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

«Утверждаю»
Декан естественнонаучного факультета
_____ Пещукович А.И.
«____»_____2026 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Основы управления информационной безопасностью

Направление подготовки - 10.03.01 «Информационная безопасность»
Профиль подготовки – Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)
Форма подготовки – Очная
Уровень подготовки – Бакалавриат

ДУШАНБЕ - 2026

Рабочая программа составлена на основе требований федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 «Информационная безопасность» **(**уровень Бакалавриат), утвержденного приказом Министерства образования и науки РФ №524 от 08.06.2017 г., Концепции преподавания Основы управления информационной безопасностью для специальностей и направлений подготовки, реализуемых в образовательных организациях высшего образования, утвержденной протоколом Экспертного совета по развитию исторического образования Минобрнауки РФ от 06.08.2024 г. №ВФ/35-ПР

При разработке рабочей программы учитываются

- содержание программ дисциплин, изучаемых на предыдущих и последующих этапах обучения;
- новейшие достижения в данной предметной области.

Рабочая программа обсуждена на заседании кафедры информатики и информационных технологий протокол №1 от «___» _____ 2025 г.

Рабочая программа утверждена УМС естественнонаучного факультета протокол №1 от «___» _____ 2025 г.

Рабочая программа утверждена Ученым советом естественнонаучного факультета, протокол № 1 от «___» _____ 2025 г.

1. ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Актуальность изучения дисциплины «Основы управления информационной безопасностью»

1.1 Цели изучения дисциплины Целью освоения дисциплины "Основы управления информационной безопасностью" является формирование у студентов теоретических знаний и практических навыков в области защиты информации, управления рисками информационной безопасности и разработки политики безопасности. Дисциплина направлена на подготовку специалистов, способных анализировать угрозы информационной безопасности, разрабатывать и реализовывать меры по защите информации, а также управлять процессами обеспечения информационной безопасности в организациях. В результате изучения дисциплины студенты должны овладеть основами обеспечения информационной безопасности, соответствующими современным требованиям и стандартам.

1.2 Задачи изучения дисциплины Изучение основных принципов, концепций и стандартов информационной безопасности. Ознакомление с различными видами угроз информационной безопасности и способами защиты от них. Формирование навыков анализа рисков информационной безопасности и разработки мер по их снижению. Обучение разработке и внедрению политики информационной безопасности в организации. Развитие навыков управления процессами обеспечения информационной безопасности.

1.3 В результате изучения дисциплины «Основы управления информационной безопасностью» у обучающихся формируются следующие универсальные и общепрофессиональные компетенции:

Код	Результаты освоения ООП	Перечень планируемых результатов обучения	Вид оценочного знания
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные	Знать: Основные принципы выбора оптимальных способов решения задач информационной	Кейс-задача

	способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	безопасности. Уметь: Анализировать задачи в области ИБ и выбирать подходящие методы решения, учитывая правовые нормы и ограничения. Владеть: Навыками применения различных подходов к решению задач, оценки ресурсов и ограничений.	
УК-3	Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	Знать: Основы командной работы и принципы эффективного взаимодействия. Уметь: Работать в команде, выполнять свою роль, решать конфликты и достигать общих целей. Владеть: Навыками коммуникации, сотрудничества и совместной работы в области информационной безопасности.	Деловая игра
ОПК-10	Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять	Знать: Основные принципы формирования политики ИБ, меры по ее обеспечению и управлению. Уметь: Участвовать в формировании политики ИБ, организовывать и поддерживать выполнение комплекса мер по обеспечению ИБ, управлять	Реферат

	процессом их реализации на объекте защиты	процессом их реализации. Владеть: Навыками разработки, внедрения и контроля выполнения политик ИБ, управления процессами обеспечения ИБ.	
ПК-1.1	Анализирует архитектуру компьютерных систем и выявляет угрозы и уязвимости информационной безопасности.	Знать: Архитектуру компьютерных систем и основные угрозы/уязвимости ИБ. Уметь: Анализировать архитектуру компьютерных систем, выявлять угрозы и уязвимости. Владеть: Навыками анализа и оценки защищенности компьютерных систем.	Тестирование
ПК-3	Способен сопровождать и совершенствовать системы обеспечения информационной безопасности компьютерных систем	Знать: Принципы работы систем обеспечения информационной безопасности. Уметь: Сопровождать и совершенствовать системы обеспечения ИБ. Владеть: Навыками настройки, администрирования и совершенствования систем обеспечения ИБ.	Защита отчета по лабораторной работе

