МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

МОДЕЛИРОВАНИЕ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Направление подготовки 10.03.01 Информационная безопасность
Направленность (профиль) Безопасность автоматизированных систем
(по отрасли или в сфере профессиональной деятельности)

Уровень высшего образования: бакалавриат
Форма обучения: очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2022

Моделирование автоматизированных систем в защищенном исполнении
Рабочая программа дисциплины

Составитель(и):
Кандидат физико-математических наук, доцент кафедры КЗИ В.И. Гришачев

Ответственный редактор
Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты информации
№ 8 от 31.03.2022

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины:
– формирование научного мировоззрения и развития системного мышления;
– комплексное и систематическое изучение теоретических основ, методов и средств (алгоритмических, программных, технических) моделирования процессов и систем защиты информации;
Задачи дисциплины:
– изучение основополагающих принципов моделирования и использования его результатов в создании автоматизированных систем в защищенном исполнении;
– изучение способов проектирования и документального оформления процесса разработки защищенных автоматизированных систем на основе специализированных международных стандартов;
– изучение методов организации и регламентации процесса эксплуатации защищенных автоматизированных систем.
– развитие умения и навыков в области разработки защищенных автоматизированных систем в соответствии с требованиями профиля защиты.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ПК-12 Способен принимать участие в проведении экспериментальных исследований системы защиты информации	ПК-12.1 Знает методы и технологии проектирования, моделирования, исследования систем защиты информации	Знать: • Принципы моделирования, классификацию способов представления моделей процессов и системам защиты информации; • Приемы, методы, и недостатки способы различных формализации способов объектов, представления процессов, моделей явлений систем и реализации их на компьютере; • Типовые системы имитационного моделирования; способы планирования машинных экспериментов с имитационными моделями;
	ПК-12.2 Умеет выполнять сбор, обработку, анализ и систематизацию информации в области защиты информации	Уметь: • Представить модель в математическом и алгоритмическом виде; • Оценить качество модели; показать теоретические основания модели; • Моделировать процессы, про-

		текающие в информационных системах;
	ПК-12.3 Владеет навыками по разработке и исследованию конкретных явлений и процессов для решения расчетных и исследовательских задач	Владеть: • Навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем; • Методами формирования требований по защите информации; • Методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем;

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Моделирование автоматизированных систем в защищенном исполнении» относится к части, формируемой участниками образовательных отношений.
Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: «Физика», «Математический анализ», «Теория вероятностей и математическая статистика».
В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Комплексная защита объектов информатизации, «Комплексная защита объектов информатизации», «Проектно-технологическая практика», «Эксплуатационная практика».

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет _2_ з.е., 76 академических часов.

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
5	Лекции	**16**
5	Лабораторные работы	**24**
	Всего:	**40**

Объем дисциплины в форме самостоятельной работы обучающихся составляет _36_ академических часов.

3. Содержание дисциплины

Тема 1. Введение. Проектирование и разработка автоматизированных информационных систем

Лекция 1. Введение. Цели и задачи курса «Разработка и эксплуатация защищенных автоматизированных систем». Предмет и содержание курса в целом, его роль и место в подготовке специалистов по комплексной защите информации.
Методология и технология проектирования АИС. Нормативно методическое обеспечение создания программного обеспечения автоматизированных информационных систем (ПО АИС)
Лекция 2. Понятие, виды и структура автоматизированных систем. Защищенные компьютерные системы. Свойства защищенных компьютерных систем. Угрозы безопасности. Подходы к созданию безопасных систем обработки информации.
Порядок создания и проектирования защищенных КС. Законодательные и правовые основы защиты компьютерной информации и информационных технологий

Тема 2 Работа с данными в автоматизированных информационных системах
Лекция 3. Жизненный цикл АС. Разработка программно-информационного ядра АИС на основе систем управления базами данных База данных информационной системы. Состав и содержание работ на стадии технорабочего проектирования.
Разработка программно-информационного ядра АИС на основе систем управления базами данных (СУБД). Общие принципы проектирования систем. Визуальное проектирование. Структурные методы анализа и проектирования ПО. Метод функционального моделирования. Метод моделирования процессов.
Лекция 4. Порядок создания изделий ИТ, удовлетворяющих требованиям безопасности. Жизненный цикл изделий ИТ. Виды требований безопасности ИТ
База данных информационной системы. В Особенности обработки данных в информационных системах. Системные базы данных и таблицы. Журнал транзакций.

