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 (профили) подготовки:
Безопасность автоматизированных систем
Уровень квалификации выпускника – бакалавр

Форма обучения – очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2021

Моделирование автоматизированных систем в защищенном исполнении
Рабочая программа дисциплины
Составитель:
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
№ 10 от 20.05.2021 г.

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Предметом дисциплины Б1.В.ДВ.05.02 «Моделирование автоматизированных систем в защищенном исполнении» являются основы знаний о моделировании, его роли в проектировании и исследовании автоматизированных систем в защищенном исполнении.
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 (модулю), соотнесённых с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	*ОПК-12.1 Моделирование автоматизированных систем в защищенном исполнении* *ОПК-12.2 Моделирование автоматизированных систем в защищенном исполнении* *ОПК-12.3 Моделирование автоматизированных систем в защищенном исполнении*	*Знать:* • *Основные угрозы безопасности информации и модели нарушителей в автоматизированных системах;* • *Основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические);* • *Основные информационные технологии, используемые в автоматизированных системах;* *Уметь:* • *Анализировать и оценивать угрозы информационной безопасности объекта;* • *Анализировать и оценивать угрозы информационной безопасности объекта;*

		Владеть: • *Навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем;* • *Методами формирования требований по защите информации;* • *Навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности;*
ПК-12 *Способен принимать участие в проведении экспериментальных исследований системы защиты информации*	*ОПК-12.1* *Моделирование автоматизированных систем в защищенном исполнении* *ОПК-12.2* *Моделирование автоматизированных систем в защищенном исполнении* *ОПК-12.3* *Моделирование автоматизированных систем в защищенном исполнении*	*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;

1.3. Место дисциплины в структуре образовательной программы

Дисциплина Б1.В.ДВ.05.02 «Моделирование автоматизированных систем в защищенном исполнении» относится к дисциплинам по выбору, 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, «Организационное проектирование систем защиты информации», «Комплексная защита объектов информатизации. Управление службой защиты информации», «Проектно-технологическая практика», «Эксплуатационная практика».

2. Структура дисциплины

Структура дисциплины для очной формы обучения

Общая трудоёмкость дисциплины составляет _2_ з.е., _76__ ч., в том числе контактная работа обучающихся с преподавателем 40_ ч., самостоятельная работа обучающихся 36_ ч.

№ п/п	Темы дисциплины/	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	**Введение. Проектирование и разработка автоматизированных информационных систем**	**5**	**4**			**4**		**6**	Опрос, выполнение лабораторной работы
2	**Работа с данными в автоматизированных информационных системах**	**5**	**4**			**4**		**6**	Опрос, выполнение лабораторной работы
3	**Разработка клиентского программного обеспечения**	**5**	**4**			**8**		**6**	Опрос, выполнение лабораторной работы
4	**Разработка клиентского программного обеспечения. Основные элементы клиентских программ**	**5**	**4**			**6**		**12**	Опрос, выполнение лабораторной работы
	Зачёт					**2**		**6**	Зачёт по билетам

	итого:		**16**			**24**		**36**	

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	**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 *Контрольные вопросы* 1. Создание приложений БД средствами Delphi. 2. Процессор баз данных BDE ? стандартизированное средство доступа к БД. 3. Схема взаимодействия программы, компонентов и БД в среде Delphi. 4. Средства для работы с БД: инструментальные средства и компоненты. Их краткая характеристика, назначение. 5. Универсальное приложение для доступа к БД? оболочка базы данных DataBase Desktop. 6. Утилита BDE Administrator. Псевдоним БД. Языковой драйвер. 7. Способы создания таблиц баз данных и форм приложения. 8. Создание формы для работы с БД через BDE. 9. Основные шаги при создании приложений, работающих с таблицами. 10. Взаимосвязи данных. Главная и подчиненная таблицы. Связь Master-Detail.
2	**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. *Контрольные вопросы* Программа Data Module Designer в составе Delphi как средство автоматизации разработки приложений. 1. Создание таблиц в ходе выполнения программы. 2. Форма для таблицы, использующая компонент типа Ttable. Обзор свойств и методов. 3. Основные компоненты для работы с БД. Наборы данных. Важнейшие свойства. Методы. 4. Наборы данных. Состояния набора данных. Режимы наборов данных. Доступ к полям. 5. Навигация по набору данных. Методы для перемещения указателя текущей записи. 6. Основные компоненты для работы с БД. Объект поля Field. 7. Создание полей Lookup. 8. Создание калькулируемых полей. 9. Основные компоненты для работы с БД. Источник данных.
3	**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: си-

