ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сведения о сертификате ЭП
Сертификат: 00eb4fb944bb8979c48d4790ead9f8071d
Владелец: Новикова Наталья Геннадьевна
Действителен: с 29.05.2024 по 22.08.2025

УТВЕРЖДЕНО:
Ученым советом Высшей школы сервиса
Протокол № 7 от «17» января 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.ДВ.3.1 ОСНОВЫ ЦИФРОВОЙ БЕЗОПАСНОСТИ

Основной профессиональной образовательной программы высшего образования – программы *бакалавриата*
по направлению подготовки: *43.03.01 Сервис*
на направленность (профиль): *Цифровые сервисы для бизнеса*
Квалификация: *бакалавр*
Год начала подготовки 2025

Разработчик:

должность	ученая степень и звание, ФИО
Доцент высшей школы сервиса	***к.т.н., доцент Деменев А.В.*** ***к.т.н., доцент Минитаева А.М.***

Рабочая программа согласована и одобрена директором ОПОП:

должность	ученая степень и звание, ФИО
Доцент высшей школы сервиса	***к.т.н., доцент Деменев А.В.***

1. Аннотация рабочей программы дисциплины (модуля)

Дисциплина «Основы цифровой безопасности» входит в часть, формируемую участниками образовательного процесса, программы бакалавриата по направлению 43.03.01 Сервис, профиль «Цифровые сервисы для бизнеса».

Содержание дисциплины охватывает круг вопросов, связанных с управлением данными при организации информационного обеспечения в решении задач в сфере жилой и коммерческой недвижимости.

Рассматриваются основы построения информационных систем и технологий, использование специализированных информационных технологий в процессе предоставления услуг, программные средства реализации информационных процессов на предприятиях сервиса. Содержание дисциплины включает вопросы создания баз данных, создания информационных систем, обеспечение безопасности данных в профессиональной деятельности.

Дисциплина направлена на формирование следующих компетенций:

ПК-6 Способен проводить аудит информационных сервисов и обеспечивать безопасность управления данными цифрового предприятия; в части индикаторов достижения компетенции ПК-6.1. (Знает критерии оценки защищенности объекта информатизации, технические средства контроля эффективности мер защиты информации, методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации), ПК-6.2. (Осуществляет контроль обеспечения уровня защищенности информационных сервисов), ПК-6.3. (Оценивает защищенность объектов информатизации с помощью типовых программных средств).

Общая трудоемкость освоения дисциплины составляет 16 зачетных единиц, 576 часов.

Преподавание дисциплины очной формы ведется на 3 курсе: 5,6 семестре, на 4 курсе в 7, 8 семестрах продолжительностью по 18 недель каждый и предусматривает проведение учебных занятий следующих видов: лекции (в форме мультимедийных лекций), практические занятия, включая практическую подготовку (в форме практической работы (демонстрации навыков владения информационной технологией).

Программой дисциплины очной формы обучения предусмотрены:

5-ый семестр - лекционные занятия (34 часов), практические занятия (36 часов), самостоятельная работа студента (70 часов);

6-ой семестр - лекционные занятия (34 часов), практические занятия (36 часов), самостоятельная работа студента (70 часов);

7-ой семестр - лекционные занятия (34 часов), практические занятия (36 часов), самостоятельная работа студента (70 часов);

8-ой семестр - лекционные занятия (34 часов), практические занятия (36 часов), самостоятельная работа студента (70 часов).

Для заочной формы преподавание ведется на 3 курсе 6 семестре, 4 курсе 7,8 семестре, 5 курсе 9 семестре.

Программой дисциплины заочной формы обучения предусмотрены:

6-ой семестр - лекционные занятия (6 часов), практические занятия (8 часов), самостоятельная работа студента (126 часов);

7-ой семестр - лекционные занятия (6 часов), практические занятия (8 часов), самостоятельная работа студента (126 часов);

8-ой семестр - лекционные занятия (10 часов), практические занятия (14 часов), самостоятельная работа студента (116 часов).
9-ый семестр - лекционные занятия (10 часов), практические занятия (14 часов), самостоятельная работа студента (116 часов).

Целью изучения дисциплины «Основы цифровой безопасности» является формирование у обучающихся базовых теоретических знаний в области цифровой безопасности и развитие необходимых практических умений и навыков их применения в будущей профессиональной деятельности и различных предметных областях бизнеса

Программой предусмотрены следующие виды контроля: текущий контроль успеваемости, предусматривающий контроль посещаемости, контроль результатов выполнения заданий для самостоятельной работы студентов (контрольные точки), в том числе контроль в форме демонстрации навыков работы с программными средствами; промежуточная аттестация в форме тестирования и решения практических задач с применением изучаемых информационных технологий. Для очной формы обучения: зачет в 5 семестре, экзамен в 6,7,8 семестрах. Для заочной формы обучения: зачет в 6 семестре, экзамен в 7,8,9 семестрах.

2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

№ пп	Индекс компетенции, индикатора достижения компетенции	Планируемые результаты обучения (компетенции, индикатора достижения компетенции)
1.	ПК-6	Способен проводить аудит информационных сервисов и обеспечивать безопасность управления данными цифрового предприятия.
	ПК-6.1.	Знает критерии оценки защищенности объекта информатизации, технические средства контроля эффективности мер защиты информации, методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации.
	ПК-6.2.	Осуществляет контроль обеспечения уровня защищенности информационных сервисов.
	ПК-6.3	Оценивает защищенность объектов информатизации с помощью типовых программных средств.

3. Место дисциплины (модуля) в структуре ОПОП:

Дисциплина «Основы цифровой безопасности» является вариативной частью программы бакалавриата по направлению 43.03.01 Сервис, профиль «Цифровые сервисы для бизнеса».

Освоение компетенции ПК-6 «Способен проводить аудит информационных сервисов и обеспечивать безопасность управления данными цифрового предприятия» начинается с изучения дисциплины «Цифровое моделирование бизнесс-процессов» в 4 семестре затем продолжается изучение компетенции при параллельном изучении дисциплины «Интеллектуальные цифровые технологии» в 6, 7, 8 семестрах и заканчивает формироваться при написании ВКР.

4. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 16 зачетных единиц/ 576 акад.часов.
(1 зачетная единица соответствует 36 академическим часам)

Для очной формы обучения:

№ п/п	Виды учебной деятельности	Всего	**Семестры**			
			5	**6**	**7**	**8**
1	**Контактная работа обучающихся**	**296**	**74**	**74**	**74**	**74**
	в том числе:	-	-	-	-	-
1.1.	Занятия лекционного типа	136	34	34	34	34
1.2.	Занятия семинарского типа, в том числе:	144	36	36	36	36
	Семинары					
	Лабораторные работы					
	Практические занятия	144	36	36	36	36
1.3.	Консультации	8	2	2	2	2
2.	**Самостоятельная работа**	280	70	70	70	70
3.	**Форма промежуточной аттестации (зачет, экзамен)**	8	**зачет**	**экз.**	**экз.**	**экз.**
			2	**2**	**2**	**2**
4	**Общая трудоемкость, час**	**576**	144	144	144	144
	з.е.	**16**	4	4	4	4

Для заочной формы обучения:

№ п/п	Виды учебной деятельности	Всего	**Семестры**			
			6	**7**	**8**	**9**
1	**Контактная работа обучающихся**	**92**	**18**	**18**	**28**	**28**
	в том числе:	-	-	-	-	-
1.1.	Занятия лекционного типа	32	6	6	10	10
1.2.	Занятия семинарского типа, в том числе:	44	8	8	14	14
	Семинары					
	Лабораторные работы					
	Практические занятия	44	8	8	14	14
1.3.	Консультации	8	2	2	2	2

2.	**Самостоятельная работа**	**484**	**126**	**126**	**116**	**116**
3.	**Форма промежуточной аттестации (зачет, экзамен)**	**8**	**зачет**	**экз.**	**экз.**	**экз.**
			2	**2**	**2**	**2**
4	**Общая трудоемкость час**	**576**	144	144	144	144
	з.е.	**16**	4	4	4	4

5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий
Для очной формы обучения:

Наименование раздела	**Наименование тем лекций, практических работ, лабораторных работ, семинаров, СРО**	**Виды учебных занятий и формы их проведения**											
		Контактная работа обучающихся с преподавателем										СРО, акад. часов	**Форма проведения СРО**
		Занятия лекционного типа, акад. часов	Форма проведения занятия лекционного типа	Практические занятия, акад.часов	Форма проведения практического занятия	Семинары, акад.часов	Форма проведения семинара	Лабораторные работы, акад.часов	Форма проведения лабораторной работы	Консультации, акад. часов	Форма проведения консультации		
5 семестр – Основы баз данных													
1. **Оценка защищенности объекта информатизации (баз данных)**	Тема 1.1.Файловые системы ПЗ: Знакомство с СУБД Access	2	ТЛ	4	ПР								
	Тема 1.2.Принципы организации баз данных. ПЗ: Создание форм в Access.	2		2	ПР							2	
	Тема 1.3. Виды дореляционных баз данных. ПЗ: Создание запросов	2	ТЛ	2	ПР							2	

	Тема 1.4.Основные концепции и термины реляционного подхода к организации БД ПЗ: Создание запросов	2	ТЛ	4	ПР							10	**К.Т.№1 Устный опрос**
	Тема 1.4.Нормализация отношений ПЗ: Создание отчётов	2	ТЛ	2	ПР							2	
	Тема 1.5. Проектирование реляционных баз данных ПЗ: Знакомство с СУБД MySQL	2	ТЛ	2	ПР							2	
	Тема 1.6.Физические структуры данных. ПЗ: Создание структуры БД	2	ТЛ	2	ПР							10	**К.Т.№2 Устный опрос**
	Тема 1.7.Индексы. ПЗ: Добавление данных в БД ПЗ: Выборка данных	4	ТЛ	2	ПР							2	
	Тема 1.8.Транзакции. ПЗ: Создание БД Компьютерная фирма.	2	ТЛ	2	ПР							2	

	Тема 1.9.Контроль доступа к БД. ПЗ: Создание БД Форум.	2	ТЛ	2	ПР							10	**К.Т.№3 Устный опрос**
	Тема 1.10.Функции и основные возможности SQL. ПЗ: Преобразование вывода и встроенные функции	4	ТЛ	2	ПР							2	
	Тема 1.11.Средства SQL для работы со структурой таблицы. ПЗ: Вычисляемые столбцы	2	ТЛ	2	ПР							2	
	Тема 1.12.Средства манипулирования данными SQL. ПЗ: Вывод данных в случае NULL-значений.	2	ТЛ	2	ПР							2	
	Тема 1.13.Операторы для условий и функций. ПЗ: Соединения таблиц	2	ТЛ	2	ПР							2	
	Тема 1.14.Представления. ПЗ: Соединения таблиц	2	ТЛ	**4**	**ПР**							20	**К.т.№4 Уст-ный опрос**
	Консультация									2			
Итог:		**34**		**36**						**2**		**70**	
6 семестр – Базы данных													

2. **Контроль обеспечения уровня защищенности объекта информатизации (баз данных).**	Тема 2.1. Использование SQL в прикладном программировании. Статический SQL. ПЗ: Знакомство с СУБД PostgreSQL	2	ТЛ	4	ПР							2	
	Тема 2.1. Динамический SQL и API. ПЗ: Транзакции в PostgreSQL.	2	ТЛ	4	ПР							2	
	Тема 2.2. Основные требования к распределённой БД. ПЗ: Создание БД Авиаперевозки в PostgreSQL	2	ТЛ	2	ПР							2	
	Тема 2.3. Разновидности распределённых баз данных. ПЗ: Создание БД Авиаперевозки.	2	ТЛ	2	ПР							2	
	Тема 2.4. Объектно-ориентированные БД. ПЗ: Восстановление из резервной копии БД Авиаперевозки	2	ТЛ	2	ПР							10	**К.т. №1**
	Тема 2.5. Другие виды баз данных. ПЗ: Простые виды запросов в PostgreSQL.	2	ТЛ	2	ПР							2	

	Тема 2.6. Базовые инструменты СУБД PostgreSQL. ПЗ: Агрегатные функции.	2	ТЛ	2	ПР							2	
	Тема 2.7. Конфигурирование сервера PostgreSQL. ПЗ: Оконные функции в PostgreSQL	2	ТЛ	2	ПР							2	
	Тема 2.8. Архитектура PostgreSQL. ПЗ: Массивы в PostgreSQL.	2	ТЛ	2	ПР							2	
	Тема 2.9. Многоверсионность, изоляция, очистка данных. ПЗ: Рекурсивные запросы.	2	ТЛ	2	ПР							12	**К.т. №2**
	Тема 2.10. Управление данными. Схемы и табличные пространства. ПЗ: Функции и расширения.	2	ТЛ	2	ПР							2	
	Тема 2.11. Управление доступом. Роли и атрибуты. Привилегии. ПЗ: Полнотекстовый поиск.	2	ТЛ	2	ПР							2	
	Тема 2.12. Управление доступом. Политики защиты строк. Аутентификация. ПЗ: Работа с JSON и	4	ТЛ	2	ПР							11	**К.т.№3**

	JSONB.												
	Тема 2.13. Резервное копирование. ПЗ: PostgeSQL для приложения. Создание пользователя.	2	ТЛ	2	ПР							2	
	Тема 2.14. Репликация в PostgeSQL.	2	ТЛ	4	ПР							**15**	**К.т.№ 4 Уст-ный опрос**
	Консультация									2			
Итог:		**34**		**36**								**70**	
7 **семестр – Основы информационной безопасности геоинформационных технологий и систем**													
3. **Информационная безопасность геоинформационных систем**	Тема 3.1.Введение информационную безопасность геоинформационных систем . ПЗ: Создание ситуационного плана	2	ТЛ	2	ПР							2	
	Тема 3.2.Возможности защиты данных ГИС ПЗ: Создание ситуационного плана.	2	ТЛ	2	ПР							2	
	Тема 3.3 Растровые модели. ПЗ: Работа со слоями и подписями.	4	ТЛ	4	ПР							12	**К.т. №1**