Тема 3 Разработка клиентского программного обеспечения
Лекция 5. Технология доступа к базам данных ADO, BDE, ODBC, COM, CORBA. Организация взаимодействия клиент-сервер. Перенос персональной базы данных на сервер.
Технология доступа к базам данных ADO, BDE, ODBC, COM, CORBA. Цифровые сертификаты и инфраструктура открытых ключей.
Лекция 6. Клиенты удаленного доступа и построение запросов к СУБД. Хранимые процедуры и триггеры. Достоинства хранимых процедур. Области видимости хранимых процедур: системные, локальные, временные, удалённые.
Разработка серверной части. Цифровые сертификаты и инфраструктура открытых ключей

Тема 4 Разработка клиентского программного обеспечения. Основные элементы клиентских программ
Лекция 7. Объекты для работы с данными. Объекты для управления работой приложений и оформления интерфейса. Объекты- контейнеры. Объекты OLE.
Организация сбора, размещения, хранения, накопления, преобразования и передачи данных в АИС. Методы и средства сбора и передачи данных. Защита информации. Основные предметные направления защиты информации. Правовые основы защиты информации. Источники права на доступ к информации. Виды доступа к информации.
Лекция 8. Администрирование и эксплуатация защищенных КС, эксплуатационная документация защищенных КС. Модель канала утечки. Методы достижения условия защищённости. Обзор систем контроля защищенности.
Обеспечение защиты данных. Восстановление информации в базах данных: системы перераспределения доверия, неявные сертификаты. Защита информации. Основные предметные направления защиты информации. Правовые основы защиты информации. Источники права на доступ к информации. Виды доступа к информации. Защита информации в АИС. Надёжность информации

Практикум

Лабораторные работы 1 – 4

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	**2**	**3**	**4**
1.	Введение. Проектирование и разработка автоматизированных информационных систем	Лекция 1-2. Самостоятельная работа	Традиционная лекция с использованием презентаций Опрос Подготовка к занятиям с использованием ЭБС
2	Работа с данными в автоматизированных информационных системах	Лекция 3-4. Самостоятельная работа	Традиционная лекция с использованием презентаций Опрос Подготовка к занятиям с использованием ЭБС
3	Разработка клиентского программного обеспечения	Лекция 5-6 Самостоятельная работа	Традиционная лекция с использованием презентаций Опрос Подготовка к занятиям с использованием ЭБС
4	Разработка клиентского программного обеспечения. Основные элементы клиентских программ	Лекция 7-8 Самостоятельная работа	Традиционная лекция с использованием презентаций Опрос Подготовка к занятиям с использованием ЭБС
5	Практикум	Лабораторная работа 1.	Выполнение лабораторной работы в физическом практикуме
6	Практикум	Лабораторная работа 2.	Выполнение лабораторной работы в физическом практикуме
7	Практикум	Лабораторная работа 3.	Выполнение лабораторной работы в физическом практикуме
8	Практикум	Лабораторная работа 4.	Выполнение лабораторной работы в физическом практикуме

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

– видео-лекции**;**

– онлайн-лекции в режиме реального времени;

– электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;

– системы для электронного тестирования;

– консультации с использованием телекоммуникационных средств.

5. Оценка планируемых результатов обучения

5.1 Система оценивания

Форма контроля	Макс. количество баллов

	За одну работу	**Всего**
Текущий контроль:		
– опрос (темы 1-3)	*2 балла*	*6 баллов*
– опрос (темы 4-5)	*7 баллов*	*14 баллов*
– лабораторная работа 1-4	*10 баллов*	*40 баллов*
Промежуточная аттестация – зачет (зачет по билетам)		*40 баллов*
Итого за семестр		100 баллов

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2 Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	зачтено	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	зачтено	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
67-50/ D,E	зачтено	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Устный опрос

Устный опрос – это средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объёма знаний, обучающегося по определённому разделу, теме, проблеме и т.п.

