим специалистам необходимые для их работы теоретические знания о современных средствах, методах и технологиях обеспечения информационной безопасности ВС/ИС;
- сформировать у студентов практические навыки организации работ по обеспечению информационной безопасности на предприятиях.

1.2. Задачи изучения дисциплины

Задачи дисциплины формулируются в соответствии с требованиями ФГОС, предъявляемые к компетенциям обучающегося. В результате освоения дисциплины ИБ формируются определенный набор компетенции обучающегося:

Код	Формируемая компетенция	Содержание этапа формирования компетенции	Форма контроля
ПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1. **Знать** принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. ОПК-3.2. **Уметь** решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. ОПК-3.3. **Владеть** навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно- исследовательской работе с учетом требований информационной безопасности.	Тестирование. Контроль самостоятельной работы. Отчеты по практическим работам. Контрольная работа. Устный опрос.

ОПК-4	Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.1.**Знать** основные стандарты оформления технической документации на раз-личных стадиях жизненного цикла информационной системы. ОПК-4.2.**Уметь** применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. ОПК-4.3.**Владеть** навыками составления технической документации на различных этапах жизненного цикла информационной системы.	Тестирование. Контроль самостоятельной работы. Отчеты по практическим работам. Контрольная работа. Устный опрос.
ПК-3	Способность проектировать ИС по видам обеспечения	ПК-3.1.**Знать** результаты применения и реализации современных технологий в корпоративных информационных системах; особенности использования КИС для поддержки принятия решений;- теоретические вопросы экономики - основные сведения о процессоре электронных таблиц Excel. ПК-3.2.**Уметь** использовать навыки менеджера в процессе управления проектной группой с использованием ИКТ; оценить существующие на предприятиях технологии обработки экономической информации по критериям экономической эффективности ПК-3.3.**Владеть** навыками менеджера в процессе управления проектной группой с использованием ИКТ	Тестирование. Контроль самостоятельной работы. Отчеты по практическим работам. Контрольная работа. Устный опрос.

ПК-9	Способность осуществлять ведение базы данных и поддержку информационного обеспечения решения прикладных задач.	ПК-9.1. **Знать** виды, правила составления и свойства алгоритмов; популярные информационно-поисковые системы в WWW их общие черты и закономерности ПК-9.2. **Уметь** составлять алгоритмы решения задач различной структуры и оформлять их в соответствии с синтаксическими правилами языка программирования VisualBasic; проводить анализ деятельности предприятия и выявлять участки производства, нуждающиеся в автоматизации; способность разрабатывать средства реализации информационных технологий (методические, информационные, математические, алгоритмические, технические и программные) ПК-9.3. **Владеть** методикой структурирования информационных ресурсов Интернет; терминологическим аппаратом дисциплины	Способность осуществлять ведение базы данных и поддержку информационн ого обеспечения решения прикладных задач.

2.МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП

Курс дает базовую основу для понимания, анализа и оценки основных проблем, связанных с обеспечением ИБ предприятия и защитой информации, а также разработкой, внедрением и сопровождением средств информационной защиты.

Курс подготавливает выпускника к работе в современной компании, внедряющей, использующей или разрабатывающей программные средства для обеспечения информационной безопасности. Она является вариативной обязательной дисциплиной (Б1.Б.19), изучается в 5 семестре. Логически и содержательно-методически взаимосвязана с дисциплинами ООП, указанных в табл. 1:

Таблица 1.

№	Название дисциплины	Семестр	Место дисциплины в структуре ООП
1.	*Математика*	*1-2*	*Б1.О.07*
2.	*Дискретная математика*	*1*	*Б1.О.08*
3.	*Теория алгоритмов*	*2*	*Б1.О.11*
4.	*Теория вероятности и математическая статистика*	*2*	*Б1.О.09*
5.	*Операционные системы*	*2*	*Б1.О.10*
6.	*Информатика*	*1*	*Б1.О.05*
7.	*Программирование*	*1-2*	*Б1.О.06*
8.	*Проектирование информационных систем*	*5*	*Б1.О.19*
9.	*Базы данных*	*3-4*	*Б1.О.15*
10.	*Вычислительные системы сети и телекоммуникации*	*3-4*	*Б1.О.16*
11.	*Программная инженерия*	*4-5*	*Б1.О.17*
12.	*Программно-аппаратные средства обеспечения информационной безопасности*	*8*	*Б1.В.ДВ.06.02*

