УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УНИВЕРСИТЕТ УПРАВЛЕНИЯ «ТИСБИ»

Кафедра информационных технологий

Утверждаю
Зав. кафедрой
О.В. Федорова
Протокол заседания
кафедры №12
от 30.04.2025

Рабочая программа дисциплины

Наименование дисциплины	Информационная безопасность
Направлению подготовки	27.03.02 «Управление качеством»
Профиль подготовки	Управление качеством в бизнес-системах
Год набора	2025

Составитель:
Ст. преп., Ахтямов Р.Р.

Казань

Содержание

1. Цели и задачи учебной дисциплины 3
2. Место дисциплины в структуре ОПОП 3
3. Требования к результатам освоения дисциплины 4
4. Структура и содержание дисциплины 4
4.1 Модульно-тематический план и пояснительная записка с указанием этапов формирования компетенций 5
4.2 Содержание дисциплины по темам (разделам) 8
4.3 Планы практических и семинарских занятий 8
4. 4 Планы практической подготовки/лабораторных занятий
5. Учебно-методическое обеспечение самостоятельной работы студентов 10
6. Учебно-методическое и информационное обеспечение дисциплины 12
7. Материально-техническое обеспечение дисциплины 13
8. Оценка компетенций по изучаемой дисциплине 13

Приложение 1. Методические указания для обучающихся по освоению дисциплины 13

Приложение 2. Фонд оценочных средств для проведения текущей и промежуточной аттестации по дисциплине 16

1. Цели и задачи учебной дисциплины

Данная дисциплина относится к обязательной части (Блок 1.Б) учебного плана подготовки бакалавров по направлению 27.03.02 «Управление качеством».

Цель дисциплины - сформировать у будущего бакалавра по направлению 27.03.02 «Управление качеством» представление о законодательстве в области информационной безопасности, о организационных и технических методах и средствах защиты компьютерной информации, о алгоритмах и компьютерных программах, пригодных для практического применения

Задачи дисциплины:

Знать требования информационной безопасности для решения стандартных задач профессиональной деятельности.
уметь выявлять угрозы информационной безопасности
Владеть основными методами предотвращения угроз информационной безопасности

2. Место дисциплины в структуре ОПОП

Данная дисциплина относится к обязательной части блока 1 учебного плана подготовки бакалавров по направлению «Управление качеством». До начала изучения дисциплины «Информационная безопасность» у студента должны быть сформированы компоненты компетенций, полученных в результате изучения дисциплины Программирование. Дисциплина находится во взаимосвязи с дисциплинами согласно схеме:

Обеспечивающие учебные дисциплины

Программирование

Информационная безопасность

Производственная практика (преддипломная практика)

3. Требования к результатам освоения дисциплины

Дисциплина «Информационная безопасность» участвует в формировании следующих компетенций в соответствии с ФГОС ВО по направлению «Управление качеством»:

ОПК-6. Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения

Знать требования информационной безопасности для решения стандартных задач профессиональной деятельности.
Уметь выявлять угрозы информационной безопасности
Владеть основными методами предотвращения угроз информационной безопасности

Декомпозиция компетенций

Индикаторы	**Результаты обучения по дисциплине**
Компетенция ОПК-6	
ОПК-6.3 Знает основы информационной безопасности при разработке компьютерных программ, пригодных для практического применения	**ОПК-6.3. З.З.** Знает требования информационной безопасности для решения стандартных задач профессиональной деятельности. **ОПК-6.3. У.З.** умеет выявлять угрозы информационной безопасности **ОПК-6.3. В.З.** Владеет основными методами предотвращения угроз информационной безопасности

4.Структура и содержание дисциплины.
4.1. Модульно-тематический план и пояснительная записка с указанием этапов формирования компетенций

4.1. Модульно-тематический план и пояснительная записка

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 академических часа)

Модульная разбивка курса					
Направление Управление качеством Дисциплина: информационная безопасность					
Наименование модулей	Количество ауд. Часов		Самостоятельная работа очное/ заочное	Всего часов	Индикаторы компетенции
	Лекции Очное/ заочное	Практика Очное/ заочное			

