Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования «Ростовский государственный экономический университет (РИНХ)»

УТВЕРЖДАЮ
Начальник
учебно-методического управления
Платонова Т.К.
«25» июня 2024 г.

Рабочая программа дисциплины
Моделирование процессов и систем защиты информации

Направление 10.03.01 "Информационная безопасность"
Направленность 10.03.01.02 Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)

Для набора 2024 года

Квалификация
Бакалавр

КАФЕДРА **Информационная безопасность**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Лабораторные	48	48	48	48
Итого ауд.	80	80	80	80
Контактная работа	80	80	80	80
Сам. работа	28	28	28	28
Итого	108	108	108	108

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 25.06.2024 г. протокол № 18.

Программу составил(и): доцент, Прохоров А.И.

Зав. кафедрой: к.э.н., доц. Радченко Ю.В.

Методический совет направления: д.э.н., профессор Тищенко Е.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	Изучение принципов и методов моделирования процессов и систем защиты информации.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-3: способен проводить анализ информационной безопасности объектов и автоматизированных систем на соответствие требованиям стандартов в области информационной безопасности

ПК-4: способен принимать участие в проведении экспериментальных исследований объекта информационной безопасности

В результате освоения дисциплины обучающийся должен:

Знать:

основы моделирования защиты информации (соотнесено с индикатором ПК-3.1)
Знать современные системы моделирования защиты информации (соотнесено с индикатором ПК-4.1)

Уметь:

анализировать процессы и системы моделирования защиты информации(соотнесено с индикатором ПК-3.2)
разрабатывать новые модели и системы защиты информации (соотнесено с индикатором ПК-4.2)

Владеть:

системами построения моделей и процессов защиты информации (соотнесено с индикатором ПК-3.2)
современными профессиональными базами угроз и уязвимостей (соотнесено с индикатором ПК-4.2)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Основы моделирования и типы моделей

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
1.1	Введение в моделирование. Основные понятия и термины / Лек /	7	2	ПК-3, ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л2.1, Л2.2, Л2.3, Л2.4
1.2	Типы моделей и их особенности. Рассмотрение различных систем моделирования ИС / Лек /	7	2	ПК-3, ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л2.1, Л2.2, Л2.3, Л2.4
1.3	Методы моделирования процессов. Методы применения моделирования ИС / Лек /	7	2	ПК-3, ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л2.1, Л2.2, Л2.3, Л2.4
1.4	Моделирование сетевой инфраструктуры и анализ уязвимостей с применением GNS3 / Лаб /	7	8	ПК-3, ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л2.1, Л2.2, Л2.3, Л2.4
1.5	Моделирование процессов аутентификации и авторизации / Ср /	7	6	ПК-3, ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л2.1, Л2.2, Л2.3, Л2.4

Раздел 2. Моделирование угроз и рисков в информационной безопасности

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
2.1	Моделирование угроз и уязвимостей. Методы применения моделирования угроз и уязвимостей / Лек /	7	4	ПК-3, ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л2.1, Л2.2, Л2.3, Л2.4

2.2	Моделирование рисков в кибербезопасности. Методы применения моделирования рисков в кибербезопасности. / Лек /	7	4	ПК-3, ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л2.1, Л2.2, Л2.3, Л2.4
2.3	Применение моделирования в практике. Построение практических моделей / Лек /	7	4	ПК-3, ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л2.1, Л2.2, Л2.3, Л2.4
2.4	Разработка сценариев угроз с использованием моделирования. Построение сценариев практических моделей / Лаб /	7	8	ПК-3, ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л2.1, Л2.2, Л2.3, Л2.4
2.5	Оценка рисков информационной безопасности с помощью методов моделирования с применением Python / Лаб /	7	8	ПК-3, ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л2.1, Л2.2, Л2.3, Л2.4
2.6	Криптографические модели защиты данных / Ср /	7	6	ПК-3, ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л2.1, Л2.2, Л2.3, Л2.4