При освоении данной дисциплины необходимы умения и готовность («входные» знания) обучающегося по дисциплинам 1-11, указанных в таблице 1. Дисциплины 12 и 13 относятся к группе «входных» знаний, вместе с тем определенная их часть изучается параллельно с данной дисциплиной («входные-параллельные» знания).

Теоретическими дисциплинами и практиками, для которых освоение данной дисциплины необходимо как предшествующее являются:14-18.

3. СТРУКТУРА И СОДЕРЖАНИЕ КУРСА, КРИТЕРИИ НАЧИСЛЕНИЯ БАЛЛОВ

Объем дисциплины «Информационная безопасность» составляет 5 зачетные единицы, всего 180 часа, из которых: лекции – 18 часов, практические занятия – 18 часов, лабораторные работы – 18 часов, КСР – 18 часов, всего часов аудиторной нагрузки - 72 часов, в том числе, в интерактивной форме 18 часов, самостоятельная работа – 72 часа, контроль – 36 часов.

Экзамен– 5-й семестр

3.1 Структура и содержание теоретической части курса

Тема 1. Общие вопросы информационной безопасности. Основные понятия и определения, относящиеся к информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности; классификация атак; модели сетевой безопасности и безопасности информационной системы.

Тема 2. Шифры замены.

Основные понятия и определения. Шифры Цезаря, Виженера, Полибия, Гронсфельда, Плейфер. Дисковые шифраторы. Исследования Шеннона в области криптографии. Не раскрываемость шифра Вернама.

Тема 3. Шифры перестановки.

Основные понятия и определения. Шифр Сцитало. Шифр маршрутной перестановки. Шифр вертикальной перестановки. Шифр поворотная решётка (Кардано). Шифр двойной перестановки

Тема 4. Асимметричные системы шифрования (системы с открытым ключом). Понятия однонаправленной функции и однонаправленной функции с лазейкой. Функции дискретного логарифмирования и основанные на ней алгоритмы: схема Диффи-Хеллмана. Шифр Шамира. Схема Эль-Гамаля. Схема RSA: алгоритм шифрования, его обратимость, вопросы стойкости

Тема 5. Элементы теории чисел. Арифметика остатков и теория сравнений. Малая теорема Ферма. Наибольший общий делитель. Обобщенный алгоритм Евклида. Инверсия по модулю m.

Тема 6. Алгоритмы симметричного шифрования. Основные понятия, относящиеся к алгоритмам симметричного шифрования: ключ шифрования, plaintext, ciphertext. Определение стойкости алгоритма, типы операций, используемые в алгоритмах симметричного шифрования. Сеть Фейштеля. Основные понятия криптоанализа, линейный и дифференциальный криптоанализ. Схема шифрования алгоритма DES. Режимы использования DES. Криптостойкость алгоритма DES. Увеличение криптостойкости DES

Тема 7. Стандарт криптографической защиты 21 века(AES). Алгоритмы Rijndael и RC6. Математические понятия, лежащие в основе алгоритма Rijndael. Структура шифра. Описание AES. Алгоритм обработки ключа. Варианты алгоритма. Криптостойкость.

Тема 8. Криптография с использованием эллиптических кривых. Математические понятия, связанные с эллиптическими кривыми, в частности задача дискретного логарифмирования на эллиптической кривой. Аналог алгоритма Диффи - Хеллмана на эллиптических кривых, алгоритма шифрования с открытым ключом получателя на эллиптических кривых.

3.2 Структура и содержание практической части курса

Структура и содержание практической части курса включает в себя тематику и содержание практических занятий, семинаров, лабораторных работ.

Практические занятия (18 час.)