Модуль 1					
Тема 1. Основы информационной безопасности.	1/1	0/0	6/8	7/9	ОПК-6.3
Тема 2. Службы информационной безопасности.	1/1	0/1	6/10	7/11	ОПК-6.3
Тема 3. Шифрование.	2/1	2/1	10/10	14/12	
Модуль 2					
Тема 4. Процедурный уровень информационной безопасности.	1/1	2/1	10/10	13/12	ОПК-6.3
Тема 5. Идентификация и аутентификация, управление доступом.	1/0	2/1	14/10	17/11	
Модуль 3					
Тема 6. Обеспечение информационной безопасности.	2/1	2/1	12/10	16/12	ОПК-6.3
Тема 7. Обеспечение сетевой безопасности.	2/1	2/1	12/10	16/12	
зачет			18/18	18/18	
Всего	10/6	10/6	88/96	108	

Пояснительная записка
с этапами формирования компетенций

Каждый модуль состоит из нескольких тем, содержащих определенный раздел учебного материала, и представляет собой законченный блок информации. По каждой теме в соответствии с учебным планом читаются лекции и проводятся практические занятия. Предусмотрена индивидуальная самостоятельная работа, состоящая из подготовки к разделам, выделенным для самостоятельного изучения, подготовки к практическим занятиям по соответствующим темам с использованием лекционного материала, учебных пособий, учебно-методических комплексов, Internet-ресурсов, а также рекомендованной дополнительной литературы.

После прохождения первого модуля, включающего в себя три темы, будут получены следующие образовательные результаты:

Студент должен иметь понятия о основных понятиях о безопасности и основах атак и защиты от них.

Знать - основы защиты компьютерной информации; правовые основы защиты компьютерной информации, организационные, технические программные методы защиты информации , модели и методы шифрования.

Уметь - выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС.

Владеть- навыками проектирования программ для криптографического шифрования

Уровень освоения полученных знаний и умений проверяется компьютерным тестированием и решением практических задач с использованием программных средств в соответствии с темами изучаемого модуля.

После прохождения второго модуля, включающего в себя две темы, будут получены следующие образовательные результаты:

Студент должен иметь понятия о: о процедурном уровне информационной безопасности, основах идентификации и аутентификации.

Знать - организационные, технические программные методы защиты информации. модели и методы аутентификации пользователей

Уметь - обосновывать организационно-технические мероприятия по защите информации в ИС, выявлять угрозы информационной безопасности.

Владеть- навыками создания программ для поддержания безопасности

Уровень освоения полученных знаний и умений проверяется компьютерным тестированием и решением практических задач с использованием программных средств в соответствии с темами изучаемого модуля.

После прохождения третьего модуля, включающего в себя две темы, будут получены следующие образовательные результаты:

Студент должен иметь понятия о основных понятиях о обеспечении сетевой и информационной безопасности

Знать – основы сетевой и информационной безопасности

Уметь выявлять угрозы информационной технической и физической безопасности

Данное деление дисциплины на модули активизирует самостоятельную работу студентов, повышает интенсивность и системность учебной работы, регулирует контроль учебной деятельности студентов в течении семестров, усиливает мотивацию студентов к изучению учебного материала.

Контроль знаний, умений и навыков является неотъемлемой частью процесса освоения учебного материала и включает в себя следующие формы:

- текущий контроль;
- промежуточный контроль.

4.2. Содержание дисциплины по темам

Тема 1. Основы информационной безопасности.
Основные понятия информационной безопасности. ФЗ "Об информации, информационных технологиях и о защите информации. Определение безопасности как процесса.

Тема 2. Службы информационной безопасности.
Конфиденциальность. Идентифицируемость.

Тема 3. Шифрование.
Основные концепции шифрования. Шифрование с открытым ключом. Цифровые подписи. Управление ключами.

Тема 4. Процедурный уровень информационной безопасности.
Основные классы мер процедурного уровня. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Основные понятия программно-технического уровня информационной безопасности.

