ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "ВОЛГОГРАДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ"

Институт приоритетных технологий

Кафедра информационной безопасности

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины (модуля): **Моделирование процессов и систем защиты информации**

Уровень ОПОП: Специалитет

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Безопасность компьютерных систем и сетей (по отрасли или в сфере профессиональной деятельности)

Форма обучения: Очная

Срок обучения: 2024 - 2030 уч. г.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.01 Компьютерная безопасность (приказ № 1459 от 26.11.2020 г.) и учебного плана, утвержденного Ученым советом (от 26.05.2023 г., протокол № 9)

Разработчики:
Петров М. В., кандидат физико-математических наук, доцент

Программа рассмотрена и утверждена на заседании кафедры, протокол № 08 от 30.08.2023 года

Зав. кафедрой Какорина О. А.

1. Цель и задачи изучения дисциплины

Цель изучения дисциплины - формирование у студентов достаточных теоретических знаний и практических навыков по использованию основополагающих принципов защиты информации, комплексного проектирования, построения, обслуживания и анализа защищенных компьютерных систем (ИС).

Задачи дисциплины:

- Формирование необходимого минимума специальных теоретических знаний и практических навыков по следующим аспектам: основные положения и история развития компьютерной безопасности, методики построения моделей гроз и злоумышленника, методология построения систем защищенных ИС, методы защиты разных видов информации, проектирование политик и моделей безопасности предприятия
- Формирование методологических основ в области компьютерной безопасности
- Формиорвание навыков работы с методами оценки рисков информационной безопасности (ИБ) предприятия

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Моделирование процессов и систем защиты информации» относится к обязательной части учебного плана.

Дисциплина изучается на 4 курсе.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование компетенций, определенных учебным планом в соответствии с ФГОС ВО.

Выпускник должен обладать следующими общепрофессиональными компетенциями (ОПК):

- ОПК-14 Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации

Знания, умения, навыки, формируемые по компетенции в рамках дисциплины

Студент должен знать:

характеристики и типы систем баз данных; основные языки запросов; физическую организацию баз данных и принципы (основы) их защиты; общие и специфические угрозы безопасности баз данных; основные критерии защищенности баз данных и методы оценивания механизмов защиты; механизмы обеспечения конфиденциальности, целостности и высокой доступности баз данных; особенности применения криптографической защиты в системах управления базами данных; этапы проектирования системы защиты в системах управления базами данных

Студент должен уметь:

проектировать реляционные базы данных и осуществлять нормализацию отношений при проектировании реляционной базы данных; настраивать и применять современные системы управления базами данных; пользоваться средствами защиты, предоставляемыми системами управления базами данных; создавать дополнительные средства защиты баз данных; умеет проводить анализ и оценивание механизмов защиты баз данных

Студент должен владеть навыками:

методикой и навыками составления запросов для поиска информации в базах данных; методикой и навыками использования средств защиты, предоставляемых системами управления базами данных

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Восьмой семестр
Контактная работа (всего)	**84**	**84**
Лабораторные	34	34

Лекции	34	34
Практические	16	16
Самостоятельная работа (всего)	**24**	**24**
Виды промежуточной аттестации	**36**	**36**
Экзамен	36	36
Общая трудоемкость часы	**144**	**144**
Общая трудоемкость зачетные единицы	**4**	**4**

5. Содержание дисциплины

5.1. Содержание дисциплины: Лекции (34 ч.)

Восьмой семестр. (34 ч.)

Тема 1. Основные понятия и определения теории моделирования. (2 ч.)

Основные понятия и определения теории моделирования. Системный подход к задачам защиты информации. Понятие модели.

Тема 2. Задачи моделирования. (2 ч.)

Объект моделирования. Цели моделирования в процессе создания систем защиты информации. Примеры моделей.

Тема 3. Этапы моделирования. (2 ч.)

Постановка задачи моделирования. Формализация. Проверка качества модели. Требования к моделям.

Тема 4. Классификация математических моделей. (2 ч.)

Функциональные модели. Структурные модели. Эмпирические модели.

Тема 5. Концептуальное моделирование (2 ч.)

Концептуальное описание систем. Концептуальные карты. Структурно-функциональное описание системы. Когнитивное моделирование. Деревья угроз. Применение графовых подходов к анализу угроз.

Тема 6. Имитационное моделирование (2 ч.)

Имитационное моделирование в задачах моделирования информационных угроз. Этапы имитационного моделирования. Классификация имитационных моделей

Тема 7. Технологии имитационного моделирования (2 ч.)

Автоматный подход к моделированию. Математическая модель абстрактного автомата. Виды конечных автоматов. Модели исследования безопасности информационных систем на основе автоматного подхода.

Тема 8. Сети Петри. (2 ч.)