1. Основные понятия и определения информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности. Классификация атак. Модели сетевой безопасности и безопасности информационной системы.
2. Классическая задача криптографии. Угрозы со стороны злоумышленника и участников процесса информационного взаимодействия.
3. Шифры замены и перестановки. Моно- и многоалфавитные подстановки Шифры Цезаря, Виженера, Вернама. Методы дешифрования.
4. Классификация методов дешифрования. Модель предполагаемого противника. Правила Керкхоффа.
5. Совершенная секретность по Шеннону. Примеры совершенно секретных систем. Шифр Вернама. Понятие об управлении ключами.
6. Блочные криптосистемы с секретным ключом. Алгоритм DES. Описание DES. Основные этапы алгоритма.
7. Схема алгоритма DES. Раунд алгоритма. Преобразование ключа.
8. Алгоритм DES. Подстановка с помощью S-блоков. Расшифрование в DES.
9. Стандарт криптографической защиты 21 века(AES). Алгоритмы Rijndael и RC6. Математические понятия, лежащие в основе алгоритма Rijndael. Структура шифра.

Лабораторные работы (18 час.)

1. Метод Диффи- Хеллмана.
2. Математические методы защиты информации.
3. Атрибутивные способы идентификации. Виды пластиковых карт.
4. Метод Эйлера.
5. Алгоритм RSA. Математическая модель алгоритма. Стойкость алгоритма.
6. Криптосистема Эль-Гамаля.
7. Однонаправленные (односторонние) функции с секретом и их применение.
8. Основы криптоанализа. Обзор возможных вариантов криптоанализа. Метод вскрытия «встреча посередине». Вскрытие со словарем. Вскрытие системы Вижинера, использующей простой XOR. Метод бесключевого чтения RSA.

Атака на подпись RSA по выбранному шифротексту. Вскрытие хэш-функций с использованием парадокса дня рождения.

9. Криптосистемы на эллиптических кривых.

3.3 Структура и содержание КСР

1. Общие вопросы информационной безопасности. Основные понятия и определения. Законодательство РФ и РТ в области информационной безопасности.
2. Разработка алгоритма и пакета программы шифрования и расшифрованные шифра замены.
3. Разработка алгоритма и пакета программы шифрования и расшифрованные шифра перестановки.
4. Разработка алгоритма и пакета программы шифрования и расшифрования системы с открытым ключом.
5. Разработка алгоритма и пакета программы для элементов теории чисел.
6. Разработка алгоритма и пакета программы шифрования и расшифрования шифра метода DES
7. Разработка алгоритма и пакета программы шифрования и расшифрования метода AES
8. Разработка алгоритма и пакета программы шифрования и расшифрования аналога алгоритма Диффи - Хеллмана на эллиптических кривых.
9. Безопасность современных сетевых технологии. Построение защищенных виртуальных сетей. Способы создания защищенных виртуальных каналов. Обзор протоколов.

№ п/п	**Раздел Дисциплины**	**Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)**				**Литература**
		Лек.	Пр.	Лаб.	КСР	
V семестр						
1.	**Тема 1. Общие вопросы информационной безопасности.** Основные понятия и определения, относящиеся к информационной безопасности: атаки, уязвимости, политика безопасности, механизмы	2				1,3,7

	и сервисы безопасности; классификация атак; модели сетевой безопасности и безопасности информационной системы. **Лабораторная работа** Выполнение и подготовка к защите работы 1 **Практическое занятие**		2	2		
2.	**Тема 2. Шифры замены.** Основные понятия и определения. Шифры Цезаря, Виженера, Полибия, Гронсфельда, Плейфер. Дисковые шифраторы. Исследования Шеннона в области криптографии. Не раскрываемость шифра Вернама. **Лабораторная работа** **Практическое занятие** Групповые консультации по темам 1-2	2	2		2	2,5,7,9
3.	**Тема 3. Шифры перестановки.** Основные понятия и определения. Шифр Сцитало. Шифр маршрутной перестановки. Шифр вертикальной перестановки. Шифр поворотная решётка (Кардано). Шифр двойной перестановки **Лабораторная работа** Выполнение и подготовка к защите работы 2 Групповые консультации по теме 3	2	2	2	2	1,3,6
4.	**Тема 4. Асимметричные системы шифрования (системы с открытым ключом).** Понятия однонаправленной функции и однонаправленной функции с	2				2,8,10

