УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УНИВЕРСИТЕТ УПРАВЛЕНИЯ «ТИСБИ»

Кафедра финансы и кредит



Рабочая программа дисциплины

Наименование дисциплины:	Средства и методы защиты информации
Специальность	38.05.01 Экономическая безопасность
Специализация подготовки	Экономико-правовое обеспечение экономической безопасности
Год набора	2023, 2024, 2025, 2026

Составитель:
канд.экон.наук., доцент Базаров Р.Т.
.

Казань

Содержание

1. Цели и задачи учебной дисциплины 3
2. Место дисциплины в структуре ОПОП 4
3. Требования к результатам освоения дисциплины 5
4. Структура и содержание дисциплины 6

4.1 Модульно-тематический план и пояснительная записка с указанием этапов формирования компетенций 6
4.2 Содержание дисциплины по темам (разделам) 8
4.3 Планы практических и семинарских занятий 11
5. Учебно-методическое обеспечение самостоятельной работы студентов 13
6. Учебно-методическое и информационное обеспечение дисциплины 13
7. Материально-техническое обеспечение дисциплины 14
8. Оценка компетенций по изучаемой дисциплине 14

Приложение 1. Методические указания для обучающихся по освоению дисциплины

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

1. Цели и задачи учебной дисциплины

Данная дисциплина относится к обязательной части дисциплин Блока 1. Б находится во взаимосвязи с дисциплинами согласно схеме:

Цель дисциплины - изучение организационных и технических методов и средств защиты компьютерной информации, законодательства и стандартов в области проектирования автоматизированных систем обработки информации и управления (АСОИУ).

Задачи дисциплины:

- получение представлений об основах защиты компьютерной информации,
- знание правовых основ защиты компьютерной информации,
- знание организационных, технические программные методов защиты информации ,
- знание моделей и методов аутентификации пользователей,
- знание правил работы с конфиденциальной информацией.

2. Место дисциплины в структуре ОПОП

Данная дисциплина относится к части «Экономико-правовое обеспечение экономической безопасности» учебного плана подготовки специалиста по 38.05.01 «Экономическая безопасность

Обеспечивающие учебные дисциплины

↓

Сквозные технологии в экономике
Учебная практика: ознакомительная практика
Учебная практика: практика по профилю профессиональной деятельности
Производственная практика: практика по профилю профессиональной деятельности

Средства и методы защиты информации

↓

Производственная практика (Преддипломная практика)

До начала изучения дисциплины «Средства и методы защиты информации» у студента должны быть сформированы компоненты компетенций, полученных в результате изучения дисциплин Информационная безопасность предприятия.

3.Требования к результатам освоения дисциплины

Дисциплина «Средства и методы защиты информации» участвует в формировании следующих компетенций в соответствии с ФГОС+++ ВО по специальности «Экономическая безопасность»:
ОПК-6 – способен использовать современные информационные технологии и программные средства при решении профессиональных задач

Декомпозиция компетенций

Индикаторы	**Результаты обучения по дисциплине**
Компетенция ОПК-6	
ОПК-6.1 ОПК-6.ОПК-6.1. Определяет методы сбора информации, способы и вид ее представления, применяя современное программное обеспечение при решении профессиональных задач	ОПК-6.1. З.4 Знает основы современных информационных технологий и программных средств при решении профессиональных задач.
	ОПК-6.1. У.4 Умеет использовать современные информационные технологии и программные средства при решении профессиональных задач.
	ОПК-6.1. В.4 Владеет навыками использования современные информационные технологии и программные средства при решении профессиональных задач.
ОПК-6.2 ОПК-6.ОПК-6.2. Выбирает соответствующие содержанию профессиональных задач инструментарий обработки и анализа данных, современные информационные технологии и программные средства	ОПК-6.2. З.8 Знает основы содержания профессиональных задач инструментарий обработки и анализа данных, современных информационных технологий и программных средств;
	ОПК-6.2. У.9 Умеет использовать соответствующие содержанию профессиональных задач инструментарии обработки и анализа данных, современные информационные технологии и программные средства;
	ОПК-6.2. В.9 Владеет навыками использования, соответствующие содержанию профессиональных задач инструментарий обработки и анализа данных, современные информационные технологии и программные средства;

4. Структура и содержание дисциплины.