Основные определения, способы представления. Маркировка, правила выполнения и пространство состояний сетей Петри. Основные свойства сетей Петри. Виды сетей Петри. Задачи и методы анализа сетей Петри.

Тема 9. Модели угроз ИБ на основе Сетей Петри. (2 ч.)

Приминение сетей Петри к решению задач обеспечения информационной безопасности.

Тема 10. Многоагентные системы. (2 ч.)

Многоагентные системы. Основные понятия и определения. Архитектура многоагентных системы и их свойства. Примеры применения многоагентных систем для защиты информации.

Тема 11. Технологии разработки многоагентых (2 ч.)

Алгоритмы реализации сценариев взаимодействия агентов. Задачи защиты информации, решаемые с помощью многоагентных систем.

Тема 12. Моделирование случайных процессов при анализе информационных угроз. (2 ч.)

Моделирование случайных процессов при анализе информационных угроз. Марковские цепи с дискретным временем. Пуассоновские потоки событий и непрерывные марковские цепи.

Тема 13. Модели на основе графов (2 ч.)

Графы состояний случайного процесса выявления и устранения уязвимостей. Марковские модели угрозы атаки на информационную систему

Тема 14. Построение математических моделей на основе данных. (2 ч.)

Идентификация моделей с помощью регрессионного анализа. Прогностическое моделирование. Классификация методов прогностического моделирования.

Тема 15. Моделирование в нечетких условиях (2 ч.)

Основные положения теории нечетких множеств. Операции на нечетких множествах. Нечеткие отношения. Нечеткие модели в ИБ.

Тема 16. Нечеткий логический вывод (2 ч.)

Этапы нечеткого логического вывода. Построение базы нечетких правил. Оценка рисков ИБ на основе нечеткого логического вывода.

Тема 17. Подходы к построению моделей безопасности (2 ч.)

Описание систем защиты с помощью матрицы доступа. Модель Харрисона-Руззо-Ульмана (HRU). Разрешимость проблемы безопасности. Модель распространения прав доступа Take-Grant. Расширенная модель Take-Grant, анализ информационных каналов. Описание модели Белла-Лападулы (BL). Основная теорема безопасности модели Белла-Лападулы. Эквивалентные подходы к определению безопасности модели Белла-Лападулы.

5.2. Содержание дисциплины: Лабораторные (34 ч.)

Восьмой семестр. (34 ч.)

Тема 1. Концептуальное моделирование систем информационной безопасности. Методы системного анализа. (2 ч.)

Описание сущностных свойств системы. Описание структуры системы и ее взаимодействия с окружением Описание функционирования системы в пространстве состояний. Выделите характеристики (параметры) системы.

Тема 2. Концептуальное моделирование систем информационной безопасности. Построение концептуальной карты в CmapTools. (2 ч.)

Определение контекста. Выделение концептов. Связи между концептами. Сценарные модели.

Тема 3. Построение гибридного автомата в среде моделирования RMD (Rand Model Designer). (2 ч.)

Изучение среды RMD.

Тема 4. Построение гибридного автомата в среде моделирования RMD (Rand Model Designer). Построение модели (2 ч.)

1. Структурная модель построения работы регуляторов в области ИБ.
2. Функциональная модель работы регуляторов в области ИБ.

Тема 5. Построение гибридного автомата в среде моделирования RMD (Rand Model Designer). Вычислительный эксперимент. (2 ч.)

1. Основные ФЗ и ГОСТы в области ИБ.
2. Нормативные правовые документа ФСТЭК.

Тема 6. Построение гибридного автомата в среде моделирования RMD (Rand Model Designer). Модели атак. (2 ч.)

1. Основыне ФЗ и ГОСТы в области ИБ.
2. Нормативно-правовые документа ФСТЭК

Тема 7. Моделирование с использованием Сетей Петри. Модели информационных систем. (2 ч.)

1. Основные понятитя
2. Методы построения модели угроз
3. Классификаторы угроз

Тема 8. Моделирование с использованием Сетей Петри. Построение модели злоумышленника. (2 ч.)

Построение модели злоумышленника информационной безопасности.

Тема 9. Моделирование с использованием Сетей Петри. Изучение среды CPN Tools . (2 ч.)

1. Основные понятитя.
2. Методы построения модели угроз.
3. Классификаторы угроз.

Тема 10. Построение прогнозных моделей на основе данных. Анализ динамики процессов. (2 ч.)

1. Основные понятия
2. Роль человека в решении вопросов защиты информации
3. Методы построения модели злоумышленника

Тема 11. Марковские модели угрозы атаки на информационную систему. Построение моделей. (2 ч.)

