МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ИНДУСТРИАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Заведующий кафедрой
_____ О.Ф. Данилов
«_____» _____ 20_ г.

РАБОЧАЯ ПРОГРАММА

дисциплины: **Информационная безопасность и защита информации**
направление подготовки: **09.03.02 Информационные системы и технологии**
направленность (профиль): **Интеллектуальные системы и технологии «Умный город»**
форма обучения: **очная**

Рабочая программа рассмотрена
на заседании кафедры интеллектуальных систем и технологий

Протокол № _____ от «___» _____ 20__ г.

1. Цели и задачи освоения дисциплины

Целью дисциплины «Информационная безопасность и защита информации» является формирование компетенций в области теоретических основ информационной безопасности, основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

Задачи дисциплины:

— знакомство с современными угрозами сетевой безопасности;

— изучение основ инженерно-технической защиты информации;

— изучение технических средств добывания и защиты информации;

— изучение криптографических систем.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Информационная безопасность и защита информации» относится к дисциплинам части, формируемой участниками образовательных отношений учебного плана.

Необходимыми условиями для освоения дисциплины являются:

знание методов защиты сетевой инфраструктуры;

умение организовывать защиту сетевого периметра организации;

владеть методами криптографии, криптоанализа, инструментами мониторинга сети и обнаружения атак.

Содержание дисциплины является логическим продолжением таких дисциплин, как «Операционные системы» и «Инфокоммуникационные системы и сети» и служит основой для освоения дисциплины «Корпоративные информационные системы» и будет полезна для выполнения выпускной квалификационной работы.

3. Результаты обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Таблица 3.1

Код и наименование компетенции	Код и наименование индикатора достижения компетенции (ИДК)	Код и наименование результата обучения по дисциплине
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1. Осуществляет выбор актуальных российских и зарубежных источников, а так же поиск, сбор и обработку информации, необходимой для решения поставленной задачи.	Знать:З1 как осуществляется поиск, сбор и обработка необходимой информации для решения поставленной задачи
		Уметь У1 искать и обрабатывать информацию для решения поставленных задач
		Владеть В1 навыками поиска , сбора и обработки необходимой информации для решения поставленных задач
	УК-1.2. Систематизирует и критически анализирует информацию, полученную из разных источников, в соответствии с	Знать З2: как осуществляется анализ информации полученной из разных источников
		Уметь У2 Систематизировать информацию полученную из разных источников в соответствии с требованиями и условиями задачи

	требованиями и условиями задачи.	Владеть В2 навыками поиска , анализа и синтеза информации, системным подходом для решения поставленных задач
	УК-1.3. Использует методики системного подхода при решении поставленных задач.	**Знать:** З3 – методики поиска, сбора и обработки информации; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности; метод системного анализа
		Уметь: У3 – применять методики поиска, сбора и обработки информации; системный подход для решения поставленных задач.
		Владеть: В3 – инструментами поиска, сбора и обработки, критического анализа и синтеза информации;
ПКС 4 – Способность выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности	ПКС-4.2. Разрабатывает мероприятия по обеспечению безопасности на уровне баз данных.	**Знать:** З4 – угрозы безопасности баз данных и способы их предотвращения; инструменты обеспечения безопасности баз данных и их возможности.
		Уметь: У4 – выявлять угрозы безопасности на уровне баз данных; разрабатывать мероприятия по обеспечению безопасности на уровне баз данных.
		Владеть: В4 – навыками выбора основных средств поддержки информационной безопасности на уровне баз данных.

4. Объем дисциплины

Общий объем дисциплины составляет 3 зачетных единицы, 108 часов.

Таблица 4.1.

Форма обучения	Курс/ семестр	Аудиторные занятия/контактная работа, час.			Самостоятельная работа, час.	Контроль, час	Форма промежуточной аттестации
		Лекции	Практические занятия	Лабораторные занятия			
очная	4/8	24	-	24	24	36	экзамен

5. Структура и содержание дисциплины

5.1. Структура дисциплины

- очная форма обучения (ОФО)

Таблица 5.1.1

№ п/п	Структура дисциплины		Аудиторные занятия, час.			СРС, час.	Всего, час.	Код ИДК	Оценочные средства
	Номер раздела	Наименование раздела	Л.	Пр.	Лаб.				
1	1	Введение в информационную безопасность.	1	-	3	2	6	УК-1.3	Вопросы коллоквиума. Задания для лабораторных работ
2	2	Правовое обеспечение информационной безопасности.	1	-	3	2	6	УК-1.3	Вопросы коллоквиума, Задания для лабораторных работ
3	3	Организационное обеспечение информационной безопасности.	1	-	3	2	6	УК-1.3	Вопросы коллоквиума, Задания для лабораторных работ
4	4	Технические средства обеспечения информационной безопасности.	4	-	3	2	9	ПКС-4.2	Вопросы коллоквиума, Задания для лабораторных работ
5	5	Общесистемные основы защиты информации и	1	-	3	2	6	ПКС-4.2	Вопросы коллоквиума, Задания для лабораторных работ