4.1. Модульно-тематический план и пояснительная записка с указанием этапов формирования компетенций

Общая трудоемкость дисциплины по очному и заочному обучению составляет 4 зачетные единицы (144 академических часа)

Модульная разбивка курса					
Направление Экономическая безопасность Дисциплина: Средства и методы защиты информации					
Наименование модулей	Количество ауд. Часов		Самостоятельная работа	Всего часов	Формируемые индикаторы
	лекции	практика			
Модуль 1 Основные понятия о безопасности					
Тема 1. Основы информационной безопасности.	4/-	3/-	-/9	7/9	ОПК-6.1 ОПК-6.2 З.4 З.8 У.4 У.9
Тема 2. Категории атак.	4	4	10/10	18/10	
Модуль 2 Основы атак и защиты от них					
Тема 3. Службы информационной безопасности.	4	4	-/9	8/9	ОПК-6.1 ОПК-6.2 З.4 З.8 У.4 У.9
Тема 4. Шифрование.	2	4	11/10	17/10	
Модуль 3 Основы идентификации и аутентификации					
Тема 5. Процедурный уровень информационной безопасности.	2		-/9	2/9	ОПК-6.1 ОПК-6.2 З.4 З.8 У.4 У.9 В. 4 В. 9
Тема 6. Идентификация и аутентификация, управление доступом.	4	6	20/9	30/9	
Модуль 4 Основы межсетевых экранов и защиты от рисков и основы защиты сетевой безопасности					
Тема 7. Межсетевые экраны.	4/2	2/2	-/10	6/14	ОПК-6.1 ОПК-6.2 З.4 З.8 У.4 У.9 В. 4 В. 9
Тема 8. Управление риском.	4/2	4/2	5/10	13/14	
Тема 9. Обеспечение информационной безопасности. *	4/2	4/2	-/10	8/14	

Тема 10. Обеспечение сетевой безопасности.	3/2	4/2	5/10	12/14	
Подготовка к зачету			5/5	5/5	
Подготовка к экзамену			18/27	18/27	
Всего	35/8	35/8	74/128	144/144	

* интерактивные занятия

Пояснительная записка с этапами формирования компетенций

Данный модульный курс состоит из 4 модулей, порядок освоения которых выстраивает траекторию и этапы формирования заявленных компетенций (или их составляющих). Порядок освоения модулей выстраивает траекторию и этапы формирования заявленных компетенций (или их составляющих).

Модуль 1 «основные понятия о безопасности» и включает в себя две учебные темы.

В результате прохождения первого модуля студент получает мотивацию к выполнению своей профессиональной деятельности и должен

Знать

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

Уметь

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

Уровень освоения полученных знаний, умений и навыков проверяется тестовым опросом и решением практических задач ОПК-6. З.4 З.8 У.4 У.9

Модуль 2 «основы атак и защиты от них» и включает в себя две учебные темы.

В результате прохождения второго модуля студент должен

Знать

основы защиты компьютерной информации;

правовые основы защиты компьютерной информации

организационные, технические программные методы защиты информации

правила работы с конфиденциальной информацией.

Уметь

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

Владеть

навыками проектирования защищенных информационных систем обработки информации и управления

Уровень освоения полученных знаний, умений и навыков проверяется тестовым опросом и решением практических задач. ОПК-6. З.4 З.8 У.4 У.9

Модуль 3 «основы идентификации и аутентификации» и включает в себя две учебные темы.

В результате прохождения второго модуля студент должен

Знать

основы защиты компьютерной информации;

организационные, технические программные методы защиты информации

модели и методы аутентификации пользователей,

правила работы с конфиденциальной информацией.

Уметь

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

Владеть

навыками проектирования защищенных информационных систем обработки информации и управления

Уровень освоения полученных знаний, умений и навыков проверяется тестовым опросом и решением практических задач. ОПК-6. З.4 З.8 У.4 У.9 В. 4 В. 9

Модуль 4 «основы межсетевых экранов и защиты от рисков и основы защиты сетевой безопасности» и включает в себя четыре учебные темы.

В результате прохождения второго модуля студент должен

Знать

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.