	ПЗ: Инструменты выбора.												
	Тема 3.4 Векторные модели. ПЗ: Оцифровка части карты и создание БД.	2	ТЛ	2	ПР							2	
	Тема 3.5 Принципы организации защиты данных в ГИС. ПЗ: Оцифровка снимка.	2	ТЛ	2	ПР							2	
	Тема 3.6 Основы оцифровки карт. ПЗ: Геокодирование.	2	ТЛ	4	ПР							2	
	Тема 3.7 Тестирование цифровых карт. ПЗ: Трассировка полигонов.	2	ТЛ	2	ПР							12	**К.т. №2**
	Тема 3.8 Анализ защиты данных в ГИС. Ч1. ПЗ: Тематические карты и оверлей.	2	ТЛ	6	ПР							2	
	Тема 3.9 Анализ защиты данных в ГИС. Ч2. ПЗ: Совмещение растрового и векторного изображений.	2	ТЛ	2	ПР							2	
	Тема 3.10 Защита от атак типа “отказ в обслуживании” (denial of service) и нарушение функционирования или	4	ТЛ	2	ПР							12	**К.т. №3**

	выведение из строя ГИС-сервера. Работа с программным пакетом ArcGIS. Структура и возможности. ПЗ: Геогруппы.												
	Тема 3.11 Дополнительные модули ArcGIS Desktop. ПЗ: Буферные зоны и объединение областей.	2	ТЛ	2	ПР							2	
	Тема 3.12 Пространственный анализ в ArcGIS. Модуль Spatial Analyst. ПЗ: Создание трехмерной карты и карты призмы.	2	ТЛ	2	ПР							2	
	Тема 3.13 Некоторые типы данных в ArcGIS. ПЗ: Создание отчёта.	6	ТЛ	4	ПР							16	**К.т.№4**
	Консультация									2			
Итог:		**34**		**36**								**70**	
8 семестр – Информационная безопасность и работа с 1С: Битрикс 24.													
4. **Информационная безопасность и работа с 1С: Битрикс 24.**	Тема 4.1. Система защиты технологии дистанционного зондирование Земли. Л: Обработка снимков ДЗЗ. ПЗ: Создание тематической карты в QGIS.	2	ТЛ	4	ПР							2	
	Тема 4.2 Система защиты	2	ТЛ	2	ПР							2	

	технологии дистанционного зондирования. ПЗ: Создание и выполнение задачи в 1С Битрикс 24.												
	Тема 4.3 Система защиты спутниковых систем навигации. ПЗ: Векторизация карты-схемы в QGIS.	2	ТЛ	4	ПР							10	**К.т.№1**
	Тема 4.4.Принципы работы СНС. ПЗ: Создание и выполнение задачи в 1С Битрикс 24.	2	ТЛ	2	ПР							2	
	Тема 4.5. Методы позиционирования. ПЗ: Анализ пространственных отношений в QGIS.	4	ТЛ	4	ПР							10	**К.т.№2**
	Тема 4.6. Основные понятия безопасности в ИС. ПЗ: Создание и выполнение задачи в 1С Битрикс 24	2	ТЛ	2	ПР							2	
	Тема 4.7. Виды угроз безопасности в ИС. ПЗ: Оптимизация местоположения в QGIS.	2	ТЛ	4	ПР							2	
	Тема 4.8. Принципы обеспечения безопасности	2	ТЛ	2	ПР							2	

	и контрмеры. ПЗ: Создание и выполнение задачи в 1С Битрикс 24												
	Тема 4.9 Организационная составляющая системы безопасности ИС. ПЗ: Анализ транспортных сетей	2	ТЛ	2	ПР							10	**К.т.№3**
	Тема 4.10 Обязанности ответственных за безопасность. ПЗ: Создание и выполнение задачи в 1С Битрикс 24	2	ТЛ	2	ПР							2	
	Тема 4.11 Средства защиты от несанкционированного доступа. ПЗ: Адресное геокодирование.	2	ТЛ	2	ПР							2	
	Тема 4.12 Классификация уязвимостей и атак в сетях. ПЗ: Создание и выполнение задачи в 1С Битрикс 24	4	ТЛ	2	ПР							2	
	Тема 4.13. Методики анализа защищенности ИС.	4	ТЛ		ПР							2	
	Тема 4.14 Сканеры защищенности веб-сайтов.	2	ТЛ	**4**	ПП							**20**	**К.т.№4 Уст-ный**

													опрос
	Консультация									2			
		34		**36**									

Для заочной формы обучения:

Наименование раздела	**Наименование тем лекций, практических работ, лабораторных работ, семинаров, СРО**	**Виды учебных занятий и формы их проведения**											
		Контактная работа обучающихся с преподавателем										СРО, акад. часов	**Форма проведения СРО**
		Занятия лекционного типа, акад. часов	Форма проведения занятия лекционного типа	Практические занятия, акад.часов	Форма проведения практического занятия	Семинары, акад.часов	Форма проведения семинара	Лабораторные работы, акад.часов	Форма проведения лабораторной работы	Консультации, акад. часов	Форма проведения консультации		
6 семестр – Основы баз данных													
1. Оценка защищенности объекта информатизации (баз данных)	Тема 1.1.Файловые системы ПЗ: Знакомство с СУБД Access	1	ТЛ									8	
	Тема 1.2.Принципы организации баз данных. ПЗ: Создание форм в Access.	1										8	
	Тема 1.3. Виды дореляционных баз данных. ПЗ: Создание запросов	0		1	ПР							10	

	Тема 1.4.Основные концепции и термины реляционного подхода к организации БД ПЗ: Создание запросов	0		1	ПР							8	**К.Т. №1 Устный опрос**
	Тема 1.4.Нормализация отношений ПЗ: Создание отчётов	0,5	ТЛ									8	
	Тема 1.5. Проектирование реляционных баз данных ПЗ: Знакомство с СУБД MySQL	0		1	ПР							10	
	Тема 1.6.Физические структуры данных. ПЗ: Создание структуры БД	0		1	ПР							8	**К.Т. №2 Устный опрос**
	Тема 1.7.Индексы. ПЗ: Добавление данных в БД ПЗ: Выборка данных	0,5	ТЛ									8	

	Тема 1.8.Транзакции. ПЗ: Создание БД Компьютерная фирма.	0										8	
	Тема 1.9.Контроль доступа к БД. ПЗ: Создание БД Форум.	0		1	ПР							8	**К.Т. №3 Устный опрос**
	Тема 1.10.Функции и основные возможности SQL. ПЗ: Преобразование вывода и встроенные функции	0,5	ТЛ									8	
	Тема 1.11.Средства SQL для работы со структурой таблицы. ПЗ: Вычисляемые столбцы	0		1	ПР							8	
	Тема 1.12.Средства манипулирования данными SQL. ПЗ: Вывод данных в случае NULL-значений.	0,5	ТЛ										
	Тема 1.13.Операторы для условий и функций. ПЗ: Соединения таблиц	0										8	
	Тема 1.14.Представления.	2	ТЛ	2	**ПР**							10	**К.т.№ 4 ПР**

	ПЗ: Соединения таблиц												
	Консультация									2			
Итог:		**6**		**8**						**2**		**126**	
7 семестр – Базы данных													
2. Контроль обеспечения уровня защищенности объекта информатизации (баз данных).	Тема 2.1. Использование SQL в прикладном программировании. Статический SQL. ПЗ: Знакомство с СУБД PostgreSQL	1	ТЛ		ПР							6	
	Тема 2.1. Динамический SQL и API. ПЗ: Транзакции в PostgreSQL.	1	ТЛ		ПР							8	
	Тема 2.2. Основные требования к распределённой БД. ПЗ: Создание БД Авиаперевозки в PostgreSQL		ТЛ	1	ПР							8	
	Тема 2.3. Разновидности распределённых баз данных. ПЗ: Создание БД Авиаперевозки.		ТЛ	1	ПР							8	

	Тема 2.4. Объектно-ориентированные БД. ПЗ: Восстановление из резервной копии БД Авиаперевозки	0,5	ТЛ		ПР							8	**К.т. №1**
	Тема 2.5. Другие виды баз данных. ПЗ: Простые виды запросов в PostgreSQL.	0	ТЛ	1	ПР							6	
	Тема 2.6. Базовые инструменты СУБД PostgreSQL. ПЗ: Агрегатные функции.		ТЛ	1	ПР							8	
	Тема 2.7. Конфигурирование сервера PostgreSQL. ПЗ: Оконные функции в PostgreSQL	0,5	ТЛ		ПР							8	
	Тема 2.8. Архитектура PostgreSQL. ПЗ: Массивы в PostgreSQL.		ТЛ		ПР							8	
	Тема 2.9. Многоверсионность, изоляция, очистка данных. ПЗ: Рекурсивные запросы.		ТЛ	1	ПР							8	**К.т. №2**

	Тема 2.10. Управление данными. Схемы и табличные пространства. ПЗ: Функции и расширения.	0,5	ТЛ		ПР							8	
	Тема 2.11. Управление доступом. Роли и атрибуты. Привилегии. ПЗ: Полнотекстовый поиск.		ТЛ	1	ПР							8	
	Тема 2.12. Управление доступом. Политики защиты строк. Аутентификация. ПЗ: Работа с JSON и JSONB.	0,5	ТЛ		ПР							8	**К.т.№ 3**
	Тема 2.13. Резервное копирование. ПЗ: PostgeSQL для приложения. Создание пользователя.		ТЛ		ПР							8	
	Тема 2.14. Репликация в PostgeSQL.	2	ТЛ	2	**ПР**							10	**К.т.№ 4 ПР**
	Консультация									2			
Итог:		**6**		**8**								**126**	
8 семестр – Основы информационной безопасности геоинформационных технологий и систем													
3. Информационная безопасность геоинформационных систем	Тема 3.1.Введение информационную безопасность геоинформационных	1	ТЛ	1	ПР							6	

	систем . ПЗ: Создание ситуационного плана												
	Тема 3.2.Возможности защиты данных ГИС ПЗ: Создание ситуационного плана.	1	ТЛ									8	
	Тема 3.3 Растровые модели. ПЗ: Работа со слоями и подписями. ПЗ: Инструменты выбора.	1	ТЛ	1	ПР							8	**К.т. №1**
	Тема 3.4 Векторные модели. ПЗ: Оцифровка части карты и создание БД.		ТЛ	1	ПР							8	
	Тема 3.5 Принципы организации защиты данных в ГИС. ПЗ: Оцифровка снимка.	1	ТЛ	1	ПР							8	
	Тема 3.6 Основы оцифровки карт. ПЗ: Геокодирование.	1	ТЛ	1	ПР							8	
	Тема 3.7 Тестирование цифровых карт. ПЗ: Трассировка полигонов.		ТЛ	1	ПР							6	**К.т. №2**
	Тема 3.8 Анализ защиты данных в ГИС. Ч1.	1	ТЛ	1	ПР							8	

	ПЗ: Тематические карты и оверлей.												
	Тема 3.9 Анализ защиты данных в ГИС. Ч2. ПЗ: Совмещение растрового и векторного изображений.		ТЛ	1	ПР							8	
	Тема 3.10 Защита от атак типа “отказ в обслуживании” (denial of service) и нарушение функционирования или выведение из строя ГИС-сервера. Работа с программным пакетом ArcGIS. Структура и возможности. ПЗ: Геогруппы.	1	ТЛ	1	ПР							8	**К.т. №3**
	Тема 3.11 Дополнительные модули ArcGIS Desktop. ПЗ: Буферные зоны и объединение областей.	1	ТЛ	1	ПР							8	
	Тема 3.12 Пространственный анализ в ArcGIS. Модуль Spatial Analyst. ПЗ: Создание трехмерной карты и карты призмы.		ТЛ	2	ПР							8	
	Тема 3.13 Некоторые	2	ТЛ	2	**ПР**							10	**К.т.№**

	типы данных в ArcGIS. ПЗ: Создание отчёта.												**4 ПР**
	Консультация									2			
Итог:		**10**		**14**								**116**	
9 семестр – Информационная безопасность и работа с 1С: Битрикс 24.													
4. Информационная безопасность и работа с 1С: Битрикс 24.	Тема 4.1. Система защиты технологии дистанционного зондирование Земли. Л: Обработка снимков ДЗЗ. ПЗ: Создание тематической карты в QGIS.	1	ТЛ	1	ПР							6	
	Тема 4.2 Система защиты технологии дистанционного зондирования. ПЗ: Создание и выполнение задачи в 1С Битрикс 24.	1	ТЛ		ПР							8	
	Тема 4.3 Система защиты спутниковых систем навигации. ПЗ: Векторизация карты-схемы в QGIS.	1	ТЛ	2	ПР							6	**К.т.№ 1**
	Тема 4.4.Принципы работы СНС. ПЗ: Создание и выполнение задачи в 1С Битрикс 24.			1	ПР							8	

	Тема 4.5. Методы позиционирования. ПЗ: Анализ пространственных отношений в QGIS.	1	ТЛ	1	ПР							8	**К.т.№ 2**
	Тема 4.6. Основные понятия безопасности в ИС. ПЗ: Создание и выполнение задачи в 1С Битрикс 24	1	ТЛ	2	ПР							6	
	Тема 4.7. Виды угроз безопасности в ИС. ПЗ: Оптимизация местоположения в QGIS.			1	ПР							6	
	Тема 4.8. Принципы обеспечения безопасности и контрмеры. ПЗ: Создание и выполнение задачи в 1С Битрикс 24	1	ТЛ	1	ПР							8	
	Тема 4.9 Организационная составляющая системы безопасности ИС. ПЗ: Анализ транспортных сетей	1	ТЛ	1	ПР							8	**К.т.№ 3**
	Тема 4.10 Обязанности ответственных за безопасность.			1	ПР							6	

	ПЗ: Создание и выполнение задачи в 1С Битрикс 24												
	Тема 4.11 Средства защиты от несанкционированного доступа. ПЗ: Адресное геокодирование.	1	ТЛ	1	ПР							8	
	Тема 4.12 Классификация уязвимостей и атак в сетях. ПЗ: Создание и выполнение задачи в 1С Битрикс 24			2	ПР							6	
	Тема 4.13. Методики анализа защищенности ИС.	2	ТЛ	1	ПР							8	
	Тема 4.14 Сканеры защищенности веб-сайтов.	1	ТЛ	2	**ПР**							10	**К.т.№ 4 ПР**
	Консультация									2			
		10		**14**						**2**		**116**	