		процесса ее обработки в вычислительных системах.							
6	6	Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств.	3	-	3	2	8	ПКС-4.2	Вопросы коллоквиума, Задания для лабораторных работ
7	7	Защита от компьютерных вирусов	1	-	3	2	6	ПКС-4.2	Задания для самостоятельной работы Задания для лабораторной работы
8	8	Криптографическое закрытие информации	1	-	3	2	6	ПКС-4.2	Задания для самостоятельной работы Задания для лабораторной работы
9	9	Уничтожение остаточных данных	2	-		1	3	УК-1.3	Задания для самостоятельной работы
10	10	Защита от потери информации и отказов программно-аппаратных средств.	1	-		1	2	УК-1.3	Задания для самостоятельной работы
11	11	Защита информационно-программного обеспечения на уровне операционных систем.	1	-		1	2	ПКС-4.2	Задания для самостоятельной работы
12	12	Защита информации на уровне систем управления базами данных.	1	-		1	2	ПКС-4.2	Задания для самостоятельной работы
13	13	Специфические особенности защиты информации в локальных и глобальных компьютерных сетях.	4	-		2	6	УК-1.3	Задания для самостоятельной работы
14	14	Современные средства защиты информации от НСД.	2	-		2	4	УК-1.3	Задания для самостоятельной работы
15	Экзамен		-	-	-	36	36	УК-1.3 ПКС-4.2	Устный экзамен
Итого:			24		24	60	108		

- заочная форма обучения (ЗФО)

не реализуется.

- очно-заочная форма обучения (ОЗФО)

не реализуется.

5.2. Содержание дисциплины.

5.2.1. Содержание разделов дисциплины (дидактические единицы).

Раздел 1. *«Введение в информационную безопасность»*. Понятие национальной безопасности: виды безопасности: государственная, экономическая, общественная, военная, экологическая, информационная; роль и место системы обеспечения информационной безопасности (ИБ) в системе национальной безопасности РФ; доктрина ИБ, история проблемы ИБ, угрозы ИБ; методы и средства обеспечения ИБ; методологические и технологические основы комплексного обеспечения ИБ; модели, стратегии и системы обеспечения ИБ; методы управления, организации и

обеспечения работ по обеспечению ИБ; обеспечение ИБ в нормальных и чрезвычайных ситуациях; проблемы информационной войны; правовые и нормативные акты в области ИБ.

Раздел 2. *«Правовое обеспечение информационной безопасности».* Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации; конституционные гарантии прав граждан на информацию и механизм их реализации; понятие и виды защищаемой информации по законодательству РФ; защита интеллектуальной собственности средствами патентного и авторского права; правовая регламентация охранной деятельности; международное законодательство в области защиты информации.

Раздел 3. *«Организационное обеспечение информационной безопасности».* Анализ и оценка угроз информационной безопасности объекта; оценка ущерба вследствие противоправного раскрытия информации ограниченного доступа и меры по его локализации; средства и методы физической защиты объектов; системы сигнализации, видеонаблюдения, контроля доступа; служба безопасности объекта; подбор, расстановка и работа с кадрами; организация и обеспечение режима секретности; организация пропускного и внутриобъектового режима; организация режима и охраны объектов в процессе транспортировки; защита информации при авариях, иных экстремальных ситуациях и в условиях чрезвычайного положения; технологические меры поддержания информационной безопасности объектов; обеспечение информационной безопасности объекта (учреждения, банка, промышленного предприятия) при осуществлении международного научно-технического и экономического сотрудничества.

Раздел 4. *«Технические средства обеспечения информационной безопасности».* Общие вопросы организации противодействия технической разведке; основные организационные и технические мероприятия, используемые для противодействия технической разведке; методы и средства защиты режимных объектов от утечки конфиденциальной информации по техническим каналам; физические основы образования побочных электромагнитных излучений от технических средств; каналы утечки информации: электромагнитные, электрические (проводные), виброакустические; защита технических средств от утечки информации по этим каналам; нормы эффективности защиты; роль и место технического контроля эффективности защиты информации; нормы, руководящие документы по организации и ведению контроля; организационный и технический контроль; методы контроля; особенности контроля объектов в различных сферах; аппаратура контроля; взаимодействие контрольных органов с подразделениями контроля на местах; методологические основы автоматизации технического контроля; основные задачи технического контроля, требующие автоматизированного решения.

Раздел 5. *«Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах».* Структура и принципы функционирования современных вычислительных систем. Проблемы обеспечения безопасности обработки и хранения информации в вычислительных системах. Базовые этапы построения системы комплексной защиты вычислительных систем. Анализ моделей нарушителя. Угрозы информационно-программному обеспечению вычислительных систем и их классификация. Функции системы защиты по предупреждению угроз и устранению последствий их реализации. Классификация способов и средств комплексной защиты информации. Классификация методов защиты информации с использованием программно-аппаратных средств вычислительной системы. Организационная структура системы комплексной защиты информационно-программного обеспечения. Управление системой защиты. Функции ядра системы комплексной защиты. Многоуровневая структура системы защиты на основе программно-аппаратных средств вычислительной системы. Стандарты по оценке безопасности вычислительных систем. Требования руководящих документов Гостехкомиссии.