Уметь

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

Владеть

навыками проектирования защищенных информационных систем обработки информации и управления

Уровень освоения полученных знаний, умений и навыков проверяется тестовым опросом и решением практических задач. ОПК-6. З.4 З.8 У.4 У.9 В. 4 В. 9

Уровень освоения полученных знаний, умений и навыков проверяется тестовым опросом и решением практических задач.

4.2. Содержание дисциплины по темам (разделам)

Тема 1. Основы информационной безопасности.

Основные понятия информационной безопасности. ФЗ "Об информации, информационных технологиях и о защите информации. Определение безопасности как процесса. О защите государственной тайны.

Тема 2. Категории атак.

Определение атаки доступа. Как выполняются атаки доступа. Информация в электронном виде. Определение атаки модификации. Как выполняются атаки модификации. Определение атак на отказ в обслуживании. Как выполняются атаки на отказ в обслуживании. Определение атаки на отказ от обязательств.

Тема 3. Службы информационной безопасности.

Конфиденциальность. Идентифицируемость.

Тема 4. Шифрование.

Основные концепции шифрования. Шифрование с открытым ключом. Цифровые подписи. Управление ключами. Доверие в информационной системе. Разработка системы шифрования. Шифрование.

Тема 5. Процедурный уровень информационной безопасности.

Основные классы мер процедурного уровня. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ. Основные программно-технические меры

Основные понятия программно-технического уровня информационной безопасности.

Тема 6. Идентификация и аутентификация, управление доступом.

Идентификация и аутентификация. Управление доступом. Ролевое управление доступом.

Тема 7. Межсетевые экраны.

Определение типов межсетевых экранов. Межсетевые экраны прикладного уровня. Межсетевые экраны с пакетной фильтрацией.

Тема 8. Управление риском.

Определение риска. Уязвимость. Угроза. Выявление риска для организации. Исследование контрмер. Оценка риска. Методика оценки риска.

Тема 9. Обеспечение информационной безопасности.

Определение риска. Оценка стоимости. Разработка политики. Порядок разработки политик. Реализация политики безопасности. Проведение профессиональной переподготовки. Проведение аудита.

Тема 10. Обеспечение сетевой безопасности.
Административная безопасность. Планы выхода из критических ситуаций. Техническая безопасность. Физическая безопасность.

4.3. Планы семинарских и практических занятий

Тема 1. Основы информационной безопасности.
1. Назовите основные понятия информационной безопасности. ФЗ "Об информации, информационных технологиях и о защите информации.
2. Дайте определение безопасности как процесса.
3. Что такое защита государственной тайны.

Тема 2. Категории атак.
1. Дайте определение атаки доступа.
2. Как выполняются атаки доступа. Информация в электронном виде.
3. Дайте определение атаки модификации.
4. Как выполняются атаки модификации.
5. Как выполняются атаки на отказ в обслуживании.
6. Дайте определение атаки на отказ от обязательств.

Тема 3. Службы информационной безопасности.
1. Что такое конфиденциальность.
2. Что такое идентифицируемость.

Тема 4. Шифрование.
1. Назовите основные концепции шифрования. Шифрование с открытым ключом.
2. Какие бывают цифровые подписи. Управление ключами.
3. Доверие в информационной системе – что это?
4. Разработка системы шифрования. Шифрование.

Тема 5. Процедурный уровень информационной безопасности.
1. Назовите основные классы мер процедурного уровня. 2. Основные программно-технические меры.
3. Назовите основные понятия программно-технического уровня информационной безопасности.
4. Планирование восстановительных работ.

Тема 6. Идентификация и аутентификация, управление доступом.
1.Идентификация и аутентификация – что это?
2. Управление доступом. Ролевое управление доступом.

Тема 7. Межсетевые экраны.
1. Дайте определение типов межсетевых экранов.
2. Дайте характеристику межсетевым экранам прикладного уровня.
3. Дайте характеристику межсетевым экранам с пакетной фильтрацией.

Тема 8. Управление риском.
1. Определение риска. Уязвимость. Угроза.
2. Выявить риски для организации.
3. Исследовать контрмер, ценку риска.
4. Методика оценки риска.

Тема 9. Обеспечение информационной безопасности.