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1. Дисциплина **«Основы управления информационной безопасностью»** входит в обязательную часть Блока Дисциплины (модули) ОПОП ВО и является

её базовой частью **(Б1.О.31).** В процессе преподавания данного курса учитываются знания студентов по таким дисциплинам, как история таджикского народа, история первобытного общества, история древнего мира и средних веков, изучавшихся ими в общеобразовательной средней школе.

2.2 Преподавание данной дисциплины является необходимым для дальнейшего освоения студентами дисциплин в структуре ОПОП бакалавриата по направлению **«Информационная безопасность».**

Таблица 2.

№ п/п	Название дисциплины	Семестр	Место дисциплины в структуре ОПОП
-	—	—	Предшествующая дисциплина
-	—	—	Последующая дисциплина

При освоении данной дисциплины необходимы умения и готовность («входные» знания) обучающегося по дисциплинам, указанных в Таблице 2. Дисциплины взаимосвязаны с данной дисциплиной, они изучаются параллельно. Теоретическими дисциплинами, для которых освоение данной дисциплины необходимо как предшествующее являются:

3. СТРУКТУРА И СОДЕРЖАНИЕ КУРСА, КРИТЕРИИ НАЧИСЛЕНИЯ БАЛЛОВ

Преподавание курса «Основы управления информационной безопасностью» планируется студентам Очная формы обучения по направлению «Информационная безопасность».

Объем дисциплины составляет __ зачетные единицы. Всего запланировано 90 часа, из которых: лекции – 16 часов, практические занятия – 14 часов, лабораторные работы 0 часов, иная контактная работа – 32 часа, самостоятельная работа – 42. Всего часов аудиторной нагрузки – 48 часа.

По итогам 8 семестра планируется сдача студентами зачета с оценкой.

3.1 Структура и содержание теоретической части курса

Лекция 1 Введение в информационную безопасность. Основные понятия и определения

Определение информационной безопасности, цели и задачи. Правовые основы информационной безопасности. Стандарты и нормативные документы.

Лекция 2 Угрозы информационной безопасности. Классификация угроз.

Виды угроз: технические, программные, социальные. Источники угроз. Модели угроз.

Лекция 3 Уязвимости информационных систем. Классификация уязвимостей.

Типы уязвимостей. Методы обнаружения и анализа уязвимостей. Сканеры уязвимостей.

Лекция 4 Методы и средства защиты информации. Обзор технологий защиты.

Криптографические методы защиты. Средства аутентификации и авторизации. Межсетевые экраны.

Лекция 5 Системы обнаружения и предотвращения вторжений (IDS/IPS)

Принципы работы IDS/IPS. Типы IDS/IPS. Развертывание и настройка IDS/IPS.

Лекция 6 Управление доступом. Модели управления доступом.

Ролевая модель управления доступом. Мандатная модель управления доступом. Дискреционная модель управления доступом.

Лекция 7 Анализ рисков информационной безопасности. Методологии анализа рисков.

Оценка рисков. Матрица рисков. Разработка плана обработки рисков.

Лекция 8 Политика информационной безопасности. Разработка и внедрение политики.

Структура политики информационной безопасности. Виды политик. Мониторинг и аудит политики.

Структура и содержание практической части курса

Практическое занятие 1 Практическое применение стандартов ISO 27001, ISO 27002 (Практика)

Анализ стандартов. Разработка политик безопасности на основе ISO 27001

Практическое занятие 2 Анализ актуальных угроз и уязвимостей (Практика)

Обзор новостей ИБ. Анализ отчетов об угрозах. Использование баз уязвимостей.

Практическое занятие 3 Практическое применение сканеров уязвимостей (Nessus, OpenVAS) (Практика)

Настройка и использование сканеров уязвимостей. Анализ отчетов сканирования. Рекомендации по устранению уязвимостей.