Раздел 3. Моделирование инцидентов и симуляция атак

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
3.1	Моделирование инцидентов информационной безопасности. Методы применения моделирования инцидентов информационной безопасности. / Лек /	7	2	ПК-3, ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л2.1, Л2.2, Л2.3, Л2.4
3.2	Симуляция атак и защитных механизмов. Использование систем симуляций кибератак / Лек /	7	4	ПК-3, ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л2.1, Л2.2, Л2.3, Л2.4
3.3	Симуляция процессов реагирования на инциденты с применением Cytoscape / Лаб /	7	8	ПК-3, ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л2.1, Л2.2, Л2.3, Л2.4
3.4	Моделирование процессов мониторинга и реагирования на кибератаки / Ср /	7	8	ПК-3, ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л2.1, Л2.2, Л2.3, Л2.4

Раздел 4. Модели защиты и системы управления информационной безопасностью

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
4.1	Модели защиты информации. Моделирование систем защиты информации способы и задачи / Лек /	7	4	ПК-3, ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л2.1, Л2.2, Л2.3, Л2.4
4.2	Системы управления информационной безопасностью. Методы управления системами ИБ / Лек /	7	4	ПК-3, ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л2.1, Л2.2, Л2.3, Л2.4
4.3	Тестирование систем защиты информации с использованием моделирования / Лаб /	7	8	ПК-3, ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6,

					Л1.7, Л1.8, Л1.9, Л1.10, Л2.1, Л2.2, Л2.3, Л2.4
4.4	Моделирование процессов управления доступом / Лаб /	7	8	ПК-3, ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л2.1, Л2.2, Л2.3, Л2.4
4.5	Моделирование распределенных систем и безопасности / Ср /	7	8	ПК-3, ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л2.1, Л2.2, Л2.3, Л2.4

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Структура и содержание фонда оценочных средств для проведения текущей и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л1.1	Аверченков В. И.	Аудит информационной безопасности: учебное пособие	Москва: ФЛИНТА, 2021	https://biblioclub.ru/index.php?page=book&id=93245 неограниченный доступ для зарегистрированных пользователей
Л1.2	Голембиовская, О. М., Рытов, М. Ю., Шинаков, К. Е.	Формализация подходов к обеспечению защиты персональных данных: монография	Саратов: Ай Пи Эр Медиа, 2019	https://www.iprbookshop.ru/81851.html неограниченный доступ для зарегистрированных пользователей
Л1.3	Шинаков, К. Е., Рытов, М. Ю., Голембиовская, О. М.	Анализ рисков безопасности информационных систем персональных данных: монография	Москва: Ай Пи Ар Медиа, 2020	https://www.iprbookshop.ru/95150.html неограниченный доступ для зарегистрированных пользователей
Л1.4	Галатенко, В. А.	Основы информационной безопасности: учебное пособие	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020	https://www.iprbookshop.ru/97562.html неограниченный доступ для зарегистрированных пользователей
Л1.5	Голембиовская, О. М., Рытов, М. Ю., Голембиовский, М. М., Шинаков, К. Е., Банников, А. И., Кондрашова, Е. В., Дорошенко, В. Ю.	Формализация подхода к определению актуальности угроз информационной безопасности: монография	Саратов: Вузовское образование, 2022	https://www.iprbookshop.ru/121143.html неограниченный доступ для зарегистрированных пользователей
Л1.6	Голембиовская, О. М., Рытов, М. Ю., Шинаков, К. Е., Горлов, А. П., Губсков, Ю. А., Голембиовский, М. М., Кондрашова, Е. В.	Этапы формирования модели угроз и модели нарушителя информационной безопасности с учетом изменений законодательства Российской Федерации: учебное пособие	Саратов: Вузовское образование, 2024	https://www.iprbookshop.ru/134999.html неограниченный доступ для зарегистрированных пользователей

