МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ ВОЛГОГРАДСКОЙ ОБЛАСТИ

Рабочая программа составлена на основе ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем», утвержденного приказом МОиН РФ от 01.12.2016 № 1509.

Рабочая программа рассмотрена и одобрена на заседании кафедры
Информатики и информационной безопасности
(наименование кафедры - разработчика)

«03» марта 2017 г., протокол № 10.

Зав. кафедрой _____ / И.И. Баранкова/
(подпись) (И.О. Фамилия)

Рабочая программа одобрена методической комиссией
института Энергетики и автоматизированных систем
(наименование факультета (института) - исполнителя)

«14» марта 2017 г., протокол № 6.

Председатель _____ / С.И. Лукьянов/
(подпись) (И.О. Фамилия)

Рабочая программа составлена: зав.кафедрой ИиИБ, д.т.н., профессор
(должность, ученая степень, ученое звание)

_____ / И.И. Баранкова /
(подпись) (И.О. Фамилия)

Рецензент: зав. кафедрой Бизнес-информатики
и информационных технологий, к.п.н. профессор
(должность, ученая степень, ученое звание)

_____ / Г.Н. Чусавитина/
(подпись) (И.О. Фамилия)

Лист регистрации изменений и дополнений

№ п/п	Раздел программы	Краткое содержание изменения/дополнения	Дата, № протокола заседания кафедры	Подпись зав. кафедрой
1.	7	Переработка фонда оценочных средств	№1 от 07.09.2018	
2.	8	Обновление списка основной и дополнительной литературы	№1 от 07.09.2018	
3.	7	Переработка фонда оценочных средств	№ 1 от 07.09.2019	
4.	8	Обновление списка основной и дополнительной литературы	№ 1 от 07.09.2019	
5.	7	Переработка фонда оценочных средств	№1 от 04.09.2020	
6.	8	Обновление списка основной и дополнительной литературы	№1 от 04.09.2020	

1 Цели освоения дисциплины

Целью освоения дисциплины «Моделирование систем и процессов защиты информации» является ознакомление с принципами моделирования систем и средств защиты информации, управления и обеспечения безопасности и целостности данных информационных систем и технологий, а также навыков и умений в области анализа потенциальных угроз информационной безопасности, выборе средств реализации защиты в информационных системах, реализующих новые информационные технологии; – изучение инструментальных (программных и технических) средств моделирования процессов информационных распределенных систем; – реализация моделирующих алгоритмов для исследования характеристик и поведения систем защиты информации; освоение принципов имитационного моделирования и математической формализации процессов, защиты информации.

2 Место дисциплины в структуре образовательной программы подготовки специалиста

Дисциплина «Моделирование систем и процессов защиты информации» входит вариативную часть блока 1 образовательной программы по специальности 10.05.03 «Информационная безопасность автоматизированных систем».

Для изучения дисциплины необходимы знания (умения, навыки), сформированные в результате изучения дисциплин «Информатика», «Основы информационной безопасности», «Информационные технологии. Базы данных», «Безопасность сетей ЭВМ» «Безопасность систем баз данных», «Безопасность операционных систем», «Анализ рисков информационной безопасности».

Знания (умения, навыки), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин «Математическое моделирование распределенных систем», «Основы теории оптимизации», «Информационная безопасность систем организационного управления», в научно-исследовательской работе и при прохождении производственной практики.

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Моделирование систем и процессов защиты информации» обучающийся должен обладать следующими компетенциями:ПК-2; ПСК-7.1

Структурный элемент компетенции	**Планируемые результаты обучения**
ПК-2 способностью создавать и исследовать модели автоматизированных систем	
Знать	-основные принципы моделирования и виды моделей, требования, предъявляемые к моделям -основные принципы моделирования и виды моделей, требования, предъявляемые к моделям -методы оценки качества моделей, методы и средства моделирования и оптимизации бизнес-процессов -основные угрозы безопасности информации и модели нарушителя в автоматизированных системах -способы реализации угроз безопасности информации и модели нарушителя в автоматизированных системах
Уметь:	-строить и изучать компьютерные модели конкретных явлений и процессов для решения расчетных и исследовательских задач -применять различные методы моделирования, исследования и верификации моделей -применять специализированные методы моделирования, исследования и верификации моделей -разрабатывать постановку задачи моделирования и выбирать методы и средства моделирования систем защиты информации

