МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Рязанский институт (филиал)

федерального государственного автономного образовательного учреждения высшего образования

«Московский политехнический университет»

ПРИНЯТО
На заседании Ученого совета
Рязанского института (филиала)
Московского политехнического
университета
Протокол № 11
от «30» 06 2023 г.

УТВЕРЖДАЮ
Директор
Рязанского института (филиала)
Московского политехнического
университета
_____ В.С. Емец
«30» 06 2023 г.

Рабочая программа дисциплины

«Защита информации»

Направление подготовки

09.03.02 Информационные системы и технологии

Направленность образовательной программы

Информационные системы и технологии в медиаиндустрии

Квалификация, присваиваемая выпускникам

Бакалавр

Форма обучения

Очная, заочная

Рязань
2023

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

1.1. Цель освоения дисциплины

Целью освоения дисциплины является (1):

К основным задачам изучения дисциплины относится подготовка обучающихся к выполнению следующих трудовых функций в соответствии с профессиональными стандартами (3).

Наименование профессиональных стандартов (ПС)	Код, наименование и уровень квалификации ОТФ, на которые ориентирована дисциплина	Код и наименование трудовых функций, на которые ориентирована дисциплина
40.057 Специалист по автоматизированным системам управления производством	*С, Проведение работ по проектированию АСУП, 6*	*С/02.6, Изучение и представление руководству отчетов о передовом национальном и международном опыте разработки и внедрения АСУП*

1.2. Перечень планируемых результатов обучения по дисциплине

В результате освоения дисциплины «Защита информации» у обучающегося формируются профессиональные компетенции УК-2, ПК-1. Содержание указанных компетенций и перечень планируемых результатов обучения по данной дисциплине представлены в таблице 1.

Таблица 1 – Планируемые результаты обучения по дисциплине

Код компетенции	Результаты освоения ОП (содержание компетенций)	Перечень планируемых результатов обучения по дисциплине
1	2	3
Универсальные		
УК-1	УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1. Осуществляет поиск необходимой информации, опираясь на результаты анализа поставленной задачи УК-1.2. Разрабатывает варианты решения проблемной ситуации на основе критического анализа доступных источников информации УК-1.3. Выбирает оптимальный вариант решения задачи, аргументируя свой выбор
Профессиональные		
ПК-1	ПК-1 Способность осуществлять проектирование взаимодействия пользователя с системой при эксплуатации программных средств в части графических пользовательских интерфейсов	ПК-1.1 Выявление потребностей пользователя при эксплуатации программных средств в части графических пользовательских интерфейсов ПК-1.2 Проектирование стилей взаимодействия пользователей с графическим пользовательским интерфейсом программного продукта

2 Место дисциплины в структуре образовательной программы Дисциплина «Защита информации» входит в состав дисциплин Блока, формируемой участниками образовательных отношений образовательной программы бакалавриата по направлению подготовки 09.03.02 Информационные системы и технологии.

3.1 Требования к входным знаниям, умениям и навыкам обучающихся

Изучение дисциплины базируется на знаниях, полученных по информатике в рамках получения среднего общего образования.

Для освоения дисциплины «Защита информации» студент должен:

знать:

- фундаментальные основы школьного курса информатики;

уметь:

- проводить вычисления в двоичной системе счисления;
- осуществлять перевод чисел между двоичной, десятичной и шестнадцатеричной системами счисления;
- решать задачи при помощи формул булевой алгебры;
- строить простейшие блок-схемы алгоритмов;

владеть:

- работой в текстовых редакторах;
- работой в редакторах электронных таблиц;
- работой в графических редакторах;
- методами алгоритмизации.

3.2 Взаимосвязь с другими дисциплинами

Взаимосвязь данной дисциплины с другими дисциплинами образовательной программы представлена в таблице 2.

Таблица 2 − Структурно-логическая схема формирования компетенций

Компетенция	**Предшествующие дисциплины**	**Данная дисциплина**	**Последующие дисциплины**
УК-2, ПК-1	Программирование и основы алгоритмизации Операционные системы Технология программирования	Защита информации	Базы данных, Архитектура вычислительных систем Математические основы теории систем

3. Структура и содержание дисциплины

Общая трудоемкость дисциплины «Защита информации» составляет 3 зачетные единицы, 108 академических часов.

Таблица 3 − Объем дисциплины «Защита информации» в академических часах (для очной/заочной форм обучения)

Вид учебной работы	**Всего часов**	
	для очной	**Для заочной**

	формы	формы
Контактная работа обучающихся с преподавателем	**24**	**8**
Аудиторная работа (всего)	**24**	**8**
в том числе:		
Лекции	12	4
Семинары, практические занятия	12	4
Лабораторные работы		
Внеаудиторная работа (всего)		
в том числе:		
Групповая консультация		
Самостоятельная работа обучающихся (всего)	**84**	**100**
в том числе		
Курсовое проектирование		
Расчетно-графические работы		
Реферат		
Другие виды занятий (*подготовка к занятиям, домашняя работа, подготовка к контрольной работе, работа с литературой*)	84	100
Вид промежуточной аттестации (*З - зачет, Э - экзамен, ЗО – зачет с оценкой*)	**Э**	**Э**
Общая трудоемкость дисциплины, час	**108**	**108**
Общая трудоемкость дисциплины, з.е.	**3**	**3**

3.1. Содержание дисциплины, структурированное по темам, для студентов <u>ОЧНОЙ ФОРМЫ ОБУЧЕНИЯ</u>

Распределение разделов дисциплины «Защита информации» по видам учебных занятий и их трудоемкость указаны в таблице 4 для очной формы обучения.

