МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Костромской государственный университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ И СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Направление подготовки 10.03.01 Информационная безопасность

Направленность «Организация и технология защиты информации»

Квалификация (степень) выпускника: Бакалавр

Кострома

Рабочая программа дисциплины «Моделирование процессов и систем защиты информации» разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования направления подготовки 10.03.01 Информационная безопасность
Приказ Минобрнауки России от 1.12.2016 № 1515. Зарегистрировано в Минюсте России, регистрационный № 44821 от 20 декабря 2016 года.

Разработал:  Виноградова Галина Леонидовна, к.т.н., доцент кафедры защиты информации

Рецензент:  Щекочихин Олег Владимирович, к.т.н., доцент, заведующий кафедры защиты информации

УТВЕРЖДЕНО:

На заседании кафедры защиты информации

Протокол заседания кафедры № 13 от 6 июля 2017 г.

Заведующий кафедрой защиты информации

 Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № 12 от 27 июня 2018 г.

Заведующий кафедрой защиты информации

 Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № _11_ от _30.05.2019_____ г.

Заведующий кафедрой защиты информации

 Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № _8_ от _6.04.2020_____ г.

Заведующий кафедрой защиты информации

 Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № _6_ от _22.01.2021_____ г.

Заведующий кафедрой защиты информации

 Щекочихин Олег Владимирович, к.т.н., доцент

1. Цели и задачи освоения дисциплины

Цель дисциплины: формирование теоретических знаний и практических навыков управления процессами и системами на основе овладения методами анализа, проектирования, моделирования и совершенствования процессов и систем защиты информации с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы организации.

В результате изучения учебной дисциплины «Моделирование процессов и систем защиты информации» у обучаемых должны сформироваться профессиональные компетенции:

- способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности результатов (ПК-11);
- способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12);
– способность формировать предложения по оптимизации функционального процесса объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объекта и локализации защищаемых элементов (ПСК-2.2);

Задачи дисциплины:

- изучить понятийный аппарат, применяемый в методологиях моделирования процессов и систем,
- изучить основные методологии моделирования процессов и систем;
- сформировать умение моделирования процессов и систем защиты информации,
- изучить методы анализа и оптимизации процессов и систем защиты информации,
- овладеть навыками применения инструментальных систем моделирования процессов и систем защиты информации.

2. Перечень планируемых результатов обучения по дисциплине

В результате освоения дисциплины обучающийся должен:

знать

- теоретические основы методологий моделирования процессов и систем защиты информации,
- целевое предназначение моделирования процессов и систем защиты информации с точки зрения информационной безопасности,
- методы анализа и оптимизации процессов и систем защиты информации;
- принципы моделирования информационных процессов и систем защиты информации;
- базовые автоматизированные информационные системы моделирования процессов и систем.

уметь

- применять методику моделирования функциональных процессов объекта защиты, а также процессов и систем защиты информации;
- применять методы анализа и оптимизации процессов и систем защиты информации на основе их моделей с целью повышения их устойчивости к деструктивным воздействиям;
- уметь формировать предложения по оптимизации функциональных процессов объекта защиты с целью повышениях их защищенности;
- уметь разрабатывать и внедрять предложения по тактике защиты объекта и локализации защищаемых элементов на основе анализа их моделей.

владеть

- навыками проводить эксперименты по моделированию и анализу процессов и систем защиты информации, оценку погрешности и достоверности результатов;

- навыками принятия участия в проведении экспериментальных исследований процессов системы защиты информации объекта;
- навыками автоматизированного моделирования процессов и систем защиты информации.

освоить компетенции:
- способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности результатов (ПК-11);
- способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12);
– способность формировать предложения по оптимизации функционального процесса объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объекта и локализации защищаемых элементов (ПСК-2.2).