1. Основные понятия
2. IT-архитектура
3. Классификация ИС предприятиялассификация атак на ИС предприяти
4. Классификация сценариев проведения компьютерных атак

Тема 12. Моделирование с использованием Сетей Петри. Модели информационных систем.Построение прогнозных моделей на основе данных. Выявление тренда. (2 ч.)

1. Основыне понятия
2. Виды рисков ИБ
3. Методы оценки рисков ИБ
4. Программные средства для оценки рисков ИБ предприяти

Тема 13. Марковские модели угрозы атаки на информационную систему. Имитационный эксперимент. (2 ч.)

1. Основные понятия
2. Методики и технологии работы с инцидентами ИБ
3. Этапы работы с инцидентами ИБ

Тема 14. Построение систем защиты от угрозы нарушения конфиденциальности, целостности, доступности (2 ч.)

1. Построение систем защиты от угрозы нарушения конфиденциальности информации
Организационно режимные меры. Защита от НСД. Построение парольных систем. Криптографические методы защиты. Защита от угрозы нарушения конфиденциальности на уровне содержания информации.
2. Построение систем защиты от угрозы нарушения целостности информации
Организационно-технологические меры защиты. Защита целостности программно-аппаратной среды. Основные методы защиты памяти. Цифровая подпись. Защита от угрозы целостности на уровне содержания информации.
3. Построение системы защиты от угрозы доступности информации
Эксплутационно-технологические меры защиты. Защита от сбоев программно-аппаратной среды. Защита семантического анализа и актуальности информации.
4. Построение системы защиты от угрозы раскрытия параметров информационной системы
Сокрытие характеристик носителей. Мониторинг использования систем защиты. Защита параметров представления и содержания информации.

Тема 15. Нечеткие модели в информационной безопасности. Изучение системы Fuzzy Tech (2 ч.)

1. Построение систем защиты от угрозы нарушения конфиденциальности информации
Организационно режимные меры. Защита от НСД. Построение парольных систем. Криптографические методы защиты. Защита от угрозы нарушения конфиденциальности на уровне содержания информации.
2. Построение систем защиты от угрозы нарушения целостности информации
Организационно-технологические меры защиты. Защита целостности программно-аппаратной среды. Основные методы защиты памяти. Цифровая подпись. Защита от угрозы целостности на уровне содержания информации.
3. Построение системы защиты от угрозы доступности информации
Эксплутационно-технологические меры защиты. Защита от сбоев программно-аппаратной

среды. Защита семантического анализа и актуальности информации.
4. Построение системы защиты от угрозы раскрытия параметров информационной системы
Сокрытие характеристик носителей. Мониторинг использования систем защиты. Защита параметров представления и содержания информации.

Тема 16. Нечеткие модели в информационной безопасности. Оценка эффективности СУИБ. (2 ч.)

1. Основные понятия
2. Политика (стратегия) безопасности. Дискреционная политика разграничения доступа. Мандатная (полномочная) политика разграничения доступа. Разработка и реализация политики безопасности.

Тема 17. Нечеткие модели в информационной безопасности. Оценка рисков ИБ в среде Fuzzy Tech. (2 ч.)

Описание систем защиты с помощью матрицы доступа. Модель Харрисона-Руззо-Ульмана (HRU). Разрешимость проблемы безопасности. Модель распространения прав доступа Take-Grant. Расширенная модель Take-Grant, анализ информационных каналов. Описание модели Белла-Лападулы (BL). Основная теорема безопасности модели Белла-Лападулы. Эквивалентные подходы к определению безопасности модели Белла-Лападулы.

5.3. Содержание дисциплины: Практические (16 ч.)

Восьмой семестр. (16 ч.)

Тема 1. Основные понятия теории информационной безопасности. Структура теории информационной безопасности. (2 ч.)

1.1. Основные понятия теории компьютерной безопасности.
Язык. Объекты. Субъекты. Доступ.
1.2. Анализ угроз информационной безопасности.
Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы.
1.3. Структура теории компьютерной безопасности.
Основные уровни защиты информации. Защита машинных носителей информации (МНИ). Защита средств взаимодействия с МНИ. Защита представления информации. Защита содержания информации.

Тема 2. Основные понятия теории информационной безопасности. Структура теории информационной безопасности. (2 ч.)

1.1. Основные понятия теории компьютерной безопасности.
Язык. Объекты. Субъекты. Доступ.
1.2. Анализ угроз информационной безопасности.
Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы.
1.3. Структура теории компьютерной безопасности.
Основные уровни защиты информации. Защита машинных носителей информации (МНИ). Защита средств взаимодействия с МНИ. Защита представления информации. Защита содержания информации.

Тема 3. Структура и функции регуляторов (2 ч.)

1. Структурная модель построения работы регуляторов в области ИБ
2. Функциональная модель работы регуляторов в области ИБ

Тема 4. Структура и функции регуляторов (2 ч.)