Раздел 6. *«Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств».* Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам. Основные этапы допуска к ресурсам вычислительной системы. Использование простого пароля. Использование динамически изменяющегося пароля. Взаимная проверка подлинности и другие случаи опознания. Способы разграничения доступа к компьютерным ресурсам. Разграничение доступа по спискам. Использование матрицы установления полномочий. Произвольное и принудительное управление доступом. Разграничение доступа по уровням секретности и категориям. Понятие меток безопасности. Управление метками безопасности. Парольное разграничение доступа и комбинированные методы. Особенности программной реализации контроля установленных полномочий. Защита программных средств от

несанкционированного копирования, исследования и модификации. Привязка программ к среде функционирования. Защита программ от несанкционированного запуска.

Раздел 7. *«Защита от компьютерных вирусов»*. История появления компьютерных вирусов и факторы, влияющие на их распространение. Понятие компьютерного вируса. Основные этапы жизненного цикла вирусов. Объекты внедрения, режимы функционирования и специальные функции вирусов. Схемы заражения файлов. Схемы заражения загрузчиков. Способы маскировки, используемые вирусами. Классификация компьютерных вирусов. Общая организация защиты от компьютерных вирусов. Транзитный и динамический режимы антивирусной защиты. Поиск вирусов по сигнатурам и обезвреживание обнаруженных вирусов. Углубленный анализ на наличие вирусов путем контроля эталонного состояния компьютерной системы. Защита от деструктивных действий и размножения вирусов. Использование средств аппаратного и программного контроля. Стратегия заблаговременной подготовки к эффективной ликвидации последствий вирусной эпидемии. Технология гарантированного восстановление вычислительной системы после заражения компьютерными вирусами.

Раздел 8. *«Криптографическое закрытие информации»*. Введение в криптографию. Представление защищаемой информации; угрозы безопасности информации; ценность информации; основные термины и понятия криптографии; открытые сообщения и их характеристики; модели открытых сообщений; исторический очерк развития криптографии; Типы криптографических систем. Простые методы шифрования: шифры подстановки и перестановки. Подстановки с переменным коэффициентом сдвига. Многослойные шифры. Использование псевдослучайных чисел для генерации ключей. Выбор порождающего числа и максимизация длины последовательности чисел ключа. Режимы шифрования. Особенности шифрования данных в режиме реального времени. Шифрование ключа при необходимости его хранения с зашифрованными данными. Скоростные и недетерминированные программные шифры. Основы скоростного шифрования. Внесение неопределенностей в процесс криптографических преобразований. Стандарты шифрования. Протоколы распределения ключей; протоколы установления подлинности; электронная цифровая подпись; Общая организация криптографической защиты информации. Использование общесистемных и специализированных программных средств для шифрования файлов и работы с секретными внешними носителями информации.

Раздел 9. *«Уничтожение остаточных данных»*. Введение в проблему. Виды остаточных данных. Способы защиты от несанкционированного использования остаточной информации. Использование специализированных программ по уничтожению остаточных данных. Специальные режимы и особенности шифрования данных в режиме реального времени с возможность мгновенного уничтожения данных. Использование общесистемных и специализированных программных средств для мгновенного уничтожения данных.

Раздел 10. *«Защита от потери информации и отказов программно-аппаратных средств»*. Основные способы защиты от потери информации и нарушений работоспособности вычислительных средств. Внесение функциональной и информационной избыточности. Способы резервировании информации. Правила обновления резервных данных. Методы сжатия информации. Архивация файловых данных. Особенности архивации на магнитные диски и магнитную ленту. Резервирование системных данных. Подготовка программных средств восстановления. Безопасная инсталляция программных средств. Общие сведения о нарушении доступа к дисковой и оперативной памяти. Технология восстановления дисковой и оперативной памяти. Диагностирование и устранение логических и физических дефектов магнитных дисков. Восстановление разметки дискеты и корневого каталога. Отмена результатов форматирования и восстановление поврежденных файлов данных. Защита файлов от удаления и восстановление удаленных файлов. Безопасное кэширование и дефрагментация дисковой памяти. Восстановление и оптимизация оперативной памяти компьютера. Ручное восстановление данных. Безопасное окончание работы на компьютере.