Таблица 4 – Разделы дисциплины «Защита информации» и их трудоемкость по видам учебных занятий (для очной формы обучения)

№ п/п	Раздел дисциплины	Общая трудоемкость (в часах)	Виды учебных занятий, включая самостоятельную работу обучающихся, и трудоемкость (в часах)					Вид промежуточной аттестации
			Лекции	Практические занятия	Лабораторные работы	Самостоятельная работа	Формы текущего контроля успеваемости	
1	2	3	4	5	6	7	8	9
	Восьмой семестр							
1	**Основные понятия и определения.**	**24**	**2**	**2**		**20**	Практические задания, тест	
1.1	Источники, риски и формы атак на информацию	12	1	1		10		
1.2	Политика и стандарты безопасности	12	1	1		10		
2	**Криптографические модели.**	**28**	**4**	**4**		**20**		
2.1	Алгоритмы шифрования. Алгоритмы аутентификации	14	2	2		10	Практические задания, тест	

	пользователей.							
2.2	Модели безопасности основных операционных систем.	14	2	2		10		
3	**Администрирование сетей**	**28**	**4**	**4**		**20**		
3.1	Защита информации в сетях.	14	2	2		10	Практические задания, тест	
3.2	Многоуровневая защита корпоративных сетей	14	2	2		10		
4	**Требования к системам защиты информации**	**28**	**2**	**2**		**24**	Практические задания, тест	
4.1	Направления развития средств безопасности предприятия.	14	1	**1**		12		
4.2	Правовые последствия несанкционированного доступа к информации	14	1	1		12		
	Форма аттестации							**З**
	Всего часов по дисциплине	**108**	**12**	**12**		**84**		

3.2 Содержание дисциплины «Защита информации», структурированное по разделам (темам)

Содержание лекционных занятий приведено в таблице 5.

Таблица 5 – Содержание лекционных занятий

№ п/п	Наименование раздела (темы) дисциплины	Содержание раздела (темы) дисциплины
1	2	3
1	**Основные понятия и определения.**	
1.1	Источники, риски и формы атак на информацию	Теория защиты информации. Основные направления. Обеспечение информационной безопасности и направления защиты. Комплексность (целевая, инструментальная, структурная, функциональная, временная). Требования к системе защиты информации. Угрозы информации. Виды угроз. Основные нарушения. Характер происхождения угроз. Источники угроз. Предпосылки появления угроз.
1.2	Политика и стандарты безопасности	Система защиты информации. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации. Методы и модели оценки уязвимости информации. Общая модель воздействия на информацию. Общая модель процесса нарушения физической целостности информации
2	**Криптографические модели.**	
2.1	Алгоритмы шифрования. Алгоритмы аутентификации пользователей.	Понятие криптографии. Основные виды шифров. Обобщенная схема криптосистемы. Понятия симметричной и асимметричной криптосистемы. Основные алгоритмы криптографических преобразований. Основные методы криптографической защиты информации в компьютерных системах и сетях. Классификация средств криптографической защиты информации. Основные достоинства и недостатки алгоритма шифрования данных с помощью DES.
2.2	Модели безопасности основных операционных систем.	Перечислите основные режимы работы алгоритма DES. Как обеспечивается криптостойкость асимметричных криптосистем? Основное назначение хеш-функции и основные принципы ее формирования. Отличительные особенности отечественного стандарта хеш-функции (ГОСТ Р 34.11-94) от алгоритмов хеширования MD5 и SHA. Основные алгоритмы электронной цифровой подписи и их

		принципиальные отличия. Современные приложения криптографии. Примеры. Типичные атаки на операционную систему. Понятие защищенной операционной системы. Аппаратное обеспечение средств защиты операционной системы. Проблемы безопасности IP-сетей. Наиболее распространенные варианты атак на компьютерную систему на основе протокола TCP/IP. Список функциональных дефектов с точки зрения защиты в используемой операционной системе (ОС). Элементы безопасности ОС Windows 2000/XP/Vista.
3	**Администрирование сетей**	
3.1	Защита информации в сетях.	Основные практические вопросы зашиты информации. Программные средства защиты и уничтожения информации. Основные принципы построения подсистемы информационной безопасности. Этапы построения подсистемы информационной безопасности.
3.2	Многоуровневая защита корпоративных сетей	Общие принципы обеспечения информационной безопасности. Средства обеспечения конфиденциальности данных. Средства идентификации и аутентификации пользователей. Приведите основные схемы идентификации и аутентификации пользователя. Достоинства биометрических способов идентификации и аутентификации по сравнению с традиционными. Средства аутентификации электронных данных. Правовые последствия несанкционированного съема и использования конфиденциальной информации. Особенности применения технических средств уничтожения информации на магнитных и оптических носителях.
4	**Требования к системам защиты информации**	
4.1	Направления развития средств безопасности предприятия.	Приведите классификацию систем защиты программного обеспечения. Сравните основные технические методы и средства защиты программного обеспечения. Отличия систем защиты от несанкционированного доступа от систем защиты от несанкционированного копирования. Определение понятий «протоколирование» и «аудит». Задачи, реализуемые протоколированием и аудитом и их характеристики
4.2	Правовые последствия несанкционированного доступа к информации	Перечислите функции и компоненты сети VPN. Классифицируйте VPN по способу технической реализации и архитектуре технического решения. Каковы способы защиты информации при межсетевом взаимодействии? Какие криптографические протоколы используются для защиты технологии «клиент-сервер»?