1. Структурная модель построения работы регуляторов в области ИБ
2. Функциональная модель работы регуляторов в области ИБ

Тема 5. Законодательство в области информационной безопасности. (2 ч.)

1. Основные ФЗ и ГОСТы в области ИБ.
2. Нормативные правовые документа ФСТЭК

Тема 6. Законодательство в области информационной безопасности. (2 ч.)

1. Основные ФЗ и ГОСТы в области ИБ.
2. Нормативные правовые документа ФСТЭК

Тема 7. Анализ угроз информационной безопасности (2 ч.)

1. Основные понятитя
2. Методы построения модели угроз
3. Классификаторы угроз

Тема 8. Анализ угроз информационной безопасности (2 ч.)

1. Основные понятитя
2. Методы построения модели угроз
3. Классификаторы угроз

6. Виды самостоятельной работы студентов по дисциплине

Восьмой семестр (24 ч.)

Вид СРС: Подготовка рефератов (24 ч.)

Тематика заданий СРС:

Тематика рефератов:

1. Основные виды вредоносных программ и методы борьбы с ними.
2. Классификация угроз информации в операционных системах, базах данных, системах электронной почты.
3. Методы обеспечения целостности программно-аппаратной среды. Основные методы защиты памяти.
4. Примеры построения систем защиты с помощью матрицы доступа.
5. Практические Методы разработки и реализации политики безопасности.
6. Сравнительный анализ стандартов оценки безопасности компьютерных систем TCSEC, руководящих документов Гостехкомиссии РФ и «Единых критериев».

Реферат – письменная работа объемом 8–10 страниц. Это краткое и точное изложение сущности какого-либо вопроса, темы.

Тему реферата студент выбирает из предложенных преподавателем или может предложить свой вариант. В реферате нужны развернутые аргументы, рассуждения, сравнения. Содержание темы излагается объективно от имени автора.

Функции реферата. Информативная, поисковая, справочная, сигнальная, коммуникативная. Степень выполнения этих функций зависит от содержательных и формальных качеств реферата и целей.

Требования к языку реферата. Должен отличаться точностью, краткостью, ясностью и простотой.

Структура реферата.

1. Титульный лист.
2. Оглавление (на отдельной странице). Указываются названия всех разделов (пунктов плана) реферата и номера страниц, указывающие начало этих разделов в тексте реферата.
3. Введение. Аргументируется актуальность исследования, т.е. выявляется практическое и теоретическое значение данного исследования. Далее констатируется, что сделано в данной области предшественниками, перечисляются положения, которые должны быть обоснованы. Обязательно формулируются цель и задачи реферата.
4. Основная часть. Подчиняется собственному плану, что отражается в разделении текста на главы, параграфы, пункты. План основной части может быть составлен с использованием различных методов группировки материала. В случае если используется чья-либо неординарная мысль, идея, то обязательно нужно сделать ссылку на того автора, у кого взят данный материал.
5. Заключение. Последняя часть научного текста. В краткой и сжатой форме излагаются полученные результаты, представляющие собой ответ на главный вопрос исследования.
6. Приложение. Может включать графики, таблицы, расчеты.
7. Библиография (список литературы). Указывается реально использованная для написания реферата литература. Названия книг располагаются по алфавиту с указанием их выходных данных.

При проверке реферата оцениваются:

- знание фактического материала, усвоение общих представлений, понятий, идей;
- характеристика реализации цели и задач исследования;
- степень обоснованности аргументов и обобщений;
- качество и ценность полученных результатов;
- использование литературных источников;
- культура письменного изложения материала;
- культура оформления материалов работы.

7. Тематика курсовых работ(проектов)

Курсовые работы (проекты) по дисциплине не предусмотрены.

8. Фонд оценочных средств. Оценочные материалы

8.1. Показатели и критерии оценивания компетенций, шкалы оценивания

В рамках изучаемой дисциплины студент демонстрирует уровни овладения компетенциями:

Повышенный уровень:

обучающийся демонстрирует глубокое знание учебного материала; способен использовать сведения из различных источников для успешного исследования и поиска решения в нестандартных ситуациях; способен анализировать, проводить сравнение и обоснование выбора методов решения практико-ориентированных заданий

Базовый уровень:

обучающийся способен понимать и интерпретировать освоенную информацию; демонстрирует осознанное владение учебным материалом и учебными умениями, навыками и способами деятельности, необходимыми для решения практико-ориентированных заданий

Пороговый уровень:

обучающийся обладает необходимой системой знаний и владеет некоторыми умениями; демонстрирует самостоятельность в применении знаний, умений и навыков к решению учебных заданий на репродуктивном уровне

Уровень ниже порогового:

система знаний, необходимая для решения учебных и практико-ориентированных заданий, не сформирована; обучающийся не владеет основными умениями, навыками и способами деятельности

Уровень сформированности компетенции	Шкала оценивания для промежуточной аттестации	Шкала оценивания по БРС
	Экзамен, зачет с оценкой	
Повышенный	5 (отлично)	91 и более
Базовый	4 (хорошо)	71 – 90
Пороговый	3 (удовлетворительно)	60 – 70
Ниже порогового	2 (неудовлетворительно)	Ниже 60

Критерии оценки знаний студентов по дисциплине

Оценка	Показатели

Отлично	Обучающийся демонстрирует: систематизированные, глубокие и полные знания по всем разделам учебной дисциплины, а также по основным вопросам, выходящим за ее пределы; точное использование научной терминологии, грамотное, логически правильное изложение ответа на вопросы; безупречное владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке и решении научных и профессиональных задач; выраженную способность самостоятельно и творчески решать сложные проблемы в нестандартной ситуации; полное и глубокое усвоение основной, и дополнительной литературы, по изучаемой учебной дисциплине; умение свободно ориентироваться в теориях, концепциях и направлениях по изучаемой учебной дисциплине и давать им аналитическую оценку, использовать научные достижения других дисциплин; творческую самостоятельную работу на учебных занятиях, активное творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.
Хорошо	Обучающийся демонстрирует: систематизированные, глубокие и полные знания по всем разделам учебной дисциплины; использование научной терминологии, грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы и обобщения; владение инструментарием учебной дисциплины (методами комплексного анализа, техникой информационных технологий), умение его использовать в постановке и решении научных и профессиональных задач; способность решать сложные проблемы в рамках учебной дисциплины; свободное владение типовыми решениями; усвоение основной и дополнительной литературы, рекомендованной рабочей программой по учебной дисциплине; умение ориентироваться в теориях, концепциях и направлениях по изучаемой учебной дисциплине и давать им аналитическую оценку; активную самостоятельную работу на учебных занятиях, систематическое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.
Удов-летвори-тельно	Обучающийся демонстрирует: достаточные знания в объеме рабочей программы по учебной дисциплине; использование научной терминологии, грамотное, логически правильно изложение ответа на вопросы, умение делать выводы без существенных ошибок; владение инструментарием учебной дисциплины, умение его использовать в решении учебных и профессиональных задач; способность самостоятельно применять типовые решения в рамках изучаемой дисциплины; усвоение основной литературы, рекомендованной рабочей программой по дисциплине; умение ориентироваться в базовых теориях, концепциях и направлениях по дисциплине; работу на учебных занятиях под руководством преподавателя, фрагментарное участие в групповых обсуждениях, достаточный уровень культуры исполнения заданий.

Неудов-летвори-тельно	Обучающийся демонстрирует: фрагментарные знания в рамках изучаемой дисциплины; знания отдельных литературных источников, рекомендованных рабочей программой по учебной дисциплине; неумение использовать научную терминологию учебной дисциплины, наличие в ответе грубых, логических ошибок; пассивность на занятиях или отказ от ответа, низкий уровень культуры исполнения заданий.

8.2. Вопросы, задания текущего контроля

В целях освоения компетенций, указанных в рабочей программе дисциплины, предусмотрены следующие вопросы, задания текущего контроля:

- ОПК-14 Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации

Студент должен знать:

характеристики и типы систем баз данных; основные языки запросов; физическую организацию баз данных и принципы (основы) их защиты; общие и специфические угрозы безопасности баз данных; основные критерии защищенности баз данных и методы оценивания механизмов защиты; механизмы обеспечения конфиденциальности, целостности и высокой доступности баз данных; особенности применения криптографической защиты в системах управления базами данных; этапы проектирования системы защиты в системах управления базами данных

Вопросы, задания:

1. Модели исследования безопасности информационных систем на основе автоматного подхода.
2. Моделирование случайных процессов при анализе информационных угроз.
3. Задачи защиты информации, решаемые с помощью многоагентных систем.

Студент должен уметь:

проектировать реляционные базы данных и осуществлять нормализацию отношений при проектировании реляционной базы данных; настраивать и применять современные системы управления базами данных; пользоваться средствами защиты, предоставляемыми системами управления базами данных; создавать дополнительные средства защиты баз данных; умеет проводить анализ и оценивание механизмов защиты баз данных

Задания:

1. Моделировать процессы, протекающие в информационных системах и сетях.
2. Представить модель в математическом и алгоритмическом виде.
3. Примеры применения многоагентных систем для защиты информации.

Студент должен владеть навыками:

методикой и навыками составления запросов для поиска информации в базах данных; методикой и навыками использования средств защиты, предоставляемых системами управления базами данных

Задания:

1. Концептуальное моделирование систем информационной безопасности.
2. Имитационное моделирование в задачах моделирования информационных угроз.
3. Приминение сетей Петри к решению задач обеспечения информационной безопасности.