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

№ п/п	Тема, трудоемкость в акад.ч.	Учебно-методическое обеспечение
5/6* семестр		
1.	Тема 1.1.Файловые системы 2 / 8 часов	**Основная литература** 1.Бабаш, А. В., Криптографические методы защиты информации : учебник / А. В. Бабаш, Е. К. Баранова. — Москва : КноРус, 2024. — 189 с. — ISBN 978-5-406-11913-6. — URL: https://book.ru/book/949929 2.Дергачев, К. В., Защита информации: лабораторный практикум : учебное пособие / К. В. Дергачев, Д. В. Титарев. — Москва : Русайнс, 2026. — 158 с. — ISBN 978-5-466-09618-7. — URL: https://book.ru/book/958732 . — Текст : электронный. 3.Максуров, А. А., Правовое обеспечение качества продукции (товаров, работ, услуг) : монография / А. А. Максуров. — Москва : Русайнс, 2022. — 100 с. — ISBN 978-5-4365-7506-3. — URL: https://book.ru/book/943421 **Дополнительная литература** 1.Краковский, Ю. М. Защита информации: Учебное пособие (ФГОС) / Краковский Ю.М. - Ростов-на-Дону :Феникс, 2016. - 347 с.ISBN 978-5-222-26911-4. - Текст : электронный. - URL: https://znanium.ru/catalog/document?pid=908844 2.Введение в системное проектирование интеллектуальных баз знаний : монография / С. А. Баркалов, А. В. Душкин, С. А. Колодяжный, В. И. Сумин ; под общ. ред. доктора техн. наук, профессора В. И. Новосельцева. - Москва : Горячая линия-Телеком, 2017. - 108 с. - ISBN 978-5-9912-0589-4. - Текст : электронный. - URL: https://znanium.ru/catalog/document?pid=1911606 3.Москвитин, Г. И., Комплексная защита информации в организации : монография / Г. И. Москвитин. — Москва : Русайнс, 2020. — 354 с. — ISBN 978-5-4365-1561-8. — URL: https://book.ru/book/934814 4.Берикашвили, В. Ш., Теория передачи информации : учебник / В. Ш. Берикашвили, С. З. Шкундин, С. П. Оськин. — Москва : КноРус, 2024. — 238 с. — ISBN 978-5-406-12428-4. — URL: https://book.ru/book/951858
1.	Тема 1.2.Принципы организации баз данных. 2 / 8 часов	
2.	Тема 1.3. Виды дореляционных баз данных. 10 / 10 часов	
3.	Тема 1.4.Нормализация отношений 2 / 8 часов	
4.	Тема 1.4.Основные концепции и термины реляционного подхода к организации БД 2 / 8 часов	
5.	Тема 1.5. Проектирование реляционных баз данных 10 / 10 часов	
6.	Тема 1.6.Физические структуры данных. 2 / 8 часов	
7.	Тема 1.7.Индексы. 2 / 8 часов	
8.	Тема 1.8.Транзакции. 10 / 8 часов	
9.	Тема 1.9.Контроль доступа к БД. 2 / 8 часов	
10.	Тема 1.10.Функции и основные возможности SQL. 2 / 8 часов	
11.	Тема 1.11.Средства SQL для работы со структурой таблицы. 2 / 8 часов	
12.	Тема 1.12.Средства манипулирования данными SQL. 2 / 8 часов	
13.	Тема 1.13.Операторы для условий и функций. 20 / 10 часов	
14.	Тема 1.14.Представления. 2 / 8 часов	
6/7* семестр		
15.	Тема 2.1. Динамический SQL и API. 2 / 6 часов	**Основная литература** 1.Бабаш, А. В., Криптографические методы защиты информации : учебник / А. В. Бабаш, Е. К. Баранова. — Москва : КноРус, 2024. — 189 с. — ISBN 978-5-406-11913-6. — URL: https://book.ru/book/949929
1.	Тема 2.1. Использование SQL в прикладном программировании. Статический SQL. 2 / 8 часов	

2.	Тема 2.2. Основные требования к распределённой БД. 2 / 8 часов	2.Дергачев, К. В., Защита информации: лабораторный практикум : учебное пособие / К. В. Дергачев, Д. В. Титарев. — Москва : Русайнс, 2026. — 158 с. — ISBN 978-5-466-09618-7. — URL: https://book.ru/book/958732 . — Текст : электронный. 3.Максуров, А. А., Правовое обеспечение качества продукции (товаров, работ, услуг) : монография / А. А. Максуров. — Москва : Русайнс, 2022. — 100 с. — ISBN 978-5-4365-7506-3. — URL: https://book.ru/book/943421 **Дополнительная литература** 1.Краковский, Ю. М. Защита информации: Учебное пособие (ФГОС) / Краковский Ю.М. - Ростов-на-Дону :Феникс, 2016. - 347 с.ISBN 978-5-222-26911-4. - Текст : электронный. - URL: https://znanium.ru/catalog/document?pid=908844 2.Введение в системное проектирование интеллектуальных баз знаний : монография / С. А. Баркалов, А. В. Душкин, С. А. Колодяжный, В. И. Сумин ; под общ. ред. доктора техн. наук, профессора В. И. Новосельцева. - Москва : Горячая линия-Телеком, 2017. - 108 с. - ISBN 978-5-9912-0589-4. - Текст : электронный. - URL: https://znanium.ru/catalog/document?pid=1911606 3.Москвитин, Г. И., Комплексная защита информации в организации : монография / Г. И. Москвитин. — Москва : Русайнс, 2020. — 354 с. — ISBN 978-5-4365-1561-8. — URL: https://book.ru/book/934814 4.Берикашвили, В. Ш., Теория передачи информации : учебник / В. Ш. Берикашвили, С. З. Шкундин, С. П. Оськин. — Москва : КноРус, 2024. — 238 с. — ISBN 978-5-406-12428-4. — URL: https://book.ru/book/951858
3.	Тема 2.3. Разновидности распределённых баз данных. 2 / 8 часов	
4.	Тема 2.4. Объектно-ориентированные БД. 10 / 8 часов	
5.	Тема 2.5. Другие виды баз данных. 2 / 6 часов	
6.	Тема 2.6. Базовые инструменты СУБД PostgreSQL. 2 / 8 часов	
7.	Тема 2.7. Конфигурирование сервера PostgreSQL. 2 / 8 часов	
8.	Тема 2.8. Архитектура PostgreSQL. 2 / 8 часов	
9.	Тема 2.9. Многоверсионность, изоляция, очистка данных. 12 / 8 часов	
10.	Тема 2.10. Управление данными. Схемы и табличные пространства. 2 / 8 часов	
11.	Тема 2.11. Управление доступом. Роли и атрибуты. Привилегии. 2 / 8 часов	
12.	Тема 2.12. Управление доступом. Политики защиты строк. Аутентификация. 11 / 8 часов	
13.	Тема 2.13. Резервное копирование. 2 / 8 часов	
14.	Тема 2.14. Репликация в PostgeSQL. 15 / 6 часов	
7/8* семестр		
15.	Тема 3.1.Введение информационную безопасность геоинформационных систем . 2 / 6 часов	**Основная литература** 1.Бабаш, А. В., Криптографические методы защиты информации : учебник / А. В. Бабаш, Е. К. Баранова. — Москва : КноРус, 2024. — 189 с. — ISBN 978-5-406-11913-6. — URL: https://book.ru/book/949929 2.Дергачев, К. В., Защита информации: лабораторный практикум : учебное пособие / К. В. Дергачев, Д. В. Титарев. — Москва : Русайнс, 2026. — 158 с. — ISBN 978-5-466-09618-7. — URL: https://book.ru/book/958732 . — Текст : электронный. 3.Максуров, А. А., Правовое обеспечение качества продукции (товаров, работ, услуг) : монография / А. А. Максуров. — Москва : Русайнс, 2022. — 100 с. — ISBN 978-5-4365-7506-3. — URL: https://book.ru/book/943421 **Дополнительная литература** 1.Краковский, Ю. М. Защита информации: Учебное
1.	Тема 3.2.Возможности защиты данных ГИС 2 / 8 часов	
2.	Тема 3.3 Растровые модели.12 / 8 часов	
3.	Тема 3.4 Векторные модели. 2 / 8 часов	
4.	Тема 3.5 Принципы организации защиты данных в ГИС. 2 / 8 часов	
5.	Тема 3.6 Основы оцифровки карт. 2 / 8 часов	
6.	Тема 3.7 Тестирование цифровых карт. 12 / 6 часов	
7.	Тема 3.8 Анализ защиты данных в ГИС. Ч1. 2 / 8 часов	

8.	Тема 3.9 Анализ защиты данных в ГИС. Ч2. 2 / 8 часов	пособие (ФГОС) / Краковский Ю.М. - Ростов-на-Дону :Феникс, 2016. - 347 с.ISBN 978-5-222-26911-4. - Текст : электронный. - URL: https://znanium.ru/catalog/document?pid=908844 2.Введение в системное проектирование интеллектуальных баз знаний : монография / С. А. Баркалов, А. В. Душкин, С. А. Колодяжный, В. И. Сумин ; под общ. ред. доктора техн. наук, профессора В. И. Новосельцева. - Москва : Горячая линия-Телеком, 2017. - 108 с. - ISBN 978-5-9912-0589-4. - Текст : электронный. - URL: https://znanium.ru/catalog/document?pid=1911606 3.Москвитин, Г. И., Комплексная защита информации в организации : монография / Г. И. Москвитин. — Москва : Русайнс, 2020. — 354 с. — ISBN 978-5-4365-1561-8. — URL: https://book.ru/book/934814 4.Берикашвили, В. Ш., Теория передачи информации : учебник / В. Ш. Берикашвили, С. З. Шкундин, С. П. Оськин. — Москва : КноРус, 2024. — 238 с. — ISBN 978-5-406-12428-4. — URL: https://book.ru/book/951858
9.	Тема 3.10 Защита от атак типа “отказ в обслуживании” (denial of service) и нарушение функционирования или выведение из строя ГИС-сервера. Работа с программным пакетом ArcGIS. Структура и возможности. 12 / 8 часов	
10.	Тема 3.11 Дополнительные модули ArcGIS Desktop. 2 / 8 часов	
11.	Тема 3.12 Пространственный анализ в ArcGIS. Модуль Spatial Analyst.2/8часов	
12.	Тема 3.13 Некоторые типы данных в ArcGIS. 16/10часов	
8/9* семестр		
13.	Тема 4.1. Система защиты технологии дистанционного зондирование Земли. 2/6часов	**Основная литература** 1.Бабаш, А. В., Криптографические методы защиты информации : учебник / А. В. Бабаш, Е. К. Баранова. — Москва : КноРус, 2024. — 189 с. — ISBN 978-5-406-11913-6. — URL: https://book.ru/book/949929 2.Дергачев, К. В., Защита информации: лабораторный практикум : учебное пособие / К. В. Дергачев, Д. В. Титарев. — Москва : Русайнс, 2026. — 158 с. — ISBN 978-5-466-09618-7. — URL: https://book.ru/book/958732 . — Текст : электронный. 3.Максуров, А. А., Правовое обеспечение качества продукции (товаров, работ, услуг) : монография / А. А. Максуров. — Москва : Русайнс, 2022. — 100 с. — ISBN 978-5-4365-7506-3. — URL: https://book.ru/book/943421 **Дополнительная литература** 1.Краковский, Ю. М. Защита информации: Учебное пособие (ФГОС) / Краковский Ю.М. - Ростов-на-Дону :Феникс, 2016. - 347 с.ISBN 978-5-222-26911-4. - Текст : электронный. - URL: https://znanium.ru/catalog/document?pid=908844 2.Введение в системное проектирование интеллектуальных баз знаний : монография / С. А. Баркалов, А. В. Душкин, С. А. Колодяжный, В. И. Сумин ; под общ. ред. доктора техн. наук, профессора В. И. Новосельцева. - Москва : Горячая линия-Телеком, 2017. - 108 с. - ISBN 978-5-9912-0589-4. - Текст : электронный. - URL: https://znanium.ru/catalog/document?pid=1911606 3.Москвитин, Г. И., Комплексная защита
1.	Тема 4.2 Система защиты технологии дистанционного зондирования. 2/8 часов	
2.	Тема 4.3 Система защиты спутниковых систем навигации. 10/6часов	
3.	Тема 4.4.Принципы работы СНС. 2/8 часов	
4.	Тема 4.5. Методы позиционирования. 10/8часов	
5.	Тема 4.6. Основные понятия безопасности в ИС. 2/6часов	
6.	Тема 4.7. Виды угроз безопасности в ИС. 2/6 часов	
7.	Тема 4.8. Принципы обеспечения безопасности и контрмеры. 2 / 8 часов	
8.	Тема 4.9 Организационная составляющая системы безопасности ИС. 10 / 8 часов	
9.	Тема 4.10 Обязанности ответственных за безопасность. 2 / 6 часов	
10.	Тема 4.11 Средства защиты от несанкционированного доступа. 2 / 8 часов	
11.	Тема 4.12 Классификация уязвимостей и атак в сетях. 2 / 6 часов	

12.	Тема 4.13. Методики анализа защищенности ИС. 2 / 8 часов	информации в организации : монография / Г. И. Москвитин. — Москва : Русайнс, 2020. — 354 с. — ISBN 978-5-4365-1561-8. — URL: https://book.ru/book/934814 4.Берикашвили, В. Ш., Теория передачи информации : учебник / В. Ш. Берикашвили, С. З. Шкундин, С. П. Оськин. — Москва : КноРус, 2024. — 238 с. — ISBN 978-5-406-12428-4. — URL: https://book.ru/book/951858
13.	Тема 4.14 Сканеры защищенности веб-сайтов. 20 / 10 часов	