	лазейкой. Функции дискретного логарифмирования и основанные на ней алгоритмы: схема Диффи-Хеллмана. Шифр Шамира. Схема Эль-Гамаля. Схема RSA: алгоритм шифрования, его обратимость, вопросы стойкости **Практическое занятие** Групповые консультации по теме 4		2	2	2	
5.	**Тема 5. Элементы теории чисел.** Арифметика остатков и теория сравнений. Малая теорема Ферма. Наибольший общий делитель. Обобщенный алгоритм Евклида. Инверсия по модулю m. **Лабораторная работа** Выполнение и подготовка к защите работы 3 Групповые консультации по темам 5	2	2	2	2	1,2,3,4
6.	**Тема 6. Алгоритмы симметричного шифрования**. Основные понятия, относящиеся к алгоритмам симметричного шифрования: ключ шифрования, plaintext, ciphertext. Определение стойкости алгоритма, типы операций, используемые в алгоритмах симметричного шифрования. Сеть Фейштеля. Основные понятия криптоанализа, линейный и дифференциальный криптоанализ. Схема шифрования алгоритма DES. Режимы использования DES. Криптостойкость алгоритма DES. Увеличение криптостойкости DES **Лабораторная работа**	2	2	2	2	1,8,11

	Выполнение и подготовка к защите работы 4 Групповые консультации по теме 6					
7.	**Тема 7. Стандарт криптографической защиты 21 века(AES).** Алгоритмы Rijndael и RC6. Математические понятия, лежащие в основе алгоритма Rijndael. Структура шифра. Описание AES. Алгоритм обработки ключа. Варианты алгоритма. Криптостойкость. **Лабораторная работа** Выполнение и подготовка к защите работы 5 **Практическое занятие**	2	2	2	2	1,5,10
8.	**Тема 8. Криптография с использованием эллиптических кривых**. Математические понятия, связанные с эллиптическими кривыми, в частности задача дискретного логарифмирования на эллиптической кривой. Аналог алгоритма Диффи - Хеллмана на эллиптических кривых, алгоритма шифрования с открытым ключом получателя на эллиптических кривых. **Лабораторная работа** Выполнение и подготовка к защите работы 5 Групповые консультации по темам 7-8	4	4	4	4	2,3,5,7
ИТОГО: лек.-18, прак.-18, лаб. – 18, КСР-18, СРС-108 ВСЕГО-180		**18**	**18**	**18**	**18**	

Формы контроля и критерии начисления баллов

Контроль усвоения студентом каждой темы осуществляется в рамках балльно-рейтинговой системы (БРС), включающей текущий, рубежный и итоговый контроль. Студенты **1 курсов**, обучающиеся по кредитно-рейтинговой системе обучения, могут получить максимально возможное количество баллов - 300. Из них на текущий и рубежный контроль выделяется 200 баллов или 49% от общего количества.

На итоговый контроль знаний студентов выделяется 51% или 100 баллов. Из них 16 баллов администрацией могут быть представлены студенту за особые заслуги (призовые места в Олимпиадах, конкурсах, спортивных соревнованиях, выполнение специальных заданий, активное участие в общественной жизни университета).

Порядок выставления баллов: 1-й рейтинг (1-9 неделя по 11,5 баллов = 8 баллов административных, итого 100 баллов), 2-й рейтинг (10-18 неделя по 11,5 баллов = 8 баллов административных, итого 100 баллов), итоговый контроль 100 баллов.

К примеру, за текущий и 1-й рубежный контроль выставляется 100 баллов: лекционные занятия – 20 баллов, за практические занятия (КСР, лабораторные) – 32 балла, за СРС – 20 баллов, требования ВУЗа – 20 баллов, административные баллы – 8 баллов.