8.3. Вопросы промежуточной аттестации

Восьмой семестр (Экзамен)

1. Основные понятия теории информационной безопасности. Структура теории информационной безопасности.

2. Классификация методов моделирования.

3. Организационно режимные меры. Защита от НСД. Построение парольных систем. Криптографические методы защиты. Защита от угрозы нарушения конфиденциальности на уровне содержания информации.

4. Эксплутационно-технологические меры защиты. Защита от сбоев программно-аппаратной среды. Защита семантического анализа и актуальности информации.

5. Политика (стратегия) безопасности. Дискреционная политика разграничения доступа. Мандатная (полномочная) политика разграничения доступа. Разработка и реализация политики безопасности.

6. Описание систем защиты с помощью матрицы доступа. Модель Харрисона-Руззо-Ульмана (HRU). Разрешимость проблемы безопасности. Модель распространения прав доступа Take-Grant. Расширенная модель Take-Grant, анализ информационных каналов. Описание модели Белла-Лападулы (BL). Основная теорема безопасности модели Белла-Лападулы. Эквивалентные подходы к определению безопасности модели Белла-Лападулы.

7. Основные положения «Единых критериев». Требования безопасности. Профили защиты.

8.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Промежуточная аттестация обучающихся ведется непрерывно и включает в себя:

для дисциплин, завершающихся (согласно учебному плану) зачетом/зачетом с оценкой (дифференцированным зачетом), – текущую аттестацию (контроль текущей работы в семестре, включая оценивание промежуточных результатов обучения по дисциплине, – как правило, по трем модулям) и оценивание окончательных результатов обучения по дисциплине;

для дисциплин, завершающихся (согласно учебному плану) экзаменом, – текущую аттестацию (контроль текущей работы в семестре, включая оценивание промежуточных результатов обучения по дисциплине, – как правило, по трем модулям) и семестровую аттестацию (экзамен) – оценивание окончательных результатов обучения по дисциплине.

По дисциплинам, завершающимся зачетом/зачетом с оценкой, по обязательным формам текущего контроля студенту предоставляется возможность набрать в сумме не менее 100 баллов.

Оценивание окончательных результатов обучения по дисциплине ведется по 100-балльной шкале, оценка формируется автоматически как сумма количества баллов, набранных обучающимся за выполнение заданий обязательных форм текущего контроля.

По дисциплинам, завершающимся экзаменом, по обязательным формам текущего контроля студенту предоставляется возможность набрать в сумме не менее 60 баллов.

Оценивание окончательных результатов обучения по дисциплине ведется по 100-балльной шкале, оценка формируется автоматически как сумма количества баллов, набранных обучающимся за выполнение заданий обязательных форм текущего контроля и количества баллов, набранных на семестровой аттестации (экзамене).

Система оценивания.

В соответствии с Положением о балльно-рейтинговой системе оценки успеваемости обучающихся Волгоградского государственного университета предусмотрена возможность предоставления студентам выполнения дополнительных заданий повышенной сложности (не включаемых в перечень обязательных и, соответственно, в перечень обязательного текущего контроля успеваемости) и получения за выполнение таких заданий «премиальных» баллов, - для поощрения обучающихся, демонстрирующих выдающие способности.

Оценка качества освоения образовательной программы включает текущий контроль успеваемости, промежуточную аттестацию обучающихся и государственную итоговую аттестацию выпускников.

Текущий контроль представляет собой проверку усвоения учебного материала теоретического и практического характера, регулярно осуществляемую на протяжении семестра. К основным формам текущего контроля можно отнести:

Форма текущего контроля: Контрольная работа

контрольные работы применяются для оценки знаний, умений, навыков по дисциплине или ее части. Контрольная работа, как правило, состоит из небольшого количества средних по трудности вопросов, задач или заданий, требующих поиска обоснованного ответа. Может занимать часть или полное учебное занятие с разбором правильных решений на следующем занятии.

Форма текущего контроля: Устный опрос, собеседование

устный опрос, собеседование являются формой оценки знаний и предполагают специальную беседу преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной. Процедуры направлены на выяснение объема знаний, обучающегося по определенному разделу, теме, проблеме и т.п.