7. Фонд оценочных средств для проведения текущей и промежуточной аттестации обучающихся по дисциплине (модулю)

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

№ пп	Индекс компетенции, индикатора достижения компетенции	Содержание компетенции (индикатора достижения компетенции)	Раздел дисциплины, обеспечивающий формирование компетенции (индикатора достижения компетенции)	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции (индикатора достижения компетенции) обучающийся должен:		
				знать	уметь	владеть
1.	ПК-6	Способен проводить аудит информационных сервисов и обеспечивать безопасность управления данными цифрового предприятия				
		ПК-6.1 Знает критерии оценки защищенности объекта информатизации, технические средства контроля эффективности мер защиты информации, методы измерений, контроля и технических расчетом характеристик программно-аппаратных средств защиты информации	Защита практических работ, тестирование	Знает организационные меры по защите информации, основные методы управления защитой информации	Умеет разрабатывать предложения по совершенствованию системы управления защиты информации, осуществлять планирование и организацию работы персонала с учетом требований по защите информации	Владеет навыками выработки рекомендаций для решения о модернизации системы защиты информации
		ПК-6.2. Осуществляет контроль обеспечения уровня защищенности информационных сервисов		Знает современные виды информационного взаимодействия, методы анализа исходных данных для проектирования подсистем обеспечения информационной безопасности	Контролирует работоспособность и эффективность применяемых программных, программно-аппаратных и технических средств защиты информации	Владеет методами анализа проектных решений по обеспечению защищенности информационных сервисов
		ПК-6.3. Оценивает защищенность объектов		Знает программно-аппаратные	Умеет конфигурировать программно-	Владеет принципами

		информатизации с помощью типовых программных средств.		средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях	аппаратные средства защиты информации в соответствии с заданными политиками безопасности	формирования политики информационной безопасности объекта информатизации

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

Результат обучения по дисциплине	Показатель оценивания	Критерий оценивания	Этап освоения компетенции
Знание аудита информационных сервисов, на основе данных и обеспечения безопасности управления данными цифрового предприятия; в части индикаторов достижения компетенции Умение выполнять аудит информационных сервисов, на основе данных и выполнять условия обеспечения безопасности управления данными цифрового предприятия; в части индикаторов достижения компетенции Владение навыками аудита информационных сервисов, на основе данных и выполнять условие обеспечения безопасности управления данными цифрового предприятия; в части индикаторов достижения компетенции	Демонстрация навыков применения методов реализации прикладных систем на основе баз данных при решении ситуационных задач, тестирование	Студент продемонстрировал умение проектировать инфологическую модель базы данных для учебного приложения, проектировать структуру базы данных в среде реляционной СУБД и осуществлять программную реализацию и отладку приложения на языке среднего уровня, использующее для хранения информации базу данных;	Закрепление способности определять потребность в технологических новациях и информационном обеспечении в сервисной деятельности организации

Критерии и шкала оценивания освоения этапов компетенций на промежуточной аттестации

Порядок, критерии и шкала оценивания освоения этапов компетенций на промежуточной аттестации определяется в соответствии с Положением о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования – программам бакалавриата,

программам магистратуры, реализуемым по федеральным государственным образовательным стандартам в ФГБОУ ВО «РГУТИС».

Виды средств оценивания, применяемых при проведении текущего контроля и шкалы оценки уровня знаний, умений и навыков при выполнении отдельных форм текущего контроля.

Критерии оценки при защите практических работ

– оценка 5 «отлично» ставится, если работа выполнена полностью и без ошибок, студент показывает умение проанализировать свои действия и правильно интерпретирует результаты, подробно и точно отвечает на контрольные вопросы.

– оценка 4 «хорошо» ставится, если работа выполнена не полностью или с незначительной ошибкой, студент умеет анализировать свои действия и правильно интерпретирует результаты, хорошо отвечает на контрольные вопросы.

– оценка 3 «удовлетворительно» ставится, если работа выполнена не полностью с ошибками, студент может с помощью преподавателя проанализировать свои действия и интерпретировать результаты, удовлетворительно отвечает на контрольные вопросы.

Шкала оценки уровня знаний, умений и навыков при решении тестовых заданий

Критерии оценки	**оценка**
выполнено верно заданий	«5», если (90 –100)% правильных ответов
	«4», если (70 – 89)% правильных ответов
	«3», если (50 – 69)% правильных ответов
	«2», если менее 50% правильных ответов

Виды средств оценивания, применяемых при проведении промежуточной аттестации и шкалы оценки уровня знаний, умений и навыков при их выполнении

Шкала оценки уровня знаний, умений и навыков при решении тестовых заданий

Критерии оценки	**оценка**
выполнено верно заданий	«5», если (90 –100)% правильных ответов
	«4», если (70 – 89)% правильных ответов
	«3», если (50 – 69)% правильных ответов
	«2», если менее 50% правильных ответов

Виды средств оценивания, применяемых при проведении текущего контроля и шкалы оценки уровня знаний, умений и навыков при выполнении отдельных форм текущего контроля

5/6* семестр – раздел « Оценка защищенности объекта информатизации (баз данных»

Контрольная точка 1. Формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся. Демонстрация навыков владения информационной технологией.

Контрольная точка 2. Формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся. Демонстрация навыков владения информационной технологией. Демонстрация навыков владения информационной технологией.

Контрольная точка 3. Формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся. Демонстрация навыков владения информационной технологией.

Контрольная точка 4. Формализованное наблюдение и оценка **отчета Практической подготовки**, и защита в форме устного опроса обучающихся. Демонстрация навыков владения информационной технологией.

6/7* семестр – Контроль обеспечения уровня защищенности объекта информатизации (баз данных).

Контрольная точка 1. Формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся. Демонстрация навыков владения информационной технологией.

Контрольная точка 2. Формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся. Демонстрация навыков владения информационной технологией. Демонстрация навыков владения информационной технологией.

Контрольная точка 3. Формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся. Демонстрация навыков владения информационной технологией.

Контрольная точка 4. Формализованное наблюдение и оценка отчета Практической подготовки, и защита в форме устного опроса обучающихся. Демонстрация навыков владения информационной технологией.

7/8* семестр –Информационная безопасность геоинформационных систем

Контрольная точка 1. Формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся Демонстрация навыков владения информационной технологией.

Контрольная точка 2. Формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся. Демонстрация навыков владения информационной технологией. Демонстрация навыков владения информационной технологией.

Контрольная точка 3. Формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся.Демонстрация навыков владения информационной технологией.

Контрольная точка 4. Формализованное наблюдение и оценка отчета Практической подготовки, и защита в форме устного опроса обучающихся. Демонстрация навыков владения информационной технологией.

8/9* семестр – Информационная безопасность и работа с 1С: Битрикс 24.

Контрольная точка 1. Формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся. Демонстрация навыков владения информационной технологией.

Контрольная точка 2. Формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся. Демонстрация навыков владения информационной технологией. Демонстрация навыков владения информационной технологией.

Контрольная точка 3. Формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся.Демонстрация навыков владения информационной технологией.

Контрольная точка 4. Формализованное наблюдение и оценка отчета Практической подготовки, и защита в форме устного опроса обучающихся. Демонстрация навыков владения информационной технологией.

Виды средств оценивания, применяемых при проведении промежуточной аттестации и шкалы оценки уровня знаний, умений и навыков при их выполнении

Зачет по дисциплине основывается на результатах выполнения индивидуальных заданий (контрольных точек) студента по данной дисциплине. Форма проведения зачета определяется преподавателем, ведущим данную дисциплину, представлен в п.7.4.

Критерии оценки «зачтено» и «незачтено»

Ответ студента на зачете оценивается одной из следующих оценок: «зачтено» и «незачтено», которые выставляются по следующим критериям.

Оценки «зачтено» заслуживает студент, обнаруживший всестороннее, систематическое и глубокое знание учебного и нормативного материала, умеющий свободно выполнять задания, предусмотренные программой, усвоивший основную и знакомый с дополнительной литературой (п.8), демонстрирующие систематический характер знаний по дисциплине и способные к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.

Оценка «незачтено» выставляется студентам, обнаружившим пробелы в знаниях основного учебного материала, допускающим принципиальные ошибки в выполнении предусмотренных программой заданий. Такой оценки заслуживают ответы студентов, носящие несистематизированный, отрывочный, поверхностный характер, когда студент не понимает существа излагаемых им вопросов, что свидетельствует о том, что студент не может дальше продолжать обучение или приступать к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине

Экзамен по дисциплине проводится в устной (по билетам) или письменной форме (в форме тестирования). Билет содержит теоретические вопросы (ТВ) для проверки усвоенных знаний, практические задания (ПЗ) для проверки освоенных умений и комплексные задания (КЗ) для контроля уровня приобретенных владений всех заявленных дисциплинарных компетенций.

Типовые вопросы и тестовые задания для экзамена приводятся в разделе 7.4.

7.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы.

Номер недели семестра	Раздел дисциплины, обеспечивающий формирование компетенции (или ее части)	Вид и содержание контрольного задания	Требования к выполнению контрольного задания и срокам сдачи
5/6* семестр –Оценка защищенности объекта информатизации (баз данных)			
4	Оценка защищенности объекта информатизации (баз данных)	Контрольная точка 1. Формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся Демонстрация навыков владения информационной технологией.	Демонстрация навыков владения информационной технологией. Устный опрос выполняется в аудитории. Суммарный вес 10 баллов. Выполняется в аудитории. Каждый студент имеет уникальное задание, состоящее из –от 5 до 10 контрольных вопросов. Каждое задание оценивается в баллы: 0 - не сделал; 1 – сделал, допустил 9 ошибки; 2 – сделал, допустил 8 ошибки; 3 – сделал, допустил 7 ошибки; 4 – сделал, допустил 6 ошибку и т.д.
8		Контрольная точка 2. Формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного *опроса* обучающихся. Демонстрация навыков владения информационной технологией. Демонстрация навыков владения информационной технологией.	Демонстрация навыков владения информационной технологией. Устный опрос выполняется в аудитории. Суммарный вес 10 баллов. Выполняется в аудитории. Каждый студент имеет уникальное задание, состоящее из –от 5 до 10 контрольных вопросов. Каждое задание оценивается в баллы: 0 - не сделал; 1 – сделал, допустил 9 ошибки; 2 – сделал, допустил 8 ошибки; 3 – сделал, допустил 7 ошибки; 4 – сделал, допустил 6 ошибку и т.д.
12		Контрольная точка 3. Формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного *опроса* обучающихся. Демонстрация навыков владения информационной технологией.	Демонстрация навыков владения информационной технологией. Устный опрос выполняется в аудитории. Суммарный вес 10 баллов. Выполняется в аудитории. Каждый студент имеет уникальное задание, состоящее из –от 5 до 10 контрольных вопросов. Каждое задание оценивается в баллы: 0 - не сделал; 1 – сделал, допустил 9 ошибки; 2 – сделал, допустил 8 ошибки; 3 – сделал, допустил 7 ошибки; 4 – сделал, допустил 6 ошибку и т.д.
18		Контрольная точка 4. Формализованное наблюдение и оценка **отчета Практической подготовки,** и защита в форме устного *опроса* обучающихся. Демонстрация навыков владения информационной технологией.	Демонстрация навыков владения информационной технологией. Устный опрос выполняется в аудитории. Суммарный вес **15 баллов**. Каждый студент имеет уникальное задание, состоящее из –от 5 до 10 контрольных вопросов. Каждое задание оценивается в баллы: 0 - не сделал; 1 –сделал, допустил 9 ошибки; 2 – сделал, допустил 8 ошибки; 3 – сделал, допустил 7 ошибки; 4 – сделал, допустил 6 ошибку и

			т.д.
6/7* семестр – Контроль обеспечения уровня защищенности объекта информатизации (баз данных).			
4	2. Контроль обеспечения уровня защищенности объекта информатизации (баз данных).	Контрольная точка 1. Формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся Демонстрация навыков владения информационной технологией.	Демонстрация навыков владения информационной технологией. Устный опрос выполняется в аудитории. Суммарный вес 10 баллов. Выполняется в аудитории. Каждый студент имеет уникальное задание, состоящее из –от 5 до 10 контрольных вопросов. Каждое задание оценивается в баллы: 0 - не сделал; 1 – сделал, допустил 9 ошибки; 2 – сделал, допустил 8 ошибки; 3 – сделал, допустил 7 ошибки; 4 – сделал, допустил 6 ошибку и т.д.
8		Контрольная точка 2. Формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся. Демонстрация навыков владения информационной технологией. Демонстрация навыков владения информационной технологией.	Демонстрация навыков владения информационной технологией. Устный опрос выполняется в аудитории. Суммарный вес 10 баллов. Выполняется в аудитории. Каждый студент имеет уникальное задание, состоящее из –от 5 до 10 контрольных вопросов. Каждое задание оценивается в баллы: 0 - не сделал; 1 – сделал, допустил 9 ошибки; 2 – сделал, допустил 8 ошибки; 3 – сделал, допустил 7 ошибки; 4 – сделал, допустил 6 ошибку и т.д.
12		Контрольная точка 3. Формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся. Демонстрация навыков владения информационной технологией.	Демонстрация навыков владения информационной технологией. Устный опрос выполняется в аудитории. Суммарный вес 10 баллов. Выполняется в аудитории. Каждый студент имеет уникальное задание, состоящее из –от 5 до 10 контрольных вопросов. Каждое задание оценивается в баллы: 0 - не сделал; 1 – сделал, допустил 9 ошибки; 2 – сделал, допустил 8 ошибки; 3 – сделал, допустил 7 ошибки; 4 – сделал, допустил 6 ошибку и т.д.
18		Контрольная точка 4. Формализованное наблюдение и оценка **отчета Практической подготовки,** и защита в форме устного опроса обучающихся. Демонстрация навыков владения информационной технологией.	Демонстрация навыков владения информационной технологией. Устный опрос выполняется в аудитории. Суммарный вес **15 баллов**. Каждый студент имеет уникальное задание, состоящее из –от 5 до 10 контрольных вопросов. Каждое задание оценивается в баллы: 0 - не сделал; 1 –сделал, допустил 9 ошибки; 2 – сделал, допустил 8 ошибки; 3 – сделал, допустил 7 ошибки; 4 – сделал, допустил 6 ошибку и т.д.
7/8* семестр – Основы геоинформационных технологий и систем			
4	3. Информационная безопасность геоинформационных	Контрольная точка 1. Формализованное наблюдение и оценка результатов выполнения	Демонстрация навыков владения информационной технологией. Устный опрос выполняется в аудитории. Суммарный вес 10 баллов. Выполняется в