1. Определение риска. Оценка стоимости. Разработка политики.
2. Порядок разработки политик.
3. Реализация политики безопасности.
4. Проведение профессиональной переподготовки.
5. Проведение аудита.

Тема 10. Обеспечение сетевой безопасности.

1. Дать определение административной безопасности.
2. Планы выхода из критических ситуаций.
3. Дать определение технической безопасности.
4. Дать определение физическая безопасности.

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 . Руководящие документы Гостехкомиссии РФ. Классификация автоматизированных систем и требования по защите информации. Критерии оценки безопасности компьютерных систем Министерства оборона США.

Тема 2.Организационная защита. Служба информационной безопасности. Политика безопасности. Работа с персоналом. Физическая защита. Защита от несанкционированного доступа. Безопасность операционных систем.

Тема 3. Статистический анализ шифрованного текста. Многоалфавитные системы. Системы одноразового использования. Гаммирование. Алгоритм DES и стандарты шифрования данных. Системы с открытым ключом. Управление ключами. Проблемы и перспективы криптографических систем. Реализация криптографических методов.

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. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2025. — 349 с. — (Высшее образование). — ISBN 978-5-534-19762-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561077.

2. Внуков, А. А. Защита информации : учебник для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561313.

3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2025. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/562070.

Дополнительная:

1. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2022. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489919

2. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/467356

3. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2020. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450998

4. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2022. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/491249

Интернет-ресурсы:

1. http://ru.wikipedia.org/wiki/Информационная_безопасность
2. www.iprbookshop.ru

3. https://www.urait.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: комплект презентационного оборудования (компьютер с выходом в интернет, проектор, интерактивная доска, экран).

Во время практики: 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:

- Операционная система Microsoft Windows XP Pro, либо Microsoft Windows 7 Pro - в зависимости от аппаратной конфигурации.

- Microsoft Office 2007, либо Microsoft Office 2013 - в зависимости от аппаратной конфигурации и потребности.

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 экзамене.

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

$З = К \times 0{,}4$, где К - количество баллов на экзамене (зачете);

$И = С + З + П$, 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 использовать современные информационные технологии и программные средства при решении профессиональных задач»
в части дисциплины «Средства и методы защиты информации»

№ 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)	Знает основы защиты компьютерной информации; правовые основы защиты компьютерной информации, организационные, технические программные методы защиты информации, правила работы с конфиденциальной информацией Умеет частично выявлять угрозы информационной безопасности Владеет частично навыками проектирования защищенных информационных систем обработки информации и управления	Компьютерное тестирование, Практические задания зачет Экзамен
2	**Базовый уровень (относительно порогового уровня)** **(**От 71 до 85 баллов**)**	Знает основы защиты компьютерной информации;правовые основы защиты компьютерной информации, организационные, технические программные методы защиты информации, правила работы с конфиденциальной информацией Умеет выявлять основные угрозы информационной безопасности Владеет основными навыками проектирования защищенных информационных систем обработки информации и управления	Компьютерное тестирование, Практические задания зачет Экзамен

3	**Повышенный уровень (относительно порогового уровня)** (От 86 до 100 баллов)	Знает основы защиты компьютерной информации; правовые основы защиты компьютерной информации, организационные, технические программные методы защиты информации, правила работы с конфиденциальной информацией Умеет выявлять угрозы информационной безопасности Владеет навыками проектирования защищенных информационных систем обработки информации и управления	Компьютерное тестирование, Практические задания Зачет Экзамен

Приложение 1

Методические рекомендации для обучающихся по освоению дисциплины.

Студентам на первом занятии необходимо ознакомиться с Рабочей программой дисциплины, где прописаны цели, задачи и трудоемкость дисциплины; с порядком изучения дисциплины, т.е. модульно-тематическим планом и пояснительной запиской с указанием этапов формирования заявленных компетенций. А также ознакомиться с порядком оценивания результатов обучения, для чего необходимо изучить следующие документы: Положение о модульно-рейтинговой системе оценивания и Принципы оценки уровня знаний, умений и навыков (характеристика ответа).

Перед началом изучения дисциплины необходимо повторить учебный материал обеспечивающих учебных дисциплин предшествующих курсов, которые дают основу для изучения дисциплины «Средства и методы защиты информации»: Сквозные технологии в экономике.