Тема 5. Идентификация и аутентификация, управление доступом.
Идентификация и аутентификация. Управление доступом. Ролевое управление доступом.

Тема 6. Обеспечение информационной безопасности.
Определение риска. Оценка стоимости. Порядок разработки политик. Проведение профессиональной переподготовки. Проведение аудита.

Тема 7. Обеспечение сетевой безопасности.
Административная безопасность. Планы выхода из критических ситуаций.

4.3. Планы практических и семинарских занятий

1. Изучить алгоритмы подстановки, перестановки, написать программу шифрования методом Виженера
2. Написать программу генерации паролей по заданным условиям.
3. Разработать презентацию по основам информационной безопасности*

4.4.Планы практической подготовки/лабораторных занятий

Не предусмотрено учебным планом.

5.Учебно-методическое обеспечение самостоятельной работы студентов

В процессе самостоятельного изучения студент обязан проработать перечисленные ниже темы, для углубления теоретических знаний и практических навыков.

Темы для самостоятельного изучения

Тема 1. Критерии и оценки защищенности информационных систем.
Тема 2.Организационная защита. Служба информационной безопасности. Политика безопасности. Работа с персоналом. Физическая защита. Защита от несанкционированного доступа. Безопасность операционных систем.
Тема 4. Виды аутентификации. Защита паролей административными методами. Криптографические методы аутентификации. Протоколы взаимной проверки подлинности. Протоколы и модели цифровых сигнатур с посредником и без участия посредника.
Тема 5. Правовая защита. Защита конфиденциальной информации. Уголовный кодекс о защите информации.

6. Учебно-методическое и информационное обеспечение

Основная:

1. Киренберг, А. Г. Системное администрирование и информационная безопасность сетей ЭВМ : учебное пособие / А. Г. Киренберг. — Кемерово : Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2022. — 119 с. — ISBN 978-5-00137-292-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/128406.html — Режим доступа: для авторизир. Пользователей Гарантированный срок размещения в IPR SMART до 22.03.2028 (автопролонгация)
2. Басыня Е.А. Сетевая информационная безопасность [Электронный ресурс]: учебник/ Басыня Е.А.— Электрон. текстовые данные.— М.: Национальный исследовательский ядерный университет «МИФИ», 2023. — 224 с. — Режим доступа: https://www.iprbookshop.ru/132693.html. — IPR SMART
3.

Дополнительная

1. Бондаренко И.С. Информационная безопасность [Электронный ресурс]: учебник/ Бондаренко И.С.— Электрон. текстовые данные.— М.: Издательский Дом МИСиС, 2023.— 254 с.— Режим доступа: https://www.iprbookshop.ru/137525.html.— IPR SMART, по паролю Лицензия: весь срок охраны авторского права

Интернет-ресурсы и перечень ежегодно обновляемых современных профессиональных баз данных и информационных справочных систем:

1. http://www.iprbookshop.ru Цифровой образовательный ресурс IPR SMART
2. http://www.urait.ru – Образовательная платформа ЮРАЙТ
3. www.securitylab.ru
4. http://citforum.ru/
5. www.SecurityPolicy.ru

7. Материально-техническое обеспечение дисциплины

В процессе изучение данной дисциплины используется учебная аудитория, кабинет для самостоятельной работы студентов, читальный зал, видеопроекционное оборудование, компьютер, оснащенный типовым пакетом системного и офисного ПО, в соответствии с Реестром материально-технического обеспечения аудиторного фонда Университета управления «ТИСБИ».

Во время лекций: проектор, экран, компьютер с выходом в интернет
Во время практики: компьютерный класс

1.Типовой пакет системного и офисного ПО, Персональный компьютер с выходом в интернет в компьютерных классах Университета для каждого студента на практических занятиях.
Учебная аудитория в соответствии с расписанием, кабинет для самостоятельной работы студентов.

Пакет лицензионного системного и офисного ПО включает в себя:
- Операционная система Microsoft Windows 10 Pro.
- Microsoft Office 2013.