В случае пропуска студентом занятий по уважительной причине (при наличии подтверждающего документа) в период академической недели, деканат факультета обращается к проректору по учебной работе с представлением об отработке студентом баллов за пропущенные дни по каждой отдельной дисциплине с последующим внесением их в электронный журнал.

Итоговая форма контроля по дисциплине (зачет, зачет с оценкой, экзамен) проводится как в форме тестирования, так и в традиционной (устной) форме. Тестовая форма итогового контроля по дисциплине предусматривает: для естественнонаучных направлений – 10 тестовых вопросов на одного студента, где правильный ответ оценивается в 10 баллов, для гуманитарных направлений/специальности – 25 тестовых вопросов, где правильный ответ оценивается в 4 балла. Тестирование проводится в электронном виде, устный экзамен на бумажном носителе с выставлением оценки в ведомости по аналогичной системе с тестированием.

Таблица 4.

Неделя	**Активное участие на лекционных занятиях,**	**Активное участие на практических**	**СРС Написание реферата,**	**Административный балл за примерно**	**Балл за рубежный и итоговы**	**Всего**

	написание конспекта и выполнение других видов работ*	**(семинарских) занятиях, КСР**	**доклада, эссе Выполнение других видов работ**	**е поведение**	**й контроль**	
1	**2**	**3**	**4**	**5**	**6**	**7**
1	-	-	-	-	-	-
2	1	1	1	-	-	3
3	1	1	1	-	-	3
4	1	1	1	-	-	3
5	1	1	1	-	-	3
6	1	1	1	-	-	3
7	1	1	1	-	-	3
8	1	1	1	-	-	3
9 (первый рубежный контроль)					**10**	**10**
Первый рейтинг	**7**	**7**	**7**	**-**	**10**	**31**
10	1	1	1	-	-	3
11	1	1	1	-	-	3
12	1	1	1	-	-	3
13	1	1	1	-	-	3
14	1	1	1	-	-	3
15	1	1	1	-	-	3
16	1	1	1	-	-	3
17	1	1	1	-	-	3
18 (второй рубежный контроль)					**10**	**10**

Второй рейтинг	**8**	**8**	**8**	**5**	**10**	**39**
ИТОГОВЫЙ КОНТРОЛЬ (зачет, зачет с оценкой, экзамен)					**30**	**30**
ИТОГО:	**15**	**15**	**15**	**5**	**20+30**	**100**

4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Системы электронного документооборота» включает в себя:

1. план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;
2. характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;
3. требования к представлению и оформлению результатов самостоятельной работы;
4. критерии оценки выполнения самостоятельной работы.

4.1. План-график выполнения самостоятельной работы по дисциплине «Информационная безопасность»

Таблица 5.

№ п/п	Объем самостоятельной работы в часах	Вид самостоятельной работы	Форма и вид самостоятельной работы	Форма контроля
1	6	Изучение теоретических материалов по темам лекций, указанных в разделе 3 «Содержание и структура дисциплины».	Конспект, реферат	К/Опрос
2	10	Выполнение индивидуальных домашних заданий и упражнений для самостоятельной работы по решению задач различными	Отчет по выполнению домашних Заданий	Опрос

		методами.		
3	10	Разработка алгоритмов и программ по лабораторным работам, предусмотренным планом.	Реализация на ПЭВМ	Собеседование
4	8	Стыковка сетевых устройств и анализ.	Реализация на ПЭВМ	Собеседование
5	8	Оформление отчётов по лабораторным работам.	Оформленный отчёт	К/опрос
6	8	Разработка блок схемы программы.	Определение устройств ввода и вывода.	Опрос
7	8	Подготовка к защите лабораторных работ.	Выполнение проверочного задания	К/опрос
8	8	Защита отчётов по лабораторным работам.	Решение задачи	К/опрос
9	6	Поиск серверов, прием передач информации	Реализация на ПЭВМ	К/опрос

4.2 Характеристика заданий для самостоятельной работы и методические рекомендации по их выполнению

Для выполнения задания, прежде всего, необходимо ознакомиться и изучить основные положения теоретических материалов соответствующей темы из литературных источников. Они указаны в разделе 3 «Содержание и структура дисциплины». Индивидуальные домашние задания берутся из лабораторного практикума по дисциплине «Системы электронного документооборота» автора Ли И. Т. по варианту, заданному преподавателем, и выполняются письменно в отдельной тетрадке.