Раздел 11. *«Защита информационно-программного обеспечения на уровне операционных систем»*. Общие сведения о реализации защиты информационно-программного обеспечения в операционных системах. Классификация функций защиты по уровням безопасности, поддерживаемых операционной системой (ОС). Ядро безопасности ОС. Аппаратная основа реализации защиты на уровне ОС. Стандарты по оценке уровня безопасности ОС. Внесение функциональной и информационной избыточности ресурсов на уровне ОС. Основы надежного

администрирования ОС. Используемые способы разграничения доступа к компьютерным ресурсам, а также службы регистрации и сигнализации. Средства ОС по диагностированию и локализации несанкционированного доступа к ресурсам ВС. Безопасные файловые системы современных ОС (HPFS, NTFS). Подсистемы безопасности современных ОС (Windows 95, Windows NT, UNIX), их недостатки и основные направления совершенствования.

Раздел 12 *«Защита информации на уровне систем управления базами данных».* Концептуальные вопросы построения уровней защиты систем управления базами данных (СУБД). Основные требования к подсистеме безопасности СУБД. Общие сведения о разграничении доступа к базам данных. Обязанности администратора по защите баз данных от несанкционированного доступа. Определение полномочий пользователей по доступу к базе данных. Использование матрицы полномочий для разграничения доступа к элементам баз данных. Мандатная система разграничения доступа. Защита данных при статистической обработке. Общее понятие о целостности базы данных. Типы ошибок, ведущих к нарушению целостности. Задание ограничений целостности. Транзакция и ее свойства. Восстановление базы данных. Особенности восстановления распределенной базы данных. Проблема непротиворечивости при параллельной обработке данных. Использование блокирования для управления параллельной обработкой. Метод независимого выполнения транзакций. Управление параллельными транзакциями на основе временных и версионных отметок. Метод обнаружения противоречивых записей журнала регистрации. Метод использования теста правильности. Разрешение тупиковых ситуаций. Инструментальные средства СУБД по обеспечению целостности баз данных.

Раздел 13 *«Специфические особенности защиты информации в локальных и глобальных компьютерных сетях».* Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности. Угрозы информационно-программному обеспечению, характерные только для распределенной вычислительной среды. Использование криптографических систем для защиты данных, циркулирующих в вычислительной сети. Особенности применения симметрических и асимметрических систем шифрования. Распределение ключей между узлами вычислительной сети. Выработка секретных ключей по Диффи-Хеллману. Распределение ключей с помощью асимметрических систем шифрования. Взаимное подтверждение подлинности при обмене сообщениями в сети. Поддержание целостности циркулирующих в сети сообщений. Формирование и проверка цифровой подписи. Защита от отрицания фактов отправки и приема сообщений. Защита от наблюдения за потоком сообщений (трафиком) в сети. Защита в Internet и Intranet. Использование межсетевых экранов (брандмауэров) для защиты информации в локальных вычислительных сетях. Типы межсетевых экранов, их достоинства и недостатки. Ограничение доступа из локальной сети в Internet с помощью proxy-серверов. Безопасность JAVA-приложений.

Раздел 14 *«Современные средства защиты информации от НСД».* Методы и средства ограничения доступа к компонентам ЭВМ, надежность средств защиты компонент; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации, типовые решения в организации ключевых систем; защита программ от изучения, способы встраивания средств защиты в программное обеспечение; защита от разрушающих программных воздействий (РПВ), понятие изолированной программной среды, защита программ от изменения и контроль целостности; системные вопросы защиты программ и данных, основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, вычислительных сетях.

5.2.2. Содержание дисциплины по видам учебных занятий.

Лекционные занятия

Таблица 5.2.1

№ п/п	Номер раздела дисциплины	Объем, час.	Тема лекции
		ОФО	
1	1	1	Введение в информационную безопасность.
2	2	1	Правовое обеспечение информационной безопасности.

3	3	1	Организационное обеспечение информационной безопасности.
4	4	4	Технические средства обеспечения информационной безопасности.
5	5	1	Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах.
6	6	3	Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств.
7	7	1	Защита от компьютерных вирусов.
8	8	1	Криптографическое закрытие информации.
9	9	2	Уничтожение остаточных данных.
10	10	1	Защита от потери информации и отказов программно-аппаратных средств.
11	11	1	Защита информационно-программного обеспечения на уровне операционных систем.
12	12	1	Защита информации на уровне систем управления базами данных.
13	13	4	Специфические особенности защиты информации в локальных и глобальных компьютерных сетях.
14	14	2	Современные средства защиты информации от НСД.
Итого:		24	

Практические занятия

учебным планом не предусмотрены

Лабораторные работы

Таблица 5.2.2

№ п/п	Номер раздела дисциплины	Объем, час.	Наименование лабораторной работы
		ОФО	
1	1	3	Управление безопасностью сети.
2	2	3	Обеспечение безопасности сетевых устройств.
3	3	3	Аутентификация, авторизация и учет.
4	4	3	Внедрение технологий межсетевого экрана.
5	5	3	Обеспечение безопасности локальной сети.
6	6	3	Анализ способов нарушений информационной безопасности..
7	7	3	Основные технологии построения защищенных систем.
8	8	3	Методы криптографии.
Итого:		24	