3. Место дисциплины в структуре ОП ВО

Дисциплина «Моделирование процессов и систем защиты информации» относится к циклу вариативных дисциплин по выбору, при этом, в значительной степени отличается от других дисциплин сферой знаний и направленностью обучения. Именно эта дисциплина формирует у обучаемых способность применения моделирования процессов и систем защиты информации в практике конкретных организаций для повышения уровня защиты данных в информационных процессах и функциональных процессах объекта защиты.

Освоению дисциплины «Моделирование процессов и систем защиты информации» предшествуют обязательные дисциплины базовой части образовательной программы специальности, такие как: «Введение в специальность», «Основы информационной безопасности», «Информационные технологии», «Организационное и правовое обеспечение информационной безопасности». Базируются на освоении дисциплины «Организационное и правовое обеспечение информационной безопасности». Изучение дисциплины является основой для освоения последующих дисциплин/практик: «Основы управления информационной безопасностью», «Комплексные системы защиты информации на предприятии», «Управление информационными ресурсами и проектами», «Информационный менеджмент».

Знания, умения и навыки, полученные в ходе освоения дисциплины безусловно будут использованы в дальнейшем в профессиональной деятельности.

Освоение данной дисциплины необходимо как предшествующее для прохождения производственной (преддипломной) практики, написания выпускной квалификационной работы.

Формирование профессиональных компетенций ПК-11; ПК-12 и ПСК-2.2 происходит также на других профильных дисциплинах, раскрывая единство и взаимосвязь профильных дисциплин, базирующихся на базовых курсах общей и теоретической физики.

4. Объем дисциплины (модуля)

4.1. Объем дисциплины в зачетных единицах с указанием академических (астрономических) часов и виды учебной работы

Виды учебной работы,	Очная форма
Общая трудоемкость в зачетных единицах	5
Общая трудоемкость в часах	180
Аудиторные занятия в часах, в том числе:	82
Лекции	32
Практические занятия	-
Лабораторные занятия	50

Самостоятельная работа в часах	98
Форма промежуточной аттестации	5,6 зачет

4.2. Объем контактной работы на 1 обучающегося

Виды учебных занятий	Очная форма
Лекции	32
Практические занятия	-
Лабораторные занятий	50
Консультации	1,6
Зачет/зачеты	0,5
Экзамен/экзамены	-
Курсовые работы	–
Курсовые проекты	–
Всего	84,1

5.Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием количества часов и видов занятий

5.1 Тематический план учебной дисциплины

№ п/п	Название раздела, темы	Всего з.е/час	Аудиторные занятия		Самостоятельная работа
			Лекции	Лаб раб	
Раздел 1. Базовые понятия методологий моделирования информационных процессов и систем					
1.1	Задачи моделирования информационных процессов и систем.	14	2	4	8
1.2	Общие принципы моделирования процессов и систем защиты информации.	14	2	4	8
1.3	Основные методологии моделирования процессов и систем защиты информации.	14	2	4	8
1.4	Методика моделирования процессов и систем защиты информации.	14	2	4	8
1.5	Классификация функциональных процессов объекта защиты.	14	2	4	8
1.6	Основные функциональные процессы объекта защиты.	14	2	4	8
1.7	Вспомогательные функциональные процессы объекта защиты.	16	4	4	8
1.8	Методы совершенствования процессов и систем	16	4	4	8
Раздел 2.Системы автоматизированного моделирования процессов и систем					

№ п/п	Название раздела, темы	Всего з.е/час	Аудиторные занятия		Самостоятельная работа
			Лекции	Лаб раб	
2.1	Основные системы автоматизированного моделирования процессов и систем защиты информации. Классификация.	18	4	6	8
2.2	Методика оценки экономической эффективности совершенствования процессов и систем защиты информации на основе анализа их моделей	18	4	6	8
2.3	Методика разработки тактики защиты объекта и локализации защищаемых элементов на основе анализа их моделей.	18	4	6	8
Зачет		10			10
Всего:		**180**	**32**	**50**	**98**

5.2. Содержание:

ТЕМА 1. Задачи моделирования информационных процессов и систем. Цель и задачи, структура курса. Цели и задачи моделирования информационных процессов и систем защиты информации. Использование моделей при обеспечении информационной безопасности объектов защиты.