Программное обеспечение, входящее в типовой установочный пакет, получает обновление в автоматическом, установленном разработчиком (компанией Microsoft) порядке, посредством сети Интернет.

Подтверждающие документы: Microsoft Open License №40962726 от 16.08.2006г., №44971865 от 24.12.2008г., №46256422 от 11.12.2009г., №61280992 от 13.12.2012г.; Акт приема-передачи неисключительного ограниченного права на лицензионное ПО № ПРСЧ-12-04326 от 18.12.2013г., №558 от 18.12.2014г., №ПРСЧ-15-01353 от 10.11.2015г., №272 от 15.04.2016г., бухгалтерск
- Открытая среда разработки программного обеспечения - Lazarus.

8. Оценка компетенций по изучаемой дисциплине

Для оценки результатов обучения рекомендуется использовать модульно-рейтинговую систему оценивания знаний, умений и навыков студентов по окончанию изучения каждого Модуля в соответствии с Положением о модульно-рейтинговой системе организации образовательного процесса. Итоговая оценка (в баллах) складывается из баллов, набранных по каждому Модулю (семестровая оценка) и баллов, набранных, непосредственно на зачете.
Расчет набранных баллов по дисциплине осуществляется в следующей последовательности:
$C = \frac{M_1 + M_2 + ...M_n}{n} \times 0{,}6$, где М – количество баллов по модулю; n – количество модулей
$З = K \times 0{,}4$, где К - количество баллов на зачете;
$И = C + З + П$, где П – поощрительные баллы (от 1 до 5).

Уровень сформированности компетенций и их основные признаки оцениваются по следующим таблицам:

Оценка уровня сформированности компетенции ОПК-6
«Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения»
в части дисциплины «Информационная безопасность»

№ п/п	Уровни сформированности компетенции	Основные признаки уровня	Инструменты оценки сформированности уровня
1	**Пороговый уровень (как минимально допустимый)** (обязательный для всех студентов-выпускников вуза по завершении освоения ОПОП ВО) (от 60 до 70 баллов)	Частично знает требования информационной безопасности для решения стандартных задач профессиональной деятельности. Частично умеет выявлять угрозы информационной безопасности Владеет основными методами предотвращения угроз информационной безопасности	Компьютерное тестирование, Практические задания зачет
2	**Базовый уровень (относительно порогового уровня)** **(**От 71 до 85 баллов**)**	В основном знает требования информационной безопасности для решения стандартных задач профессиональной деятельности. В основном умеет выявлять угрозы информационной безопасности Владеет основными методами предотвращения угроз информационной безопасности	Компьютерное тестирование, Практические задания зачет
3	**Повышенный уровень (относительно порогового уровня)** (От 86 до 100 баллов)	Знает требования информационной безопасности для решения стандартных задач профессиональной деятельности. умеет выявлять угрозы информационной безопасности Владеет основными методами предотвращения угроз информационной безопасности	Компьютерное тестирование, Практические задания зачет

Приложение 1

Методические рекомендации для обучающихся по освоению дисциплины.

Самостоятельная работа является важным элементом освоения основной программы курса. В соответствии со спецификой предмета, самостоятельная работа включает в себя:

- подготовку к практическим занятиям по темам;
- самостоятельное изучение материала по заданным преподавателем темам;
- работу с литературой и учебно-методическими пособиями;

Самостоятельная подготовка к практическим занятиям выполняется студентом в свободное от занятий время и включает в себя:

- проработку лекционного материала по указанной теме;
- подготовку к семинарам по темам, предложенным преподавателем;
- предоставление результатов самостоятельной работы преподавателю.