	систем	практических заданий в форме устного опроса обучающихся Демонстрация навыков владения информационной технологией.	аудитории. Каждый студент имеет уникальное задание, состоящее из –от 5 до 10 контрольных вопросов. Каждое задание оценивается в баллы: 0 - не сделал; 1 – сделал, допустил 9 ошибки; 2 – сделал, допустил 8 ошибки; 3 – сделал, допустил 7 ошибки; 4 – сделал, допустил 6 ошибку и т.д.
10		Контрольная точка 2. Формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся. Демонстрация навыков владения информационной технологией. Демонстрация навыков владения информационной технологией.	Демонстрация навыков владения информационной технологией. Устный опрос выполняется в аудитории. Суммарный вес 10 баллов. Выполняется в аудитории. Каждый студент имеет уникальное задание, состоящее из –от 5 до 10 контрольных вопросов. Каждое задание оценивается в баллы: 0 - не сделал; 1 – сделал, допустил 9 ошибки; 2 – сделал, допустил 8 ошибки; 3 – сделал, допустил 7 ошибки; 4 – сделал, допустил 6 ошибку и т.д.
14		Контрольная точка 3. Формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся. Демонстрация навыков владения информационной технологией.	Демонстрация навыков владения информационной технологией. Устный опрос выполняется в аудитории. Суммарный вес 10 баллов. Выполняется в аудитории. Каждый студент имеет уникальное задание, состоящее из –от 5 до 10 контрольных вопросов. Каждое задание оценивается в баллы: 0 - не сделал; 1 – сделал, допустил 9 ошибки; 2 – сделал, допустил 8 ошибки; 3 – сделал, допустил 7 ошибки; 4 – сделал, допустил 6 ошибку и т.д.
18		Контрольная точка 4. Формализованное наблюдение и оценка **отчета Практической подготовки,** и защита в форме устного опроса обучающихся. Демонстрация навыков владения информационной технологией.	Демонстрация навыков владения информационной технологией. Устный опрос выполняется в аудитории. Суммарный вес **15 баллов**. Каждый студент имеет уникальное задание, состоящее из –от 5 до 10 контрольных вопросов. Каждое задание оценивается в баллы: 0 - не сделал; 1 –сделал, допустил 9 ошибки; 2 – сделал, допустил 8 ошибки; 3 – сделал, допустил 7 ошибки; 4 – сделал, допустил 6 ошибку и т.д.
8/9* семестр – Информационная безопасность и работа с 1С: Битрикс 24.			
4	4. Информационная безопасность и работа с 1С: Битрикс 24.	Контрольная точка 1. Формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся Демонстрация навыков владения информационной технологией.	Демонстрация навыков владения информационной технологией. Устный опрос выполняется в аудитории. Суммарный вес 10 баллов. Выполняется в аудитории. Каждый студент имеет уникальное задание, состоящее из –от 5 до 10 контрольных вопросов. Каждое задание оценивается в баллы: 0 - не сделал; 1 – сделал, допустил 9 ошибки; 2 – сделал, допустил 8 ошибки; 3 – сделал, допустил 7 ошибки; 4 – сделал, допустил 6 ошибку и

			т.д.
10		Контрольная точка 2. Формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся. Демонстрация навыков владения информационной технологией. Демонстрация навыков владения информационной технологией.	Демонстрация навыков владения информационной технологией. Устный опрос выполняется в аудитории. Суммарный вес 10 баллов. Выполняется в аудитории. Каждый студент имеет уникальное задание, состоящее из –от 5 до 10 контрольных вопросов. Каждое задание оценивается в баллы: 0 - не сделал; 1 – сделал, допустил 9 ошибки; 2 – сделал, допустил 8 ошибки; 3 – сделал, допустил 7 ошибки; 4 – сделал, допустил 6 ошибку и т.д.
14		Контрольная точка 3. Формализованное наблюдение и оценка результатов выполнения практических заданий в форме устного опроса обучающихся. Демонстрация навыков владения информационной технологией.	Демонстрация навыков владения информационной технологией. Устный опрос выполняется в аудитории. Суммарный вес 10 баллов. Выполняется в аудитории. Каждый студент имеет уникальное задание, состоящее из –от 5 до 10 контрольных вопросов. Каждое задание оценивается в баллы: 0 - не сделал; 1 – сделал, допустил 9 ошибки; 2 – сделал, допустил 8 ошибки; 3 – сделал, допустил 7 ошибки; 4 – сделал, допустил 6 ошибку и т.д.
14		Контрольная точка 4. Формализованное наблюдение и оценка отчета по практическим заданиям**,** и защита в форме устного опроса обучающихся. Демонстрация навыков владения информационной технологией.	Демонстрация навыков владения информационной технологией. Устный опрос выполняется в аудитории. Суммарный вес **15 баллов**. Каждый студент имеет уникальное задание, состоящее из –от 5 до 10 контрольных вопросов. Каждое задание оценивается в баллы: 0 - не сделал; 1 –сделал, допустил 9 ошибки; 2 – сделал, допустил 8 ошибки; 3 – сделал, допустил 7 ошибки; 4 – сделал, допустил 6 ошибку и т.д.

Типовые контрольно-измерительные задания текущего контроля для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Раздел 1. Оценка защищенности объекта информатизации (баз данных) 5/6* семестр

Терминология СУБД: банк и база данных, ЯОД, ЯМД. Эталонная архитектура СУБД. Категории СУБД, различия и возможности. Категории пользователей СУБД (администраторы, непостоянные пользователи, конечные пользователи, прикладные программисты, информационные аналитики), их требования к СУБД и необходимые

навыки. Жизненный цикл базы данных. Проектирование реляционных баз данных. Физические структуры данных. Индексы. Транзакции. Контроль доступа к БД. Функции и основные возможности SQL. Средства SQL для работы со структурой таблицы. Средства манипулирования данными SQL. Операторы для условий и функций. Представления.

Количество часов аудиторной работы – 34/6 часов

Примерный перечень вопросов к **зачету** по Разделу 1. Оценка защищенности объекта информатизации (баз данных)

1. Вопрос каждому, случайное понятие. Понятия: *файловая система, база данных, реляционная БД, СУБД, отношение, ключ, транзакция, индекс, первичный ключ, внешний ключ*.
2. Классификация БД (перечислить все и рассказать об одной).
3. Как осуществляется контроль логической целостности БД?
4. Как осуществляется контроль физической целостности БД?
5. Дореляционные БД. Перечислите и расскажите об одной. Достоинства и недостатки.
6. Фундаментальные свойства *отношений*.
7. Нормализация и нормальные формы отношений. Что это, цель, сколько форм.
8. ER - диаграммы (модель «сущность-связь») и её понятия: сущность, атрибут сущности, ключ сущности, связь, типы связей, особенность.
9. Виды индексов. Их взаимосвязь со структурами хранения индексов и с ключами.
10. Структуры хранения индексов. Перечислить и рассказать об одной. Их взаимосвязь с видами индексов.
11. Транзакции и целостность БД, их свойства (ACID), виды конфликтов, уровни изолированности пользователей согласно стандарту SQL.
12. Виды разграничения доступа к БД.
13. Назовите операторы создания и удаления домена в SQL
14. Какая из команд в языке манипулирования данными (DML) обозначает «выбрать»?
15. Операторы создания, использования и удаления базы данных?
16. Оператор для добавления столбца в таблицу (изменить структуру таблицы)?
17. Для чего используется ключевое слово DISTINCT
18. Как удалить таблицу "my_table"?
19. Для чего применяются индексы?
20. Что такое первичный ключ и для чего он используется? Его отличие от unique?
21. Для чего используется команда GRANT
22. Что делает выражение: ORDER BY DESC
23. Команда объединения двух запросов, выдающих одинаковое количество строк и столбцов в MySQL
24. Вычисляемые столбцы в MySQL
25. Оператор, который подсчитывает количество записей в таблице (заполненных и пустых)
26. Какой оператор SQL используется для задания условия после оператора GROUP BY?

    Представление (view). Что это, цель, операторы создания и удаления.

Практические задания в форме устного зачета, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы дисциплины

1. В данном случае сотрудник учреждения может быть привлечен к ответственности за нарушения правил информационной безопасности:
1. Выход в интернет без разрешения администратора
2. При установке компьютерных игр
3. В случаях установки нелицензионного по
4. В случае не выхода из информационной системы
5. В любом случае неправомочного использования конфиденциальной информации при условии письменного предупреждения сотрудника об ответственности

2. Может ли сотрудник быть привлечен к уголовной ответственности за нарушения правил информационной безопасности предприятия:
1. Нет, только к административной ответственности
2. Нет, если это государственное предприятие
3. Да
4. Да, но только в случае, если действия сотрудника нанесли непоправимый вред
5. Да, но только в случае осознанных неправомочных действий сотрудника

3. Процедура, проверяющая, имеет ли пользователь с предъявленным идентификатором право на доступ к ресурсу это:
1. Идентификация
2. Аутентификация
3. Стратификация
4. Регистрация
5. Авторизация

4. Наиболее опасным источником угроз информационной безопасности предприятия являются:
1. Другие предприятия (конкуренты)
2. Сотрудники информационной службы предприятия, имеющие полный доступ к его информационным ресурсам
3. Рядовые сотрудники предприятия
4. Возможные отказы оборудования, отключения электропитания, нарушения в сети передачи данных
5. Хакеры

5. Выберите, можно ли в служебных целях использовать электронный адрес (почтовый ящик), зарегистрированный на общедоступном почтовом сервере, например на mail.ru:
1. Нет, не при каких обстоятельствах
2. Нет, но для отправки срочных и особо важных писем можно
3. Можно, если по нему пользователь будет пересылать информацию, не содержащую сведений конфиденциального характера
4. Можно, если информацию предварительно заархивировать с помощью программы winrar с паролем

5. Можно, если других способов электронной передачи данных на предприятии или у пользователя в настоящий момент нет, а информацию нужно переслать срочно

6. Документированная информация, доступ к которой ограничивает в соответствии с законадельством рф:
1. Информация составляющая государственную тайну
2. Информация составляющая коммерческую тайну
3. Персональная
4. Конфиденциальная информация
5. Документированная информация

7. Для того чтобы снизить вероятность утраты информации необходимо:
1. Регулярно производить антивирусную проверку компьютера
2. Регулярно выполнять проверку жестких дисков компьютера на наличие ошибок
3. Регулярно копировать информацию на внешние носители (сервер, компакт-диски, флэш-карты)
4. Защитить вход на компьютер к данным паролем
5. Проводить периодическое обслуживание пк

8. Пароль пользователя должен
1. Содержать цифры и буквы, знаки препинания и быть сложным для угадывания
2. Содержать только цифры
3. Содержать только буквы
4. Иметь явную привязку к владельцу (его имя, дата рождения, номер телефона и т.п.)
5. Быть простым и легко запоминаться, например «123», «111», «qwerty» и т.д.

9. Информационная безопасность обеспечивает…
1. Блокирование информации
2. Искажение информации
3. Сохранность информации
4. Утрату информации
5. Подделку информации

10. Закон российской федерации «о государственной тайне» был принят в следующем году:
1. 1982
2. 1985
3. 1988
4. 1993
5. 2005

Материалы для промежуточной аттестации в форме устного экзамена по 6/7* семестр «Контроль обеспечения уровня защищенности объекта информатизации (баз данных)»

Материалы промежуточной аттестации включают в себя вопросы по практическим работам в виде опроса или теста, позволяющие оценить теоретические знания студента и степень владения изучаемыми информационными технологиями. Экзамен должен

проводиться в аудитории с установленным программным обеспечением PostgreSQL. Билет содержит два теоретических и один практический вопросы.

