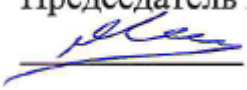
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ИНДУСТРИАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Председатель КСН

О.Н. Кузяков

«10» июня 2019 г.

РАБОЧАЯ ПРОГРАММА

дисциплины: **Информационная безопасность и защита информации**

направление подготовки: **09.03.02 Информационные системы и технологии**

направленность: **Информационные системы и технологии в геологии**

форма обучения: **очная**

Рабочая программа разработана в соответствии с утвержденным учебным планом от 22 апреля 2019г. и требованиями ОПОП ВО по направлению подготовки 09.03.02 Информационные системы и технологии, направленность Информационные системы и технологии к результатам освоения дисциплины «Информационная безопасность и защита информации».

Рабочая программа рассмотрена
на заседании кафедры автомобильного транспорта, дорожных и строительных машин

Протокол № _11_ от «23» ____05____ 2019 г.

Заведующий кафедрой О.Ф.Данилов

СОГЛАСОВАНО:
Заведующий выпускающей кафедрой
Руководитель образовательной программы О.Ф.Данилов

«23» ____05____ 2019 г.

Рабочую программу разработал:

А.И. Вяткин, к.т.н., доцент

1. Цели и задачи освоения дисциплины

Цель освоения дисциплины – изучение 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 относится к дисциплинам части, формируемой участниками образовательных отношений.

Содержание дисциплины является логическим продолжением таких дисциплин, как «Операционные системы» и «Инфокоммуникационные системы и сети».

Содержание дисциплины 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.З1. Знать методики поиска, сбора и обработки информации; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности;	УК-1.З1. Знать методики поиска, сбора и обработки информации; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности;
	УК-1.З2. Знать метод системного анализа	УК-1.З2. Знать метод системного анализа
	УК-1.У1. Уметь применять методики поиска, сбора и обработки информации;	УК-1.У1. Уметь применять методики поиска, сбора и обработки информации;
	УК-1.У2. Уметь осуществлять критический анализ и синтез информации, полученной из разных источников;	УК-1.У2. Уметь осуществлять критический анализ и синтез информации, полученной из разных источников;
	УК-1.У3. Уметь применять системный подход для решения поставленных задач.	УК-1.У3. Уметь применять системный подход для решения поставленных задач.
	УК-1.В1. Владеть методами поиска, сбора и обработки, критического анализа и синтеза информации;	УК-1.В1. Владеть методами поиска, сбора и обработки, критического анализа и синтеза информации;
	УК-1.В2. Владеть методикой системного подхода для решения поставленных задач.	УК-1.В2. Владеть методикой системного подхода для решения поставленных задач.

ПКС 4 – Способность выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности	ПКС-4.З9. Знать угрозы безопасности баз данных и способы их предотвращения;	ПКС-4.З9. Знать угрозы безопасности баз данных и способы их предотвращения;
	ПКС-4.З10. Знать инструменты обеспечения безопасности баз данных и их возможности.	ПКС-4.З10. Знать инструменты обеспечения безопасности баз данных и их возможности.
	ПКС-4.У6. Уметь выявлять угрозы безопасности на уровне баз данных;	ПКС-4.У6. Уметь выявлять угрозы безопасности на уровне баз данных;
	ПКС-4.У7. Уметь разрабатывать мероприятия по обеспечению безопасности на уровне баз данных.	ПКС-4.У7. Уметь разрабатывать мероприятия по обеспечению безопасности на уровне баз данных.
	ПКС-4.В8. Владеть навыками выбора основных средств поддержки информационной безопасности на уровне баз данных.	ПКС-4.В8. Владеть 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.	Форма промежуточной аттестации
		Лекции	Практические занятия	Лабораторные занятия		
очная	4/8	18	-	27	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		1	2	4	УК-1.З1	Вопросы и задания для коллоквиума, Вопросы экзамена, Задания для лабораторных работ
2	2.	Правовое обеспечение информационной безопасности.	1		0	2	3	УК-1.У1	Вопросы коллоквиума, Вопросы экзамена, Задания для лабораторных работ
3	3.	Организационное обеспечение информационной безопасности.	1		0	2	3	УК-1.В1	Вопросы коллоквиума, Вопросы экзамена, Задания для лабораторных работ Задания для самостоятельн