Приложение 2

УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УНИВЕРСИТЕТ УПРАВЛЕНИЯ «ТИСБИ»
Кафедра информационных технологий

Фонд оценочных средств
для проведения текущей и промежуточной аттестации
по дисциплине
«Информационная безопасность»

направление подготовки: Управление качеством

профиль подготовки: Управление качеством в бизнес-системах

Казань

Содержание

1. Паспорт фонда оценочных средств
2. Наполнение фонда оценочных средств по формам контроля
   2.1 Фонд оценочных средств и шкала оценивания для текущего контроля.
      2.1.1 Компьютерное тестирование
      2.1.2 Практические задания

   2.2 Фонд оценочных средств и шкала оценивания для промежуточного контроля.
      2.2.1 Фонд оценочных средств для проверки знаний и умений (вопросы к зачету)
      2.2.2 Фонд оценочных средств для проверки сформированности навыков (задачи к зачету)

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Формы контроля / **Фор-мируемые компетенции и их индикаторы**	**ОПК-6**		
	ОПК-6.3		
Формы текущего контроля			
Компьютерное тестирование	ЗЗ		
Выполнение практических заданий	ЗЗ	УЗ	ВЗ
Формы промежуточного контроля			
зачет	ЗЗ	УЗ	ВЗ

З- знания, У- умения, В-владения

2.1 Фонд оценочных средств и шкала оценивания для текущего контроля

2.1.1 Тестирование компьютерное

Тестирование заключается в ответе студентом на тестовые вопросы по определенной теме или блоку тем, заданных преподавателем. Данный вид работы способствует в актуализации знаний студентами по данной дисциплине.

Образцы заданий для компьютерного тестирования

1. Сколько главных элементов оценки в организации.
a) 3
b) 4
c) 5
d) 6
2. Назовите этапы процесса информационной безопасности.
a) оценку;
b) политику;
c) реализацию;
d) квалифицированную подготовку;
e) аудит.

3. Почему информационная политика и политика безопасности разрабатываются в первую очередь?

a)она формирует основу понимания того, почему внутренняя информация важна.
b)она формирует основу понимания того, насколько внутренняя информация должна быть защищена
c)этот документ послужит основой для программы обучения специалистов по вопросам безопасности, наряду с политикой использования и политикой паролей
d)информационную политику безопасности проще всего создать
4. Система защиты государственных секретов определяется Законом
"Об информации, информатизации и защите информации"
"Об органах ФСБ"
"О государственной тайне"
"О безопасности"

Критерии оценивания компьютерного тестирования

Результат компьютерного тестирования выдается в процентах. Порог прохождения компьютерного тестирования – 60%. 1% приравнивается к 1 баллу. Правильно ответив на все вопросы теста студент может набрать 100 баллов.

В качестве промежуточного контроля (зачет,) знаний введен устный опрос

2.1.2 Выполнение практических заданий

Практические задания выполняются в соответствии с методическими указаниями по выполнению практических заданий изданных в УВО УУ «ТИСБИ».

Темы практических заданий

1. Задание 1: написать программу: Шифрование методом Виженера
2. Задание 2: написать программу: Генератор паролей
3. Задание 3: Задачи построения системы защиты информации
4. Задание 4: Задача обеспечения корректной реализации базового уровня защиты

Критерии оценивания практического задания

Результат	Балл
Демонстрирует полное понимание практического задания, логично и последовательно выполняет его.	100-86
Демонстрирует частичное понимание практического задания, после дополнительного объяснения последовательно выполняет его.	85-71
Демонстрирует непонимание практического задания, после	70-60

дополнительного объяснения выполняет задание, но не все работает верно.	
Демонстрирует непонимание практического задания.	Менее 60

2.2 Фонд оценочных средств и шкала оценивания для промежуточного контроля

2.2.1 Фонд оценочных средств для проверки знаний/умений

Вопросы к зачету

1. Определение информационной безопасности
2. Понятие об информационной безопасности
3. Определение безопасности как процесса
4. Обзор российского законодательства в области информационной безопасности
5. Наиболее распространенные угрозы
6. Основные определения и критерии классификации угроз
7. Наиболее распространенные угрозы доступности
8. Основные концепции шифрования
9. Шифрование с открытым ключом
10. Службы информационной безопасности: Конфиденциальность, Целостность, Доступность, Идентифицируемость
11. Настройки паролей
12. Контроль доступа к файлам
13. Процедурный уровень информационной безопасности
14. Основные классы мер процедурного уровня
15. Управление персоналом
16. Идентификация и аутентификация
17. Управление доступом
18. Административная безопасность Политики и процедуры
19. Обучение: Превентивные меры, Принудительные меры, Поощрительные меры.
20. Техническая безопасность