Структурный элемент компетенции	**Планируемые результаты обучения**
	− анализировать и оценивать угрозы информационной безопасности объекта; − разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем
Владеть:	-основами построения моделей систем передачи информации -навыками пользования библиотеками прикладных программ для решения прикладных задач -навыками применения аппарата моделирования для решения прикладных теоретико-информационных задач -навыками формализации задач и постановки задач моделирования -навыками выбора и обоснования критериев эффективности функционирования моделей -навыками разработки, документирования информационных систем с учетом требований по обеспечению информационной безопасности; -навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите -методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем
ПСК 7.1 способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах	
Знать	− цели и задачи моделирования систем и процессов защиты информации; этапы моделирования и виды моделей систем и процессов защиты информации;- способы обеспечения информационной безопасности информационных систем; - основные принципы построения моделей систем защиты информации - различные информационные технологии, используемые в моделировании процессов защиты информации - методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем
Уметь	- обосновать выбор подходящего метода и привести алгоритм решения задачи; - формировать множество альтернативных решений, ставить цель и выбирать оценочный критерий оптимальности способа решения - применять новые технологии проектирования и анализа систем - проводить мониторинг угроз безопасности информационных систем
Владеть	- приемами исследования проблем моделирования процессов защиты информации, возникающих в различных сферах человеческой деятельности - навыками решения моделирования процессов защиты информации - навыками проектирования информационных структур - навыками семантического моделирования данных, методами снижения угроз безопасности информационных систем, вызванных ошибками на этапе проектирования, разработки и внедрения - навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; − навыками анализа основных узлов и устройств современных автоматизированных систем

4 Структура и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет **5** зачетных единиц **180** акад. часов, в том числе:

- контактная работа – 90 акад. часов:
  - аудиторная – 85 акад. часов;
  - внеаудиторная – 5 кад. часов
- самостоятельная работа – 54,3 акад. часов;
- подготовка к экзамену – 35,7 акад. часа

Семестр 9, экзамен, курсовая работа

Раздел/ тема дисциплины	**Аудиторная контактная работа (в акад. часах)**		самост. раб.	Вид самост работы	Формы текущего и промежуточного контроля успеваемости	Код и структурный элемент компетенции
	илекц	практ ич.				
Тема 1. Математическое моделирование. Форма и принципы представления математических моделей Моделирование как метод научного исследования. Типы моделей.	2	1/1	2	Поиск дополнительной информации по заданной теме. Выполнение ИДЗ	Опрос, коллоквиум, проверка ИДЗ	ПК-2-зу, ПСК 7.1-з
Тема 2. Компьютерное моделирование и вычислительный эксперимент. Понятие псевдослучайности. Псевдослучайные объекты. Базовый датчик: критерии качества, используемые методы. Генерация непрерывных случайных величин: метод отбраковки и метод обратной функции. Специальные методы генерации нормально распределѐнных случайных величин Генерация дискретных случайных величин, выборка с возвращением и выборка без возвращения. Генерация случайных	2	1	2	Подбор, описание, экспертная оценка сайтов Интернет. Подготовка к компьютерному тестированию. Самостоятельная работа с интернет-источниками, Выполнение ИДЗ	Опрос, коллоквиум, проверка ИДЗ	ПК-2-зу, ПСК 7.1-зу

Раздел/ тема дисциплины	Аудиторная контактная работа (в акад. часах)		самост. раб.	Вид самост работы	Формы текущего и промежуточного контроля успеваемости	Код и структурный элемент компетенции
	илекц	практ ич.				
процессов: основные подходы. Генерация Гауссовских процессов						
Тема 3. Этапы проектирования СИБ и требования к ним. Предпроектное обследование, техническое задание. Техническое проектирование, рабочее проектирование, испытания и внедрение в эксплуатацию.	2	4/1	2	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала.	Презентация, защита	ПК-2-зув, ПСК 7.1-з
Тема 4. Компьютерное имитационное моделирование. Статистическое имитационное моделирование. Особенности имитационного моделирования. Этапы имитационного моделирования. Статистическое имитационное моделирование	2	4/2	4	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала.	Опрос, коллоквиум, ИДЗ	ПК-2-зув, ПСК 7.1-з
Тема 5. Обобщенные модели систем защиты	4	4/1	4	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала.	Опрос, коллоквиум	ПК-2-зу, ПСК 7.1-зу
Тема 6.Модели, построенные с использованием теории случайных процессов	2	2/1	3	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к практическим занятиям.	Опрос, коллоквиум, ИДЗ	ПК-2-з, ПСК 7.1-зу
Тема 7. Модели,	2	2/1	3	Самостоятельное	Опрос,	ПК-2-з, ПСК