Таблица 6 – Содержание практических занятий

№ п/п	**Наименование раздела (темы) дисциплины**	**Содержание раздела дисциплины**
1	2	3
1	**Основные понятия и определения.**	
1.1	Источники, риски и формы атак на информацию	Требования к системе защиты информации. Угрозы информации. Виды угроз. Основные нарушения. Характер происхождения угроз. Источники угроз. Предпосылки появления угроз.

1.2	Политика и стандарты безопасности	Методы и модели оценки уязвимости информации. Общая модель воздействия на информацию. Общая модель процесса нарушения физической целостности информации
2	**Криптографические модели.**	
2.1	Алгоритмы шифрования. Алгоритмы аутентификации пользователей.	Основные виды шифров. Обобщенная схема криптосистемы. Основные алгоритмы криптографических преобразований. Основные методы криптографической защиты информации в компьютерных системах и сетях..
2.2	Модели безопасности основных операционных систем.	Основные режимы работы алгоритма DES. Основное назначение хеш-функции и основные принципы ее формирования. Отличительные особенности отечественного стандарта хеш-функции (ГОСТ Р 34.11-94) от алгоритмов хеширования MD5 и SHA. Основные алгоритмы электронной цифровой подписи и их принципиальные отличия. Современные приложения криптографии. Примеры. Проблемы безопасности IP-сетей. Наиболее распространенные варианты атак на компьютерную систему на основе протокола TCP/IP.
3	**Администрирование сетей**	
3.1	Защита информации в сетях.	. Программные средства защиты и уничтожения информации. Основные принципы построения подсистемы информационной безопасности. Этапы построения подсистемы информационной безопасности.
3.2	Многоуровневая защита корпоративных сетей	Средства идентификации и аутентификации пользователей. Приведите основные схемы идентификации и аутентификации пользователя. Средства аутентификации электронных данных. Особенности применения технических средств уничтожения информации на магнитных и оптических носителях.
4	**Требования к системам защиты информации**	
4.1	Направления развития средств безопасности предприятия.	Сравните основные технические методы и средства защиты программного обеспечения. Определение понятий «протоколирование» и «аудит». Задачи, реализуемые протоколированием и аудитом и их характеристики
4.2	Правовые последствия несанкционированного доступа к информации	Классифицируйте VPN по способу технической реализации и архитектуре технического решения. Каковы способы защиты информации при межсетевом взаимодействии? Какие криптографические протоколы используются для защиты технологии «клиент-сервер»?

4. Методические указания для обучающихся по освоению дисциплины

4.1. Общие методические рекомендации по освоению дисциплины, образовательные технологии

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

Контактная работа может быть аудиторной, внеаудиторной, а также проводиться в электронной информационно-образовательной среде института (далее - ЭИОС). В случае проведения части контактной работы по дисциплине в ЭИОС (в соответствии с расписанием учебных занятий), трудоемкость контактной работа в ЭИОС эквивалентна аудиторной работе.

При проведении учебных занятий по дисциплине обеспечивается развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренин-

гов, анализ ситуаций и имитационных моделей, преподавание дисциплины в форме курса, составленного на основе результатов научных исследований, проводимых институтом, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

- *электронное обучение;*
- *проблемное обучение;*
- *разбор конкретных ситуаций;*

Результат обучения считается сформированным (повышенный уровень), если теоретическое содержание курса освоено полностью; при устных собеседованиях студент исчерпывающе, последовательно, четко и логически стройно излагает учебный материал; свободно справляется с задачами, вопросами и другими видами заданий, требующих применения знаний, использует в ответе дополнительный материал; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданийчто соответствует повышенному уровню сформированности результатов обучения.

Результат обучения считается сформированным (пороговый уровень), если теоретическое содержание курса освоено полностью; при устных собеседованиях студент последовательно, четко и логически стройно излагает учебный материал; справляется с задачами, вопросами и другими видами заданий, требующих применения знаний; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, что соответствует пороговому уровню сформированности результатов обучения.

Результат обучения считается несформированным, если студент при выполнении заданий не демонстрирует знаний учебного материала, допускает ошибки, неуверенно, с большими затруднениями выполняет задания, не демонстрирует необходимых умений, качество выполненных заданий не соответствует установленным требованиям, что соответствует допороговому уровню.

4.2. Методические указания для обучающихся по освоению дисциплины на занятиях лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов тематического плана. В ходе лекционных занятий раскрываются базовые вопросы в рамках каждой темы дисциплины. Обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложные и важные положения изучаемого материала. Материалы лекций являются опорной основой для подготовки обучающихся к практическим занятиям / лабораторным работам и выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

В ходе лекционных занятий рекомендуется вести конспектирование учебного материала. Возможно ведение конспекта лекций в виде интеллект-карт.

4.4. Методические указания для обучающихся по освоению дисциплины на занятиях семинарского типа

Практические (семинарские) занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы. Основной формой проведения семинаров и практических занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение задач и разбор примеров и ситуаций в аудиторных условиях.

Практические (семинарские) занятия обучающихся обеспечивают:

- проверку и уточнение знаний, полученных на лекциях;
- получение умений и навыков составления докладов и сообщений, обсуждения вопросов по учебному материалу дисциплины;

- подведение итогов занятий по рейтинговой системе, согласно технологической карте дисциплины.

4.5. Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обеспечивает подготовку обучающегося к аудиторным занятиям и мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине. Результаты этой подготовки проявляются в активности обучающегося на занятиях и в качестве выполненных практических заданий и других форм текущего контроля.