ТЕМА 2. Общие принципы моделирования процессов и систем защиты информации. Виды моделирования. Место формализации и моделирования при исследовании процессов в системе защиты информации. Понятие и виды моделей. Классификация и структура моделей. Характеристики моделей. Преимущества и недостатки. Исходные данные и ограничения, обработка и интерпретация результатов моделирования. Имитационное моделирование, особенности и преимущества. Логико-лингвистическая модель процесса возникновения угроз в человеко-машинной системе. Принципы имитационного моделирования процессов и систем информационной защиты.

ТЕМА 3. Основные методологии моделирования процессов и систем защиты информации. Классификация подходов к моделированию процессов и систем защиты информации. Структурные методы разработки моделей процессов и систем. Принципы разработки моделей. Метод «черного ящика». Принцип декомпозиции моделей процессов и систем. Методология SADT. Стандарты моделирования процессов семейства IDEF (IDEF0, IDEF 3, DFD). Достоинства и недостатки методологии SADT. Объектно-ориентированные методы построения моделей. Критерии выбора методологии моделирования процессов и систем.

ТЕМА 4. Методика моделирования процессов и систем защиты информации. Описание границ процессов и систем. Методы сбора информации для построения моделей. Описание процессов и систем. Установление контрольных точек в процессах. Показатели процессов. Этапы моделирования.

ТЕМА 5. Классификация функциональных процессов объекта защиты. Понятие функциональных процессов объекта защиты. Характеристики функциональных процессов. Виды функциональных процессов. Классификационные признаки. Классификация процессов.

ТЕМА 6. Основные функциональные процессы объекта защиты.
Понятие основных функциональных процессов объекта защиты. Пошаговое выделение процесса, его регламентация. Цели и особенности моделирования функциональных процессов. Способы формализации и моделирования процесса возникновения угроз. Основные понятия и виды диаграмм причинно-следственных связей. Символы, применяемые при графическом изображении процесса возникновения угроз.

ТЕМА 7. Вспомогательные функциональные процессы объекта защиты.
Понятие вспомогательных функциональных процессов объекта защиты. Пошаговое выделение вспомогательного процесса, его регламентация. Цели и особенности моделирования вспомогательных процессов. Применение моделей причинно-следственных связей для анализа возникновения угроз в процессах объекта защиты.

ТЕМА 8. Методы совершенствования процессов и систем. Методы оптимизации функционального процесса объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы. Разработка обоснованных предложений по реорганизации существующих процессов объекта защиты. Выявление «узких мест» в процессах и разработка методики их совершенствования.

ТЕМА 9. Основные системы автоматизированного моделирования процессов и систем защиты информации. Классификация. Необходимость компьютерной поддержки. Методы машинной реализации моделей и области их предпочтительного использования при моделировании процессов системы защиты информации. Классификация систем моделирования (CASE-средства). Этапы их развития. Анализ CASE-средства по признаку поддерживаемой методологии моделирования. Основные отличия популярных средств моделирования процессов и систем. Критерии выбора CASE-средства для моделирования процессов.
ТЕМА 10. Методика оценки экономической эффективности совершенствования процессов и систем защиты информации на основе анализа их моделей. Цели и задачи оценки экономической эффективности совершенствования процессов и систем защиты. Методы и подходы к оценке. Метод АВС. Этапы проведения оценки. Проведение оценки экономической эффективности в CASE-средствах.
ТЕМА 11.Методика разработки тактики защиты объекта и локализации защищаемых элементов на основе анализа их моделей. Цели и задачи разработки тактики защиты объекта на базе моделей его процессов. Этапы методики. Инструменты разработки. Документирование мероприятий тактики защиты объекта.

6. Методические материалы для обучающихся по освоению дисциплины

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторные занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы.