Раздел/ тема дисциплины	Аудиторная контактная работа (в акад. часах)		самост. раб.	Вид самост работы	Формы текущего и промежуточного контроля успеваемости	Код и структурный элемент компетенции
	лекц	практ и ич.				
построенные с использованием теории сетей Петри				изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к практическим занятиям.	коллоквиум	7.1-зу
Тема 8Модели, построенные с использованием теории автоматов	2	3/1	3	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к практическим занятиям.	Доклад, обсуждение	ПК-2-з,
Тема 9.Модели, построенные с использованием теории графов	2	3/2	2	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к практическим занятиям.	Опрос, обсуждение теоретических концепций	ПК-2-з,
Тема 10. Модели, построенные с использованием теории нечетких множеств	1	2/1	3	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к практическим занятиям.	Опрос, обсуждение теоретических концепций	ПК-2-з,
Тема 11.Модели, построенные с использованием теории катастроф	1	2/1	3	Поиск дополнительной информации по заданной теме. Подготовка к практическим занятиям	Кейс, Проверка ИДЗ, представление отчетов по работам в электронной	ПК-2-з,

Раздел/ тема дисциплины	Аудиторная контактная работа (в акад. часах)		самост. раб.	Вид самост работы	Формы текущего и промежуточного контроля успеваемости	Код и структурный элемент компетенции
	илекц	практ ич.				
					форме	
Тема 12.Модели, построенные с использованием теории игр	1	2/1	2	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала	Проверка ИДЗ, представление отчетов по работам в электронной форме	ПК-2-з,
Тема 13. Модели, построенные с использованием энтропийного подхода.	2	4/2	4	Поиск дополнительной информации по заданной теме. Подготовка к практическим занятиям	Проверка ИДЗ, представление отчетов по работам в электронной форме	ПК-2-зу,
Тема 14 Сравнительный анализ моделей систем защиты информации	1	2/1	2	Поиск дополнительной информации по заданной теме. Подготовка к практическим занятиям	Опрос, коллоквиум	ПК-2-зув,
Тема 15. Особенности многопользовательских систем. Типовые элементы структуры КСИБ, включающей организационные и программно-технические решения по	1	2	2	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала	Опрос, коллоквиум	ПК-2-зув, ПСК 7.1-зу
Тема16. Методы и методики проектирования: методика выявления возможных каналов НСД, последовательность работ при проектировании комплексной системы защиты информации от НСД и утечки за счет ПЭМИН, моделирование как инструментарий	1	2/1	2	Поиск дополнительной информации по заданной теме. Подготовка к практическим занятиям	Доклад, презентация	ПК-2-зу, ПСК 7.1-зу

Раздел/ тема дисциплины	Аудиторная контактная работа (в акад. часах)		самост. раб.	Вид самост работы	Формы текущего и промежуточного контроля успеваемости	Код и структурный элемент компетенции
	илекц	практ ич.				
проектирования, методика построения административного управления КСИБ.						
Тема 17. Целевая функция задач защиты информации. Критерии достижения требуемого уровня. Последовательность работ и особенности при проектировании системы защиты информации от НСД. Утечка информации за счет ПЭМИН. Типовые решения защиты от ПЭМИН.	2	3	4	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала	Доклад, презентация	ПК-2-зу, ПСК 7.1-зув
Тема 18. Моделирование процессов утечки информации, модели нарушителя, основные критерии, типовые этапы моделирования. Последовательность использования административного управления СИБ.	2	4/2	3	Поиск дополнительной информации по заданной теме. Подготовка к практическим занятиям	Доклад, презентация	ПК-2-зув, ПСК 7.1-зув
Тема 19.Методы и методики оценки качества СИБ: методы нормативного функционального наблюдения. Метод экспертных структурных вопросников, метод оценки уязвимости информации Хоффмана, метод оценки риска Фишера, требования к эксплуатационной документации СИБ.	1	2/1	3,3	Поиск дополнительной информации по заданной теме. Выполнение ИДЗ	Опрос, коллоквиум, проверка ИДЗ	ПК-2-зув, ПСК 7.1-зув
Подготовка к экзамену			35,7			
Итого по дисциплине	**34**	**51/22**	54,3		**Экзамен**	