Практическое занятие 4 Настройка межсетевых экранов (Firewall). (Практика)

Практические занятия по настройке и конфигурированию межсетевых экранов.

Практическое занятие 5 Настройка и развертывание систем обнаружения вторжений (IDS) (Практика)

Практическое применение IDS Snort и Suricata. Анализ журналов событий.

Практическое занятие 6 Применение инструментов для анализа трафика (Wireshark) (Практика)

Анализ сетевого трафика. Выявление аномалий и подозрительной активности.

Практическое занятие 7 Разработка плана реагирования на инциденты информационной безопасности (Практика)

Структура плана реагирования. Процедуры реагирования. Практическое моделирование инцидентов.

Практическое занятие 8 Разработка политики паролей и управления учетными записями (Практика)

Создание безопасной политики паролей. Практическое применение инструментов для управления учетными записями.

Структура и содержание лабораторной части курса

Структура и содержание КСР

КСР 1 Анализ нормативных актов в области информационной безопасности

Анализ и сравнение ФЗ, ГОСТов и других нормативных документов. Подготовка презентации.

КСР 2 Анализ угроз и уязвимостей конкретной организации

Выбор организации. Анализ актуальных угроз и уязвимостей. Подготовка отчета.

КСР 3 Разработка политик информационной безопасности для организации

Разработка политик информационной безопасности. Структура политики. Презентация.

КСР 4 Моделирование инцидента информационной безопасности

Моделирование инцидента. Описание шагов по реагированию. Подготовка отчета.

КСР 5 Аудит безопасности информационной системы

Проведение аудита безопасности. Подготовка отчета по результатам аудита.

КСР 6 Практическое применение SIEM-систем

Использование SIEM-систем для мониторинга событий и выявления аномалий.

КСР 7 Защита облачных сервисов

Анализ безопасности облачных сервисов. Подготовка презентации.

КСР 8 Разработка плана обеспечения непрерывности бизнеса

Разработка плана обеспечения непрерывности бизнеса. Подготовка презентации.

Структура и содержание СРС

СРС 1 Изучение стандартов ISO 27001, ISO 27002

Самостоятельное изучение стандартов. Подготовка реферата.

СРС 2 Изучение современных угроз информационной безопасности

Анализ последних отчетов об угрозах. Подготовка презентации.

СРС 3 Анализ уязвимостей веб-приложений

Самостоятельное изучение уязвимостей веб-приложений. Подготовка реферата.

СРС 4 Разработка модели нарушителя

Построение модели нарушителя. Подготовка презентации.

СРС 5 Исследование методов криптографической защиты информации

Изучение методов криптографии. Подготовка реферата.

СРС 6 Анализ инструментов защиты от DDoS-атак

Изучение инструментов защиты от DDoS. Подготовка презентации.

СРС 7 Практическое применение SIEM-систем

Работа с SIEM-системами. Анализ логов. Подготовка отчета.

СРС 8 Изучение этического хакинга

Изучение методик этичного хакинга. Подготовка презентации.

Структура и содержание теоретической, лабораторной части курса, КСР и СРС

Таблица 3.

№ п/п	Наименование темы	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Литра	Количество баллов
		Лек	Прак	КСР	Лаб	СРС	ИКР		
1	Введение в информационную безопасность. Основные понятия и опреде-ления	2				2		1,5	
	Практическое применение стандартов ISO 27001, ISO 27002		2			2		2,3	12,5
2	Анализ нормативных актов в области информационной безопасности			2		2		6,5	12,5
3	Угрозы информационной безопасности. Классификация угроз.	2				2		7,2	
	Анализ актуальных угроз и уязвимостей		2			2		2,3	12,5
4	Анализ угроз и уязвимостей конкретной организации			2		2		2,1	12,5