Самостоятельная работа студента

Таблица 5.2.3

№ п/п	Номер раздела дисциплины	Объем, час.	Тема	Вид СРС
		ОФО		
1	1	2	Методологические и технологические основы комплексного обеспечения ИБ; модели, стратегии и системы обеспечения ИБ; методы управления, организации и обеспечения работ по обеспечению ИБ; обеспечение ИБ в нормальных и чрезвычайных ситуациях; проблемы информационной войны; правовые и нормативные акты в области ИБ.	Изучение теоретического материала. Подготовка к коллоквиуму. Подготовка отчета по лабораторной работе
2	2	2	Защита интеллектуальной собственности средствами патентного и авторского права; правовая регламентация охранной деятельности; международное законодательство в области защиты информации.	Изучение теоретического материала. Подготовка к коллоквиуму. Подготовка отчета по лабораторной работе
3	3	2	Защита информации при авариях, иных экстремальных ситуациях и в условиях чрезвычайного положения; технологические меры	Изучение теоретического материала. Подготовка к коллоквиуму.

			поддержания информационной безопасности объектов; обеспечение информационной безопасности объекта (учреждения, банка, промышленного предприятия) при осуществлении международного научно-технического и экономического сотрудничества.	Подготовка отчета по лабораторной работе
4	4	2	Методологические основы автоматизации технического контроля; основные задачи технического контроля, требующие автоматизированного решения.	Изучение теоретического материала. Подготовка к коллоквиуму. Подготовка отчета по лабораторной работе
5	5	2	Функции ядра системы комплексной защиты. Многоуровневая структура системы защиты на основе программно-аппаратных средств вычислительной системы. Стандарты по оценке безопасности вычислительных систем. Требования руководящих документов Гостехкомиссии.	Изучение теоретического материала. Подготовка к коллоквиуму. Подготовка отчета по лабораторной работе
6	6	2	Защита программных средств от несанкционированного копирования, исследования и модификации. Привязка программ к среде функционирования. Защита программ от несанкционированного запуска.	Изучение теоретического материала. Подготовка к коллоквиуму. Подготовка отчета по лабораторной работе Подготовка отчета по выполнению самостоятельной работы
7	7	2	Стратегия заблаговременной подготовки к эффективной ликвидации последствий вирусной эпидемии. Технология гарантированного восстановление вычислительной системы после заражения компьютерными вирусами.	Изучение теоретического материала. Подготовка отчета по лабораторной работе Подготовка отчета по выполнению самостоятельной работы
8	8	2	Режимы шифрования. Особенности шифрования данных в режиме реального времени.	Изучение теоретического материала. Подготовка отчета по лабораторной работе Подготовка отчета по выполнению самостоятельной работы
9	9	1	Использование общесистемных и специализированных программных средств для мгновенного уничтожения данных.	Подготовка отчета по выполнению самостоятельной работы
10	10	1	Технология восстановления дисковой и оперативной памяти. Диагностирование и устранение логических и физических дефектов магнитных дисков. Восстановление разметки дискеты и корневого каталога	Подготовка отчета по выполнению самостоятельной работы
11	11	1	Аппаратная основа реализации защиты на уровне ОС. Стандарты по оценке уровня безопасности ОС. Внесение функциональной и информационной избыточности ресурсов на уровне ОС.	Подготовка отчета по выполнению самостоятельной работы
12	12	1	Метод независимого выполнения транзакций. Управление параллельными транзакциями на основе временных и версионных отметок. Метод обнаружения противоречивых записей журнала регистрации. Метод использования теста правильности. Разрешение тупиковых ситуаций. Инструментальные средства СУБД по обеспечению целостности баз данных.	Подготовка отчета по выполнению самостоятельной работы
13	13	2	Защита в Internet и Intranet.	Подготовка отчета по выполнению самостоятельной работы
14	14	2	Понятие изолированной программной среды,	Подготовка отчета по

			защита программ от изменения и контроль целостности; системные вопросы защиты программ и данных, основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, вычислительных сетях.	выполнению самостоятельной работы
15	1-14	36	Экзамен	Подготовка к экзамену
Итого:		60		

5.2.3. Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

– лекция –беседа и лекция -визуализация учебного материала в PowerPoint в диалоговом режиме (лекционные занятия);

– работа в малых группах (лабораторные занятия);

– индивидуальные задания по вариантам (лабораторные занятия).

6. Тематика курсовых работ/проектов

Курсовые работы/проекты учебным планом не предусмотрены.

7. Контрольные работы

Контрольные работы учебным планом не предусмотрены.

8. Оценка результатов освоения дисциплины

8.1. Критерии оценивания степени полноты и качества освоения компетенций в соответствии с планируемыми результатами обучения приведены в Приложении 1.

8.2. Рейтинговая система оценивания степени полноты и качества освоения компетенций обучающихся очной формы обучения представлена в таблице 8.1.