При выполнении заданий для самостоятельной работы рекомендуется проработка материалов лекций по каждой пройденной теме, а также изучение рекомендуемой литературы, представленной в Разделе 5.

В процессе самостоятельной работы при изучении дисциплины студенты могут использовать в специализированных аудиториях для самостоятельной работы компьютеры, обеспечивающему доступ к программному обеспечению, необходимому для изучения дисциплины, а также доступ через информационно-телекоммуникационную сеть «Интернет» к электронной информационно-образовательной среде института (ЭИОС) и электронной библиотечной системе (ЭБС), где в электронном виде располагаются учебные и учебно-методические материалы, которые могут быть использованы для самостоятельной работы при изучении дисциплины.

Для обучающихся по заочной форме обучения самостоятельная работа является основным видом учебной деятельности.

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Вся литература, включенная в данный перечень, представлена в виде электронных ресурсов в электронной библиотеке института (ЭБС). Литература, используемая в печатном виде, представлена в научной библиотеке университета в объеме не менее 0,25 экземпляров на одного обучающегося.

Основная литература

1. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства [Текст]: учебное пособие для студ. вузов / В. Ф. Шаньгин. - М. : ДМК Пресс, 2010. - 544 с
2. Васильков, А. В. Информационные системы и их безопасность [Текст] : учебное пособие / А. В. Васильков, А. А. Васильков, И. А. Васильков. - М. : Форум, 2011. - 528 с. - (Профессиональное образование).
3. Долозов Н. Л. Программные средства защиты информации [Электронный ресурс]: конспект лекций / Долозов Н. Л., Гультяева Т. А. - Новосибирск: НГТУ • 2015. - 63 с. - Режим доступа: http://www.knigafund.ru/books/185990/read#page2

Дополнительная литература:

1. Корнеев, И. К. Защита информации в офисе [Текст] : учебник / И. К. Корнеев, Е. А. Степанов. - М. : Проспект, 2008. - 336 с.
2. Мельников, В. П. Информационная безопасность и защита информации [Текст]: учебное пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейманова. - 3-е изд., стер. - М. : Академия, 2008. - 336 с.
3. Ищейнов, В. Я. Защита конфиденциальной информации [Текст] : учебное пособие / В. Я. Ищейнов, М. В. Мецатунян. - М. : Форум, 2009. - 254 с.
4. Чубукова, С. Г. Основы правовой информатики [Текст] : учебное пособие / С. Г. Чубукова, В. Д. Элькин. - Изд. 2-е, испр. и доп. - М. : Инфра-М : Контракт, 2010. - 276 с.
5. Обеспечение защиты персональных данных [Текст] : методическое пособие / И. А. Баймакова [и др.]. - М. : ООО "1С-Паблишинг", 2011.

Таблица 7 – Учебно-методическое обеспечение самостоятельной работы обучающихся

№ п/п	Раздел (тема) дисциплины	Литература (ссылка на номер в списке литературы)
1	2	3
1	**Основные понятия и определения**	
1.1	Источники, риски и формы атак на информацию	Основная: 1 Дополнительная: 1,2,3,4,5
1.2	Политика и стандарты безопасности	Основная: 1 Дополнительная1,2,3,4,5
2	**Криптографические модели.**	
2.1	Алгоритмы шифрования. Алгоритмы аутентификации пользователей.	Основная: 1 Дополнительная: 1,2,3,4,5
2.2	Модели безопасности основных операционных систем.	Основная: 1 Дополнительная: 1,2,3,4,5
3	**Администрирование сетей**	
3.1	Защита информации в сетях.	Основная: 3 Дополнительная: 1,2,3,4,5
3.2	Многоуровневая защита корпоративных сетей	Основная: 3 Дополнительная: 1,2,3,4,5
4	**Требования к системам защиты информации**	
4.1	Направления развития средств безопасности предприятия.	Основная: 1, 3 Дополнительная: 1,2,3,4,5
4.2	Правовые последствия несанкционированного доступа к информации	Основная: 1, 3 Дополнительная: 1,2,3,4,5

5.2. Профессиональные базы данных, информационно-справочные системы, интернет-ресурсы

1. КонсультантПлюс [Электронный ресурс] Справочная правовая система. – Режим доступа: http//www.consultant.ru
2. Электронная библиотечная система Рязанского института (филиала) Московского политехнического института [Электронный ресурс]. - Режим доступа: http://bibl.rimsou.loc/ - Загл. с экрана.
3. Электронно-библиотечная система «Издательства Лань» [Электронный ресурс]. - Режим доступа: https://lanbook.com/. - Загл. с экрана.
4. Электронно-библиотечная система Юрайт [Электронный ресурс]. – Режим доступа: https://urait.ru/- Загл. с экрана.
5. Электронно-библиотечная система IPR SMART [Электронный ресурс]. - Режим доступа: https://www.iprbookshop.ru/. - Загл. с экрана.

5.3. Программное обеспечение

Информационное обеспечение учебного процесса по дисциплине осуществляется с использованием следующего программного обеспечения (лицензионного и свободно распространяемого), в том числе отечественного производства:

№ п/п	Наименование	Условия доступа
1	Microsoft Windows	из внутренней сети университета (лицензионный договор)
2	Microsoft Office	из внутренней сети университета (лицензи-

		онный договор)
3	КонсультантПлюс	из внутренней сети университета (лицензионный договор)
4	СДО MOODLE	из любой точки, в которой имеется доступ к сети Интернет (лицензионный договор)

6. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных учебным планом и рабочей программой дисциплины, оснащенные оборудованием и техническими средствами обучения.