5	Уязвимости информационных систем. Классификация уязвимостей.	2				2		6,2	
	Практическое применение сканеров уязвимостей (Nessus, OpenVAS)		2			2		4,3	12,5
6	Разработка политик информационной безопасности для организации			2				5,1,3,5	12,5
7	Методы и средства защиты информации. Обзор технологий защиты.	2				2		5,6	
	Настройка межсетевых экранов		2			2		2,3	12,5
8	Моделирование инцидента информационной безопасности			2		2		6,5	12,5
9	Системы обнаружения и предотвращения вторжений (IDS/IPS)	2				2		7,2	
	Настройка и развертывание систем обнаружения вторжений (IDS)		2			2		2,3	12,5
10	Аудит безопасности информационной системы			2		2		2,1	12,5
11	Управление доступом. Модели управления доступом.	2				2		6,2	
	Применение инструментов для анализа трафика (Wireshark)		2			2		2,3	12,5
12	Практическое применение SIEM-систем			2		2		6,5	12,5
13	Анализ рисков информационной безопасности. Методологии анализа рисков.	2				2		7,2	
	Разработка плана реагирования на инциденты информационной безопасности		2			2		2,3	12,5
14	Защита облачных сервисов			2		2		2,1	12,5
15	Политика информационной безопасности. Разработка и внедрение политики.	2						6,2	
	Разработка политики паролей и управления учетными записями		2			2		4,3	12,5
16	Разработка плана обеспечения непрерывности бизнеса			2				5,1,3,5	12,5
Итог		16	16	16	0	42	0		200

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 **4 -го курса**, 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.

Порядок выставления баллов: 1-й рейтинг (1-7 недели до 12,5 баллов+12,5 баллов (8 неделя – Рубежный контроль №1) = 100 баллов), 2-й рейтинг (9-15 недели до 12,5 баллов+12,5 баллов (16 неделя – Рубежный контроль №2) = 100 баллов), итоговый контроль 100 баллов.

К примеру, за текущий и 1-й рубежный контроль выставляется 100 баллов: лекционные занятия – 21 балл, за практические занятия (КСР, лабораторные) – 31,5 балл, за СРС – 17,5 баллов, требования ВУЗа – 17,5 баллов, рубежный контроль – 12,5 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, 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 – 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, написание конспекта и выполнение других видов работ*	Активное участие на практических (семинарских) занятиях, КСР	СРС Написание реферата, доклада, эссе Выполнение других видов работ	Выполнение положения высшей школы (установленная форма одежды, наличие рабочей папки, а также других пунктов устава высшей школы)	РК №1	Всего
1	2	3	4	5	6	7
1	3	4,5	2,5	2,5	-	12,5

2	3	4,5	2,5	2,5	-	12,5
3	3	4,5	2,5	2,5	-	12,5
4	3	4,5	2,5	2,5	-	12,5
5	3	4,5	2,5	2,5	-	12,5
6	3	4,5	2,5	2,5	-	12,5
7	3	4,5	2,5	2,5	-	12,5
8	-	-	-	-	12,5	12,5
Первый рейтинг	21	31,5	17,5	17,5	12,5	100
1	2	3	4	5	6	7
1	3	4,5	2,5	2,5	-	12,5
2	3	4,5	2,5	2,5	-	12,5
3	3	4,5	2,5	2,5	-	12,5
4	3	4,5	2,5	2,5	-	12,5
5	3	4,5	2,5	2,5	-	12,5
6	3	4,5	2,5	2,5	-	12,5
7	3	4,5	2,5	2,5	-	12,5
8	-	-	-	-	12,5	12,5
Второй рейтинг	21	31,5	17,5	17,5	12,5	100
Итог						200

Формула вычисления результатов дистанционного контроля и итоговой формы контроля по дисциплине за семестр для студентов 4 -го курсов:

$$ИБ = \left[\frac{(P_1 + P_2)}{2}\right] \cdot 0{,}49 + Эи \cdot 0{,}51 \ ,$$

где ИБ –итоговый балл, P_1- итоги первого рейтинга, P_2- итоги второго рейтинга, *Эи*– результаты итоговой формы контроля (экзамен).

4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Методы обработки информации» 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.