Теоретические вопросы:

1. Файловая система
2. База данных и СУБД
3. Реляционная БД
4. Отношение
5. Виды ключей
6. Транзакция
7. Классификация БД.
8. Фундаментальные свойства отношений.
9. Нормализация и нормальные формы отношений.
10. Модель «сущность-связь» и её понятия.
11. Индексы. Их взаимосвязь со структурами хранения индексов и с ключами.
12. Структуры хранения индексов.
13. Транзакции и целостность БД, ACID, виды конфликтов, уровни изолированности пользователей согласно стандарту SQL.
14. Виды разграничения доступа к БД.
15. Какие Вы знаете способы внедрения языка SQL в прикладные программы?
16. INTO-переменные
17. Bind-переменные
18. Индикаторные переменные в SQL
19. Назовите и опишите интерфейсы программирования приложений для БД (API)
20. Какая модель архитектуры может служить базовой для распределенной БД?
21. Назовите разновидности однородных распределенных БД
22. Назовите разновидности разнородных распределенных БД
23. В каких распределенных СУБД каждый узел имеет часть информации о других узлах РБД?
24. Назовите вид СУБД, в котором приложения, выполняемые в среде СУБД, сами ответственны за интерфейсы между различными СУБД, вне зависимости от их однородности?
25. Назовите определение Распределённая СУБД
26. Определите Объектно-ориентированную СУБД
27. Назовите основные понятия объектно-ориентированных БД
28. Назовите виды баз данных направления NoSQL
29. Назовите понятия графовых БД

Практические вопросы

1. Тестовое задание открытого типа. Назовите определение: субъект доступа, ответственный за защиту АС от несанкционированного доступа к информации;
2. Тестовое задание открытого типа. Назовите определение: комплекс организационных и технических мероприятий, в результате которых подтверждается соответствие системы защиты информации объекта информатизации требованиям безопасности информации;
3. Тестовое задание открытого типа. Назовите определение: состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность;

4. Тестовое задание открытого типа. Назовите определение: - лицо, самостоятельно и по своему усмотрению определяющее порядок использования сайта в сети "Интернет", в том числе порядок размещения информации на таком сайте;
5. Тестовое задание открытого типа. Назовите определение: – технические средства и системы, не предназначенные для передачи, обработки и хранения секретной информации, устанавливаемые совместно с основными техническими средствами и системами;
6. Тестовое задание открытого типа. Назовите определение: - обозначение символами, предназначенное для адресации сайтов в сети "Интернет" в целях обеспечения доступа к информации, размещенной в сети "Интернет";
7. Тестовое задание открытого типа. Назовите определение: – ознакомление с информацией, ее обработка; в частности, копирование, модификация или уничтожение информации;
8. Тестовое задание открытого типа. Назовите определение: – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;
9. Тестовое задание открытого типа. Назовите определение: - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
10. Тестовое задание открытого типа. Назовите определение: - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;
11. Тестовое задание открытого типа. Назовите определение: – отдельные документы и отдельные массивы документов, содержащиеся в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах), а также машинные носители информации (жесткие магнитные диски, гибкие магнитные диски, оптические диски и т.п.);
12. Тестовое задание открытого типа. Назовите определение: - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
13. Тестовое задание открытого типа. Назовите определение: - сведения (сообщения, данные) независимо от формы их представления;
14. Тестовое задание открытого типа. Назовите определение: - пространство, в котором организационными (режимными) мерами исключается возможность нахождения (размещения) средств иностранной технической разведки, а также неконтролируемое пребывание лиц, не имеющих пропуска, и нахождение посторонних транспортных средств;
15. Тестовое задание открытого типа. Назовите определение: - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя; Ответ: конфиденциальность информации
16. Тестовое задание открытого типа. Назовите определение: – доступ к информации, осуществляемый с нарушением установленных прав и(или) правил доступа к информации с применением штатных средств информационной системы или средств, аналогичных им по своему функциональному предназначению и техническим характеристикам;
17. Тестовое задание открытого типа. Назовите определение: – физическое лицо или материальный объект, в том числе физическое поле, в которых информация находит

свое отображение в виде символов, образов, сигналов, технических решений, процессов и количественных характеристик физических величин;
18. Тестовое задание открытого типа. Назовите определение: - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
19. Тестовое задание открытого типа. Назовите определение: – совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения, осуществляемых над информацией;
20. Тестовое задание открытого типа. Назовите определение: – информация или носитель информации или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации;
21. Тестовое задание открытого типа. Назовите определение: - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;
22. Тестовое задание открытого типа. Назовите определение: - лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети "Интернет";
23. Тестовое задание открытого типа. Назовите определение: - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;
24. Тестовое задание открытого типа. Назовите определение: – совокупность требований, правил, организационных, технических и иных мер, направленных на сохранность сведений, составляющих государственную тайну;
25. Тестовое задание открытого типа. Назовите определение: - совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети "Интернет" по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети "Интернет";
26. Тестовое задание открытого типа. Назовите определение: - идентификатор в сети передачи данных, определяющий при оказании телематических услуг связи абонентский терминал или иные средства связи, входящие в информационную систему;
27. Тестовое задание открытого типа. Назовите определение: – совокупность всех технических, программных и программно-технических средств защиты информации и средств контроля эффективности защиты информации;
28. Тестовое задание открытого типа. Назовите определение: – комплекс организационных мер и программно-технических (в том числе и криптографических) средств защиты от несанкционированного доступа к информации в автоматизированной системе;
29. Тестовое задание открытого типа. Назовите определение: – проверка автоматизированной системы, осуществляемая с целью поиска и изъятия закладного устройства;
30. Тестовое задание открытого типа. Назовите определение: – выявление с использованием контрольно-измерительной аппаратуры возможных технических каналов утечки защищаемой информации от основных и вспомогательных технических средств и систем, оценка соответствия защиты информации требованиям нормативных документов по ее защите;

31. Тестовое задание открытого типа. Назовите определение: – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем;
32. Тестовое задание открытого типа. Назовите определение: – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации;
33. Тестовое задание открытого типа. Назовите определение: - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

Практические/ситуационные задачи

Задание 34.
При использовании сканеров защищенности информационной инфраструктуры предприятия, Вы, как специалист по защите информации, должны составить отчёт сканирования. Какие разделы должны входить в такой отчёт (в любом порядке)?
Задание 35
Вы эксперт по информационной безопасности. Задача – найти уязвимости сайта предприятия. Перечислите ваши действия и их результаты.
Задание 36.
Какие меры защиты нужно предпринять для защиты компьютеров фирмы от вывода их из строя по сети.
Задание 37.
Какие меры противодействия несанкционированному доступу к информации на предприятии Вы можете предпринять?
Задание 38
Вы – администратор безопасности предприятия. Какие организационно-технические мероприятия по обеспечению безопасности нужно проводить постоянно?

Материалы для промежуточной аттестации в форме устного экзамена по 7/8* семестр «Основы информационной безопасности геоинформационных технологий и систем»

Материалы промежуточной аттестации включают в себя вопросы по практическим работам и лекциям в виде экзамена, позволяющие оценить теоретические знания студента и степень владения изучаемыми информационными технологиями. Экзамен должен проводиться в аудитории с установленным программным обеспечением MapInfo или Axioma. Билет состоит из двух теоретических и одного практического вопросов.

Вопросы к экзамену

Теория:

1. Геоинформационная система. Определение, виды, функции, отличия от других информационных систем.
2. Связанные с ГИС технологии.
3. Топология в ГИС. Определение и виды.
4. Растровые модели в ГИС. Характеристики растра.
5. Растровые модели в ГИС. Привязка растра.
6. Растровые модели в ГИС. Модели хранения растров.
7. Векторные модели. Виды, как хранятся в ГИС (деревья).
8. Векторные модели. TIN, полигоны Тиссена/диаграммы Вороного.

9. Модели хранения данных в ГИС.
10. Типичные ошибки оцифровки и качество цифровых карт.
11. Возможности атрибутивного анализа данных в ГИС.
12. Оверлейный анализ пространственных данных.
13. Анализ географических сетей.
14. Тематические карты. Геогруппы.
15. Построение буферных зон. Анализ видимости-невидимости.
16. Переклассификация.

Практические задания:

1. Как создать карту в ГИС Mapinfo/Axioma? Из каких элементов она состоит?
2. Инструменты выборки данных в ГИС.
3. Этапы привязки растрового изображения в ГИС.
4. Имеется таблица с адресными данными. Задача – нанести эти данные на карту. Каким инструментом нужно воспользоваться?
5. Инструмент трассировки – что это, принцип работы.
6. Как совместить растровое и векторное изображения и зачем это нужно?
7. Имеется таблица с почтовыми индексами по областям их действия, визуализированная на карте. Каким инструментом можно воспользоваться для изменения количества регионов, соответствующих одному индексу?
8. Каким инструментом нужно воспользоваться для создания равноудаленных зон шаговой доступности от точек на карте, обозначающих магазины?

Материалы для промежуточной аттестации в форме устного экзамена по 8/9* семестр «Информационная безопасность и работа с 1С: Битрикс 24.»

Материалы промежуточной аттестации включают в себя вопросы по практическим работам и лекциям в виде экзамена, позволяющие оценить теоретические знания студента и степень владения изучаемыми информационными технологиями. Экзамен должен проводиться в аудитории с установленным программным обеспечением QGIS и доступом в интернет. Билет состоит из двух теоретических и одного практического вопросов.

Теория

1. Геоинформационная система. Определение, виды, функции, отличия от других информационных систем.
2. Программный пакет ArcGIS. Структура и возможности.
3. Дополнительные модули ArcGIS. Перечислить и рассказать об одном.
4. Типы данных в ArcGIS (Классы и наборы классов, аннотации и надписи, шейп-файлы, топология, САПР, KML, Terrain).
5. Дистанционное зондирование Земли. Определение, этапы, сравнительная точность измерений по эм-спектру.
6. Фотографическая съемка в ДЗЗ.
7. Сканерная съемка в ДЗЗ.
8. Радиолокационная съемка в ДЗЗ.
9. ИК-съемка в ДЗЗ.
10. Лидарная съемка в ДЗЗ.
11. Спутниковые системы навигации. Основные элементы системы. Принцип работы. Современные ГНСС.
12. Системы, повышающие точность измерений в спутниковых навигационных системах.
13. Технология A-GPS.

14. Абсолютные методы позиционирования и их точность. Пример методики измерений.
15. Относительные методы позиционирования и их точность. Пример методики измерений.
16. Факторы точности измерений.
17. Основные понятия безопасности в информационных системах.
18. Виды угроз безопасности в информационных системах.
19. Принципы обеспечения безопасности и контрмеры.
20. Организация системы безопасности ИС.
21. Обязанности ответственных за безопасность.
22. Средства защиты от несанкционированного доступа.
23. Классификация уязвимостей и атак в сетях.
24. Методики анализа защищенности ИС.
25. Классификация сканеров защищенности веб-сайтов.

Практические задания

1. Как добавить данные в проект?
2. Использование атрибутов объекта для его визуализации.
3. Настройка системы координат карты.
4. Инструменты навигации по карте.
5. Добавление векторных наборов данных на карту.
6. Таблица атрибутов объектов.
7. Настройка и включение подписей.
8. Компоновка карты.
9. Стили слоя.
10. Привязка растрового изображения и оценка точности привязки.
11. Оцифровка растра.
12. Атрибутивный и пространственный запросы.
13. Оверлей. Его отличие от пространственного запроса. Взвешенный оверлей.
14. Какой смысл и разница между соединением и связью атрибутивных таблиц. Виды соединений.
15. Переклассификация наборов данных.
16. Геокодирование и его виды и режимы.
17. Какие данные нужны для проведения сетевого анализа?
18. Необходимые условия для построения геометрической сети.
19. Как изменить названия и порядок символов в легенде карты?
20. За что отвечают системные поля атрибутивной таблицы Shape и ObjectID?

Типовые задания для оценивания уровня освоения компетенции ПК-6 Способен проводить аудит информационных сервисов и обеспечивать безопасность управления данными цифрового предприятия; в части индикаторов достижения компетенции

Задание закрытого типа на установление соответствия и **последовательности**

Задание 1 закрытого типа на установление последовательности

Сценарий выполнения задания: Установить правильную последовательность шагов для обеспечения защиты информации при использовании электронной почты. Выберите правильный порядок действий из предложенных вариантов:

A.	1. Шифрование сообщения
B.	2. Установка антивирусного ПО
C.	3. Отправка письма
D.	4. Аутентификация отправителя
E.	5. Проверка подлинности получателя
F.	6. Создание резервной копии данных
G.	7. Использование двухфакторной аутентификации
H.	8. Настройка правил фильтрации спама
I.	9. Обновление программного обеспечения
J.	10. Удаление конфиденциальных данных после отправки
K.	11 Анализ ситуации: Студенты должны понимать важность каждого шага для обеспечения безопасности при использовании электронной почты. Для этого необходимо ознакомиться с основными угрозами и методами их предотвращения.
L.	12. студенты должны выбрать те, которые действительно необходимы для обеспечения безопасности электронного общения. Некоторые шаги могут быть избыточными или не иметь прямого отношения к защите информации.
M.	13. Определение порядка: после выбора необходимых шагов, студентам нужно установить логически правильную последовательность их выполнения. Например, установка антивируса должна предшествовать отправке письма, а шифрование должно происходить до отправки.
N.	14. Проверка правильности: Преподаватель проверяет правильность установленной последовательности, обращая внимание на соответствие теоретическим основам цифровой безопасности и практическим рекомендациям.

Впишите в таблицу правильную последовательность этапов согласно сценарию задания, обозначенных цифрами.

A.	B.	C.	D.	E.	F.	G.	H.	I.	J.	K.	L.	M.	N.

Задание 2 закрытого типа на установление последовательности

Сценарий выполнения задания: Установить правильную последовательность. Выберите правильный порядок действий из перечисленных и обозначенных цифрами согласно буквенному обозначению

A.	1)	Установка антивирусного ПО
B.	2)	Отслеживание доставки письма
C.	3)	Удаление конфиденциальных данных после отправки
D.	4)	Архивирование сообщений
E.	5)	Резервное копирование настроек
F.	6)	Мониторинг активности аккаунта

G.	7)	Регулярное обновление паролей
H.	8)	Информирование об изменениях политики безопасности
I.	9)	Обновление программного обеспечения
J.	10)	Настройка правил фильтрации спама
K.	11)	Использование двухфакторной аутентификации
L.	12)	Аутентификация отправителя
M.	13)	Проверка подлинности получателя
N.	14)	Шифрование сообщения
O.	15)	Использование безопасного соединения (HTTPS)
P.	16)	Отправка письма

Впишите в таблицу ответов правильную последовательность этапов согласно сценарию задания, обозначенных цифрами.

A.	B.	C.	D.	E.	F.	G.	H.	I.	J.	K.	L.	M.	N.	O.	P.

Задание 3 закрытого типа на установление последовательности

Прочитайте текст и установите соответствие.

Последовательность установки системы безопасности для корпоративной сети
Установите правильную последовательность шагов для настройки базовой системы безопасности корпоративной сети. Студентам предлагается определить последовательность шагов, которая позволит эффективно настроить систему безопасности корпоративной сети. Они должны учитывать, что сначала необходимо разработать политику безопасности, затем установить базовые средства защиты, такие как антивирус и межсетевые экраны, и только потом переходить к более сложным мерам, таким как мониторинг и аудит.

Последовательность действий при обнаружении инцидента информационной безопасности Определите правильную последовательность действий при обнаружении инцидента информационной безопасности.

A.	1) Развертывание межсетевого экрана (Firewall).
B.	2) Установка антивирусного ПО.
C.	3) Настройка системы обнаружения вторжений (IDS/IPS).
D.	4) Определение политик безопасности.
E.	5) Разработка плана реагирования на инциденты.
F.	6) Проведение аудита безопасности.
G.	7) Обучение сотрудников правилам информационной безопасности.
H.	8) Установка обновлений безопасности.
I.	9) Мониторинг сетевой активности.
J.	10) Внедрение системы управления доступом (Access Control System).