Обучающемуся важно помнить, что лекция эффективно помогает ему овладеть программным материалом благодаря расстановке преподавателем необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации. Кроме того, во время лекции имеет место прямой визуальный и эмоциональный контакт обучающегося с преподавателем, обеспечивающий более полную реализацию воспитательной компоненты обучения.

Самостоятельная работа преследует следующие цели:
- закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;
- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;
- совершенствование навыков применения CASE-средств при моделировании процессов и систем защиты информации.
- совершенствование навыков поиска публикаций и образовательных ресурсов, размещенных в сети Интернет;
- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем и учитываются при аттестации студента.

Предметом «Моделирование процессов и систем защиты информации» являются модели процессов и систем защиты информации. Значимость моделей в построении систем защиты информации объектов защиты, а также его процессов определяется тем, что вооружает специалиста по защите информации знаниями и данными и наглядным представлением о существующих процессах. Построенные модели позволяют правильно оценить «узкие места», уязвимости процессов и разработать мероприятия по их реорганизации и защите, а также выполнить оценку экономической эффективности для объекта для принятия решений.

6.1. Самостоятельная работа обучающихся по дисциплине (модулю)

№ п/п	Раздел (тема)	Задание	Методические рекомендации по выполнению задания	Форма контроля
1	**2**	**3**	**4**	**5**
Раздел 1. Базовые понятия методологий моделирования информационных процессов и систем				
1.	Тема № 1.1.	Усвоить	1. Изучить цели и задачи моделирования процессов. 2. Изучить пути использования моделей при обеспечении безопасности объекта.	Контрольный опрос
2.	Тема № 1.2.	Усвоить	1. Изучить понятия и виды моделей. 2. Изучить классификацию и структуру моделей. 3. Изучить имитационное моделирование, его особенности и преимущества.	Контрольный опрос
3.	Тема № 1.3.	Приобрести навык	1.Изучить классификация подходов к моделированию процессов и систем. 2.Изучить структурные методы разработки моделей. 3.Изучить основы методологии SADT. 4.Изучить объектно-ориентированные методы построения процессов и систе.	Проверка выполнения практического задания
4.	Тема № 1.4.	Усвоить	1. Изучить методы сбора информации для построения моделей.. 2. Изучить основные этапы моделирования. 3. Изучить показатели процессов.	Контрольный опрос
5.	Тема № 1.5	Приобрести навык	1. Изучить понятие функциональных процессов объекта защиты. 2. Изучить характеристики и виды функциональных процессов.	Контрольный опрос

6	Тема № 1.6	Приобрес-ти навык	1.Изучить понятие основных функциональных процессов объекта защиты. 2.Изучить способы формализации и моделирования процесса возникновения угроз. 3. Изучить основные понятия и виды диаграмм причинно-следственных связей.	Проверка выполнения практическ ого задания
7	Тема № 1.7	Усвоить	1. Изучить понятие вспомогательных функциональных процессов объекта защиты. 2. Изучить пошаговое выделение вспомогательного процесса. 3. Изучить применение моделей причинно-следственных связей для анализа возникновения угроз	Контрольный опрос
8	Тема № 1.8		1. Изучить методы оптимизации функционального процесса объекта защиты 2. Изучить подходы к разработке обоснованных предложений по реорганизации существующих процессов объекта защиты 3. Изучить подходы Выявление «узких мест» в процессах и разработка методики их совер-шенствования.	Контрольный опрос
Раздел 2. Системы автоматизированного моделирования процессов и систем				
6.	Тема № 2.1.	Усвоить	1. Изучить методы машинной реализации мо-делей. 2. Изучить классификацию систем моделирования (CASE-средства).	Проверка выполнения практическог о задания
8.	Тема № 2.2.	Усвоить	1. Изучить методы и подходы к оценке. 2. Изучить метод АВС. Этапы проведения оценки в системе. 3. Изучить этапы проведения оценки эконо-мической эффективности в CASE-средствах.	Проверка выполнения практическог о задания
9.	Тема № 2..3.	Приобрес-ти навык	1. Изучить этапы разработки тактики защиты объекта на базе моделей его процессов 2. Изучить инструменты разработки.	Проверка выполнения

6.2. Тематика и задания для практических занятий

Формой отчетности по данной дисциплине является зачет . Необходимые условия допуска к зачету :

- Наличие полного конспекта лекций
- Сдача всех практических работ с положительным результатом

Занятие 1.