План-график выполнения самостоятельной работы по дисциплине

4.1. План-график выполнения самостоятельной работы по дисциплине

№	Объем СРС, ч.	Тема СРС	Форма и вид результатов самостоятельной работы	Форма контроля
1	4	Понятие управления информационной безопасностью	Вопросы 1–4. Описание технологии разработки, реферат	Опрос
2	4	Цели, задачи и принципы управления ИБ	Вопросы 5–8. Презентация методов	Выступление
3	6	Система менеджмента информационной безопасности (СМИБ)	Вопросы 8–10. Презентация, доклад	Выступление
4	6	Политика и стратегия информационной безопасности	Вопросы 11–13. Выполнение задания 1 (1–10)	Защита работы, выступление
5	4	Организационная структура управления ИБ	Выполнение задания 1. Конспект, презентация (вопросы 14–15)	Опрос, выступление
6	4	Управление активами информационной системы	Выполнение задания 2	Защита работы
7	6	Управление рисками информационной безопасности	Вопросы 16–17. Выполнение задания 3	Защита работы
8	6	Управление уязвимостями и угрозами	Вопросы 16–17. Выполнение задания 4	Защита работы
9	4	Планирование мер защиты информации	Выполнение задания 5	Защита работы
10	4	Контроль и аудит информационной безопасности	Вопросы 18–25. Выполнение задания 6	Защита работы
11	4	Документирование процессов управления ИБ	Вопросы 26–29. Выполнить задания 2 и описать в терминах классов	Опрос, защита работы
12	4	Правовое и нормативное обеспечение управления ИБ	Вопросы 30–31. Реферат. Выполнение задания 7	Защита реферата, защита работы

13	4	Подготовка и обучение персонала по вопросам ИБ	Вопросы 32–37. Презентация	Опрос, выступление
14	4	Управление инцидентами информационной безопасности	Вопросы 38–40. Выполнение задания 8 (1–4)	Защита работы
15	4	Управление непрерывностью деятельности и восстановлением	Вопросы 41–44. Выполнение задания 9	Защита работы
16	4	Оценка эффективности системы управления ИБ	Вопросы 45–46. Выполнение задания 8 (4–10)	Защита работы

4.2 Характеристика заданий для самостоятельной работы обучающихся 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 «Содержание и структура дисциплины». Конспекты и задания можно выполнить в отдельном тетради или в лекционной (практической) тетради в произвольной форме.

4.3 Критерии оценки выполнения самостоятельной работы.

Критерии оценки выполнения самостоятельной работы является полнота освещения вопроса, логичность изложения, проявления самостоятельность в обработке материала.

4.4. Критерии оценки выполнения самостоятельной работы.

Самостоятельная работа прививает студентам навыки работы с источниками и учебной литературой, помогает повысить уровень знаний по предмету, 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 ОБЕСПЕ- ЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература:

1. 1. Галатенко В. А. Основы информационной безопасности. – М.: Изд. дом «Интернет-Университет Информационных технологий», 2020. – 584 с.
2. Герасимов А. В., Малюк А. А. Информационная безопасность. Учебник для вузов. — СПб.: Питер, 2018. — 560 с.
3. Долгов А. П. Информационная безопасность: Учебное пособие. - М.: ИНТУИТ, 2019. – 320 с.
4. Зегжда Д. П., Ивашко А. А. Основы информационной безопасности. – М.: Горячая линия – Телеком, 2017. – 320 с.
5. Карташев С. П., Федосов А. А. Информационная безопасность. Защита информации в компьютерных системах и сетях. Учебник и практикум для академического бакалавриата. — М.: Юрайт, 2019. — 355 с.
6. Лисицин С. А. Информационная безопасность: Учебник. – М.: Юрайт, 2020. – 362 с.
7. Петров А. А. Информационная безопасность: Учебник и практикум для академического бакалавриата. — М.: Юрайт, 2018. — 336 с.