Занятия лекционного типа *(при наличии в учебном плане)*. Учебные аудитории для занятий лекционного типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук), учебно-наглядные пособия (презентации по темам лекций), обеспечивающие тематические иллюстрации, соответствующие данной программе дисциплины.

Занятия семинарского типа *(при наличии в учебном плане)*. Учебные аудитории для занятий семинарского типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук).

Промежуточная аттестация. Для проведения промежуточной аттестации по дисциплине используются компьютерные классы, оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду университета и/или учебные аудитории, укомплектованные мебелью и техническими средствами обучения.

Самостоятельная работа. Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде института. Для организации самостоятельной работы обучающихся используются:

компьютерные классы института;

библиотека, имеющая места для обучающихся, оснащенные компьютерами с доступом к базам данных и сети Интернет.

Электронная информационно-образовательная среда института (ЭИОС). Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде института (ЭИОС) из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети "Интернет", как на территории института, так и вне ее.

ЭИОС института обеспечивает:

доступ к учебным планам, рабочим программам дисциплин (модулей), программам практик, электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочих программах дисциплин (модулей), программах практик;

формирование электронного портфолио обучающегося, в том числе сохранение его работ и оценок за эти работы.

В случае реализации образовательной программы с применением электронного обучения, дистанционных образовательных технологий ЭИОС дополнительно обеспечивает:

фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения образовательной программы;

проведение учебных занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;

взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействия посредством сети "Интернет".

Защита информации	Аудитория № 33 Аудитория для практических и семинарских занятий Аудитория для курсового проектирования Столы, стулья, классная доска, кафедра для преподавателя компьютер, проектор, экран - Microsoft Win Starter 7 Russian Academic OPEN 1 License No Level Legalization Get Genuine. Лицензия № 47945625 от 14.01.2011 - Microsoft Office 2010 Russian Academic OPEN 1 License No Level. Лицензия № 47945625 от 14.01.2011 - Kaspersky Security Cloud 21.1.15.500. Отечественного производства, бесплатная версия - LibreOffice 7.0.3. Свободно распространяемая Срок действия Лицензий: до 30.08.2024.	390000, Рязанская область, г. Рязань, ул. Колхозная, д. 2а
	Аудитория № 217 Лекционная аудитория Аудитория для групповых и индивидуальных консультаций - Столы, стулья, классная доска, кафедра для преподавателя; экран, жалюзи, проектор, ноутбук.	390000, Рязанская область, г. Рязань, ул. Право-Лыбедская, 26/53
	Аудитория № 206 Компьютерная аудитория Аудитория для курсового проектирования Аудитория для самостоятельной работы оснащенная компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в Электронную информационно-образовательную среду института Рабочее место преподавателя: - персональный компьютер; Рабочее место учащегося: - персональный компьютер программное обеспечение - Microsoft Win Starter 7 Russian Academic OPEN 1 License	390000, Рязанская область, г. Рязань, ул. Право-Лыбедская, 26/53

	No Level Legalization Get Genuine. Лицензия № 47945625 от 14.01.2011 - Microsoft Office 2010 Russian Academic OPEN 1 License No Level. Лицензия № 47945625 от 14.01.2011 - Kaspersky Security Cloud 21.1.15.500. Отечественного производства, бесплатная версия - LibreOffice 7.0.3. Свободно распространяемая Срок действия Лицензий: до 30.08.2024.	

7 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине «Защита информации»

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Таблица 8 – Этапы формирования компетенций в процессе освоения дисциплины

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Период формирования компетенции	Наименование оценочного средства
1	Источники, риски и формы атак на информацию	УК-2, ПК-1	В течение восьмого семестра	Вопросы к экзамену, вопросы для подготовки к практическим занятиям, тестовые задания
2	Политика и стандарты безопасности	УК-2, ПК-1		
3	Алгоритмы шифрования. Алгоритмы аутентификации пользователей.	УК-2, ПК-1		
4	Модели безопасности основных операционных систем.	УК-2, ПК-1		
5	Защита информации в сетях.	УК-2, ПК-1		
6	Многоуровневая защита корпоративных сетей	УК-2, ПК-1		
7	Направления развития средств безопасности предприятия.	УК-2, ПК-1		
8	Правовые последствия несанкционированного доступа к информации	УК-2, ПК-1		

7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Таблица 9 – Планируемые результаты обучения, характеризирующие этапы формирования компетенций

Компетенция	Уровень освоения компетенции	Показатели сформированности компетенции	Наименование оценочного средства
УК-2, ПК-1	Пороговый	Способность осуществлять поиск, хранение, некоторые виды обработки информации из раз-	

		личных источников и баз данных	
	Высокий	Способность осуществлять поиск, хранение, обработку и анализ информации из различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий	

Таблица 10 – Описание показателей и критериев оценивания компетенций

Компетенция	**Результаты обучения (по этапам формирования компетенций)**	**Шкала оценивания, критерии оценивания уровня освоения компетенции**			
		Не освоена	**Освоена частично**	**Освоена в основном**	**Освоена**
УК-2, ПК-1	**Знать:** методы и средства получения, хранения и переработки информации; форматы представления данных; основные принципы построения ЭВМ, **Уметь:** сформулировать требования к техническим средствам для решения определенных задач; разрабатывать алгоритмы обработки данных; организовывать вычислительную сеть. **Владеть:** основными методами, способами и средствами получения, хранения, переработки информации и применять их при решении поставленных задач; средствами организации вычислительной сети	Не способен осуществлять поиск, хранение, обработку и анализ информации из различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий	Частично владеет способностью осуществлять поиск, хранение, обработку и анализ информации из различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий	Показывает хорошую способность осуществлять поиск, хранение, обработку и анализ информации из различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий	Полностью владеет способностью осуществлять поиск, хранение, обработку и анализ информации из различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий

7.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

7.3.1 Вопросы для подготовки к экзамену по дисциплине «Защита информации»:

1. Компьютерные вирусы. Их разновидности.
2. Антивирусные средства. Примеры антивирусных программ.
3. Понятие информационной безопасности.
4. Понятие конфиденциальности информации.
5. Понятие доступа к информации (санкционированный и несанкционированный доступ).
6. Понятия идентификация, аутентификация и авторизация.
7. Понятие угроза безопасности.
8. Понятие уязвимость системы (сети).
9. Понятие атаки на компьютерную систему.
10. Охарактеризуйте подходы к обеспечению компьютерной информации.
11. Перечислите основные и вспомогательные сервисы безопасности, дайте их классификацию.
12. Дайте характеристику групп требований к системе защиты.
13. «Фрагментарный» подход в обеспечении безопасности компьютерной системы.
14. «Комплексный» подход в обеспечении безопасности компьютерной системы.
15. В чем заключается политика безопасности компьютерной системы?
16. На чем основана «избирательная» политика безопасности?
17. На чем основана «полномочная» политика безопасности?
18. Понятие криптографии. Основные виды шифров.
19. Обобщенная схема криптосистемы. Понятия симметричной и асимметричной криптосистемы.
20. Перечислите основные алгоритмы криптографических преобразований.
21. Перечислите основные методы криптографической защиты информации в компьютерных системах и сетях.
22. Как классифицируются средства криптографической защиты информации?
23. Основные достоинства и недостатки алгоритма шифрования данных с помощью DES.
24. Перечислите основные комбинации, используемые при шифровании алгоритмом DES.
25. Перечислите основные режимы работы алгоритма DES.
26. Как обеспечивается криптостойкость асимметричных криптосистем?
27. Каково основное назначение хеш-функции?
28. Каковы основные принципы формирования хеш-функции?
29. Отличительные особенности отечественного стандарта хеш-функции (ГОСТ Р 34.11-94) от алгоритмов хеширования MD5 и SHA.
30. Перечислите основные алгоритмы электронной цифровой подписи и укажите на их принципиальные отличия.
31. Современные приложения криптографии. Примеры.
32. Типичные атаки на операционную систему.
33. Понятие защищенной операционной системы.
34. Аппаратное обеспечение средств защиты операционной системы.
35. Проблемы безопасности IP-сетей.
36. Наиболее распространенные варианты атак на компьютерную систему на основе протокола TCP/IP.
37. Сформулируйте список функциональных дефектов с точки зрения защиты в используемой операционной системе (ОС).

38. Какие элементы безопасности содержит ОС Windows 2000/XP/Vista?
39. Назовите элементы безопасности ОС UNIX?
40. Основные практические вопросы зашиты информации.
41. Программные средства защиты и уничтожения информации.
42. Основные принципы построения подсистемы информационной безопасности.
43. Этапы построения подсистемы информационной безопасности.
44. Общие принципы обеспечения информационной безопасности.
45. Средства обеспечения конфиденциальности данных.
46. Средства идентификации и аутентификации пользователей.
47. Приведите основные схемы идентификации и аутентификации пользователя.
48. Достоинства биометрических способов идентификации и аутентификации по сравнению с традиционными.
49. Средства аутентификации электронных данных.
50. Правовые последствия несанкционированного съема и использования конфиденциальной информации.
51. Особенности применения технических средств уничтожения информации на магнитных и оптических носителях.
52. Приведите классификацию систем защиты программного обеспечения.
53. Сравните основные технические методы и средства защиты программного обеспечения.
54. Назовите отличия систем защиты от несанкционированного доступа от систем защиты от несанкционированного копирования.
55. Приведите определение понятий «протоколирование» и «аудит»
56. Назовите задачи, реализуемые протоколированием и аудитом.
57. Дайте характеристику задачи активного аудита.
58. Перечислите функции и компоненты сети VPN.
59. Классифицируйте VPN по способу технической реализации и архитектуре технического решения.
60. Каковы способы защиты информации при межсетевом взаимодействии?
61. Какие криптографические протоколы используются для защиты технологии «клиент-сервер»?

(Фонд оценочных средств представлен в приложении к рабочей программе)

7.3.2 Образцы тестовых заданий

Самостоятельная работа студентов предусмотрена учебным планом по дисциплине в объеме 72 часов (очная форма обучения) и 94 часов (заочная форма обучения).

Тематика самостоятельной работы:

Раздел 1. Корректирующие коды

1. Оценка и выбор корректирующего кода для контроля достоверности информации.
2. Построение циклического кода с минимальным кодовым расстоянием.
3. Алгоритм определения количества вариантов ошибок, не обнаруживаемых циклическим кодом.
4. Алгоритм построения кода Плоткина.
5. Алгоритм построения интерактивного кода.
6. Алгоритм построения кода Макдональда.
7. Алгоритм построения мажоритарного циклического кода.

Раздел 2. Современные симметричные криптосистемы

1. Американский стандарт шифрования данных DES.
2. Алгоритм шифрования данных IDEA.
3. Отечественный стандарт шифрования данных ГОСТ 28147–89.
4. Алгоритм построения криптосистемы Хилла.
5. Алгоритм шифрования информации методом гаммирования для симметричных систем.