Студент должен внимательно изучить перечень основной (дополнительной) литературы и взять необходимые учебники в библиотеке.

При сдаче модулей упор делается на выявление основных причинно-следственных связей, понимания их логики и грамотной формулировки ответа, а также – ориентацию на максимальное удовлетворение потребностей покупателей, т.к. от этого зависит эффективность маркетинга.

При подготовке к семинарскому занятию необходимо уточнить план проведения занятий, подготовить необходимую информационную базу. Практические занятия проводятся после лекционного изучения темы в различных формах, активизирующих работу студента.

При изучении данного курса преподавателем используются интерактивные методы обучения, что помогает эффективнее сформировать заявленные компетенции. При проведении занятий с помощью интерактивных технологий группа или разбивается на команды или студенты работают индивидуально. Каждая команда или студент обеспечивается необходимой информацией. Занятие проводится в основном в виде решения ситуационных заданий (кейсов), позволяющих освоить методику и приобрести необходимые навыки в организации маркетинговой деятельности. Только после приобретения навыков по решению ситуационных заданий, можно говорить о формировании желаемых компетенций у студентов.

Интерактивные формы обучения обеспечивают высокую мотивацию, прочность знаний, творчество, коммуникабельность, командный дух, ценность индивидуальности, свободу самовыражения, акцент на деятельность, взаимоуважение и демократичность.

Приложение 2

УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УНИВЕРСИТЕТ УПРАВЛЕНИЯ «ТИСБИ»
Кафедра финансы и кредит

Фонд оценочных средств
для проведения текущей и промежуточной аттестации
по дисциплине
«Средства и методы защиты информации»

По специальности: Экономическая безопасность

Специализация подготовки	Экономико-правовое обеспечение экономической безопасности

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 и экзамену)
      2.2.2 Фонд оценочных средств для проверки сформированности навыков (задачи к зачету и экзамену)

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Формы контроля / Формируемые компетенции	ОПК 6	
	ОПК 6.1	ОПК 6.2
Формы текущего контроля		
Компьютерное тестирование,	З-4	З-8
Практические задания	З-4, У-4	З-8, У-9
Формы промежуточного контроля		
зачет	З-4, У-4, В-4	З-8, У-9, В-9
Экзамен	З-4, У-4, В-4	З-8, У-9, В-9

З- знания, У- умения, В- владения

2.1 Фонд оценочных средств и шкала оценивания для текущего контроля

2.1.1 Компьютерное тестирование

Для текущего контроля успеваемости студентов введено компьютерное тестирование по пройденным темам. Преподаватель формирует сценарий контрольного опроса, который содержит наименование тем и количество задаваемых вопросов по каждой теме. Рекомендуется охватывать 2-3 темы по 10-15 вопросов.

Примерный тест по теме:

1. Выберите формулу подсчета общих затрат на безопасность в ответной модели.
a) Стоимость ущерба от происшествия + Стоимость контрмер
b) Стоимость ущерба от происшествия - Стоимость контрмер
c) Стоимость ущерба от чрезвычайного происшествия + Стоимость контрмер
d) Стоимость ущерба от чрезвычайного происшествия - Стоимость контрмер
2. Сколько главных элементов оценки в организации.
a) 3
b) 4
c) 5
d) 6

3. Назовите этапы процесса информационной безопасности.
a) оценку;
b) политику;
c) реализацию;
d) квалифицированную подготовку;
e) аудит.

Критерии оценивания письменного 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, экзамен) знаний введен устный опрос по билетам. Экзаменационные билеты включают в себя по 2 вопроса.

2.1.2 Практические задания

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

Темы практических заданий

1. Физическая безопасность
2. Информационная безопасность
3. Генератор паролей
4. Аутентификация пользователей
5. Комплексная защита здания

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 дополнительного объяснения выполняет задание, но не все работает верно.	70-60
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

Примерный перечень вопросов к зачету

1. Понятие информационной безопасности. Основные составляющие.
2. Распространение объектно-ориентированного подхода на информационную безопасность
3. Наиболее распространенные угрозы
4. Законодательный уровень информационной безопасности
5. Стандарты и спецификации в области информационной безопасности
6. Административный уровень информационной безопасности
7. Управление рисками