Промежуточная аттестация (примерные вопросы) – проверка сформированности компетенций –ПК-12

Модуль 1 Введение. Стойкость криптографических систем

Контрольные вопросы

1. История криптографии, основные понятия и определения, требования к криптографическим системам.
2. История развития криптографии.
3. Классификация криптографических систем.
4. Законодательные и правовые основы защиты компьютерной информации и информационных технологий
5. Энтропия, теоретическая и практическая стойкость, вычислительная стойкость. Теоретико-информационная стойкость.
6. Вычислительная и временная сложность алгоритма.
7. Шифр DES, режимы работы DES
8. Шифр AES
9. Шифр ГОСТ 28147-89.
10. Поточные шифр РСЛОС
11. Шифр RC4
12. Шифр Рона

13. Выбор ключа, время жизни ключа, разделение секрета.
14. Схема обмена секретными ключами: широкоротой лягушки
15. Схема обмена секретными ключами - Ниджейма-Шредера
16. Схема обмена секретными ключами - Отвэй-Риса
17. Схема обмена секретными ключами – Цербер
18. Схема обмена секретными ключами Шамира
19. Схема обмена секретными ключами Диффи-Хеллмана

Модуль 2 Современные симметричные криптосистемы. Распределение ключей.

Контрольные вопросы

1. Протоколы основанные на эллиптических кривых
2. Общая схема функционирования систем с открытыми ключами.
3. Криптосистема RSA и ее модификации.
4. Криптосистема Эль Гамаля.
5. Криптосистема Рабина
6. Целостность данных и аутентификация сообщений.
7. Хэш-функции (MD4, SHA).
8. Алгоритмы ЭЦП: RSA
9. Алгоритмы ЭЦП: Эль Гамаля
10. Алгоритмы ЭЦП: Шнорра
11. Алгоритмы ЭЦП: Нибберга-Руппеля
12. Характеристика протоколов идентификации и аутентификации
13. Идентификация на основе пароля.
14. Взаимная проверка подлинности пользователей.
15. Идентификация с нулевой передачей знаний.
16. Схемы обязательств.
17. Системы электронного голосования.
18. Системы перераспределения доверия: PGP
19. Системы перераспределения доверия: SSL
20. Системы перераспределения доверия: X509 (PKIX)

Модуль 3 Асимметричные криптосистемы.

Контрольные вопросы

1. Протоколы основанные на эллиптических кривых
2. Общая схема функционирования систем с открытыми ключами.
3. Криптосистема RSA и ее модификации.
4. Криптосистема Эль Гамаля.
5. Криптосистема Рабина
6. Целостность данных и аутентификация сообщений.
7. Хэш-функции (MD4, SHA).
8. Алгоритмы ЭЦП: RSA
9. Алгоритмы ЭЦП: Эль Гамаля
10. Алгоритмы ЭЦП: Шнорра
11. Алгоритмы ЭЦП: Нибберга-Руппеля
12. Характеристика протоколов идентификации и аутентификации
13. Идентификация на основе пароля.
14. Взаимная проверка подлинности пользователей.
15. Идентификация с нулевой передачей знаний.
16. Схемы обязательств.

Модуль 4 Криптографические протоколы.