2.2.2.Фонд оценочных средств для проверки умений/навыки задачи для проверки сформированности умений и навыков студентов

1. Прописать моделирование защиты информационной системы при помощи шифрования
2. Прописать моделирование защиты информационной системы при помощи аутентификации и паролей
3. Рассказать о основных законах Российского законодательства по информационной безопасности
4. Прописать основы сетевой безопасности для разных предприятий по выбору (ВУЗ, Торговый Центр, Офис)
5. Прописать основы информационной безопасности для разных предприятий по выбору (ВУЗ, Торговый Центр, Офис)

Критерии оценки уровня усвоения знаний, умений и навыков по результатам зачета

Характеристика ответа	Европейская оценка	Рубежные баллы	Оценка	Уровень сформированности
Дан полный, развернутый ответ на поставленный теоретический вопрос, показана совокупность осознанных знаний об объекте, проявляющаяся в свободном ориентировании понятиями, умении выделить существенные и несущественные его признаки, причинно-следственные связи. Знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Ответ формулируется в терминах науки, изложен литературным языком, логичен, доказателен, демонстрирует авторскую позицию студента. При ответе студент демонстрирует применение знаний к реальным профессиональным ситуациям, объясняет решение задачи на уровне анализа, синтеза и дает свою оценку решения проблемы. Причем студент не затрудняется с ответом при видоизменении задания и правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач. Знает основы защиты компьютерной информации; правовые основы защиты компьютерной информации, организационные, технические программные методы защиты информации, модели и методы шифрования, модели и методы аутентификации пользователей, правила работы с конфиденциальной информацией Умеет выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС Владеет навыками проектирования защищенных информационных систем обработки информации и управления	**A**	**100-96**	**зачтено**	**Повышенный уровень сформированности компетенций**
Дан полный, развернутый ответ на поставленный теоретический вопрос, показана совокупность осознанных знаний об объекте, доказательно раскрыты основные положения темы; в ответе прослеживается четкая структура,	**A**	**95-91**	**зачтено**	**Повышенный уровень сформирова**

логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Умеет тесно увязывать теорию с практикой. Задача решена правильно и с обоснованием принятого решения. Ответ изложен литературным языком в терминах науки. Могут быть допущены недочеты в определении понятий, исправленные студентом самостоятельно в процессе ответа. Знает основы защиты компьютерной информации; правовые основы защиты компьютерной информации, организационные, технические программные методы защиты информации, модели и методы шифрования, модели и методы аутентификации пользователей, правила работы с конфиденциальной информацией Умеет выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС Владеет навыками проектирования защищенных информационных систем обработки информации и управления				
Дан полный, развернутый ответ на поставленный вопрос, доказательно раскрыты основные положения темы; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Задача решена верно, правильно обосновывает принятую методику решения задачи. Ответ изложен литературным языком в терминах науки. В ответе допущены недочеты, исправленные студентом с помощью преподавателя. Знает основы защиты компьютерной информации; правовые основы защиты компьютерной информации, организационные, технические программные методы защиты информации, модели и методы шифрования, модели и методы аутентификации пользователей,	**A**	**90-86**	**зачтено**	