		стемные, локальные, временные, удалённые. Разработка серверной части. Цифровые сертификаты и инфраструктура открытых ключей *Контрольные вопросы* 1. Создание навигационного интерфейса с помощью визуальных компонент для работы с данными. 2. Настройка столбцов таблицы типа TDBGrid. 3. Компоненты для визуализации полей текущей записи: DBEdit, DBText, DBMemo, DBCheckBox, DBRadioGroup, DBNavigator. 4. Навигационный способ доступа к данным. 5. Реляционный способ доступа к данным. 6. Создание и выполнение SQL-запросов. Статические, динамические, параметрические запросы. 7. Запросы с использованием компонента Tquery. 8. Динамическое создание новой таблицы. 9. Организация поиска записей в таблице. Метод Locate. Метод Lookup. 10. Фильтрация. Возможность фильтрации по выражению и по диапазону.
4	**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 *Контрольные вопросы* 1. Особенности проектирования форм для ввода и редактирования информации на основе первичных документов. Макет экранной формы. 2. Типы макетов экранной формы. Информационная часть макета экранной формы. Служебная часть макета экранной формы. 3. Особенности проектирования форм документов результатной информации. 4. Рекомендации по проектированию пользовательского интерфейса. 5. Принципы построения пользовательского интерфейса. 6. Три размерности согласованности пользовательского интерфейса. 7. Два вида стилей взаимодействия между пользователем и компьютером и способы для связи. 8. Принципы использования цвета при проектировании эргономичного интерфейса. 9. Тексты и диалоги. Принципы создания текстовых диалогов и отображений. 10. Средства управления графического интерфейса пользователя.

4. Образовательные технологии

№ п/п	**Наименование раздела**	**Виды учебных занятий**	**Образовательные технологии**
1	**2**	**3**	**4**
1.	**Тема 1**	*Лекция 1-2.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Подготовка к занятиям с использованием ЭБС*
2	**Тема 2**	*Лекция 3-4.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Подготовка к занятиям с использованием ЭБС*
3	**Тема 3**	*Лекция 5-6* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Подготовка к занятиям с использованием ЭБС*
4	**Тема 4**	*Лекция 7-8* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *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 1.*	*Выполнение лабораторной работы в физическом практикуме*

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: *– опрос (темы 1-3)* *– опрос (темы 4-5)* *– лабораторная работа 1-4* *– практические занятия*	 *2 балла* *5 баллов* *10 баллов* *4 балла*	 *6 баллов* *10 баллов* *40 баллов* *4 балла*
Промежуточная аттестация *экзамен*		*40 баллов*
Итого за дисциплину *экзамен*		*100 баллов*

Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины представляется в виде таблицы:

№ п/п	***Контролируемые разделы дисциплины***	***Код контролируемой компетенции***	***Наименование оценочного средства***
1.	Темы 1 – 5	ОПК-12.1, ОПК-12.2, ОПК-12.3, ПК-12.1, ПК-12.2, ПК-12.3	Опрос
2.	Лабораторные работы 1-4	ОПК-12.1, ОПК-12.2, ОПК-12.3, ПК-12.1, ПК-12.2, ПК-12.3	План лабораторного практикума

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	«отлично»/ «зачтено (отлично)»/ «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	«хорошо»/ «зачтено (хорошо)»/ «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».
67-50/ D,E	«удовлетворительно»/ «зачтено (удовлетворительно)»/ «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.

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	«неудовлетворительно»/ 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

Промежуточная аттестация (примерные вопросы) – проверка сформированности компетенций – ОПК-12, 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.

7 Материально-техническое обеспечение дисциплины

Для материально-технического обеспечения дисциплины необходимо:

1) для лекционных занятий – лекционный класс с видеопроектором и компьютером, на котором должно быть установлено следующее ПО:

№ п/п	Наименование ПО	Производитель	Способ распространения
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 10 Pro	Microsoft	лицензионное

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

Перечень БД и ИСС

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2020 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2020 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

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.
– 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 – проверка сформированности компетенций – ОПК-12, ПК-12.

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 ДИСЦИПЛИНЫ

Дисциплина Б1.В.ДВ.05.02 «Моделирование автоматизированных систем в защищенном исполнении» реализуется на факультете Информационных систем и безопасности для студентов 3-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профили подготовки –Безопасность автоматизированных систем) 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:

ОПК-12 – Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений.

ОПК-12.1, 12.2, 12.3 – Моделирование автоматизированных систем в защищенном исполнении.

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

ПК-12.1, 12.2, 12.3 – Моделирование автоматизированных систем в защищенном исполнении.

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.

Приложение 2

УТВЕРЖДЕНО
Протокол заседания кафедры
№_____ от_____

ЛИСТ ИЗМЕНЕНИЙ

в рабочей программе дисциплины
«Моделирование автоматизированных систем в защищенном исполнении»

по направлению подготовки Информационная безопасность

на 20__/20__ учебный год

1. В _____ вносятся следующие изменения:
(элемент рабочей программы)
1.1. ……..;
1.2. ……...;
…
1.9. …… .

2. В _____ вносятся следующие изменения:
(элемент рабочей программы)
2.1. ……..;
2.2. ……...;
…
2.9. …… .

3. В _____ вносятся следующие изменения:
(элемент рабочей программы)
3.1. ……..;
3.2. ……...;
…
3.9. …… .

Составитель подпись расшифровка подписи
дата