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины используются:

a) **Традиционная технология**, включающая в себя объяснение преподавателя на лекциях, самостоятельную работу с учебной и справочной литературой по дисциплине, выполнение заданий по методическим указаниям.

b) ***Вводная лекция*** – для целостного представления об учебном предмете и анализа учебно-методической литературы;

c) ***Обзорные лекции*** – для систематизации научных знаний на высоком уровне с использованием ассоциативных связей в процессе представления и осмысления информации;

d) ***Проблемные лекции***– для ведения диалога обучающихся с преподавателем по сложным темам, для более полного раскрытия содержания проблемы по некоторым темам, а так же для развития исследовательских навыков и изучения способов решения задач;

2) ***Лекции-визуализации*** – для наглядного представления материалов курса. Лекционные занятия проводятся с использованием презентационного оборудования (проектор, экран, ноутбук), в качестве наглядных материалов используются: Web-ориентированные программные учебные материалы, электронные плакаты, презентации к лекциям.

3) **Модульно-компетентностная технология**, включающая в себя жесткое структурирование содержания учебного материала, сопровождающаяся обязательными блоками домашних заданий, контрольных работ и тестированием по каждой теме содержания курса. Для формирования у обучающихся основных понятий дисциплины используются:

a) ***Кейс-методы*** – для овладения системой знаний и умений и творческого их использования в профессиональной деятельности и самообразовании; для квалифицированного и независимого решения профессиональных задач; для ориентации в многообразии учебных программ, пособий, литературы и выбора наиболее эффективных в применении к конкретной ситуации; для осуществления саморефлексии для дальнейшего профессионального, творческого роста и социализации личности.

4) **Интерактивное обучение**.. Все практические занятия проводятся в интерактивной форме. В рамках интерактивного обучения обучающихся применяются:

a) *Case-study* – для анализа реальных проблемных ситуаций и поиска лучших вариантов решений, разбор результатов тематических контрольных работ, анализ ошибок, совместный поиск вариантов рационального решения проблемы.

b) *Методы IT* – для применения компьютеров в процессе освоения дисциплины и доступа к ЭОР кафедры и Интернет-ресурсам.

c) *Проблемное обучение* – для стимулирования к самостоятельной «добыче» знаний, необходимых для решения конкретной проблемы. Для этого каждому обучающемуся выдаётся индивидуальная тема, по которой он должен составит реферат.

5) ***Контекстное обучение*** – для мотивации обучающихся к усвоению знаний путем выявления связей между конкретным знанием и его применение. Овладев в рамках изучения дисциплины навыками обеспечения безопасности информации с помощью типовых программных средств, обучающийся приобретет способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности;

a) ***Междисциплинарное обучение*** – для использования знаний из различных областей, их группировки и концентрации в контексте решаемой задачи. Для реализации данного метола обучения обучающимся выдаются задания по решения задач из другой предметной области.

6) Для приобретения **новых фактических знаний и практических умений** используются практические занятия:

a) компьютерный практикум;
b) разбор результатов тематических контрольных работ, анализ ошибок, совместный поиск вариантов рационального решения учебной проблемы.

6. Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Моделирование систем и процессов защиты информации» предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.

Аудиторная самостоятельная работа обучающихся предполагает решение контрольных задач на практических занятиях.

Аудиторная самостоятельная работа обучающихся на практических занятиях осуществляется под контролем преподавателя в виде решения задач и выполнения упражнений, которые определяет преподаватель для обучающегося.

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде изучения литературы по соответствующему разделу с проработкой материала; выполнения домашних заданий, подготовки к аудиторным контрольным работам и выполнения домашних заданий с консультациями преподавателя.

Примерные индивидуальные домашние задания (ИДЗ):

***Тема 1*. Задание: 1) Используя средства моделирования пакета MathCad, провести моделирование случайной величины с заданным законом распределения.**

2) Используя средства моделирования пакета MathCad, провести моделирование типовой радиотехнической цепи методом комплексной огибающей.

Тема 2. Реализовать один из выбранных алгоритмов получения случайных чисел на языке программирования. Обосновать выбор алгоритма. Провести проверку на соответствие характеристик полученной выборки.

Тема 4. Задание : Разработать, используя среду программирования (Delphi, VisualStudio, и т.д.)вероятностную модель контроля доступа.