Тема: Задачи моделирования информационных процессов и систем

Обсуждаемые вопросы: Цель и задачи, структура курса. Цели и задачи моделирования информационных процессов и систем защиты информации. Использование моделей при обеспечении информационной безопасности объектов защиты.

Задание. Выбрать объект защиты (организацию, процесс). Сформулировать цели и задачи моделирования объекта защиты.

Занятие 2.

Тема: Общие принципы моделирования процессов и систем защиты информации

Обсуждаемые вопросы: Виды моделирования. Место формализации и моделирования при исследовании процессов в системе защиты информации. Понятие и виды моделей. Классификация и структура моделей. Характеристики моделей. Преимущества и недостатки. Исходные данные и ограничения, обработка и интерпретация результатов моделирования. Имитационное моделирование, особенности и преимущества. Логико-лингвистическая модель процесса возникновения угроз в человеко-машинной системе. Принципы имитационного моделирования процессов и систем информационной защиты.

Задание. Сформулировать данные и ограничения моделей объекта защиты.

Занятие 3.

Тема: Основные методологии моделирования процессов и систем защиты информации.

Обсуждаемые вопросы: Классификация подходов к моделированию процессов и систем защиты информации. Структурные методы разработки моделей процессов и систем. Принципы разработки моделей. Метод «черного ящика». Принцип декомпозиции моделей процессов и систем. Методология SADT. Стандарты моделирования процессов семейства IDEF (IDEF0, IDEF 3, DFD). Достоинства и недостатки методологии SADT. Объектно-ориентированные методы построения моделей. Критерии выбора методологии моделирования процессов и систем.

Задание. Построение моделей процессов объекта защиты в стандартах IDEF0, IDEF 3, DFD с использованием ПП BPWin , Ramus (или аналогов).

Занятие 4.

Тема: Методика моделирования процессов и систем защиты информации

Обсуждаемые вопросы: Описание границ процессов и систем. Методы сбора информации для построения моделей. Описание процессов и систем. Установление контрольных точек в процессах. Показатели процессов. Этапы моделирования.

Задание. Дать описание методов сбора информации для построения моделей процессов объекта защиты. Установление контрольных точек в процессах и разработка системы показателей.

Занятие 5.

Тема: Классификация функциональных процессов объекта защиты.

Обсуждаемые вопросы: Понятие функциональных процессов объекта защиты. Характеристики функциональных процессов. Виды функциональных процессов. Классификационные признаки. Классификация процессов.

Задание. Выделение функциональных процессов объекта защиты, дать их классификации.

Занятие 6.

Тема: Основные функциональные процессы объекта защиты.

Обсуждаемые вопросы: Понятие основных функциональных процессов объекта защиты. Пошаговое выделение процесса, его регламентация. Цели и особенности моделирования функциональных процессов. Способы формализации и моделирования процесса возникновения угроз. Основные понятия и виды диаграмм причинно-следственных связей. Символы, применяемые при графическом изображении процесса возникновения угроз.

Задание. Сформулировать цели моделирования основных процессов объекта защиты**.** Построение моделей основных процессов объекта защиты в стандартах IDEF0, IDEF 3, DFD с использованием ПП BPWin , Ramus (или аналогов). Модель «как есть».

Занятие 7.

Тема: Вспомогательные функциональные процессы объекта защиты.

Обсуждаемые вопросы: Понятие вспомогательных функциональных процессов объекта защиты. Пошаговое выделение вспомогательного процесса, его регламентация. Цели и особенности моделирования вспомогательных процессов. Применение моделей причинно-следственных связей для анализа возникновения угроз в процессах объекта защиты.