Форма текущего контроля: Письменные задания или лабораторные работы

письменные задания являются формой оценки знаний и предполагают подготовка письменного ответа, решение специализированной задачи, выполнение теста. являются формами контроля и средствами применения и реализации полученных обучающимися знаний, умений и навыков в ходе выполнения учебно-практической задачи, связанной с получением значимого результата с помощью реальных средств деятельности. Рекомендуются для проведения в рамках тем (разделов), наиболее значимых в формировании компетенций. Тест является простейшей формой контроля, направленной на проверку владения терминологическим аппаратом, современными информационными технологиями и конкретными знаниями в области фундаментальных и прикладных дисциплин. Тест состоит из небольшого количества элементарных задач; может предоставлять возможность выбора из перечня ответов; занимает часть учебного занятия (10–30 минут); правильные решения разбираются на том же или следующем занятии; частота тестирования определяется преподавателем.

Промежуточная аттестация, как правило, осуществляется в конце семестра и может завершать изучение, как отдельной дисциплины, так и ее раздела (разделов) /модуля (модулей). Промежуточная аттестация помогает оценить более крупные совокупности знаний, умений и навыков, в некоторых случаях – даже формирование определенных компетенций.

К формам промежуточного контроля можно отнести:

Форма промежуточной аттестации: Экзамен

экзамен по дисциплине или ее части имеет цель оценить сформированность компетенций, теоретическую подготовку студента, его способность к творческому мышлению, приобретенные им навыки самостоятельной работы, умение синтезировать полученные знания и применять их при решении практических задач. Форма проведения, как правило, предусматривает ответы на вопросы экзаменационного билета, выполнение которых направленно на проверку сформированности компетенций по соответствующей учебной дисциплине.

Методика формирования результирующей оценки:

Восьмой семестр

1. Контрольная работа - от 0 до 30 баллов
2. Устный опрос, собеседование - от 0 до 10 баллов
3. Письменные задания или лабораторные работы - от 0 до 60 баллов

4. Экзамен - от 0 до 40 баллов

9. Перечень основной и дополнительной учебной литературы

9.1 Основная литература

1. Е.К. Баранова, А.В. Бабаш Моделирование системы защиты информации. Практикум : учебное пособие [Электронный ресурс]: - Москва : РИОР : ИНФРА-М, 2020. - 320 с.

2. В.М. Градов, Г.В. Овечкин, П.В. Овечкин, И.В. Рудаков Компьютерное моделирование : учебник [Электронный ресурс]: - Москва : КУРС : ИНФРА-М, 2023. - 264 с.

3. А. И. Безруков, О. Н. Алексенцева Математическое и имитационное моделирование : учебное пособие [Электронный ресурс]: - Москва : ИНФРА-М, 2019. - 227 с.

9.2 Дополнительная литература

1. Тарасик Владимир Петрович Математическое моделирование технических систем [Электронный ресурс]: учебное - ИНФРА-М, 2017. - 592 с. - Режим доступа: http://new.znanium.com/go.php?id=773106

2. Морозов Виктор Михайлович Системное моделирование и методы исследования математических моделей [Электронный ресурс]: - КУРС, 2016. - 243 с. - Режим доступа: http://znanium.com/go.php?id=544536

В качестве учебно-методического обеспечения могут быть использованы другие учебные, учебно-методические и научные источники по профилю дисциплины, содержащиеся в электронно-библиотечных системах, указанных в п. 11.2 «Электронно-библиотечные системы».

9.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://elibrary.ru - Научная электронная библиотека

2. http://new.volsu.ru/umnik - Образовательный портал Волгоградского государственного университета «УМНИК»

3. http://fstec.ru - Официальный сайт Федеральной службы по техническому и экспортному контролю

4. https://www.book.ru/ - Электронно-библиотечная система

5. http://www.garant.ru/ - Гарант

6. https://e.lanbook.com/ - ЭБС "Лань"

7. https://www.biblio-online.ru/ - ЭБС Юрайт

8. https://habr.com - Интернет- ресурс "Хабр"

9. https://znanium.com/ - ЭБС Znanium.com

10.Методические указания по освоению дисциплины для лиц с ОВЗ и инвалидов

При необходимости обучения студентов-инвалидов и лиц с ограниченными возможностями здоровья аудиторные занятия могут быть заменены или дополнены изучением полнотекстовых лекций, презентаций, видео- и аудиоматериалов в электронной информационно-образовательной среде (ЭИОС) университета. Индивидуальные задания подбираются в адаптированных к ограничениям здоровья формах (письменно или устно, в форме презентаций). Выбор методов обучения зависит от их доступности для инвалидов и лиц с ограниченными возможностями здоровья.

В целях реализации индивидуального подхода к обучению студентов, осуществляющих учебный процесс по индивидуальной траектории в рамках индивидуального учебного плана (при необходимости), изучение данной дисциплины базируется на следующих возможностях:

- индивидуальные консультации преподавателя;
- максимально полная презентация содержания дисциплины в ЭИОС (в частности, полнотекстовые лекции, презентации, аудиоматериалы, тексты для перевода и анализа и т.п.).