1. Расчет вероятности нахождения системы в состоянии «защита обеспечена».
2. Расчет вероятности нахождения системы в состоянии «защита нарушена».
3. Расчет вероятности нахождения системы в состоянии «защита разрушена».

7. Оценочные средства для проведения промежуточной аттестации

а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:

Структурный элемент компетенции	**Планируемые результаты обучения**	**Оценочные средства**
ПК-2 способностью создавать и исследовать модели автоматизированных систем		
Знать	-основные принципы моделирования и виды моделей, требования, предъявляемые к моделям -основные принципы моделирования и виды моделей, требования, предъявляемые к моделям	**Теоретические вопросы к экзамену** 1. Основы теории моделирования. Основные термины и определения . 2. Классификация методов моделирования. 3. Этапы построения моделей. 4. Подходы и программные средства при структурно-функциональном моделировании.

	-методы оценки качества моделей, методы и средства моделирования и оптимизации бизнес-процессов -основные угрозы безопасности информации и модели нарушителя в автоматизированных системах -способы реализации угроз безопасности информации и модели нарушителя в автоматизированных системах	5. Имитационное моделирование. Основные понятия. Принципы и методы построения имитационных моделей. 6. Имитационное моделирование как специфический вид компьютерного моделирования. 7. Достоинства и недостатки имитационного моделирования. 8. Инструментарии имитационного моделирования. 9. Математические модели. Математические схемы описания информационных систем. Дискретно – непрерывные модели. Дискретно – стохастические модели. 10. Непрерывно-стохастические модели. Стохастические минимаксные модели. 11. Максиминный показатель. Лексикографический метод. Принципы системного подхода в моделировании. 12. Системный подход к управлению защитой информации. Системные принципы 13. создания комплексной защиты информации. 14. Выбор уровня описания системы в модели. Этапы моделирования. 15. Выбор уровня описания системы в модели. Методология разработки моделей 16. Алгоритм создания системы комплексной защиты. 17. Модель формирования множества функций защиты информации 18. Метод статистических испытаний (метод Монте-Карло). 19. Моделирование случайных факторов. Проверка равномерности и стохастичности. 20. Метод интерпретации. Моделирование непрерывных случайных величин. 21. Модель нарушителя. 22. Виды представления времени в модели (моделирование по ΔT). 23. Моделирование по событиям. Моделирование параллельных процессов. 24. Метод фон - Неймана. 25. Алгоритм получения нормально-распределенной случайной величины. 26. 17. Алгоритм получения случайной величины, распределенной по Пуассону. Условия применения пуассоновских процессов для моделирования атак.
Уметь:	-строить и изучать компьютерные модели конкретных явлений и процессов для решения расчетных и исследовательских задач -применять различные методы моделирования, исследования и верификации моделей -применять	***Задача:*** Составить алгоритм получения нормально распределенной случайной величины на основе закона распределения Релея. Для этого сгенерировать два равномерно распределенных случайных числа β_1 и β_2 на интервале [0,1] и сформировать вектор, длина которого будет распределена по релеевскому закону с параметром σ А фаза будет вычисляться

	специализированные методы моделирования, исследования и верификации моделей -разрабатывать постановку задачи моделирования и выбирать методы и средства моделирования систем защиты информации − анализировать и оценивать угрозы информационной безопасности объекта; − разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем	Графически представить, что в соответствии с законом распределения Релея , любая проекция на координатные оси x или y будет распределена по нормальному закону.
Владеть:	-основами построения моделей систем передачи информации -навыками пользования библиотеками прикладных программ для решения прикладных задач -навыками применения аппарата моделирования для решения прикладных теоретико-информационных задач -навыками формализации задач и постановки задач моделирования -навыками выбора и обоснования критериев эффективности функционирования моделей -навыками разработки, документирования информационных систем с учетом требований по обеспечению информационной безопасности; -навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите -методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем	Задача: Охарактеризовать алгоритмы получения случайной величины, их свойства и характеристики, реализовать один из выбранных алгоритмов на языке программирования. Обосновать выбор алгоритма. Задание: 1. Моделирование приложения для обнаружения подвижных объектов. 2. Моделирование угроз информационной безопасности для заданного объекта информатизации (варианты различаются исходными данными на объект). 3. Моделирование нарушителя информационной безопасности для заданного объекта информатизации (варианты различаются исходными данными на объект).
ПСК 7.1 способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах		