правила работы с конфиденциальной информацией Умеет выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС Владеет навыками проектирования защищенных информационных систем обработки информации и управления				
Дан полный, развернутый ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, изложен литературным языком в терминах науки. Студент владеет разносторонними навыками и приемами выполнения практических задач. Могут быть допущены недочеты или незначительные ошибки, исправленные студентом с помощью преподавателя. Знает основы защиты компьютерной информации; правовые основы защиты компьютерной информации, организационные, технические программные методы защиты информации, модели и методы шифрования, модели и методы аутентификации пользователей, правила работы с конфиденциальной информацией Умеет выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС Владеет основными навыками проектирования защищенных информационных систем обработки информации и управления	**B**	**85-81**	**зачтено**	**Базовый уровень сформированности компетенций**
Дан полный, развернутый ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, изложен в терминах науки. Студент владеет разносторонними навыками и приемами выполнения практических задач. Ответы на дополнительные вопросы логичны, изложены в терминах науки, однако допущены незначительные ошибки или недочеты, исправленные студентом с	**C**	**80-76**	**зачтено**	

помощью "наводящих" вопросов преподавателя. Знает основы защиты компьютерной информации; правовые основы защиты компьютерной информации, организационные, технические программные методы защиты информации, модели и методы шифрования, модели и методы аутентификации пользователей, правила работы с конфиденциальной информацией Умеет выявлять основными угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС Владеет основными навыками проектирования защищенных информационных систем обработки информации и управления				
Студент демонстрирует достаточные теоретические и практические знания. Дан полный, но недостаточно последовательный ответ на поставленный вопрос, но при этом показано умение выделить существенные и несущественные признаки и причинно-следственные связи. Ответ логичен и изложен в терминах науки. Могут быть допущены 1-2 ошибки в определении основных понятий или решении практической задачи, которые студент затрудняется исправить самостоятельно. Знает основы защиты компьютерной информации; правовые основы защиты компьютерной информации, организационные, технические программные методы защиты информации, модели и методы шифрования, модели и методы аутентификации пользователей, правила работы с конфиденциальной информацией Умеет частично выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС Владеет частично навыками проектирования защищенных информационных систем обработки информации и управления	**С**	**75-71**	**зачтено**	

Дан недостаточно полный и развернутый ответ. Логика и последовательность изложения имеют нарушения. Допущены ошибки в раскрытии понятий, употреблении терминов. Студент не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи. Студент может конкретизировать обобщенные знания, доказав на примерах их основные положения только с помощью преподавателя. Речевое оформление требует поправок, коррекции. Студент испытывает затруднения при выполнении практической задачи и не может связать теорию с практикой. Знает основы защиты компьютерной информации; правовые основы защиты компьютерной информации, организационные, технические программные методы защиты информации, стандарты, модели и методы шифрования, модели и методы аутентификации пользователей, правила работы с конфиденциальной информацией Умеет частично выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС	**D**	**70-66**	**зачтено**	**Пороговый уровень сформированности компетенций**
Дан неполный ответ, логика и последовательность изложения имеют существенные нарушения. Допущены грубые ошибки при определении сущности раскрываемых понятий, теорий, явлений, вследствие непонимания студентом их существенных и несущественных признаков и связей. В ответе отсутствуют выводы. Умение раскрыть конкретные проявления обобщенных знаний не показано. Испытывает затруднения при выполнении практических задач. Речевое оформление требует поправок, коррекции. Знает основы защиты компьютерной информации; правовые основы защиты компьютерной информации, организационные, технические программные методы защиты информации, стандарты, модели и методы шифрования, модели и методы аутентификации пользователей, правила работы с конфиденциальной информацией	**E**	**65-61**	**зачтено**	

Умеет частично выявлять угрозы информационной безопасности.				
Дан неполный ответ. Присутствует нелогичность изложения. Студент затрудняется с доказательностью. Масса существенных ошибок в определениях терминов, понятий, характеристике фактов, явлений. В ответе отсутствуют выводы. Речь неграмотна. При ответе на дополнительные вопросы студент начинает понимать связь между знаниями только после подсказки преподавателя	**E**	**60**	**зачтено**	
Ответ отсутствует. Студент затрудняется с доказательностью. Масса существенных ошибок в определениях терминов, понятий, характеристике фактов, явлений. В ответе отсутствуют выводы. Речь неграмотна. При ответе на дополнительные вопросы студент не понимает связь между знаниями	**F**	**Менее 60**	**Не зачтено**	Компетенции не сформированы