11. Перечень информационных технологий

В учебном процессе активно используются информационные технологии с применением современных средств телекоммуникации; электронные учебники и обучающие компьютерные программы. Каждый обучающийся обеспечен неограниченным доступом к электронной информационно-образовательной среде (ЭИОС) университета. ЭИОС предоставляет открытый доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к электронным библиотечным системам и электронным образовательным ресурсам.

11.1 Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)

Перечень лицензионного и свободно распространяемого программного обеспечения:
1. Microsoft Windows 7 Professional, 11 лицензий, номер 60357707
2. Microsoft Windows 7 Home Premium, 1 лицензия, OEM-лицензия
3. Microsoft Windows 8.1 Home, 1 лицензия OEM-лицензия
4. Microsoft Office 2007 Standart, 1 лицензия, номер 43847745
6. LibreOffice 12 лицензий (свободно-распространяемое программное обеспечение)
7. FreeBSD, 1 лицензия FreeBSD license свободное программное обеспечение
8. Oracle VM VirtualBox, 14 лицензий GNU GPL свободное программное обеспечение
9. Mozila FireFox, 13 лицензий Mozilla Public License 2.0 (MPL) сободное программное обеспечение
10. Visual Studio Community 2017, 13 лицензий, учебное программное обеспечение
11. Python 2.7, 13 лицензий PSFL (свободно-распространяемое программное обеспечение)
15. Microsoft Windows 10 PRO. Номер лицензии: 65946188
16. Microsoft Office профессиональный 2016. Номер лицензии: нет. Номер договора 31604241628.2016 от 21.11.2016 г.
17. Kaspersky Endpoint Security. Номер лицензии: 280E-201102-083042-350-950
18. 7-zip-открытая лицензия
19. Adope Acrobat Reader – открытая лицензия

11.2 Современные профессиональные базы данных и информационно-справочные системы, в т.ч. электронно-библиотечные системы
(обновление выполняется еженедельно)

Название	Краткое описание	URL-ссылка
Научная электронная библиотека	Крупнейший российский информационный портал в области науки, технологии, медицины и образования.	http://elibrary.ru/
ЭБС "Лань"	Электронно-библиотечная система	https://e.lanbook.com/
ЭБС Znanium.com	Электронно-библиотечная система	https://znanium.com/
ЭБС BOOK.ru	Электронно-библиотечная система	https://www.book.ru/
ЭБС Юрайт	Электронно-библиотечная система	https://www.biblio-online.ru/
Scopus	Scopus – крупнейшая единая база данных, содержащая аннотации и информацию о цитируемости рецензируемой научной литературы, со встроенными инструментами отслеживания, анализа и визуализации данных. В базе содержится 23700 изданий от 5000 международных издателей, в области естественных, общественных и гуманитарных наук, техники, медицины и искусства.	http://www.scopus.com/

Web of Science	Наукометрическая реферативная база данных журналов и конференций. С платформой Web of Science вы можете получить доступ к непревзойденному объему исследовательской литературы мирового класса, связанной с тщательно отобранным списком журналов, и открыть для себя новую информацию при помощи скрупулезно записанных метаданных и ссылок.	https://apps.webofknowledge.com/
КонсультантПлюс	Информационно-справочная система	http://www.consultant.ru/
Гарант	Информационно-справочная система по законодательству Российской Федерации	http://www.garant.ru/
Научная библиотека ВолГУ им О.В. Иншакова		http://library.volsu.ru/

12. Материально-техническое обеспечение дисциплины

Аудитория 2-30 К
Специализированная мебель:
Парта со скамьей- 106 шт.
Учебные места - 260 шт.
Рабочее место преподавателя (стол и стул) – 3 шт.
Доска аудиторная-1 шт.
Технические средства обучения:
Компьютерный комплекс кафедры мультимедийной -1 шт.
Мультимедийная кафедра -1 шт.
Мультимедийный проектор (EIKI EK DLP Projector EK-625U) -1 шт.
Интерактивная доска-1 шт
Аудитория 2-24б К
Специализированная мебель:
1. Столы – 8 шт.
2. стулья – 16 шт.
3. парта со скамьей – 8 шт.
4. рабочее место преподавателя (стол и стул) – 1 шт.
Демонстрационное оборудование:
1. Проектор BenQ MX 505
2. Экран проекционный
3. Доска (магнитная, маркерная)
Рабочие места на базе вычислительной техники (18 шт):
1.Моноблок VPS 5000 (16 шт.);
2. Ноутбук Acer AS5738G;
3. Ноутбук HP Pavilion экран 15,6” Intel Pentium N3540.
Сетевое оборудование:
1. Wi-Fi роутер ASUS RT-N10
2. Концентратор.
3. Комплекс "Сетевое оборудование "Cisco" часть 1

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в ЭИОС ВолГУ.