Знать	– цели и задачи моделирования систем и процессов защиты информации; этапы моделирования и виды моделей систем и процессов защиты информации;- способы обеспечения информационной безопасности информационных систем; - основные принципы построения моделей систем защиты информации - различные информационные технологии, используемые в моделировании процессов защиты информации - методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем	**Теоретические вопросы** 1. Модели выбора рационального варианта средства защиты информации на основе экспертной информации. 2. Вероятностная модель системы контроля доступа к информации. 3. Модель на основе нейронных сетей в задачах защиты информации. 4. Стратегическое планирование имитационного экспериментов. 5. Тактическое планирование имитационного экспериментов. 6. Оценка качества имитационной модели. Методы оценки адекватности. 7. Методы оценки устойчивости модели. 8. Методы оценки чувствительности модели. 9. Оценка влияния и взаимосвязи факторов. Однофакторный и дисперсионный анализ. 10. Методы и методики оценки качества СИБ: методы нормативного функционального наблюдения. 11. Метод экспертных структурных вопросников, метод оценки уязвимости информации Хоффмана, метод оценки риска Фишера, требования к эксплуатационной документации СИБ. 12. Аттестация по требованиям безопасности; особенности эксплуатации СИБ на объекте защиты. 13. Организационно-функциональные задачи службы безопасности. 14. Требования к эксплуатационной документации СИБ. Аттестация по требованиям безопасности; особенности эксплуатации СИБ на объекте защиты, организационно-функциональные задачи службы безопасности. 15. Организационные вопросы обеспечения СИБ. Допуск на объект. Служба безопасности: основные положения, регламентные документы, подбор кадров.
Уметь	- обосновать выбор подходящего метода и привести алгоритм решения задачи; - формировать множество альтернативных решений, ставить цель и выбирать оценочный критерий оптимальности способа решения - применять новые технологии проектирования и анализа систем - проводить мониторинг угроз безопасности информационных систем	***Задача***: Подобрать распределение случайной величины для моделирования D-Dos – атак типа DNS Reflection. Каждый бот в такой сети генерирует несколько DNS-запросов, но в качестве IP источника использует один и тот же IP-адрес цели . DNS-сервис отвечает по этому IP-адресу. Учесть, что запрос DNS – это обычно менее 50 байт, ответ раз в десять длиннее. Предположим, атакующий выдал 100 000 коротких запросов DNS по 50 байт (всего 5 Мбайт). Если каждый ответ содержит 1 Кбайт, то в сумме это уже 100 Мбайт.
Владеть	- приемами исследования проблем моделирования процессов защиты	***Задача:*** 1. В центр обработки запросов приходят запросы пользователей(id, размер пакета), которые распределяются для

	информации, возникающих в различных сферах человеческой деятельности - навыками решения моделирования процессов защиты информации - навыками проектирования информационных структур - навыками семантического моделирования данных, методами снижения угроз безопасности информационных систем, вызванных ошибками на этапе проектирования, разработки и внедрения - навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; − навыками анализа основных узлов и устройств современных автоматизированных систем	обработки на N серверов. Запросы приходят с случайным нормальным интервалом времени, с мат. ожиданием 2 мс. Каждый сервер имеет разную производительность(количество обработанных бит в единицу времени). Запросы стремятся захватить свободный сервер с максимальной производительностью, если свободных серверов нет, ставятся в очередь. Если время ожидания запроса истекло, запрос аннулируется и ставится в очередь повторно. После M необработанных очередей запрос удаляется и остается необработанным. Подобрать количество серверов для гарантированной обработки всех поступивших запросов. 1. Создание модели «Шифратора». 2. Создание модели «Дешифратора». 3. Создание приложения для определения координат малоразмерных объектов. 4. Моделирование тепловизионного изображения объекта с учетом свойств поверхности и влияния блоков тепловизора. 5. Моделирование приложения для обнаружения подвижных объектов. 6. Моделирование угроз информационной безопасности для заданного объекта информатизации (варианты различаются исходными данными на объект). 7. Моделирование нарушителя информационной безопасности для заданного объекта информатизации (варианты различаются исходными данными на объект). 8. Выбор решения по обеспечению защиты от вредоносного программного обеспечения локального компьютера (варианты различаются кругом задач, решаемых на ПК).