Запишите ответ в таблицу. В соответствие с буквами напишите цифры из задания

A.	B.	C.	D.	E.	F.	G.	H.	I.	J.

Задание 4 закрытого типа на установление последовательности Сценарий выполнения задания:

Последовательность шагов для создания защищенного веб-приложения

Укажите правильную последовательность шагов для разработки и внедрения защищенного веб-приложения.

Сначала студенты должны спроектировать архитектуру приложения, учитывая возможные риски. Затем они выбирают технологии и инструменты, реализуют механизмы аутентификации и авторизации, обеспечивают конфиденциальность данных и пишут код. Перед развертыванием проводится тестирование безопасности, а после запуска приложение требует мониторинга и поддержки.

Последовательность этапов проведения аудита информационной безопасности

Установите правильную последовательность этапов проведения аудита информационной безопасности.

A.	1) Развертывание межсетевого экрана (Firewall).
B.	2) Установка антивирусного ПО.
C.	3) Настройка системы обнаружения вторжений (IDS/IPS).
D.	4) Определение политик безопасности.
E.	5) Разработка плана реагирования на инциденты.
F.	6) Проведение аудита безопасности.
G.	7) Обучение сотрудников правилам информационной безопасности.
H.	8) Установка обновлений безопасности.
I.	9) Мониторинг сетевой активности.
J.	10) Внедрение системы управления доступом (Access Control System).

Впишите в таблицу ответов правильную последовательность этапов согласно сценарию задания, обозначенных цифрами.

A.	B.	C.	D.	E.	F.	G.	H.	I.	J.

Задание 5 закрытого типа на установление последовательности

Сначала разрабатываем политику безопасности, затем устанавливаем обновления и базовую защиту, далее настраиваем мониторинг и аудит, завершаем обучением сотрудников

Последовательность действий при обнаружении инцидента информационной безопасности Начинаем с локализации угрозы, затем собираем доказательства и уведомляем руководство. После оценки ущерба и анализа причин устраняем последствия и разрабатываем меры профилактики. Завершаем документированием и уведомлением всех заинтересованных сторон.

Последовательность шагов для создания защищённого веб-приложения

Начинаем с проектирования архитектуры и анализа рисков, затем выбираем технологии и реализуем механизмы безопасности. После написания кода проводим тестирование и разворачиваем приложение. Завершаем мониторингом и поддержкой, а также обучением пользователей.

Последовательность этапов проведения аудита информационной безопасности

A.	1. Оценка ущерба.
B.	2. Планирование дальнейших действий.
C.	3. Оповещение руководства.
D.	4. Сбор доказательств.
E.	5. Локализация угрозы.
F.	6. Анализ причин инцидента.
G.	7. Устранение последствий.
H.	8. Разработка мер по предотвращению повторения инцидента.
I.	9. Документирование инцидента.
J.	10. Уведомление заинтересованных сторон.

Впишите в таблицу ответов правильную последовательность этапов согласно сценарию задания, обозначенных цифрами.

A.	B.	C.	D.	E.	F.	G.	H.	I.	J.

<u>Задания открытого типа с развёрнутым ответом</u>

Задание 1 открытого типа с развернутым ответом

Описание ситуации: Вы работаете системным администратором в крупной компании. В последнее время участились случаи утечек данных и попыток несанкционированного доступа к внутренним ресурсам компании через корпоративную сеть. Руководство поставило перед вами задачу разработать комплекс мер для повышения уровня цифровой безопасности сотрудников при работе в сети.

Задание 2 открытого типа с развернутым ответом

Описание ситуации: Вы являетесь специалистом по информационной безопасности в компании, которая занимается разработкой программного обеспечения. Ваша команда недавно обнаружила несколько инцидентов, связанных с утечкой данных и попытками взлома внутренней инфраструктуры. Вам поручено провести анализ существующих рисков и предложить стратегию защиты информационных активов компании.

Задание 3 открытого типа с развернутым ответом

Сценарий выполнения задания:

1. Изучите доступные материалы о рисках использования облачных сервисов.
2. Определите ключевые риски, характерные для вашей организации.
3. Найдите информацию о мерах защиты, применяемых в облачной инфраструктуре.
4. Проведите сравнительный анализ нескольких поставщиков облачных услуг.
5. Разработайте план действий на случай инцидента.
6. Оформите отчет, включая все необходимые разделы.
7. Представьте отчет преподавателю/руководителю группы.

Задание4 открытого типа с развернутым ответом

1.Ознакомьтесь с существующими стандартами и рекомендациями по информационной безопасности для удаленных работников.

2. Проанализируйте возможные угрозы, связанные с работой из дома (например, использование ненадежного Wi-Fi, отсутствие физической охраны рабочих мест).

3. Разработайте конкретные требования к оборудованию и ПО, которые помогут снизить эти риски.
4. Создайте политику паролей и аутентификации, учитывающую специфику удаленной работы.
5. Напишите инструкции по безопасному поведению в Интернете и защите конфиденциальной информации.
6. Предложите методы контроля за выполнением ваших рекомендаций.
7. Оформите документ с вашими рекомендациями и представьте его преподавателю/руководителю группы.

Задание 5 открытого типа с развернутым ответом
Разработка стратегии реагирования на киберинциденты Определение целей и задач стратегии: определяются цели и задачи стратегии реагирования на киберинцидент, такие как минимизация ущерба от атаки, восстановление нормальной работы информационных систем, предотвращение повторных инцидентов.

Задание 6 открытого типа с развернутым ответом
Разработка стратегии реагирования на киберинциденты Сбор информации о существующих угрозах: проводится анализ текущих киберугроз, характерных для отрасли, в которой работает организация. Например, рассматриваются виды атак, которые наиболее вероятны (DDoS, фишинг, вирусы-шпионы и др.).

Задание 7 открытого типа с развернутым ответом
Разработка стратегии реагирования на киберинциденты Разработка плана действий на случай инцидента: описываются пошаговые действия команды реагирования на инцидент, начиная от обнаружения аномалий в системе до полного устранения последствий атаки. План включает этапы оповещения, анализа ситуации, локализации проблемы, восстановления данных и оценки ущерба.

Задание 8 открытого типа с развернутым ответом
Разработка стратегии реагирования на киберинциденты Создание процедур мониторинга и раннего предупреждения: разрабатывается система мониторинга и оповещения о потенциальных угрозах. Указываются инструменты и методы, которые будут использованы для своевременного обнаружения инцидентов.

Задание 9 открытого типа с развернутым ответом
Разработка стратегии реагирования на киберинциденты Обучение персонала: подготавливается программа обучения сотрудников основам кибербезопасности и правилам поведения в случае возникновения инцидента. Включаются сценарии тренингов и симуляций для отработки навыков реагирования.

Задание 10 открытого типа с развернутым ответом

Разработка стратегии реагирования на киберинциденты Тестирование стратегии: проводятся тесты разработанной стратегии, чтобы оценить её эффективность и выявить слабые места. Тесты могут включать моделирование различных типов атак и оценку времени реакции команды.

Задание 11 открытого типа с развернутым ответом

Разработка стратегии реагирования на киберинциденты Корректировка и утверждение стратегии: на основе результатов тестирования вносятся коррективы в стратегию. После этого стратегия утверждается руководством организации и становится частью общей политики информационной безопасности.

Задание 12 открытого типа с развернутым ответом
Анализ и выбор средств защиты информации для малого бизнеса Оценка текущего уровня защиты информации: проводится аудит существующих мер защиты информации в малом бизнесе. Определяется, какие средства уже используются (антивирусы, межсетевые экраны, системы резервного копирования), и насколько они эффективны.

Задание 13 открытого типа с развернутым ответом
Анализ и выбор средств защиты информации для малого бизнеса Определение потребностей в защите информации: анализируются бизнес-процессы компании и выявляются критические данные, требующие дополнительной защиты. Рассматриваются возможные угрозы и риски, связанные с потерей или компрометацией этих данных.
Задание 14 открытого типа с развернутым ответом
Анализ и выбор средств защиты информации для малого бизнеса Исследование рынка средств защиты информации: собирается информация о доступных на рынке продуктах и услугах, предназначенных для защиты информации. Проводится сравнение функциональных возможностей, стоимости и надежности различных решений.

Задание 15 открытого типа с развернутым ответом
Анализ и выбор средств защиты информации для малого бизнеса Выбор подходящих средств защиты: на основании проведенного исследования выбираются оптимальные средства защиты, соответствующие потребностям малого бизнеса. При выборе учитываются бюджетные ограничения, простота внедрения и эксплуатации, а также совместимость с существующей IT-инфраструктурой.

Задание 16 открытого типа с развернутым ответом
Анализ и выбор средств защиты информации для малого бизнеса Разработка плана внедрения выбранных средств: составляется подробный план внедрения новых средств защиты, включая этапы установки, настройки и тестирования. Определяются ответственные лица и сроки выполнения каждого этапа.

Задание 17 открытого типа с развернутым ответом
Анализ и выбор средств защиты информации для малого бизнеса Мониторинг и поддержка внедренных решений: после успешного внедрения проводится мониторинг эффективности новых средств защиты. Регулярно выполняются обновления и проверки на предмет наличия новых уязвимостей. Организуется техническая поддержка для оперативного решения возникающих проблем.

Задание 18 открытого типа с развернутым ответом
Анализ и выбор средств защиты информации для малого бизнеса Документирование процесса выбора и внедрения: Все этапы выбора и внедрения средств защиты документируются. Это позволяет в будущем проводить анализ эффективности принятых решений и вносить необходимые коррективы.

Задание 19 открытого типа с развернутым ответом
Управление правами доступа в корпоративной сети Анализ текущей структуры прав доступа: Исследуйте текущую структуру прав доступа в выбранной вами корпоративной сети. Определите, кто имеет доступ к каким ресурсам, и оцените, соответствуют ли эти права актуальным требованиям безопасности.

Задание 20 открытого типа с развернутым ответом
Защита персональных данных в соответствии с законодательством Сценарий выполнения задания:
1. Изучение законодательства: изучите актуальные законы и нормативные акты, регулирующие защиту персональных данных (например, Федеральный закон №152-ФЗ "О персональных данных"). Определите основные требования к обработке, хранению и защите персональных данных.

7.4. Содержание занятий семинарского типа (практические работы)

Практическое занятие № 1.

Вид практического занятия: Семинар, контрольная точка 1, в форме устного опроса
Раздел: Концепция цифровой безопасности
Тема и содержание занятия: Тема 1.1. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности.
Практическое занятие, предусматривающее выполнение практической работы, контроль в форме устного опроса
Цель занятия: Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности.
Практические навыки: Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности.
Вопросы, выносимые на обсуждение:
Понятие информации
Доступ к информации
Информационные системы
Обработка информации
Защита информации
Информационная безопасность
Продолжительность занятия – 9 часов / 2 часа (входит опрос по контрольной точке – 1)

Практическое занятие № 2.

Вид практического занятия: Практическая работа, контрольная точка 2, в форме устного опроса
Раздел: Концепция цифровой безопасности
Тема и содержание занятия: Тема 1.2. Организационное обеспечение информационной безопасности.
Практическое занятие, предусматривающее выполнение практической работы, контроль в форме устного опроса
Цель занятия:
Практические навыки:

Вопросы, выносимые на обсуждение:
1. Какие основные международные стандарты в области информа-ционной безопасности существуют?
2. Что такое "Единые критерии"
3. Как связаны международные стандарты и стандарты РФ?
4. Какие основные стандарты РФ в области информационной безо-пасности существуют?
5. Охарактеризуйте стандарт ГОСТ Р ИСО/МЭК 27002-2014.
6. Что такое политика безопасности?
7. Какое количество средств бюджета организации эффективно тратить для обеспечения информационной безопасности?

Продолжительность занятия – 9 часов / 2 часа (входит опрос по контрольной точке – 2).

Практическое занятие № 3.

Вид практического занятия: Практическая работа, контрольная точка 3, в форме устного опроса
Раздел: Концепция цифровой безопасности
Тема и содержание занятия: Тема 1.3.Технические средства и методы защиты информации.
Практическое занятие, предусматривающее выполнение практической работы, контроль в форме устного опроса
Цель занятия:
Практические навыки:
Вопросы, выносимые на обсуждение:
1. Что такое инженерная защита объектов?
2. Какие виды сигнализаций устанавливаются для обеспечения ин-женерной защиты?
3. Что такое технические каналы утечки информации?
4. Перечислите основные виды технических каналов утечки ин-формации?
5. Перечислите методы защиты информации от утечки по визуаль-ному каналу.
6. Перечислите методы защиты информации от утечки по воздуш-ному каналу.
7. Перечислите методы защиты информации от утечки по вибраци-онному каналу.
8. Перечислите методы защиты информации от утечки по индук-ционному каналу.
9. Перечислите средства и методы защиты информации от утечки в телефонных линиях.
10. Перечислите основные мероприятия по обеспечению защиты информации от утечки по техническим каналам.

Продолжительность занятия – 9 часов / 2 часа (входит опрос по контрольной точке – 3).

Практическое занятие № 4.

Вид практического занятия: Практическая работа, контрольная точка 1, контроль в форме устного опроса.
Раздел: Криптографические и стеганографические методы защиты
Тема и содержание занятия: Тема 2.1. Криптографические методы защиты информации.
Практическое занятие, предусматривающее выполнение практической работы, контроль в форме устного опроса
Цель занятия: Использование криптографических средств защиты информации
Практические навыки:

Вопросы, выносимые на обсуждение:
Что такое криптография?
2. Какие используются симметричные алгоритмы шифрования?
3. Какие используются ассиметричные алгоритмы шифрования?
4. Что такое криптографическая хеш-функция?
5. Какие используются криптографические хеш-функции?
6. Что такое цифровая подпись?
7. Что такое инфраструктура открытых ключей?
8. Какие российские и международные стандарты на формирование цифровой подписи существуют?
9. Какие основные криптографические протоколы используются в сетях?