Примерный перечень вопросов к экзамену

1. Процедурный уровень информационной безопасности
2. Основные программно-технические меры
3. Идентификация и аутентификация, управление доступом
4. Протоколирование и аудит, шифрование, контроль целостности
5. Экранирование, анализ защищенности
6. Обеспечение высокой доступности
7. Туннелирование и управление

2.2.2.Фонд оценочных средств для проверки умений/навыки

Примеры практических заданий для экзамена

Задание 1.
Написать программу, представляющую собой модель классических криптографических алгоритмов: код Цезаря, таблица Виженера.
Программа должна иметь оконный интерфейс, в ней возможен ввод пользовательского текста, а также предусмотрена возможность ввода из файла и вывода в файл. В программе доступен латинский алфавит и кириллический алфавит, оба регистра. В программе должны быть предусмотрены поля для изменения ключа.
Используемые группы символов для шифрования: цифры (0-9) и латинские строчные буквы (a-z)

Задание №2. Запишите признаки заражения ПК вирусом.

Задание №3. Проанализируйте и запишите, какие типы файлов подвержены заражению?

Задание. 5 Создать презентацию, тема «Классификация вирусов» (8-10 слайдов).

Примеры практических заданий для зачета

Задание №1. Проанализируйте и запишите основные способы заражения ПК. Запишите меры профилактики заражения ПК вирусом.

Задание №2. Запишите классификацию вирусов в виде таблицы

Задание №3 Сравните виды антивирусных программ, дайте им краткую характеристику.

Задание №4. Перечислите функции, выполняемые антивирусом Касперского.

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

Характеристика ответа	Европейская оценка	Рубежные баллы	Оценка	Уровень сформированности компетенций

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 на экзаменационный билет 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, стандарты, 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	**А**	**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, 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	**А**	**95-91**	**зачтено**	**Повышенный уровень сформированности компетенций**

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, стандарты, 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, стандарты, 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**	**90-86**	**зачтено**	
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	**B**	**85-81**	**зачтено**	**Базовый уровень**

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, стандарты, 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				
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 помощью "наводящих" вопросов преподавателя. 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 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	**С**	**80-76**	**зачтено**	
Студент демонстрирует достаточные теоретические и практические знания. Дан полный, но недостаточно последовательный ответ на поставленный вопрос, но при этом показано умение выделить существенные и	**С**	**75-71**	**зачтено**	

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, 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 Владеет частично навыками проектирования защищенных информационных систем обработки информации и управления				
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,	**E**	**65-61**	**зачтено**	

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 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**	
Студент испытывает значительные трудности в ответе на вопросы. Присутствует масса существенных ошибок в определениях терминов, понятий по контролю и ревизии. Речь неграмотна. На дополнительные вопросы студент не отвечает. Задача не решена	**F**	**Менее 60**	**Не зачтено**	**Компетенции не сформированы**

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

Характеристика ответа	Европейская оценка	Рубежные баллы	Оценка	Уровень сформированности компетенций

Дан полный, развернутый ответ на поставленный теоретический вопрос экзаменационного билета, 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 на экзаменационный билет 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, стандарты, 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**	**5+**	**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, 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	**A**	**95-91**	**5**	**Повышенный уровень сформированности компетенций**

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, стандарты, 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, стандарты, 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**	**90-86**	**5-**	
Дан полный, развернутый ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ	**B**	**85-81**	**4+**	**Базовый уровень**

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, стандарты, 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				
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 помощью "наводящих" вопросов преподавателя. 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 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	**С**	**80-76**	**4**	

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, 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 Владеет частично навыками проектирования защищенных информационных систем обработки информации и управления	**C**	**75-71**	**4-**	
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	**D**	**70-66**	**3+**	**Пороговый уровень сформированности компетенций**

защите информации в ИС				
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 Умеет частично выявлять угрозы информационной безопасности.	**E**	**65-61**	**3**	
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**	**3-**	
Студент испытывает значительные трудности в ответе на вопросы. Присутствует масса существенных ошибок в определениях терминов, понятий по контролю и ревизии. Речь неграмотна. На дополнительные вопросы студент не отвечает. Задача не решена	**F**	**Менее 60**	**2**	**Компетенции не сформированы**