Контрольные вопросы

1. Системы электронного голосования.
2. Системы перераспределения доверия: PGP
3. Системы перераспределения доверия: SSL

4. Системы перераспределения доверия: X509 (PKIX)
5. Системы перераспределения доверия: SPKI
6. Неявные сертификаты
7. Тесты на простоту: пробное деление
8. Тесты на простоту: тест Ферма
9. Тесты на простоту: тест Миллера-Рабина.
10. Алгоритмы факторизации: пробное деление
11. Алгоритмы факторизации: гладкие числа
12. Алгоритмы факторизации: (P-1)-метод Полларда
13. Алгоритмы факторизации: разность квадратов
14. Современные методы факторизации.
15. Виды атак: Атака Винера на RSA
16. Атаки на RSA основанные на решетках
17. Атака Хостада
18. Атака Франклина-Рейтера
19. Частичное раскрытие ключа
20. Стойкость актуальных алгоритмов шифрования
21. Доказуемая стойкость со случайным оракулом
22. Доказуемая стойкость без случайного оракула

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Литература

Основная

1. Кравченко В.Б., Зиновьев П.В., Селютин И.Н. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении // М.: Издательский центр «Академия», 2018. - 304 с
2. Малюк А.А., Пазизин С.В., Погожий Н.С. Введение в защиту информации в автоматизированных системах / М.: Горячая линия - Телеком, 2004. - 147 с.
3. Трещев И.А. Защищенные автоматизированные системы. Для студентов технических специальностей // Создано в интеллектуальной издательской системе Ridero, 2019 – 360 с. ISBN 978-5-4496-3257-9
4. Гагарина Л.Г., Киселев Д.В., Федотова Е.Л. Разработка и эксплуатация автоматизированных информационных систем: Учебник / М.: Изд-во ИНФРА-М, 2009. - 384 с.

Дополнительная

5. ФСТЭК РФ. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Москва: Воениздат, 1992.
6. ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Разработан ФАУ «ГНИИИ ПТЗИ ФСТЭК России» Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 28 января 2014 г. № 3-ст.
7. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Разработан ФАУ «ГНИИИ ПТЗИ ФСТЭК России», ФГУП «ЦентрИнформ», ЗАО «ЭМСОТЕХ». Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 18 сентября 2014 г. № 1123-ст.

8. Язов Ю.К. Технология проектирования систем защиты информации в информационно-телекоммуникационных системах / Воронеж: ВГТУ, 2004. - 146 с
9. Колесов Ю., Сениченков Ю. Моделирование систем. Практикум по компьютерному моделированию // СПб .: БХВ Петербург, Гриф УМО, 2010. - 352с. http://ibooks.ru
10. Шелухин О. И. Моделирование информационных систем. Учебное пособие для вузов. // М.. : Горячая линия–Телеком, УМО, 2012. - 516 с. http://ibooks.ru
11. Афонин В.В., Федосин С.А. Моделирование систем: учебно-практическое пособие // М.: Интернет –Университет Информационных технологий: Бином. Лаборатория знаний, 2012.- 231 с. http://ibooks.ru
12. Аверченков В.И., Казаков П.В., Эволюционное моделирование и его применение // М.: Флинта, 2011. - 200 с. http://ibooks.ru
13. Благодаров А. В., Пылькин А. Н., Скуднев Д. М., Шибанов А. П. Моделирование и синтез оптимальной структуры сети Ethernet // М.: Горячая линия – Телеком, 2011.

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Информационный комплекс РГГУ «Научная библиотека» [Электронный ресурс] / Проект Российского Государственного Гуманитарного Университета – Режим доступа: https://liber.rsuh.ru/ru, свободный. – Загл. с экрана.
2. Федеральный образовательный портал. Библиотека. Единое окно доступа к образовательным ресурсам [Электронный ресурс] – Режим доступа: http://window.edu.ru/library, свободный. – Загл. с экрана.
3. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс] / Проект Российского фонда фундаментальных исследований – Режим доступа: http://elibrary.ru, свободный. – Загл. с экрана.
4. Образовательный портал «УМНИК» [Электронный ресурс] / Проект Волгоградского Государственного Университета – Режим доступа: http://new.volsu.ru/umnik, свободный. – Загл. с экрана.

Национальная электронная библиотека (НЭБ) www.rusneb.ru
ELibrary.ru Научная электронная библиотека www.elibrary.ru
Электронная библиотека Grebennikon.ru www.grebennikon.ru
Cambridge University Press
ProQuest Dissertation & Theses Global
SAGE Journals
Taylor and Francis
JSTOR

6.3 Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:
1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения:

1) для лекционных занятий - учебная аудитория, доска, компьютер или ноутбук, проектор (стационарный или переносной) для демонстрации учебных материалов.