									ой работы
4	4.	Технические средства обеспечения информационной безопасности.	4		6	10	16	ПКС-4.З2	Вопросы коллоквиума, Вопросы экзамена, Задания для лабораторных работ
5	5.	Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах.	1		2	2	5	ПКС-4.У2	Вопросы коллоквиума, Вопросы экзамена, Задания для лабораторных работ
6	6.	Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств.	1		1	2	4	ПКС-4.У2	Вопросы коллоквиума, Вопросы экзамена, Задания для самостоятельной работы
7	7.	Защита от компьютерных вирусов.	1		2	2	5	ПКС-4.У2	Вопросы экзамена, Вопросы экзамена, Задания для самостоятельной работы
8	8.	Криптографическое закрытие информации.	1		2	2	5	ПКС-4.У2	Вопросы экзамена, Вопросы экзамена, Задания для самостоятельной работы
9	9.	Уничтожение остаточных данных.	0		2	2	4	УК-1.В1	Вопросы экзамена, Вопросы экзамена, Задания для самостоятельной работы
10	10.	Защита от потери информации и отказов программно-аппаратных средств.	1		2	2	5	УК-1.У1	Вопросы экзамена, Вопросы экзамена, Задания для самостоятельной работы
11	11.	Защита информационно-программного обеспечения на уровне операционных систем.	1		2	2	5	ПКС-4.У2	Вопросы экзамена, Вопросы экзамена, Задания для самостоятельной работы
12	12.	Защита информации на уровне систем управления базами данных.	1		1	2	4	ПКС-4.З2	Вопросы экзамена, Вопросы экзамена, Задания для самостоятельной работы

13	13.	Специфические особенности защиты информации в локальных и глобальных компьютерных сетях.	4		4	2	6	УК-1.У1	Вопросы экзамена, Вопросы экзамена, Задания для самостоятельной работы
14	14.	Современные средства защиты информации от НСД.	0		2	2	4	УК-2.В2	Вопросы экзамена, Вопросы экзамена, Задания для самостоятельной работы
		Итого:	18		27	36	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).

№ п/п	Наименование раздела дисциплины	Содержание раздела
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.
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.
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.
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.
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.
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.
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.
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.
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.
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.
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.
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.
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.
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	ЗФО	ОЗФО	
1	1	1	0	0	Введение в информационную безопасность.
2	2	1	0	0	Правовое обеспечение информационной безопасности.
3	3	1	0	0	Организационное обеспечение информационной безопасности.
4	4	4	0	0	Технические средства обеспечения информационной безопасности.
5	5	1	0	0	Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах.
6	6	1	0	0	Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств.
7	7	1	0	0	Защита от компьютерных вирусов.
8	8	1	0	0	Криптографическое закрытие информации.
9	9	0	0	0	Уничтожение остаточных данных.
10	10	1	0	0	Защита от потери информации и отказов программно-аппаратных средств.
11	11	1	0	0	Защита информационно-программного обеспечения на уровне операционных систем.
12	12	1	0	0	Защита информации на уровне систем управления базами данных.
13	13	4	0	0	Специфические особенности защиты информации в локальных и глобальных компьютерных сетях.
14	14	0	0	0	Современные средства защиты информации от НСД.
Итого:		18	0	0	

Практические занятия

Практические занятия учебным планом не предусмотрены

Лабораторные работы

Таблица 5.2.2

№ п/п	Номер раздела дисциплины	Объем, час.			Тема лабораторной работы
		ОФО	ЗФО	ОЗФО	
1	3	3	0	0	Управление безопасностью сети.
2	4	3	0	0	Обеспечение безопасности сетевых устройств.
3	5	3	0	0	Аутентификация, авторизация и учет.
4	6	3	0	0	Внедрение технологий межсетевого экрана.
5	7	3	0	0	Обеспечение безопасности локальной сети.
6	8	4	0	0	Анализ способов нарушений информационной безопасности.
7	9	4	0	0	Основные технологии построения защищенных систем.

8	10	4	0	0	Методы криптографии.
Итого:		27	0	0	

Самостоятельная работа студента

Таблица 5.2.3

№ п/п	Номер раздела дисциплины	Объем, час.			Тема	Вид СРС
		ОФО	ЗФО	ОФО		
1	1	2	0	0	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.	Отчет по выполнению самостоятельной работы
2	2	2	0	0	Защита интеллектуальной собственности средствами патентного и авторского права; правовая регламентация охранной деятельности; международное законодательство в области защиты информации.	Отчет по выполнению самостоятельной работы
3	3	2	0	0	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.	Отчет по выполнению самостоятельной работы
4	4	10	0	0	Методологические основы автоматизации технического контроля; основные задачи технического контроля, требующие автоматизированного решения.	Отчет по выполнению самостоятельной работы
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.	Отчет по выполнению самостоятельной работы
6	6	2			Защита программных средств от несанкционированного копирования, исследования и модификации. Привязка программ к среде функционирования. Защита программ от несанкционированного запуска.	Отчет 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.	Отчет по выполнению самостоятельной работы