Отчет должен содержать следующие разделы:

1. Титульный лист;
2. Постановку задачи;
3. Описание порядка решения задачи;
4. Результаты вычислений.

Отчет по лабораторным работам должен содержать:

1. Титульный лист;
2. Цель работы;
3. Краткие теоретические сведения;
4. Описание постановки задачи и её порядок выполнения;
5. Листинг программы на одном из языков программирования;
6. Результаты вычисления и их интерпретацию;
7. Выводы по работе.

4.3. Требования к представлению и оформлению результатов самостоятельной работы;

Индивидуальные домашние задания по самостоятельной работе должны быть выполнены в отдельной тетрадке. В каждом задании должны быть приведены постановка задачи и описана последовательность ее решения. В конце решения задачи приводятся результаты выполненной работы.

При выполнении самостоятельной работы студент должен предварительно изучить методы решения задач данного типа и правильно выбрать соответствующий метод ее решения.

По лабораторным работам студенты должны представить отчеты в соответствии с содержанием, приведенным в пункте 4.2, которые должны быть защищены у преподавателя. На защите лабораторных работ студентам задается один теоретический вопрос и задача, которые он должен самостоятельно подготовить и решить.

4.4. Критерии оценки выполнения самостоятельной работы.

Самостоятельная работа прививает студентам навыки работы с источниками и учебной литературой, помогает повысить уровень знаний по предмету, а также самостоятельно анализировать и проектировать электронные документы для систем электронного документооборота, которые можно использовать на практике.

Оценка «отлично» выставляется студенту, если индивидуальное задание выполнено полностью и по данной теме защищена лабораторная работа.

Оценка «хорошо» выставляется студенту, если лабораторная работа по теме индивидуального задания защищена, а само индивидуальное задание выполнено с отдельными замечаниями.

Оценка «удовлетворительно» выставляется студенту, если лабораторная работа по теме индивидуального задания защищена, а само индивидуальное

задание выполнено не до конца, т.е. не полностью.

Оценка «неудовлетворительно» выставляется студенту, если лабораторная работа по теме индивидуального задания не защищена, а само индивидуальное задание выполнено не до конца, т.е. не полностью.

5. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

В данном разделе РПД приводится перечень основной литературы (учебники, учебные пособия, монографии) и перечень дополнительной литературы, в который включаются издания, рекомендуемые для углубленного изучения. В перечень основной литературы должны входить учебники, учебные пособия и монографии, изданные в течение последних 5 лет для гуманитарных, социальных и экономических дисциплин и 10 лет для технических, математических и естественнонаучных дисциплин.

Не менее трех источников основной литературы, указанных в РПД, должны быть доступны обучающимся в одной или нескольких электронно-библиотечных системах (электронных библиотеках), сформированных на основании прямых договорных отношений с правообладателями. В данном случае необходимо привести полное библиографическое описание источника и рабочую гиперссылку на соответствующий электронный ресурс. В список основной литературы также могут быть включены печатные издания, имеющиеся в фондах РТСУ в количестве, предусмотренном соответствующим ФГОС ВО

5.1. Основная литература

1. Бабенко, Л. К. Криптографическая защита информации[Электронный ресурс]: симметричное шифрование : учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. — Москва: Издательство Юрайт, 2020. — 220 с. — URL: http://biblio-online.ru/bcode/452871
2. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2020. — 349 с. — URL: http://biblio-online.ru/bcode/450998.
3. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты [Электронный ресурс]: учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2020. — 209 с. — URL: http://biblio-online.ru/bcode/450820.
4. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты[Электронный ресурс]: учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией

В. М. Фомичёва. — Москва : Издательство Юрайт, 2020. — 245 с. — (Высшее образование). — URL: http://biblio-online.ru/bcode/451486.
5. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность[Электронный ресурс]: учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2020. — 473 с. — URL: http://biblio-online.ru/bcode/450277 .