Таблица 8.1

№ п/п	Виды мероприятий в рамках текущего контроля	Количество баллов
1 текущая аттестация		
1	Защита лабораторных работ	0-20
2	Коллоквиум	0-10
	ИТОГО за первую текущую аттестацию	**0-30**
2 текущая аттестация		
3	Защита лабораторных работ	0-20
4	Коллоквиум	0-10
5	Защита отчетов по самостоятельной работы	0-40
	ИТОГО за вторую текущую аттестацию	**0-70**
	ВСЕГО	**100**

9. Учебно-методическое и информационное обеспечение дисциплины

9.1 Перечень рекомендуемой литературы представлен в Приложении 2.

9.2. Современные профессиональные базы данных и информационные справочные системы:

- Электронный каталог/Электронная библиотека ТИУ http://webirbis.tsogu.ru/
- Цифровой образовательный ресурс – библиотечная система IPR SMART — https://www.iprbookshop.ru/
- Электронно-библиотечная система «Консультант студента» www.studentlibrary.ru
- Электронно-библиотечная система «Лань» https://e.lanbook.com
- Образовательная платформа ЮРАЙТ www.urait.ru
- Научная электронная библиотека ELIBRARY.RU http://www.elibrary.ru
- Национальная электронная библиотека (НЭБ)
- Библиотеки нефтяных вузов России :
- Электронная нефтегазовая библиотека РГУ нефти и газа им. Губкина http://elib.gubkin.ru/,
- Электронная библиотека Уфимского государственного нефтяного технического университета http://bibl.rusoil.net/ ,
- Библиотечно-информационный комплекс Ухтинского государственного технического университета УГТУ http://lib.ugtu.net/books
- Электронная справочная система нормативно-технической документации «Технорматив»
- ЭКБСОН- информационная система доступа к электронным каталогам библиотек сферы образования и науки.

9.3. Лицензионное и свободно распространяемое программное обеспечение, в т.ч. отечественного производства:

1. VirtualBox
2. Microsoft Windows.
3. Cisco Packet Tracer

10. Материально-техническое обеспечение дисциплины

Помещения для проведения всех видов работы, предусмотренных учебным планом, укомплектованы необходимым оборудованием и техническими средствами обучения.

Таблица 10.1

Обеспеченность материально-технических условий реализации ОПОП ВО

№ п/п	Наименование учебных предметов, курсов, дисциплин, практики, иных видов учебной деятельности, предусмотренных учебным планом образовательной программы	Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно-наглядных пособий	Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом (в случае реализации образовательной программы в сетевой форме дополнительно указывается наименование организации, с которой заключен договор)
1	Информационная безопасность и защита информации	Лекционные занятия: Учебная аудитория для проведения занятий лекционного типа; групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации, №602, Учебная мебель: столы, стулья, доска аудиторная. Компьютер в комплекте – 1 шт., проектор – 1 шт., проекционный экран – 1 шт., акустическая система (колонки) - 2 шт.	625001, Тюменская область, г.Тюмень, ул. Луначарского, д.2 корп.1
		Лабораторные занятия: Учебная аудитория для проведения занятий лабораторного типа на ПК (компьютерный класс); групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации, № 612, Учебная мебель: столы, стулья, доска аудиторная. Компьютеры с установленным на них ПО	625001, Тюменская область, г.Тюмень, ул. Луначарского, д.2 корп.1
		Самостоятельная работа: Помещение для самостоятельной работы обучающихся с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду, № 610, Учебная мебель: столы, стулья, доска аудиторная. Компьютер в комплекте – 5 шт., проектор – 1 шт., проекционный экран – 1 шт.	625001, Тюменская область, г.Тюмень, ул. Луначарского, д.2 корп.1

11. Методические указания по организации СРС

11.1. Методические указания по подготовке к лабораторным занятиям

Информационная безопасность и защита информации: методические указания для лабораторных и самостоятельных работ студентов, обучающихся по направлению 09.03.02 «Информационные системы и технологии» / сост. А.А. Яйлеткан; Тюменский индустриальный университет. –Тюмень: Издательский центр БИК ТИУ, 2016. – 21 с.

11.2. Методические указания по организации самостоятельной работы.

Самостоятельная работа обучающихся заключается в получении заданий (тем) у преподавателя для индивидуального освоения, подготовке отчетов по лабораторным работам и

подготовке к коллоквиумам. Преподаватель на занятии дает рекомендации необходимые для освоения материала. В ходе самостоятельной работы обучающиеся должны работать с информацией в сети Интернетом и учебной литературой. Обучающиеся должны понимать содержание выполненной работы (знать определения основных понятий, уметь разъяснить значение и смысл любого термина, используемого в работе и т.п.).