Темы курсовых работ:

9. Моделирование работы видеорегистратора.
10. Моделирование поляризационных тепловизионных изображений на основе степени и азимута поляризации теплового изображения.
11. Моделирование тепловизионного изображения объекта.
12. Моделирование работы ПНВ. 8
13. Создание модели «Шифратора».
14. Создание модели «Дешифратора».
15. Создание приложения для определения координат малоразмерных объектов.
16. Моделирование тепловизионного изображения объекта с учетом свойств поверхности и влияния блоков тепловизора.
17. Моделирование приложения для обнаружения подвижных объектов.
18. Моделирование угроз информационной безопасности для заданного объекта информатизации (варианты различаются исходными данными на объект).
19. Моделирование нарушителя информационной безопасности для заданного объекта информатизации (варианты различаются исходными данными на объект).
20. Выбор решения по обеспечению защиты от вредоносного программного обеспечения локального компьютера (варианты различаются кругом задач, решаемых на ПК).

Методические указания для подготовки курсовой работы

Курсовая работа выполняется с использованием среды разработки приложений на любом языке высокого уровня. Приложение представляет собой компьютерную модель, согласно варианту задания. Курсовая работа является формой самостоятельной работы, выполняемой обучающимся на определенную тему, в соответствии с перечнем тем курсовых работ по

дисциплине. Курсовая работа выполняется под руководством преподавателя, в процессе ее написания обучабщийся развивает навыки к научной работе, закрепляя и одновременно расширяя знания, полученные при изучении курса «Моделирование систем и процессов защиты информации». При выполнении курсовой работы обучающийся должен показать свое умение работать с нормативным материалом и другими литературными источниками, а также возможность систематизировать и анализировать фактический материал и самостоятельно творчески его осмысливать.

В начале изучения дисциплины преподаватель предлагает обучабщимся на выбор перечень тем курсовых работ. Обучающийся самостоятельно выбирает тему курсовой работы. Совпадение тем курсовых работ у обучающихся одной учебной группы не допускается.

После выбора темы преподаватель формулирует задание по курсовой работе и рекомендует перечень литературы для ее выполнения. Исключительно важным является использование информационных источников, а именно системы «Интернет», что даст возможность обучающимся более полно изложить материал по выбранной им теме.

В процессе написания курсовой работы обучающийся должен разобраться в теоретических вопросах избранной темы, самостоятельно проанализировать практический материал, разобрать и обосновать практические предложения.

Преподаватель, проверив работу, может возвратить ее для доработки вместе с письменными замечаниями. обучающийся должен устранить полученные замечания в установленный срок, после чего работа окончательно оценивается.

Курсовая работа должна быть оформлена в соответствии с СМК-О-СМГТУ-42-09 (http://www.magtu-epp.narod.ru/literature/Bakalavr_rab_STP.pdf) «Курсовой проект (работа): структура, содержание, общие правила выполнения и оформления».

Критерии оценки (в соответствии с формируемыми компетенциями и планируемыми результатами обучения):

– на оценку «***отлично***» – обучающийся должен показать высокий уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам, оценки и вынесения критических суждений;

– на оценку «***хорошо***» – обучающийся должен показать знания не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам;

– на оценку «***удовлетворительно***» – обучающийся должен показать знания на уровне воспроизведения и объяснения информации, интеллектуальные навыки решения простых задач;

– на оценку «***неудовлетворительно***» – обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач.

Курсовая работа выполняется под руководством преподавателя, в процессе ее написания обучающийся развивает навыки к научной работе, закрепляя и одновременно расширяя знания, полученные при изучении дисциплины. При выполнении курсовой работы, обучающийся должен показать свое умение работать с нормативным материалом и другими литературными источниками, а также возможность систематизировать и анализировать фактический материал и самостоятельно творчески его осмысливать.

В процессе написания курсовой работы, обучающийся должен разобраться в теоретических вопросах избранной темы, самостоятельно проанализировать практический материал, разобрать и обосновать практические предложения.