5.2. Учебники и учебные пособия в сети Интернет:

1. 1. Баранов А. В. Технологии защиты информации в компьютерных сетях. – М.: Гелиос АРВ, 2016. – 288 с.
2. Ермаков А. В. Теория защиты информации. – М.: Юрайт, 2017. – 304 с.
3. Кузнецов А. А., Кузнецова Н. В. Информационная безопасность. Методы и средства защиты информации. - М.: Форум, 2018. – 288 с.
4. Осипов В. В. Безопасность компьютерных сетей. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2019. – 320 с.
5. Родионов А. Е. Информационная безопасность. Конспект лекций. – СПб.: Питер, 2019. – 208 с.
6. Скляров Д. В. Защита информации в компьютерных сетях. – М.: Издательство

ДМК Пресс, 2018. – 208 с.
7. Щеглов И. Б. Защита информации в компьютерных системах. – СПб.: БХВ-Петербург, 2018. – 704 с.

5.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. 1. Официальный сайт ФСТЭК России: https://fstec.ru/
2. Сайт CERT-RU: https://cert.gov.ru/
3. OWASP (Open Web Application Security Project): https://owasp.org/
4. NIST (National Institute of Standards and Technology): https://www.nist.gov/
5. SANS Institute: https://www.sans.org/

5.4. Перечень информационных технологий и программного обеспечения

Используются лицензионное программное обеспечение ОС Windows -/11 и программное обеспечение открытого доступа (Open source), среды программирования (Denwer, CodeBlock, Dev_C++ и др.). Для разработки моделей проекта ИС используются CASE – средства: ERWin, Visual UML, Rational Rose и т.д.

6. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Для обеспечения систематической и регулярной работы по изучению дисциплины «Основы управления информационной безопасностью» и успешного прохождения текущих и итоговых контрольных испытаний студенту рекомендуется придерживаться следующего порядка обучения:

1. Самостоятельно определить объем времени, необходимого для проработки каждой темы.

2. Регулярно изучать каждую тему дисциплины, используя различные формы индивидуальной работы.

3. Согласовывать с преподавателем виды работы по изучению дисциплины.

4. По завершении отдельных тем передавать выполненные работы (рефераты) преподавателю.

Обучение по дисциплине «Основы управления информационной безопасностью» строится следующим образом. На лекциях преподаватель дает общую

характеристику рассматриваемого вопроса, различные научные концепции или позиции, которые есть по данной теме. Во время лекции рекомендуется составлять конспект, фиксирующий основные положения лекции и ключевые определения по пройденной теме. Во время лекционного занятия необходимо фиксировать все спорные моменты и проблемы, на которых останавливается преподаватель. Потом именно эти аспекты станут предметом самого пристального внимания и изучения на практических занятиях.

При подготовке к практическому занятию обязательно требуется изучение дополнительной литературы по теме занятия. Без использования нескольких источников информации невозможно проведение дискуссии на занятиях, обоснование собственной позиции, построение аргументации. Если обсуждаемый аспект носит дискуссионный характер, следует изучить существующие точки зрения и выбрать тот подход, который вам кажется наиболее верным. При этом следует учитывать необходимость обязательной аргументации собственной позиции. Во время практических занятий рекомендуется активно участвовать в обсуждении рассматриваемой темы, выступать с подготовленными заранее рефератами, докладами и презентациями.

Самостоятельная работа должна соответствовать графику прохождения программы дисциплины. Самостоятельная работа по дисциплине «Основы управления информационной безопасностью» включает:

а) работу с литературой;

б) подготовку устного выступления на практическом занятии;

в) подготовку к занятию в интерактивной форме;

г) подготовку реферата с презентацией;

д) подготовку к дискуссии;

е) заполнение хронологической таблицы;

ж) подготовку к текущей и итоговой аттестации по дисциплине.

Для теоретического и практического усвоения дисциплины большое значение имеет самостоятельная работа студентов, которая может осуществляться студентами индивидуально и под руководством преподавателя.

Самостоятельная работа студентов предполагает самостоятельное изучение отдельных тем, дополнительную подготовку студентов к каждому практическому занятию.

Самостоятельная работа студентов является важной формой образовательного процесса. Она реализуется непосредственно в процессе аудиторных занятий, в контакте с преподавателем, а также в библиотеке, дома, при выполнении студентом учебных и творческих задач.

Цель самостоятельной работы студентов - научить студента осмысленно и самостоятельно работать сначала с учебным материалом, затем с научной информацией, заложить основы самоорганизации и самовоспитания с тем, чтобы привить умение в дальнейшем непрерывно повышать свою квалификацию.