8	8	2			Режимы шифрования. Особенности шифрования данных в режиме реального времени.	Отчет по выполнению самостоятельной работы
9	9	2			Использование общесистемных и специализированных программных средств для мгновенного уничтожения данных.	Отчет по выполнению самостоятельной работы
10	10	2			Технология восстановления дисковой и оперативной памяти. Диагностирование и устранение логических и физических дефектов магнитных дисков. Восстановление разметки дискеты и корневого каталога	Отчет по выполнению самостоятельной работы
11	11	2			Аппаратная основа реализации защиты на уровне ОС. Стандарты по оценке уровня безопасности ОС. Внесение функциональной и информационной избыточности ресурсов на уровне ОС.	Отчет по выполнению самостоятельной работы
12	12	2			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.	Отчет по выполнению самостоятельной работы
13	13	2			Защита в Internet и Intranet.	Отчет по выполнению самостоятельной работы
14	14	2			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.	Отчет по выполнению самостоятельной работы
Итого:		36	0	0		

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

– решение задач, выполнение практических заданий, проектов (практические занятия);

– работа в малых группах (практические занятия);

– разбор практических ситуаций (лекционные 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

№	Виды контрольных мероприятий	Баллы	№ недели
1	Работа на лабораторных занятиях	0-10	1-5
2	Тест по теоретическому курсу: «Введение в информационную безопасность. Правовое обеспечение информационной безопасности. Организационное обеспечение информационной безопасности. Технические средства обеспечения информационной безопасности».	0-15	5
3	Коллоквиум по СРС	0-5	4
	ИТОГО	**30**	
4	Работа на лабораторных занятиях	0-10	6-10
5	Тест по теоретическому курсу: «Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств. Защита от компьютерных вирусов. Криптографическое закрытие информации. Уничтожение остаточных данных.».	0-15	10
6	Коллоквиум по СРС	0-5	9
	ИТОГО	**30**	
7	Работа на лабораторных занятиях	0-15	11-17
8	Тест по теоретическому курсу: «Защита от потери информации и отказов программно-аппаратных средств. Защита информационно-программного обеспечения на уровне операционных систем. Защита информации на уровне систем управления базами данных. Специфические особенности защиты информации в локальных и глобальных компьютерных сетях. Современные средства защиты информации от НСД.».	0-15	17
9	Коллоквиум по СРС	0-10	16
	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.

1. Собственная полнотекстовая база (ПБД) БИК ТИУ [Электронный ресурс]. Режим доступа: http://elib.tyuiu.ru/
2. Библиотека «E-library» (ООО «РУНЭБ») [Электронный ресурс]. Режим доступа: http://elibrary.ru/
3. ЭБС «Юрайт» [Электронный ресурс]. Режим доступа (https://www.biblio-online.ru).
4. ЭБС издательства «Лань» [Электронный ресурс]. Режим доступа: http://e.lanbook.com.
5. ЭБС IPR BOOKS [Электронный ресурс]. Режим доступа: http://www.iprbookshop.ru/.
6. ЭБС «ПРОСПЕКТ» BOOKS [Электронный ресурс]. Режим доступа: http://ebs.prospekt.org.
7. ЭБС "КОНСУЛЬТАНТ СТУДЕНТА" [Электронный ресурс]. Режим доступа: http://www.studentlibrary.ru/.
8. ЭБС BOOK.RU [Электронный ресурс]. Режим доступа: https://www.book.ru
9. Электронный каталог библиотеки РГУ нефти и газа имени И.М. Губкина [Электронный ресурс]. Режим доступа: http://elib.gubkin.ru/

10. Электронный каталог УГНТУ (г. Уфа). [Электронный ресурс]. Режим доступа: http://bibl.rusoil.net.
11. Электронный каталог библиотеки УГТУ (г. Ухта). [Электронный ресурс]. Режим доступа: http://lib.ugtu.net/books.

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

Таблица 9.1.

Название	Условия доступа
Windows 7 Pro x32/[64	Авторизационный номер: 94360684ZZE1612 Номер лицензии 64448516. Договор № 480-16 от 30 июня 2006 г.
Windows 8.1 Pro x32/[64	
Cisco Packet Tracer 6.2	Бесплатная студенческая версия

10. Материально-техническое обеспечение дисциплины/модуля

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

Таблица 10.1

№ п/п	Перечень оборудования, необходимого для освоения дисциплины/модуля	Перечень технических средств обучения, необходимых для освоения дисциплины/модуля (демонстрационное оборудование)
	Компьютеры с установленным на них ПО (см. Табл. 9.1) – 15 шт.	Моноблок iRUA10510/4130/4Gb/500Gb/HDG4400 /DVDRW/CRW8, мультимедийный экран PanasonicUB-T880W, проектор PanasonicPT-CW330, колонки APart

11. Методические указания по организации СРС

11.1. Методические указания по подготовке к лабораторным занятиям

Порядок подготовки к лабораторным занятиям изложен в следующем учебно-методическом пособии:

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. – 1-е изд.– Тюмень: Издательский центр БИК, ТИУ, 2016. – 21 с.