Приложение 1

Планируемые результаты обучения для формирования компетенции и критерии их оценивания

Дисциплина: **Информационная безопасность и защита информации**
Код, направление подготовки: **09.03.02 Информационные системы и технологии**
Направленность (профиль): **Интеллектуальные системы и технологии «Умный город»**

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
УК-1	УК-1.1. Осуществляет выбор актуальных российских и зарубежных источников, а так же поиск, сбор и обработку информации, необходимой для решения поставленной задачи.	Знать:З1 как осуществляется поиск, сбор и обработка необходимой информации для решения поставленной задачи	Не знает как осуществляется поиск, сбор и обработка необходимой информации для решения поставленной задачи	Не достаточно хорошо знает как осуществляется поиск, сбор и обработка необходимой информации для решения поставленной задачи	Знает с замечаниями как осуществляется поиск, сбор и обработка необходимой информации для решения поставленной задачи	Хорошо знает как осуществляется поиск, сбор и обработка необходимой информации для решения поставленной задачи
		Уметь У1 искать и обрабатывать информацию для решения поставленных задач с помощью актуальных российских и зарубежных источников	Не знает как искать и обрабатывать информацию для решения поставленных задач с помощью актуальных российских и зарубежных источников	Не достаточно хорошо знает как искать и обрабатывать информацию для решения поставленных задач с помощью актуальных российских и зарубежных источников	Знает с замечаниями как искать и обрабатывать информацию для решения поставленных задач с помощью актуальных российских и зарубежных источников	Хорошо знает как искать и обрабатывать информацию для решения поставленных задач с помощью актуальных российских и зарубежных источников
		Владеть В1 навыками поиска , сбора и обработки необходимой информации для решения поставленных задач а так же с актуальных российских и зарубежных источников	Не владеет навыками поиска , сбора и обработки необходимой информации для решения поставленных задач а так же с актуальных российских и зарубежных источников	Не достаточно хорошо владеет навыками поиска , сбора и обработки необходимой информации для решения поставленных задач а так же с актуальных российских и зарубежных источников	Владеет навыками поиска , сбора и обработки необходимой информации для решения поставленных задач а так же с актуальных российских и зарубежных источников с замечаниями	Владеет навыками поиска , сбора и обработки необходимой информации для решения поставленных задач а так же с актуальных российских и зарубежных источников без замечаний
	УК-1.2. Систематизирует и критически анализирует информацию, полученную из разных источников, в	Знать З2: как осуществляется анализ информации полученной из разных источников	Не знает как осуществляется анализ информации полученной из разных источников	Не достаточно хорошо как осуществляется анализ информации полученной из разных источников	Знает как осуществляется анализ информации полученной из разных источников с замечаниями	Хорошо знает как осуществляется анализ информации полученной из разных источников без замечаний

	соответствии с требованиями и условиями задачи.	Уметь У2 Систематизировать информацию полученную из разных источников в соответствии с требованиями и условиями задачи	Не умеет систематизировать информацию полученную из разных источников в соответствии с требованиями и условиями задачи	Не достаточно хорошо систематизировать информацию полученную из разных источников в соответствии с требованиями и условиями задачи	Знает как систематизировать информацию полученную из разных источников в соответствии с требованиями и условиями задачи	Со знанием дела систематизирует информацию полученную из разных источников в соответствии с требованиями и условиями задачи
		Владеть В2 навыками поиска , анализа и синтеза информации, системным подходом для решения поставленных задач	Не владеет навыками поиска , анализа и синтеза информации, системным подходом для решения поставленных задач	Не достаточно хорошо владеет навыками поиска , анализа и синтеза информации, системным подходом для решения поставленных задач	Владеет навыками поиска , анализа и синтеза информации, системным подходом для решения поставленных задач	отлично владеет навыками поиска, анализа и синтеза информации, системным подходом для решения поставленных задач
	УК-1.3. Использует методики системного подхода при решении поставленных задач.	Знать: З3 – методики поиска, сбора и обработки информации; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности; метод системного анализа	Не знает методики поиска, сбора и обработки информации; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности; метод системного анализа	Недостаточно знает методики поиска, сбора и обработки информации; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности; метод системного анализа	Знает методики поиска, сбора и обработки информации; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности; метод системного анализа с замечаниями	Знает методики поиска, сбора и обработки информации; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности; метод системного анализа
		Уметь: У3 – применять методики поиска, сбора и обработки информации; применять системный подход для решения поставленных задач	Не умеет применять методики поиска, сбора и обработки информации; применять системный подход для решения поставленных задач	Некорректно применяет методики поиска, сбора и обработки информации; применять системный подход для решения поставленных задач	Умеет применять методики поиска, сбора и обработки информации; применять системный подход для решения поставленных задач с замечаниями	Умеет методики применять методики поиска, сбора и обработки информации; применять системный подход для решения поставленных задач
		Владеть: В3 – инструментами поиска, сбора и обработки, критического анализа и синтеза информации	Не владеет инструментами поиска, сбора и обработки, критического анализа и синтеза информации	Слабо владеет инструментами поиска, сбора и обработки, критического анализа и синтеза информации	Владеет инструментами поиска, сбора и обработки, критического анализа и синтеза информации с замечаниями	Владеет инструментами поиска, сбора и обработки, критического анализа и синтеза информации