6. Алгоритм шифрования информации методом Вернама для симметричных систем.
7. Обзор методов генерации, хранения и распространения криптографических ключей.

Раздел 3. Защита в операционных системах

1. Защита в операционной системе UNIX.
2. Защита в операционной системе Windows NT.
3. Защита в операционной системе IBM OS/390.
4. Методы и средства защиты от удаленных атак через сеть Internet.

Раздел 4. Ассиметричные криптосистемы

1. Схема шифрования Полига-Хеллмана.
2. Схема шифрования Эль-Гамаля.
3. Алгоритм цифровой подписи RSA.
4. Алгоритм цифровой подписи Эль-Гамаля.
5. Обзор методов и средств защиты от удаленных атак через сеть Internet.
6. Защита информации в электронных платежных системах.
7. Обеспечение безопасности электронных платежей через сеть Internet.
8. Программная реализация однонаправленной хэш-функции на основе симметричных блочных алгоритмов.
9. Алгоритм цифровой подписи Эль-Гамаля для аутентификации электронных документов.
10. Реализация протокола идентификации с нулевой передачей знаний

7.3.2 Образцы билетов для проведения экзамена

Рязанский институт (филиал) Московского государственного политехнического университета	**Экзаменационный билет № 1** по дисциплине «Защита информации» для очной формы обучения, направление 09.03.02 семестр 8	**«УТВЕРЖДАЮ»** Зав. кафедрой _____ «__» _____ 2023г.

1. Общие принципы обеспечения информационной безопасности.
2. Средства аутентификации электронных данных.

Рязанский институт (филиал) Московского государственного политехнического университета	**Экзаменационный билет № 2** по дисциплине «Защита информации» для очной формы обучения, направление 09.03.02 семестр 8	**«УТВЕРЖДАЮ»** Зав. кафедрой _____ «__» _____ 2023г.

1. Каковы основные принципы формирования хеш-функции
2. Дайте характеристику групп требований к системе защиты

7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

7.4.1 Методические рекомендации по проведению экзамена

1) Цель проведения

Основной целью проведения экзамена является определение степени достижения целей по учебной дисциплине или ее разделам. Осуществляется это проверкой и оценкой уровня теоретических знаний, полученных студентами, умения применять их к решению практических задач, степени овладения студентами практическими навыками и умениями в объеме требований рабо-

чей программы по дисциплине, а также их умение самостоятельно работать с учебной литературой.

2) Форма проведения

Формой промежуточной аттестации по данной дисциплине восьмом семестре в соответствии с учебным графиком, является экзамен. Экзамен проводится в объеме рабочей программы в устной форме. Экзаменационные билеты могут иметь две части - теоретическую и практическую. Практическая часть может оцениваться с помощью технических средств, при этом билеты содержат только теоретические вопросы. Информация о структуре билетов доводится студентам заблаговременно.

3) Метод проведения

Экзамен проводится по билетам или с использованием списка вопросов.

По практическим вопросам допускается проверка знаний с помощью технических средств контроля. При необходимости могут рассматриваться дополнительные вопросы и проблемы, решаться задачи и примеры.

4) Критерии допуска студентов к экзамену

В соответствии с требованиями руководящих документов и согласно Положению о текущем контроле знаний и промежуточной аттестации студентов института, к экзамену допускаются студенты, выполнившие все требования учебной программы.

5) Организационные мероприятия

5.1. Назначение преподавателя, принимающего экзамен.

Экзамены принимаются лицами, которые читали лекции по данной дисциплине, Решением заведующего кафедрой определяются помощники основному экзаменатору из числа преподавателей, ведущих в данной группе практические занятия, а если лекции по разделам учебной дисциплины читались несколькими преподавателями, то определяется состав комиссии для приема экзамена. Студентам при этом оценка выставляется методом потока.

5.2. Конкретизация условий, при которых студенты освобождаются от сдачи экзамена (основа - результаты рейтинговой оценки текущего контроля).

По представлению преподавателя, ведущего занятия в учебной группе, заведующий кафедрой может освободить студентов от сдачи экзамена. От экзамена освобождаются студенты, показавших отличные и хорошие знания по результатам рейтинговой оценки текущего контроля, с выставлением им оценки «хорошо». Со студентами, имеющими претензии на оценку «отлично», проводится собеседование во время зачета или во время проведения консультации перед экзаменом.

6) Методические указания экзаменатору

6.1. Конкретизируется работа преподавателей в пред зачётный период и в период непосредственной подготовки обучающихся к экзамену.

Во время подготовки к зачету возможны индивидуальные консультации.

6.2. Уточняются организационные мероприятия и методические приемы при проведении экзамена.

Количество одновременно находящихся экзаменующихся в аудитории. В аудитории, где принимается экзамен, может одновременно находиться студентов из расчета не более десяти экзаменующихся на одного экзаменатора.

Время, **отведенное на подготовку** ответа по билету, не должно превышать: для зачета – 40 минут. По истечению данного времени после получения билета (вопроса) студент должен быть готов к ответу.

Организация практической части экзамена**.** Практическая часть экзамена организуется так, чтобы обеспечивалась возможность проверить умение студентов применять теоретические знания при решении практических заданий, освоение компетенций. Она проводится путем постановки экзаменующимся отдельных задач, упражнений, заданий, требующих практических действий по решению заданий. Каждый студент выполняет задание самостоятельно путем производства расчетов, решения задач, работы с документами и др. При выполнении заданий студент отвечает на дополнительные вопросы, которые может ставить экзаменатор.