	Авторы,	Заглавие	Издательство, год	Колич-во
Л1.7	Голембиовская, О. М., Рытов, М. Ю., Шинаков, К. Е., Голембиовский, М. М., Кондрашова, Е. В.	Формализация подхода к определению степени ущерба и потенциала нарушителя: монография	Саратов: Вузовское образование, 2024	https://www.iprbookshop.ru/135004.html неограниченный доступ для зарегистрированных пользователей
Л1.8	Целых, А. Н., Котов, Э. М.	Выявление инцидентов информационной безопасности и мошеннических транзакций методами машинного обучения: учебное пособие	Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2023	https://www.iprbookshop.ru/138009.html неограниченный доступ для зарегистрированных пользователей
Л1.9	Трайнев В. А.	Системный подход к обеспечению информационной безопасности предприятия (фирмы): монография	Москва: Дашков и К°, 2022	https://biblioclub.ru/index.php?page=book&id=698555 неограниченный доступ для зарегистрированных пользователей
Л1.10	Бутырский Е. Ю., Цехановский В. В., Жукова Н. А., Баймуратов И. Р., Куликов И. А.	Машинное обучение: учебник	Москва: Директ-Медиа, 2023	https://biblioclub.ru/index.php?page=book&id=701807 неограниченный доступ для зарегистрированных пользователей

5.2. Дополнительная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.1		БИТ. Бизнес & Информационные технологии: журнал	Москва: Положевец и партнеры, 2019	https://biblioclub.ru/index.php?page=book&id=562412 неограниченный доступ для зарегистрированных пользователей
Л2.2	Гулак, М. Л., Рытов, М. Ю., Голембиовская, О. М.	Аудит информационной безопасности. Прикладная статистика: учебное пособие	Москва: Ай Пи Ар Медиа, 2020	https://www.iprbookshop.ru/97630.html неограниченный доступ для зарегистрированных пользователей
Л2.3	Замятин, А. В.	Интеллектуальный анализ данных: учебное пособие	Томск: Издательский Дом Томского государственного университета, 2020	https://www.iprbookshop.ru/116889.html неограниченный доступ для зарегистрированных пользователей
Л2.4	Колесниченко, О. Ю.	Data Science (наука о данных) в становлении информационного общества: учебное пособие	Москва: Прометей, 2021	https://www.iprbookshop.ru/125600.html неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

Консультант Плюс

5.4. Перечень программного обеспечения

Операционная система РЕД ОС
Python с библиотеками (SimPy, PyDSTool, AgentPy) (открытое программное обеспечение)
GNS3 (открытое программное обеспечение)
Cytoscape (открытое программное обеспечение)

5.5. Учебно-методические материалы для студентов с ограниченными возможностями здоровья

При необходимости по заявлению обучающегося с ограниченными возможностями здоровья учебно-методические материалы предоставляются в формах, адаптированных к ограничениям здоровья и восприятия информации. Для лиц с нарушениями зрения: в форме аудиофайла; в печатной форме увеличенным шрифтом. Для лиц с нарушениями слуха: в форме электронного документа; в печатной форме. Для лиц с нарушениями опорно-двигательного аппарата: в форме электронного документа; в печатной форме.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Помещения для всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения:
- столы, стулья;
- персональный компьютер / ноутбук (переносной);
- проектор;
- экран / интерактивная доска.

Лабораторные занятия проводятся в компьютерных классах, рабочие места в которых оборудованы необходимыми лицензионными и/или свободно распространяемыми программными средствами и выходом в Интернет.