Показатели и критерии оценивания курсовой работы:

– на оценку **«отлично»** (5 баллов) – работа выполнена в соответствии с заданием, обучающийся показывает высокий уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам, оценки и вынесения критических суждений;

– на оценку **«хорошо»** (4 балла) – работа выполнена в соответствии с заданием, обучающийся показывает знания не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам;

– на оценку **«удовлетворительно»** (3 балла) – работа выполнена в соответствии с заданием, обучающийся показывает знания на уровне воспроизведения и объяснения ин-формации, интеллектуальные навыки решения простых задач;

– на оценку **«неудовлетворительно»** (2 балла) – задание преподавателя выполнено частично, в процессе защиты работы обучающийся допускает существенные ошибки, не может показать интеллектуальные навыки решения поставленной задачи.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) основная литература:

1. Баранкова И. И. Определение критически значимых ресурсов объекта защиты при составлении модели угроз информационной безопасности [Электронный ресурс] : учебное пособие / И. И. Баранкова, О. В. Пермякова. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - Режим доступа: https://magtu.informsystema.ru/uploader/ fileUpload? name=3323.pdf&show=dcatalogues/1/1138331/3323.pdf&view=true. –Загл. с экрана.- ISBN 978-5-9967-1031-7.
2. Моделирование информационных ресурсов: теория и решение задач [Электронный ресурс]: учебное пособие / Г.Н. Исаев. - М.: Альфа-М: ИНФРА-М, 2010. – 224 с. http://znanium.com/bookread2.php?book=193771–Загл. с экрана.
3. Моделирование систем и процессов [Электронный ресурс]: Учебное пособие / Н.Г. Чикуров. - М.: ИЦ РИОР: НИЦ Инфра-М, 2013. - 398 с. - Режим доступа: http://znanium.com/bookread2.php?book=392652 –Загл. с экрана.
4. Баранкова И. И. Применение СКМ MathCAD в моделировании [Электронный ресурс] : учебное пособие / И. И. Баранкова, Т. Н. Носова. Магнитогорск: МГТУ, 2010. - 99 с. : ил., табл. - Режим доступа: https://magtu.informsystema.ru/uploader/fileUpload?name=466.pdf&show =dcatalogues/1/1080722/466.pdf&view=true –Загл. с экрана.

5. Имитационное моделирование: Учебное пособие [Электронный ресурс] / Н.Б. Кобелев, В.А. Половников, В.В. Девятков. - М.: КУРС: НИЦ Инфра-М, 2013. - 368 с. Режим доступа: http://znanium.com/bookread.php?book=361397 –Загл. с экрана. - ISBN 978-5-905554-17-9

б) дополнительная литература:

1. Пакеты прикладных программ [Электронный ресурс]: Учебное пособие/ С.В.Синаторов.- М.:ИНФРА-М, 2012.-256 с.-Режим доступа:http://znanium.com/bookread.php?book=310140.- Загл. с экрана.– ISBN 978-5-98281-275-9.

2. Моделирование систем и процессов [Электронный ресурс]: Учебное пособие / Н.Г. Чикуров. - М.: ИЦ РИОР: НИЦ Инфра-М, 2013. - 398 с. Режим доступа: http://znanium.com/bookread.php?book=392652 –Загл. с экрана. - ISBN 978-5-369-01167-6

в) Интернет – ресурсы:

3. Государственная публичная научно-техническая библиотека России [Электронный ресурс] / – Режим доступа: http://www.gpntb.ru, свободный.– Загл. с экрана. Яз.рус.
4. Российская государственная библиотека [Электронный ресурс] /Центр информ. Технологий РГБ; ред. Власенко Т.В., Web - мастер Козлова Н.В. – Электрон. Дан. – М.: Рос. Гос. б-ка, 1997. -URL: http://www.rsl.ru, свободный.– Загл. с экрана. Яз. рус., англ.
5. Российская национальная библиотека. [Электронный ресурс] / –URL: http://www.nlr.ru. Яз.рус.

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Тип и название аудитории	Оснащение аудитории
Мультимедийные поточные аудитории университета	Мультимедийные средства хранения, передачи и представления информации
Компьютерный класс	Персональные компьютеры с пакетом MS Office, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета
Программные средства:	ОС Windows, (Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021) MSOffice(Microsoft Open License 42649837, бессрочная) MathCad(43813518 D-1662-13 от 22.11.2013), Microsoft Visual Studio(Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021)
Аудитории для самостоятельной работы (ауд. 132а): компьютерные классы; читальные залы библиотеки.	Персональные компьютеры с ПО: Операционная система MS Windows 7 (Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021); Пакет MS Office 2007 (Microsoft Open License 42649837, бессрочная); Выход в Интернет и доступ в электронную информационно-образовательную среду университета.

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций и ПрООП ВО для специальности *10.05.03. Информационная безопасность автоматизированных систем.Специализация «Обеспечение информационной безопасности распределенных информационных систем».*