Состав программного обеспечения:
1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

2) для проведения лабораторных работ - специализированная аудитория (учебная лаборатория), оборудованная техническими средствами для проведения лабораторных работ

№	Оборудование
ЛР_1.	Общие вопросы проектирования АИС. Язык моделирования UML.
ЛР_2.	Основные возможности современных СУБД. Разработка концептуальной модели данных.
ЛР_3.	Технологии доступа к БД. Разработка серверной части БД.
ЛР_4.	Особенности хранения информации в СУБД. Разработка клиентской части БД.

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением или могут быть заменены устным ответом; обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; письменные задания оформляются увеличенным шрифтом; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.
- для глухих и слабослышащих: лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования; письменные задания выполняются на компьютере в письменной форме; экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.
- для лиц с нарушениями опорно-двигательного аппарата: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих: в печатной форме увеличенным шрифтом, в форме электронного документа, в форме аудиофайла.
- для глухих и слабослышащих: в печатной форме, в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата: в печатной форме, в форме электронного документа, в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих: устройством для сканирования и чтения с камерой SARA CE; дисплеем Брайля PAC Mate 20; принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих: автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата: передвижными, регулируемыми эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1 Планы лабораторных занятий

Темы учебной дисциплины предусматривают проведение лабораторных занятий, которые служат как целям текущего и промежуточного контроля подготовки студентов, так и целям получения практических навыков применения методов выработки решений, закрепления изученного материала, развития умений, приобретения опыта решения конкретных проблем, ведения дискуссий, аргументации и защиты выбранного решения. Помощь в этом оказывают задания для лабораторных занятий, выдаваемые преподавателем на каждом занятии.

Целью лабораторных занятий является закрепление теоретического материала и приобретение практических навыков работы с соответствующим оборудованием, программным обеспечением и нормативными правовыми документами.

Тематика практических занятий соответствует программе дисциплины.

ЛАБОРАТОРНЫЙ ПРАКТИКУМ.

ЛР_1_
ЛР_2_
ЛР_3_
ЛР_4_

Описание лабораторных работ представляется в электронном виде

Приложение 1. Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина «Моделирование автоматизированных систем в защищенном исполнении» реализуется на факультете Информационных систем и безопасности кафедрой комплексной защиты информации.

Цель дисциплины:

– формирование научного мировоззрения и развития системного мышления;

– комплексное и систематическое изучение теоретических основ, методов и средств (алгоритмических, программных, технических) моделирования процессов и систем защиты информации.

Задачи дисциплины:

– изучение основополагающих принципов моделирования и использования его результатов в создании автоматизированных систем в защищенном исполнении;

– изучение способов проектирования и документального оформления процесса разработки защищенных автоматизированных систем на основе специализированных международных стандартов;

– изучение методов организации и регламентации процесса эксплуатации защищенных автоматизированных систем.

– развитие умения и навыков в области разработки защищенных автоматизированных систем в соответствии с требованиями профиля защиты;

Дисциплина направлена на формирование следующих компетенций:

ПК-12 – Способен принимать участие в проведении экспериментальных исследований системы защиты информации.

В результате освоения дисциплины обучающийся должен:

Знать: принципы моделирования, классификацию способов представления моделей процессов и системам защиты информации; приемы, методы, и недостатки способы различных формализации способов объектов, представления процессов, моделей явлений систем и реализации их на компьютере; типовые системы имитационного моделирования; способы планирования машинных экспериментов с имитационными моделями;

Уметь: представить модель в математическом и алгоритмическом виде; оценить качество модели; показать теоретические основания модели; моделировать процессы, протекающие в информационных системах;

Владеть: навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем; методами формирования требований по защите информации; методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем;

По дисциплине предусмотрена промежуточная аттестация в форме зачета.

Общая трудоёмкость освоения дисциплины составляет 2 зачётные единицы.