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

1 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

1.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
ПК-3: способен проводить анализ информационной безопасности объектов и автоматизированных систем на соответствие требованиям стандартов в области информационной безопасности			
Знать основы моделирования защиты информации	Описывает способы стандартных систем моделирования при построении систем защиты информации	Полный, развёрнутый ответ на поставленный вопрос, изложение материала при ответе – грамотное и логически стройное	Опрос (вопросы 1-40) Вопросы к зачету (вопросы 1-50)
Уметь анализировать процессы и системы моделирования защиты информации	Анализирует состояние информационной системы, выявляет ее уязвимые места и определяет направления ее совершенствования при выполнении практико-ориентированного и практического задания	Полнота и правильность решения практико-ориентированного задания или практического задания	Лабораторные работы (задания 1-6) Практико-ориентированные задания к зачету (задания 1-10)
Владеть системами построения моделей и процессов защиты информации	Использует методы и средствами построения моделей и процессов защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России и ФСТЭК России при выполнении практико-ориентированного и практического задания	Обоснованность и правильность обращения к нормативным источникам, методам и средствам при выполнении практико-ориентированного и практического задания	Лабораторные работы (задания 1-6) Практико-ориентированные задания к зачету (задания 1-10)
ПК-4: способен принимать участие в проведении экспериментальных исследований объекта информационной безопасности			
Знать современные системы моделирования защиты информации	Описывает современные способы моделирования процессов и систем в рамках профессиональной деятельности в области информационной безопасности	Полный, развёрнутый ответ на поставленный вопрос, изложение материала при ответе – грамотное и логически стройное	Опрос (вопросы 1-40) Вопросы к зачету (вопросы 1-50)
Уметь разрабатывать новые модели и системы защиты информации	Анализирует информационной системы, выявляет ее уязвимые места и определяет направления ее совершенствования при выполнении практико-ориентированного и практического задания	Полнота и правильность решения практико-ориентированного задания или практического задания	Лабораторные работы (задания 1-6) Практико-ориентированные задания к зачету (задания 1-10)
Владеть современными профессиональными базами угроз и уязвимостей	Использует методы и средствами управления программного обеспечения в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России и ФСТЭК России при выполнении практико-ориентированного и практического задания	Обоснованность и правильность обращения к нормативным источникам, методам и средствам при выполнении практико-ориентированного и практического задания	Лабораторные работы (задания 1-6) Практико-ориентированные задания к зачету (задания 1-10)

1.2 Шкалы оценивания:
Текущий контроль успеваемости и промежуточная аттестация осуществляется в рамках накопительной балльно-рейтинговой системы в 100-балльной шкале:
50-100 баллов (зачтено)
0-49 баллов (не зачтено)

2 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

Вопросы к зачету

1. Что такое системный анализ и каковы его основные задачи в моделировании?
2. В чем заключаются цели моделирования в различных областях?
3. Какие существуют типы моделей? Приведите примеры.
4. В чем отличие статических и динамических моделей?
5. Чем отличаются детерминированные и стохастические модели?
6. Какие преимущества и недостатки имеют динамические модели?
7. Какие методы моделирования используются для анализа процессов?
8. В чем особенности системной динамики в моделировании?
9. Каковы основные принципы дискретно-событийного моделирования?
10. Что такое агентное моделирование и где оно применяется?
11. Какие существуют инструменты для моделирования бизнес-процессов?
12. Как моделирование помогает в оценке уязвимостей информационных систем?
13. Каковы основные этапы процесса моделирования рисков в кибербезопасности?
14. Как определяется угроза в процессе моделирования информационной безопасности?
15. Какие модели защиты информации используются для обеспечения безопасности данных?
16. В чем заключается принцип работы модели ISO/IEC 27001?
17. Как моделируются инциденты информационной безопасности?
18. Какие сценарии используются для моделирования инцидентов кибербезопасности?
19. Как моделируется система управления информационной безопасностью (ISMS)?
20. Какие методы оценки рисков используются в моделировании киберугроз?
21. Что такое количественный и качественный анализ рисков в кибербезопасности?
22. Как моделируются кибератаки и как оценивается их воздействие?
23. Какие типы симуляций применяются для тестирования защитных механизмов?
24. Как моделируются процессы аутентификации и авторизации в системах безопасности?
25. В чем заключаются особенности моделирования криптографических алгоритмов?
26. Как моделируются распределенные системы и какие вызовы возникают в плане их безопасности?
27. Какие инструменты используются для моделирования мониторинга кибератак?
28. Как моделируется работа межсетевых экранов?
29. Какие методы используются для моделирования систем предотвращения вторжений (IDS/IPS)?
30. Как моделируется распространение вредоносного ПО?
31. Как оценивается влияние вредоносного ПО на информационные системы?
32. Как моделируются угрозы, связанные с человеческим фактором?
33. Какие модели безопасности интегрируются в жизненный цикл разработки программного обеспечения (SDLC)?
34. Как моделируются экономические последствия кибератак для бизнеса?
35. Какие показатели используются для оценки экономического ущерба от кибератак?
36. Что такое модели устойчивости информационных систем и как они применяются?
37. Как моделируются сценарии защиты от DDoS-атак?
38. Какие меры моделируются для минимизации уязвимостей при управлении обновлениями ПО?
39. Как моделируются угрозы, исходящие от внутренних пользователей?
40. Какие методы используются для моделирования безопасности в беспроводных сетях?
41. Как моделируются угрозы безопасности в IoT-устройствах?
42. В чем особенности моделирования процессов защиты критической инфраструктуры?