5.2. Дополнительная литература

1. Нестеров, С. А. Информационная безопасность[Электронный ресурс]: учебник и практикум для среднего профессионального образования / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — URL: http://biblio-online.ru/bcode/442312 .
2. Нестеров, С. А. Информационная безопасность [Электронный ресурс]: учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — (Университеты России). — URL: http://biblio-online.ru/bcode/434171.
3. Коржик В.И. Основы криптографии [Электронный ресурс] : учебное пособие / В.И. Коржик, В.А. Яковлев. — Электрон. текстовые данные. — СПб. : Интермедия, 2017. — 312 с. — Режим доступа: http://www.iprbookshop.ru/66798.html.
4. Подбельский, В. В. Программирование. Базовый курс C#[Электронный ресурс]: учебник для среднего профессионального образования / В. В. Подбельский. — Москва: Издательство Юрайт, 2019. — 369 с.— URL: https://biblio-online.ru/bcode/445334.
5. Кувшинов, Д. Р. Основы программирования [Электронный ресурс]: учебное пособие для вузов / Д. Р. Кувшинов. — Москва: Издательство Юрайт, 2019. — 104 с.— URL: https://biblio-online.ru/bcode/441475
6. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты[Электронный ресурс]: учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва: Издательство Юрайт, 2019. — 245 с.— URL: https://biblio-online.ru/bcode/434104

5.3Нормативно-правовые материалы (по мере необходимости)

1. Концепция государственной информационной политики Республики Таджикистан от 30 апреля 2008 года № 451
2. Закон республики Таджикистан о безопасности (Ахбори Маджлиси Оли Республики Таджикистан, 2011 г., № 6, ст. 434; 2014 г., №11, ст. 646; Закон РТ от 15.03.2016 г., № 1283)

3. Закон республики Таджикистан о внесении дополнения в закон республики таджикистан "Об органах национальной безопасности республики Таджикистан" от 19 марта 2018 года, №1033
4. Рохнамо А. Ислам и национальной безопасности в Таджикистане. Душанбе «Ирфон».2011.
5. Сайидзода З., Саидов Ф. Таджикистан: информационный ресурс, внешняя политика, имидж государства .-Душанбе: ОО «Иттилоот ва муошират»,2008.С.3.
6. "О Концепции информационной безопасности Республики Таджикистан" от 7 ноября 2003 года.
7. Закон Российской Федерации от 5 марта 1992 г. № 2446-1 "О безопасности"
8. Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите и информации"
9. Федеральный закон от 10 января 2002 г. № 1-ФЗ "Об электронной цифровой подписи"
10. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена"
11. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 "Вопросы Федеральной службы по техническому и экспортному контролю"
12. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 "Об утверждении Перечня сведений конфиденциального характера"
13. Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных""
14. Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 "Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти"
15. Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 "О сертификации средств защиты информации"
16. Постановление Правительства Российской Федерации от 26 января 2006 г. № 45 " Об организации лицензирования отдельных видов деятельности"

17. Постановление Правительства Российской Федерации от 15 августа 2006 г. № 504 "О лицензировании деятельности по технической защите конфиденциальной информации"
18. Постановление Правительства Российской Федерации от 31 августа 2006 г. № 532 "О лицензировании деятельности но разработке и (или) производству средств защиты конфиденциальной информации"

5.4 Перечень ресурсов информационно-телекоммуникационной сети Интернет

В данном разделе приводится перечень ресурсов информационно телекоммуникационной сети «Интернет», необходимых для освоения дисциплины, в виде названия сайта, интернет - портала и т.п. и рабочей гиперссылки. Не допускается размещение ресурсов, содержащих материалы, несоответствующие этическим нормам, в том числе в формате баннеров и т.п.