Продолжительность занятия – 9 часов / 2 часа (входит опрос по контрольной точке – 1).

Практическое занятие № 5.

Вид практического занятия: Практическая работа, контрольная точка 2, в форме устного опроса
Раздел:
Тема и содержание занятия: Тема 2.2. Реализация работы инфраструктуры открытых ключей.
Практическое занятие, предусматривающее выполнение практической работы, контроль в форме устного опроса
Цель занятия: Использование инфраструктуры открытых ключей
Практические навыки:
Вопросы, выносимые на обсуждение:
Продолжительность занятия – 9 часов / 2 часа (входит опрос по контрольной точке – 2).

Практическое занятие № 6.

Вид практического занятия: Практическая работа, контрольная точка 3, в форме устного опроса
Раздел:
Тема и содержание занятия: Тема 2.3. Средства стеганографии для защиты информации.
Практическое занятие, предусматривающее выполнение практической работы, контроль в форме устного опроса
Цель занятия: Использование средств стеганографии для защиты файлов
Практические навыки: Использование средств стеганографии для защиты файлов
Вопросы, выносимые на обсуждение:
Использование средств стеганографии для защиты файлов
Продолжительность занятия – 9 часов / 2 часа (входит опрос по контрольной точке – 3).

Практическое занятие № 7.

Вид практического занятия: Дискуссии по актуальным темам и разбор практических кейсов , контрольная точка 1, в форме группового обсуждения рефератов
Раздел: Инстументы защиты информации

Тема и содержание занятия: Тема 3.1. Место информационной безопасности экономических систем в национальной безопасности страны.
Практическое занятие, предусматривающее Обсуждение рефератов, подготовленных студентами. Выступления приглашенных экспертов-практиков. Проведение круглых столов. Разбор кейсов.
Цель занятия:
Практические навыки:
Вопросы, выносимые на обсуждение:
Информационная безопасность страны. Защита экономических систем.
Обмен конфиденциальной информацией. Структура банковских информационных систем в области защиты информации. Важность защиты экономических систем. Электронные деньги и безопасность финансовых переводов. Концепция информационной безопасности. Основные сведения и положения.
Продолжительность занятия – 9 часов / 3,5 часа (входит опрос по контрольной точке – 1)

Практическое занятие № 8.

Вид практического занятия: Практическая работа, контрольная точка 2, в форме устного опроса
Раздел: Инстументы защиты информации
Тема и содержание занятия: Тема 3.2. Антивирусные средства защиты информации.
Практическое занятие, предусматривающее выполнение практической работы, контроль в форме устного опроса
Цель занятия: закрепить полученные в ходе практического занятия знания, приобрести навыки использования настроек средств антивирусной защиты информации
Практические навыки: Изучение настроек средств антивирусной защиты информации
Вопросы, выносимые на обсуждение:
1. Какие виды компьютерных угроз существуют?
2. Что такое брандмауэр?
3. Что такое антивирусная программа?
4. Что такое эвристический алгоритм поиска вирусов?
5. Что такое сигнатурный поиск вирусов?
6. Методы противодействия сниффингу?
7. Какие программные реализации программно-аппаратных средств защиты информации вы знаете?
8. Что такое механизм контроля и разграничения доступа?
9. Какую роль несет журналирование действий в программно-аппаратных средствах защиты информации?
10. Что такое средства стеганографической защиты информации?

Продолжительность занятия – 9 часов / 3,5 часа (входит опрос по контрольной точке – 2).

Практическое занятие № 9.

Вид практического занятия: Дискуссии по актуальным темам и разбор практических кейсов , контрольная точка 3, в форме группового обсуждения рефератов
Раздел: Инстументы защиты информации

Тема и содержание занятия: Тема 3.3. Объектно-ориентированный подход к проектированию программного обеспечения.
Практическое занятие, предусматривающее Обсуждение рефератов, подготовленных студентами. Выступления приглашенных экспертов-практиков. Проведение круглых столов. Разбор кейсов.
Цель занятия: закрепить полученные в ходе практического занятия знания, приобрести навыки использования объектно-ориентированного подхода к проектированию программного обеспечения
Практические навыки: Изучение объектно-ориентированного подхода к проектированию программного обеспечения
Вопросы, выносимые на обсуждение:
Определение и описание архитектуры программного обеспечения. Базовые средства по созданию архитектуры ПО. Способы формального представления знаний. Основы устройства и использование экспертных систем в разработке адаптируемого программного обеспечения. Основные направления интеллектуализации ПО.
Продолжительность занятия – 9 часов / 3,5 часа (входит опрос по контрольной точке – 3).

Практическое занятие № 10.

Вид практического занятия: Практическая работа, контрольная точка 1, контроль в форме устного опроса.
Раздел: Стандартизация, сертификация и управление качеством программного обеспечения
Тема и содержание занятия: Тема 4.1. Жизненный цикл программного обеспечения. Понятие жизненного цикла (ЖЦ) программного обеспечения.
Практическое занятие, предусматривающее Обсуждение. Выполнение проектного задания
Цель занятия:
Практические навыки:
Вопросы, выносимые на обсуждение:
Жизненный цикл программного обеспечения. Понятие жизненного цикла (ЖЦ) программного обеспечения. Определение ЖЦ международным стандартом ISO/IEC 12207:1995. Основные процессы ЖЦ ПО. Вспомогательные процессы ЖЦ ПО. Организационные процессы ЖЦ ПО. Взаимосвязь между процессами ЖЦ ПО.
Продолжительность занятия – 9 часов / 3,5 часа (входит опрос по контрольной точке – 1).

Практическое занятие № 11.

Вид практического занятия: Дискуссии по актуальным темам и разбор практических кейсов , контрольная точка 2, контроль в форме устного опроса.
Раздел: Стандартизация, сертификация и управление качеством программного обеспечения
Тема и содержание занятия: Тема 4.2. Управление разработкой ПО..

Практическое занятие, предусматривающее Обсуждение рефератов, подготовленных студентами. Выступления приглашенных экспертов-практиков. Проведение круглых столов. Разбор кейсов.
Цель занятия: закрепить полученные в ходе практического занятия знания, приобрести навыки управления разработкой ПО.
Практические навыки:
Вопросы, выносимые на обсуждение:
Разработка требований и внешнее проектирование ПО. Анализ и разработка требований к ПО. Определение целей создания ПО. Разработка внешний спецификаций проекта. Использование программной инженерии при разработки ПО. Понятие CASE ? технологии. Обзор CASE-средств для проектирования ПО. Стандартизация и метрология в разработке программного обеспечения. Понятие качественного ПС и связанные с ним характеристики. Стандартизация показателей качества ПС. Характеристики качества базового международного стандарта ISO 9126:1991. Надежность ПО. Основные количественные показатели надежности. Классификация моделей надежности.
Продолжительность занятия – 9 часов / 3,5 часа (входит опрос по контрольной точке – 2).

Практическое занятие № 12.

Вид практического занятия: Дискуссии по актуальным темам и разбор практических кейсов , контрольная точка 3.
Раздел: Стандартизация, сертификация и управление качеством программного обеспечения
Тема и содержание занятия: Тема 4.3. Структурный подход к проектированию и управление качеством программного обеспечения.
Практическое занятие, предусматривающее Обсуждение рефератов, подготовленных студентами. Выступления приглашенных экспертов-практиков. Проведение круглых столов. Разбор кейсов.
Цель занятия: закрепить полученные в ходе практического занятия знания, приобрести навыки подхода к проектированию и управлению качеством программного обеспечения
Практические навыки:
Вопросы, выносимые на обсуждение:
Структурный подход к проектированию программного обеспечения. Характеристика и основные принципы структурного подхода. SADT (Structured Analysis and Design Technique), DFD (Data Flow Diagrams) и ERD (Entity-Relationship Diagrams) модели структурного подхода. Концепции функциональной модели SADT. Состав функциональной модели. Построение иерархии диаграмм моделей стандарта IDEF0. Типы связей между функциями.
Продолжительность занятия – 9 часов / 3,5 часа (входит опрос по контрольной точке – 3).

8. Перечень основной и дополнительной учебной литературы; перечень ресурсов информационно-телекоммуникационной сети «Интернет», перечень информационных технологий, необходимых для освоения дисциплины

8.1 Основная литература

1.Бабаш, А. В., Криптографические методы защиты информации : учебник / А. В. Бабаш, Е. К. Баранова. — Москва : КноРус, 2024. — 189 с. — ISBN 978-5-406-11913-6. — URL: https://book.ru/book/949929
2.Дергачев, К. В., Защита информации: лабораторный практикум : учебное пособие / К. В. Дергачев, Д. В. Титарев. — Москва : Русайнс, 2026. — 158 с. — ISBN 978-5-466-09618-7. — URL: https://book.ru/book/958732 . — Текст : электронный.
3.Максуров, А. А., Правовое обеспечение качества продукции (товаров, работ, услуг) : монография / А. А. Максуров. — Москва : Русайнс, 2022. — 100 с. — ISBN 978-5-4365-7506-3. — URL: https://book.ru/book/943421

8.2. Дополнительная литература

1.Краковский, Ю. М. Защита информации: Учебное пособие (ФГОС) / Краковский Ю.М. - Ростов-на-Дону :Феникс, 2016. - 347 с.ISBN 978-5-222-26911-4. - Текст : электронный. - URL: https://znanium.ru/catalog/document?pid=908844
2.Введение в системное проектирование интеллектуальных баз знаний : монография / С. А. Баркалов, А. В. Душкин, С. А. Колодяжный, В. И. Сумин ; под общ. ред. доктора техн. наук, профессора В. И. Новосельцева. - Москва : Горячая линия-Телеком, 2017. - 108 с. - ISBN 978-5-9912-0589-4. - Текст : электронный. - URL: https://znanium.ru/catalog/document?pid=1911606
3.Москвитин, Г. И., Комплексная защита информации в организации : монография / Г. И. Москвитин. — Москва : Русайнс, 2020. — 354 с. — ISBN 978-5-4365-1561-8. — URL: https://book.ru/book/934814
4.Берикашвили, В. Ш., Теория передачи информации : учебник / В. Ш. Берикашвили, С. З. Шкундин, С. П. Оськин. — Москва : КноРус, 2024. — 238 с. — ISBN 978-5-406-12428-4. — URL: https://book.ru/book/951858

8.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Электронно-библиотечная система «Znanium.ru»:http://znanium.ru/
2. Служба тематических толковых словарей «Глоссарий.ру»:http://www.glossary.ru/
3. Научная электронная библиотека «КиберЛенинка»:https://cyberleninka.ru/
4. Научно-технологическая инфраструктура Российской Федерации - URL:https://ckp-rf.ru/ntirf/objects/istc/

8.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

1. zbMATH – самая полная математическая база данных, охватывающая материалы с конца 19 века. zbMath содержит около 4 000 000 документов, из более 3 000 журналов и 170 000 книг по математике, статистике, информатике, а также машиностроению, физике, естественным наукам и др.[профессиональная база данных]: URL: https://zbmath.org/

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Процесс изучения дисциплины «Основы цифровой безопасности» предусматривает аудиторную (работа на лекциях и практических занятиях) и внеаудиторную (самоподготовка к лекциям и практическим занятиям) работу обучающегося.

В качестве основной методики обучения была выбрана методика, включающая - совокупность приёмов, с помощью которых происходит целенаправленно организованный, планомерно и систематически осуществляемый процесс овладения знаниями, умениями и навыками.

В качестве основных форм организации учебного процесса по дисциплине «Основы цифровой безопасности» в предлагаемой методике обучения выступают лекционные и практические занятия (с использованием интерактивных технологий обучения), а так же самостоятельная работа обучающихся.

Лекции

Лекция с мультимедийными презентациями и применением видеоматериалов, которая предполагает научное выступление лектора с обоснованием процессов и явлений, предусмотренных областью лекционного материала.

Теоретические занятия(лекции) организуются по потокам. На лекциях излагаются темы дисциплины, предусмотренные рабочей программой, акцентируется внимание на наиболее принципиальных и сложных вопросах дисциплины, устанавливаются вопросы для самостоятельной проработки. Конспект лекций является базой при подготовке к практическим занятиям, к экзаменам, а также самостоятельной научной деятельности.

Изложение лекционного материала проводится в мультимедийной форме (презентаций). Смысловая нагрузка лекции смещается в сторону от изложения теоретического материала к формированию мотивации самостоятельного обучения через постановку проблем обучения и показ путей решения профессиональных проблем в рамках той или иной темы. При этом основным методом ведения лекции является метод проблемного изложения материала.

Практические занятия

Практические занятия по дисциплине «Основы цифровой безопасности» проводятся с целью приобретения практических навыков в области разработки разделов компьютерное проектирование сферы сервиса.

Занятия проводятся в форе: интерактивного практического занятия с использованием компьютерной техники. Практическая работа заключается в выполнении студентами, под руководством преподавателя, комплекса учебных заданий направленных на приобретение практических навыков разработки разделов дисциплины «Основы цифровой безопасности». Выполнения практической работы студенты производят в интерактивном виде, в виде презентаций результата преподавателя. Отчет предоставляется преподавателю, ведущему данный предмет, в электронном и печатном виде.

Практические занятия способствуют более глубокому пониманию теоретического материала учебного курса, а также развитию, формированию и становлению различных уровней составляющих профессиональной компетентности студентов.

10. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю):

Учебные занятия по дисциплине «Основы цифровой безопасности» проводятся в следующих оборудованных учебных кабинетах:

Вид учебных занятий по дисциплине	Наименование оборудованных учебных кабинетов, объектов для проведения практических занятий с перечнем основного оборудования
Лекции	Поточная аудитория (видеопроекционная аппаратура с возможностью подключения к ПК, персональный компьютер, экран, доска, учебная мебель)
Практические занятия	Компьютерный класс 1109 или 1409 (персональные компьютеры, доска, учебная мебель)
Самостоятельная работа обучающихся	Читальный зал Научно-технической библиотеки университета Компьютерный класс 1409 (Учебная мебель, 20 компьютеров с возможностью выхода в информационно-телекоммуникационную сеть «Интернет», Экран, 19 компьютеров)