При изучении дисциплины организация самостоятельной работы студентов форм представлена следующим образом:

1) внеаудиторная самостоятельная работа;

2)аудиторная самостоятельная работа, которая осуществляется под непосредственным руководством преподавателя.

Аудиторная самостоятельная работа может реализовываться при проведении практических занятий и во время чтения лекций.

На практических занятиях различные виды самостоятельной работы позволяют сделать процесс обучения более интересным и поднять активность значительной части студентов в группе.

Для проведения занятий необходимо иметь большой банк заданий, причем эти задания могут быть дифференцированы по степени сложности.

На каждом этапе самостоятельной работы следует разъяснять цели работы, контролировать понимание этих целей студентами, постепенно формируя у них умение самостоятельной постановки задачи и выбора цели.

При чтении лекционного курса непосредственно в аудитории необходимо контролировать усвоение материала основной массой студентов

путем проведения экспресс-опросов по конкретным темам.

На практических занятиях различные виды самостоятельной работы

позволяют сделать процесс обучения более интересным и поднять активность значительной части студентов в группе.

На практических занятиях нужно не менее 1 часа из двух (50% времени) отводить на самостоятельное рассмотрение заданий.

По результатам самостоятельного рассмотрения задания следует выставлять по каждому занятию оценку. Оценка предварительной подготовки студента к практическому занятию может быть сделана путем экспресс-опроса в течение 5, максимум - 10 минут.

По материалам раздела целесообразно выдавать студенту домашнее задание и на последнем практическом занятии по разделу подвести итоги его изучения (например, провести контрольную работу), обсудить оценки каждого студента, выдать дополнительные задания тем студентам, которые хотят повысить оценку.

Результативность самостоятельной работы студентов во многом определяется наличием активных методов ее контроля. Существуют следующие виды контроля:

- входной контроль знаний и умений студентов при начале изучения очередной дисциплины;

- текущий контроль, то есть регулярное отслеживание уровня усвоения материала на лекциях, практических занятиях;

- самоконтроль, осуществляемый студентом в процессе изучения дисциплины при подготовке к контрольным мероприятиям;

- итоговый контроль по дисциплине в виде зачета, зачета с оценкой (в устной форме).

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации дисциплины при кафедре информатики и ИТ РТСУ имеются 4 компьютерных классов. Для занятий используются лицензионное программное обеспечение ОС Windows -7/8/10/11 и программное обеспечение открытого доступа (Open source), среды программирования (Denwer, CodeBlock, Dev_C++ и др.). Для разработки моделей проекта ИС используются CASE – средства: ERWin, Visual UML, Rational Rose и т.д.

В Университете созданы специальные условия для обучающихся с ограниченными возможностями здоровья - специальные учебники, учебные пособия и дидактические материалы, специальные технические средства обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, проведение групповых и индивидуальных коррекционных занятий, обеспечение доступа в здания организаций и другие условия, без которых невозможно или затруднено освоение дисциплины обучающимися с ограниченными возможностями здоровья.

Обучающимся с ограниченными возможностями здоровья предоставляются бесплатно специальные учебники и учебные пособия, иная учебная литература, а также обеспечивается:

- наличие альтернативной версии официального сайта организации в сети "Интернет" для слабовидящих;

- присутствие ассистента, оказывающего обучающемуся необходимую помощь;

- обеспечение выпуска альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы);

- возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения организации, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проёмов, лифтов).

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

Промежуточная аттестации осуществляется: для зачета – контрольная работа и опрос. Экзамен проводится в форме тестирования. Защита курсового проекта: представляется пояснительная записка и презентация выступления.

Текущий контроль студентов осуществляется путем защиты лабораторных

работ, выполнения самостоятельного задания, обсуждения теоретических вопросов.

Контролирующие материалы по дисциплине содержат:

Контрольные вопросы и задания для текущего контроля знаний по дисциплине.

Тестовые задания для промежуточного контроля знаний по дисциплине;

Методические рекомендации и тематика курсового проектирования.

Также указаны критерии оценки курсового проекта.

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.