1. Sun Microsystems, Inc. JDK 6 Documentation - Режим доступа: http://java.sun.com/javase/6/docs/www.osborne.com
2. https://habrahabr.ru
3. https://www.java.com/ru
4. www.ibm.com/developerworks/ru
5. https://info.javarush.ru/
6. https://students.uni-vologda.ac.ru

Перечень информационных технологий и программного обеспечения

Используются лицензионное программное обеспечение ОС Windows -7 и программное обеспечение открытого доступа (Open source) среда NetBeans (Eclipse).

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Студенты, изучающие курс «Информационная безопасность», должны в первую обратить внимание на общие подходы к реализации информационной безопасности современного предприятия. Здесь следует обратить особое внимание на то, что в переходный период к построению информационного общества информационные ресурсы становятся востребуемым продуктом, имеющим высокую потребительскую ценность. Отсюда следует объективная необходимость развития мер защиты информации и данных. Для свободной ориентации в информационном пространстве современного общества специалист любого профиля должен уметь получать, грамотно обрабатывать и использовать информацию с помощью средств вычислительной техники и телекоммуникаций.

Студенты должны знать общие подходы к построению защищенной информационной или вычислительной системы. Основным моментом этого

раздела следует считать системный подход формированию моделей угроз, общей модели информационной защиты, модели политики ИБ и структуре документов в сфере ИБ современного предприятия. Для каждого вида угроз необходимо выстраивать цепочку: <вид угрозы> - <оценка риска реализации> - <оценка достаточности средств защиты> - <компенсация возможного ущерба>.

Студенты должны знать стандарты информационной безопасности. Развитие семейства стандартов следует рассматривать в контексте развития информационных технологий в целом. При этом особое внимание следует обратить на построение системы оценки рисков, которая является одной из основных составляющих общей системы безопасности. Здесь необходимо достаточно подробно рассматривать содержание современных стандартов обеспечения ИБ и информационных рисков.

Студенты должны уметь использовать современные технологии и инструменты информационной безопасности. Важным аспектом является то, что вследствие быстрого развития ИТ постоянно изменяются методы и технологии работы с информацией, появляются способы проникновения в информационные системы предприятия, а также всё новые и новые семейства вирусов. Всё это приводит к необходимости постоянного совершенствования защиты информационной инфраструктуры предприятия и необходимости построения комплексной информационной защиты ПО.

Основа для изучения дисциплины «Информационная безопасность» - конспекты лекций, результаты лабораторных занятий и выполненные самостоятельные работы самыми студентами.

На лабораторных занятиях с использованием средств вычислительной техники студенты выполняют задания, предусмотренные для приобретения пользовательских навыков, решают задачи вычислительного характера, устанавливают и настраивают программные продукты, разрабатывают алгоритмы и программы для решения прикладных задач, выполняют типовые расчеты. Во время самостоятельной работы студента с преподавателем обсуждаются проблемные лекции, решаются сложные алгоритмы.

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации дисциплины при кафедре информатики и ИС РТСУ имеются 4 компьютерных классов обеспеченны электронными досками.

8. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Форма итоговой аттестации: экзамен.

Итоговая система оценок по кредитно-рейтинговой системе с использованием буквенных символов

Оценка по буквенной системе	Диапазон соответствующих наборных баллов	Численное выражение оценочного балла	Оценка по традиционной системе
A	10	95-100	Отлично
A-	9	90-94	
B+	8	85-89	Хорошо
B	7	80-84	
B-	6	75-79	
C+	5	70-74	Удовлетворительно
C	4	65-69	
C-	3	60-64	
D+	2	55-59	
D	1	50-54	
Fx	0	45-49	Неудовлетворительно
F	0	0-44	

Содержание текущего контроля, промежуточной аттестации, итогового контроля раскрываются в фонде оценочных средств, предназначенных для проверки соответствия уровня подготовки по дисциплине требованиям ФГОС ВО.

ФОС по дисциплине является логическим продолжением рабочей программы учебной дисциплины. ФОС по дисциплине прилагается.