43. Какие меры по предотвращению кибератак на энергетические системы могут быть смоделированы?
44. Как моделируются угрозы в транспортных и медицинских системах?
45. Каковы основные подходы к моделированию процессов восстановления после инцидентов?
46. Какие методы используются для моделирования процессов аудита информационной безопасности?
47. В чем заключается роль автоматизированных систем мониторинга в моделировании безопасности?
48. Как моделирование помогает в прогнозировании будущих угроз кибербезопасности?
49. Какие меры по управлению кризисными ситуациями в кибербезопасности могут быть смоделированы?
50. Как оценить эффективность внедренных моделей безопасности на основе результатов моделирования?

Практико-ориентированные задания к зачету

1. **Моделирование процесса аутентификации и авторизации**
Разработайте модель процесса аутентификации и авторизации для корпоративной сети, используя системную динамику. Определите ключевые шаги и точки возможных уязвимостей.
2. **Симуляция атаки с использованием вредоносного ПО**
Создайте симуляцию распространения вредоносного ПО в корпоративной сети. Определите, как заражение распространяется, и протестируйте защитные механизмы, такие как антивирусное ПО и IDS/IPS.
3. **Моделирование процессов обновления и патч-менеджмента**
Разработайте модель процесса управления обновлениями и патчами в организации. Проанализируйте, как своевременное или запоздалое обновление влияет на уязвимости системы.
4. **Моделирование и оценка рисков кибератак с использованием агентного моделирования**
Используйте агентное моделирование для создания модели поведения злоумышленников и сотрудников организации. Проанализируйте риски возникновения кибератак и их последствия для инфраструктуры.
5. **Разработка модели для реагирования на инциденты информационной безопасности**
Создайте сценарии кибератак и разработайте модель реагирования на инциденты с учетом всех этапов – от обнаружения угрозы до восстановления системы.
6. **Моделирование работы межсетевых экранов**
Создайте модель сетевой архитектуры компании с использованием межсетевых экранов. Смоделируйте попытки атак на различные уровни сети и оцените, как межсетевые экраны защищают периметр.
7. **Моделирование процессов управления информационной безопасностью (ISMS)**
Постройте модель системы управления информационной безопасностью (ISMS) для организации на основе стандарта ISO/IEC 27001. Включите ключевые процессы управления рисками и внедрения защитных мер.
8. **Анализ уязвимостей IoT-устройств**
Разработайте модель IoT-сети, включающую различные типы устройств. Оцените потенциальные уязвимости и протестируйте защитные механизмы, такие как шифрование и контроль доступа.
9. **Моделирование угроз для критической инфраструктуры**
Постройте модель информационной системы критически важного объекта (например, энергетической или транспортной системы). Смоделируйте сценарии атак и проанализируйте возможные последствия и методы защиты.
10. **Моделирование криптографических механизмов для защиты данных**
Разработайте модель, демонстрирующую работу различных криптографических алгоритмов (например, AES или RSA) при передаче данных в распределенной системе. Проанализируйте их эффективность и устойчивость к атакам.