Действия экзаменатора.

Студенту на экзамене разрешается брать один билет. В случае, когда экзаменующийся не может ответить на вопросы билета, ему может быть предоставлена возможность выбрать второй билет при условии снижения оценки на 1 балл.

Во время испытания промежуточной аттестации студенты могут пользоваться рабочими программами учебных дисциплин, а также справочниками и прочими источниками информации, перечень которых устанавливается преподавателем.

Использование материалов, не предусмотренных указанным перечнем, а также попытка общения с другими студентами или иными лицами, в том числе с применением электронных средств связи, несанкционированные преподавателем перемещение по аудитории и т.п. не разрешается и являются основанием для удаления студента из аудитории с последующим проставлением в ведомости оценки «неудовлетворительно».

Студент, получивший на экзамене неудовлетворительную оценку, ликвидирует задолженность в сроки, устанавливаемым приказом директора института. Окончательная пересдача экзамена принимается комиссией в составе трех человек (заведующий кафедрой, лектор потока, преподаватель родственной дисциплины).

Задача преподавателя на экзамене заключается в том, чтобы внимательно заслушать студента, проконтролировать решение практических заданий, предоставить ему возможность полностью изложить ответ. Заслушивая ответ и анализируя методы решений практических заданий, преподаватель постоянно оценивает насколько полно, системно и осмысленно осуществляется ответ, решается практическое задание.

Считается бестактностью прерывать ответ студента, преждевременно давать оценку его ответам и действиям.

В тех случаях, когда ответы на вопросы или практические действия были недостаточно полными или допущены ошибки, преподаватель после ответов студентом на все вопросы задает дополнительные вопросы с целью уточнения уровня освоения дисциплины. Содержание индивидуальных вопросов не должно выходить за рамки рабочей программы. Если студент затрудняется сразу ответить на дополнительный вопрос, он должен спросить разрешения предоставить ему время на подготовку и после подготовки отвечает на него.

Шкала и критерии оценивания

Таблица 11 – Шкала и критерии оценивания ответа на экзамене

Критерии	**Оценка**		
	«отлично»	**«хорошо»**	**«удовлетворительно»**
Объем	Глубокие знания, уверенные действия по решению практических заданий в полном объеме учебной программы, освоение всех компетенций	Достаточно полные знания, правильные действия по решению практических заданий в объеме учебной программы, освоение всех компетенций	Твердые знания в объеме основных вопросов, в основном правильные решения практических заданий, освоение всех компетенций

Системность	Ответы на вопросы логично увязаны с учебным материалом, вынесенным на контроль, а также с тем, что изучал ранее	Ответы на вопросы увязаны с учебным материалом, вынесенным на контроль, а также с тем, что изучал ранее	Ответы на вопросы в пределах учебного материала, вынесенного на контроль	Имеется необходимость в постановке наводящих вопросов
Осмысленность	Правильные и убедительные ответы. Быстрое, правильное и творческое принятие решений, безупречная отработка решений заданий. Умение делать выводы	Правильные ответы и практические действия. Правильное принятие решений. Грамотная отработка решений по заданиям	Допускает незначительные ошибки при ответах и практических действиях. Допускает неточность в принятии решений по заданиям	

Интегральная оценка знаний, умений и навыков студента определяется по частным оценкам за ответы на все вопросы (задания) билета, в соответствии с разработанными и утвержденными критериями.

Инновационные формы проведения занятий

В ходе аудиторных учебных занятий используются различные инновационные формы и средства обучения, которые направлены на совместную работу преподавателя и обучающихся, обсуждение, принятие группового решения. Такие методы способствуют сплочению группы и обеспечивают возможности коммуникаций не только с преподавателем, но и с другими обучаемыми, опираются на сотрудничество в процессе познавательной деятельности.

Успешная реализация содержания курса основывается на использовании активных и интерактивных методов обучения (таблица 13).

Таблица 13 – Интерактивные образовательные технологии, используемые в аудиторных занятиях

№ п/п	Раздел (тема) дисциплины	Вид занятия	Форма работы
1	Алгоритмы шифрования. Алгоритмы аутентификации пользователей.	Практическое занятие	Представление и обсуждение докладов
2	Защита информации в сетях.	Практическое занятие	Представление и обсуждение докладов

8. Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости рабочая программа дисциплины может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе для дистанционного обучения. Для этого требуется заявление студента (его законного представителя) и заключение психолого-медико-педагогической комиссии (ПМПК).

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида, могут предлагаться следующие варианты восприятия учеб-

ной информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.

- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

Рабочая программа дисциплины разработана в соответствии с:

- Федеральный государственный образовательный стандарт по направлению подготовки (специальности) 09.03.02 «Информационные системы и технологии» и уровню высшего образования Бакалавриат, утвержденный приказом Минобрнауки России от 19.09.2017 № 929 (далее – ФГОС ВО);
- учебным планом (очной, заочной форм обучения) по направлению подготовки 09.03.02 Информационные системы и технологии.

Рабочая программа дисциплины включает в себя оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине (п.7 Оценочные материалы (фонд оценочных средств) для текущего контроля успеваемости и промежуточной аттестации).

Автор: О.В. Тихонова, к.ф.-м.н., доцент кафедры «Информатика и информационные технологии»

Программа одобрена на заседании кафедры «Информатика и информационные технологии» (протокол № 10 от 24.06.2023).