ПКС -4	ПКС-4.2. Разрабатывает мероприятия по обеспечению безопасности на уровне баз данных.	Знать: З4 – угрозы безопасности баз данных и способы их предотвращения; инструменты обеспечения безопасности баз данных и их возможности.	Не знает угрозы безопасности баз данных и способы их предотвращения; инструменты обеспечения безопасности баз данных и их возможности	Слабо знает угрозы безопасности баз данных и способы их предотвращения; инструменты обеспечения безопасности баз данных и их возможности	Знает угрозы безопасности баз данных и способы их предотвращения; инструменты обеспечения безопасности баз данных и их возможности с замечаниями	Знает угрозы безопасности баз данных и способы их предотвращения; инструменты обеспечения безопасности баз данных и их возможности.
		Уметь: У4 – выявлять угрозы безопасности на уровне баз данных; разрабатывать мероприятия по обеспечению безопасности на уровне баз данных	Не умеет выявлять угрозы безопасности на уровне баз данных; разрабатывать мероприятия по обеспечению безопасности на уровне баз данных	Некорректно выявляет угрозы безопасности на уровне баз данных; разрабатывает мероприятия по обеспечению безопасности на уровне баз данных	Умеет выявлять угрозы безопасности на уровне баз данных; разрабатывать мероприятия по обеспечению безопасности на уровне баз данных с замечаниями	Умеет выявлять угрозы безопасности на уровне баз данных; разрабатывать мероприятия по обеспечению безопасности на уровне баз данных
		Владеть: В4– навыками выбора основных средств поддержки информационной безопасности на уровне баз данных	Не владеет навыками выбора основных средств поддержки информационной безопасности на уровне баз данных	Слабо владеет навыками выбора основных средств поддержки информационной безопасности на уровне баз данных	Владеет навыками выбора основных средств поддержки информационной безопасности на уровне баз данных с замечаниями	Владеет навыками выбора основных средств поддержки информационной безопасности на уровне баз данных

Приложение 2

КАРТА
обеспеченности дисциплины учебной и учебно-методической литературой

Дисциплина: **Информационная безопасность и защита информации**
Код, направление подготовки: **09.03.02 Информационные системы и технологии**
Направленность (профиль): **Интеллектуальные системы и технологии «Умный город»**

№ п/п	Название учебного, учебно-методического издания, автор, издательство, вид издания, год издания	Количество экземпляров БИК	Контингент обучающихся, использующих указанную литературу	Обеспеченность обучающихся литературой, %	Наличие электронного варианта в ЭБС (+/-)
1	Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. - Саратов: Профобразование, 2019. - 543 с. - ISBN 978-5-4488-0074-0 – Текст: электронный // ЭБС "IPR BOOKS": [сайт] – URL: http://www.iprbookshop.ru/87992.html	ЭР*	30	100	+
2	Комплексное обеспечение информационной безопасности автоматизированных систем : лабораторный практикум / М. А. Лапина, Д. М. Марков, Т. А. Гиш [и др.]. - Ставрополь : Северо-Кавказский федеральный университет, 2016. - 242 с. – Текст: электронный // ЭБС "IPR BOOKS" – [сайт] – URL: http://www.iprbookshop.ru/62945.html	ЭР*	30	100	+
3	Башлы, П. Н. Информационная безопасность и защита информации: учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва: Евразийский открытый институт, 2012. - 311 с. - ISBN 978-5-374-00301-7 – Текст: электронный // ЭБС "IPR BOOKS" – [сайт] – URL: http://www.iprbookshop.ru/10677.html	ЭР*	30	100	+
4	Артемов, А. В. Информационная безопасность: курс лекций / А. В. Артемов. - Орел : Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. - 256 с. – Текст: электронный // ЭБС "IPR BOOKS". – [сайт] – URL: http://www.iprbookshop.ru/33430.html	ЭР*	30	100	+

ЭР* – электронный ресурс для авторизированных пользователей доступен через Электронный каталог/Электронную библиотеку ТИУ http://webirbis.tsogu.ru/

Лист согласования

Внутренний документ "Информационная безопасность и защита информации_2023_09.03.02_СМАРТб"

Документ подготовил: Зубарева Ирина Васильевна

Документ подписал:

Серийный номер ЭП	Должность	ФИО	ИО	Результат	Дата	Комментарий
49 0B E1 D3 D3 A7 A3 CB	Профессор, имеющий ученую степень доктора наук и ученое звание профессор (базовый уровень)	Данилов Олег Федорович		Согласовано	30.09.2023	
09 07 DF B5 51 36 14 E9	Специалист 1 категории		Радичко Диана Викторовна	Согласовано	03.10.2023	
5A 75 76 26 3B FE 18 E8	Директор	Каюкова Дарья Хрисановна		Согласовано	04.10.2023	