Критерии оценивания:
Максимальное количество баллов за зачетное задание – 100 (30 баллов максимально за каждый теоретический вопрос, 40 баллов максимально за практико-ориентированное задание).

Критерии оценивания одного теоретического вопроса:

– 25-30 баллов выставляется студенту, если изложенный материал фактически верен, продемонстрированы глубокие исчерпывающие знания в объеме пройденной программы в соответствии с поставленными программой курса целями и задачами обучения, изложение материала при ответе - грамотное и логически стройное;

– 20-24 баллов выставляется студенту, если продемонстрированы твердые и достаточно полные знания в объеме пройденной программы дисциплины в соответствии с целями обучения; материал изложен достаточно полно с отдельными логическими и стилистическими погрешностями;

– 15-19 баллов выставляется студенту, если продемонстрированы твердые знания в объеме пройденного курса в соответствие с целями обучения, ответ содержит отдельные ошибки, уверенно исправленные после дополнительных вопросов;

– 0-14 балла выставляется студенту, если ответы не связаны с вопросами, допущены грубые ошибки в ответе, продемонстрированы непонимание сущности излагаемого вопроса, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

Критерии оценивания практико-ориентированного задания:

– 35-40 баллов выставляется, если задание решено полностью, в представленном решении обоснованно получены правильные ответы.

– 25-34 балла выставляется, если задание решено полностью, но при ответе допущены незначительные ошибки.

– 11-24 балла выставляется, если задание решено частично.

– 0-10 баллов выставляется, если решение неверно или отсутствует.

Итоговый результат формируется из суммы набранных баллов за выполнение зачетного задания и соответствует шкале:

– 50-100 баллов (зачтено);

– 0-49 баллов (не зачтено).

Опрос

1. Какие методы моделирования используются для построения систем аутентификации и авторизации?
2. Какие этапы включает процесс создания модели аутентификации в корпоративной сети?
3. В чем заключается отличие централизованной и децентрализованной аутентификации в моделировании?
4. Какие ключевые уязвимости можно выявить при моделировании процесса авторизации?
5. Как моделировать сценарии атаки с использованием вредоносного ПО?
6. Какие факторы влияют на скорость распространения вредоносного ПО в сети?
7. Как симулировать защитные меры, такие как IDS/IPS, для предотвращения распространения вредоносного ПО?
8. Какие преимущества и недостатки имеет агентное моделирование при симуляции кибератак?
9. Какие типы данных необходимо собирать для создания модели угроз с помощью агентного моделирования?
10. Как моделировать реакцию пользователей на фишинговые атаки в агентной модели?
11. Какие основные шаги включает процесс реагирования на инциденты информационной безопасности?
12. Какие инструменты используются для создания сценариев кибератак?
13. Какие показатели используются для оценки эффективности модели реагирования на инциденты?
14. Как моделировать взаимодействие команд реагирования на инциденты и сетевых администраторов?
15. Какие параметры важно учитывать при моделировании работы межсетевых экранов?
16. Как моделируются правила фильтрации трафика в межсетевом экране?
17. Какие виды атак могут быть симулированы для тестирования эффективности межсетевых экранов?