11.2. Методические указания по организации самостоятельной работы.

Самостоятельная работа обучающихся заключается в подготовке отчетов по лабораторным работам, подготовке к коллоквиумам.

Преподаватель на занятии дает рекомендации, необходимые для выполнения заданий.

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: **Информационные системы и технологии в геологии и нефтегазовой отрасли**

Код компетенции	Код и наименование результата обучения по дисциплине (модулю)	Критерии оценивания результатов обучения			
		1-2	3	4	5
УК-1.	УК-1.З1. Знать методики поиска, сбора и обработки информации; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности; УК-1.З2. Знать метод системного анализа.	Не освоил виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность	Частично освоил виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность	В основном освоил виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность	Полноценно освоил виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность
	УК-1.У1. Уметь применять методики поиска, сбора и обработки информации; УК-1.У2. Уметь осуществлять критический анализ и синтез информации, полученной из разных источников; УК-1.У3. Уметь применять системный подход для решения поставленных задач.	Не умеет проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности	Частично проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности	В основном умеет проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности	Полноценно умеет проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности

	УК-1.В1. Владеть методами поиска, сбора и обработки, критического анализа и синтеза информации; УК-1.В2. Владеть методикой системного подхода для решения поставленных задач.	Не владеет методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта; навыками работы с нормативно-правовой документацией	Частично владеет методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта; навыками работы с нормативно-правовой документацией	В основном владеет методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта; навыками работы с нормативно-правовой документацией	Полноценно владеет методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта; навыками работы с нормативно-правовой документацией
ПКС-4	ПКС-4.З9. Знать угрозы безопасности баз данных и способы их предотвращения; ПКС-4.З10. Знать инструменты обеспечения безопасности баз данных и их возможности.	Не воспроизводит основные стандарты оформления технической документации на различных стадиях жизненного цикла объекта профессиональной деятельности	Воспроизводит некоторые основные стандарты оформления технической документации на различных стадиях жизненного цикла объекта профессиональной деятельности	Частично воспроизводит основные стандарты оформления технической документации на различных стадиях жизненного цикла объекта профессиональной деятельности	Воспроизводит основные стандарты оформления технической документации на различных стадиях жизненного цикла объекта профессиональной деятельности
	ПКС-4.У6. Уметь выявлять угрозы безопасности на уровне баз данных; ПКС-4.У7. Уметь разрабатывать мероприятия по обеспечению безопасности на уровне баз данных.	Не умеет анализировать и применять стандарты, нормы, правила и техническую документацию при решении задач профессиональной деятельности	Умеет анализировать и применять стандарты, нормы, правила и техническую документацию при решении задач профессиональной деятельности, допуская ряд ошибок	Умеет анализировать и применять стандарты, нормы, правила и техническую документацию при решении задач профессиональной деятельности, допуская незначительные ошибки	Умеет анализировать и применять стандарты, нормы, правила и техническую документацию при решении задач профессиональной деятельности
	ПКС-4.В8. Владеть навыками выбора основных средств поддержки информационной безопасности на уровне баз данных.	Не владеет методами составления, компоновки, оформления нормативной и технической документации, адресованной другим специалистам	Владеет методами составления, компоновки, оформления нормативной и технической документации, адресованной другим специалистам , допуская ряд ошибок	Хорошо владеет методами составления, компоновки, оформления нормативной и технической документации, адресованной другим специалистам, допуская незначительные ошибки	В совершенстве владеет методами составления, компоновки, оформления нормативной и технической документации, адресованной другим специалистам

Приложение 2

КАРТА

обеспеченности дисциплины (модуля) учебной и учебно-методической литературой

Дисциплина: **Информационная безопасность и защита информации**
Код, направление подготовки: **09.03.02 Информационные системы и технологии**
Направленность: **Информационные системы и технологии**

№ 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 [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. Текстовые данные.— Саратов: Проф-образование, 2017.— 544 с.— Режим доступа: http://www.iprbookshop.ru/63592.html	ЭР*	20	100	+
2	Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс]: лабораторный практикум/ М.А. Лапина [и др.].— Электрон. текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2016.— 242 с.— Режим доступа: http://www.iprbookshop.ru/62945.html	ЭР*	20	100	+
3	Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 с.— Режим доступа: http://www.iprbookshop.ru/10677.html	ЭР*	20	100	+
4	Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.— Электрон. текстовые данные.— Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.— 256 с.— Режим доступа: http://www.iprbookshop.ru/33430.html	ЭР*	20	100	+

Заведующий кафедрой _____ О.Ф. Данилов

«____» _____ 2019 г.

Директор БИК _____ Д. Х. Каюкова

«____» _____ 2019 г.

М.П.

Согласовано БИК Вайнберг М.И.