18. Как межсетевые экраны взаимодействуют с другими элементами сетевой архитектуры?
19. Какие ключевые процессы включаются в систему управления информационной безопасностью (ISMS)?
20. Как моделируются процедуры управления рисками в рамках ISMS?
21. Какие элементы жизненного цикла безопасности можно отразить в модели ISMS?
22. Какие стандарты безопасности учитываются при моделировании ISMS?
23. Какие уязвимости чаще всего встречаются в IoT-устройствах?
24. Как моделируются угрозы в беспроводных сетях, таких как Wi-Fi или Bluetooth?
25. Какие методы шифрования используются для защиты данных в IoT-сетях?
26. Как моделировать взаимодействие IoT-устройств с основной инфраструктурой организации?
27. Какие особенности критической инфраструктуры необходимо учитывать при её моделировании?
28. Какие типы атак на критическую инфраструктуру могут быть смоделированы?
29. Как моделировать сценарии восстановления системы после инцидента в критической инфраструктуре?
30. Как оценивается влияние атак на системы критической инфраструктуры?
31. Какие криптографические алгоритмы чаще всего используются для защиты данных в информационных системах?
32. Как моделируются процессы шифрования и дешифрования данных в распределенных системах?
33. Какие атаки на криптографические алгоритмы можно смоделировать и как они влияют на безопасность данных?
34. Какие критерии учитываются при выборе криптографического алгоритма для системы безопасности?
35. Какие процессы обновления и патч-менеджмента можно смоделировать в корпоративной сети?
36. Как моделируются сценарии возникновения уязвимостей при запоздалом обновлении ПО?
37. Какие типы уязвимостей наиболее критичны при отсутствии своевременных обновлений ПО?
38. Как моделировать взаимодействие IT-отдела с пользователями в процессе патч-менеджмента?
39. Как моделировать атаки изнутри (внутренние угрозы) на информационные системы организации?
40. Какие защитные меры можно смоделировать для предотвращения внутренних угроз?

Критерии оценивания*:*
Максимальное количество баллов, которые обучающийся может набрать – 40 баллов (за 40 ответов).
Ответ на вопрос оценивается:
– 1 балл – правильный и полный ответ;
– 0 баллов – неправильный ответ или ответ не представлен.

Лабораторные работы

1. Моделирование сетевой инфраструктуры и анализ уязвимостей с применением GNS3
2. Разработка сценариев угроз с использованием моделирования
3. Симуляция процессов реагирования на инциденты с применением Cytoscape
4. Оценка рисков информационной безопасности с помощью методов моделирования с применением python
5. Тестирование систем защиты информации с использованием моделирования
6. Моделирование процессов управления доступом

Критерии оценивания:
Максимальное количество баллов, которые обучающийся может набрать – 60 баллов (за 6 работ).
Каждое задание оценивается:
– 10 баллов. – задание выполнено верно;
– 9-7 баллов. – при выполнении задания были допущены неточности, не влияющие на результат;
– 6-3 баллов. – при выполнении задания были допущены ошибки;
– 2- 1 баллов. – при выполнении задания были допущены существенные ошибки;
– 0 баллов. – задание не выполнено.

3 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.
Текущий контроль успеваемости проводится с использованием оценочных средств, представленных в п. 2 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.
Промежуточная аттестация проводится в форме зачета.
Зачет проводится по расписанию промежуточной аттестации в устной форме. Количество вопросов в зачетном задании – 3 (2 теоретических, 1 практико-ориентированное задание). Результаты аттестации заносятся в ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику, должны ликвидировать задолженность в установленном порядке.

Приложение 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:
- лекции;
- лабораторные работы

В ходе лекционных занятий рассматриваются основные понятия в области информационной безопасности и защиты информации, методы обнаружения и организации противодействия атак на информационные сети, требования по защите конфиденциальной информации, даются рекомендации для самостоятельной работы и подготовки к практическим занятиям.

В ходе лабораторных работ углубляются и закрепляются знания студентов по ряду рассмотренных на лекциях вопросов, развиваются навыки решения задач по защите информационных объектов.

При подготовке к практическим занятиям каждый студент должен:
- изучить рекомендованную учебную литературу;
- изучить конспекты лекций;
- ознакомиться с описанием лабораторной работы;

В процессе подготовки к лабораторным занятиям студенты могут воспользоваться консультациями преподавателя.

Вопросы, не рассмотренные на лекциях и лабораторных занятиях, должны быть изучены студентами в ходе самостоятельной работы. В ходе самостоятельной работы каждый студент обязан прочитать основную и, по возможности, дополнительную литературу по изучаемой теме, дополнить конспекты лекций недостающим материалом, выписками из рекомендованных источников. Выделить непонятные термины и найти их значение в энциклопедических словарях.

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронно-библиотечными системами. Также обучающиеся могут взять на дом необходимую литературу на абонементе университетской библиотеки или воспользоваться читальными залами.