Задание. Сформулировать цели моделирования вспомогательных процессов объекта защиты**.** Построение моделей вспомогательных процессов объекта защиты в стандартах IDEF0, IDEF 3, DFD с использованием ПП BPWin , Ramus (или аналогов). Модель «как есть».

Занятие 8.

Тема: Методы совершенствования процессов и систем.

Обсуждаемые вопросы: Методы оптимизации функционального процесса объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы. Разработка обоснованных предложений по реорганизации существующих процессов объекта защиты. Выявление «узких мест» в процессах и разработка методики их совершенствования.

Задание. Выявить «узкие места» в процессах объекта защиты (уязвимости). Выбрать метод совершенствования процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы.

Занятие 9.

Тема: Основные системы автоматизированного моделирования процессов и систем защиты информации. Классификация.

Обсуждаемые вопросы: Необходимость компьютерной поддержки. Методы машинной реализации моделей и области их предпочтительного использования при моделировании процессов системы защиты информации. Классификация систем моделирования (CASE-средства). Этапы их развития. Анализ CASE-средства по признаку поддерживаемой методологии моделирования. Основные отличия популярных средств моделирования процессов и систем. Критерии выбора CASE-средства для моделирования процессов.

Задание. Построить модели усовершенствованных процессов объекта защиты в стандартах IDEF0, IDEF 3, DFD с использованием ПП BPWin , Ramus (или аналогов). Модель «как должно быть».

Занятие 10.

Тема: Методика оценки экономической эффективности совершенствования процессов и систем защиты информации на основе анализа их моделей

Обсуждаемые вопросы: Цели и задачи оценки экономической эффективности совершенствования процессов и систем защиты. Методы и подходы к оценке. Метод АВС. Этапы проведения оценки. Проведение оценки экономической эффективности в CASE-средствах.

Задание. Выполнить оценку экономической эффективности усовершенствования процессов объекта защиты в CASE-средствах методом АВС, методом затрат.

Занятие 11.

Тема: Методика разработки тактики защиты объекта и локализации защищаемых элементов на основе анализа их моделей.

Обсуждаемые вопросы: Цели и задачи разработки тактики защиты объекта на базе моделей его процессов. Этапы методики. Инструменты разработки. Документирование мероприятий тактики защиты объекта.

Задание. Сформулировать цели и разработать план тактических мероприятий защиты объекта на базе моделей его процессов.

7. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины (модуля)

а) основная

1. Аверченков, В.И. Служба защиты информации: организация и управление : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стереотип. - Москва : Флинта,

2016. - 186 с. - Библиогр. в кн. - ISBN 978-5-9765-1271-9 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93356
2. Прохорова, О.В. Информационная безопасность и защита информации : учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». - Самара : Самарский государственный архитектурно-строительный университет, 2014. - 113 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-9585-0603-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=438331
3. Скрипник, Д.А. Общие вопросы технической защиты информации / Д.А. Скрипник. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=429070

б) дополнительная

1. Поддержка принятия решений при проектировании систем защиты информации : монография / В.В. Бухтояров, М.Н. Жукова, В.В. Золотарев [и др.]. — М. : ИНФРА-М, 2018. – 131 с. — (Научная мысль). — . http://znanium.com/catalog.php?bookinfo=947806
2. Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - 4-е изд., стер. - Москва : Флинта, 2016. - 224 с. - (Организация и технология защиты информации). - Библиогр.: с. 192-193. - ISBN 978-5-9765-1274-0 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93351
3. Хорев, П. Б. Методы и средства защиты информации в компьютерных системах : Учеб. пособие для студ. высш. учеб. заведений / П. Б. Хорев. - М. : Академия, 2005. - 256 с. - (Высшее профессиональное образование) (Информатика и вычислительная техника). - Библиогр.: с. 251-252. - ISBN 5-7695-1839-1 : 197.73. Рекомендовано УМО
4. Хорев, П. Б**.** Методы и средства защиты информации в компьютерных системах : учеб. пособие для вузов напр. 230100 "Информ. и выч. техн." / Хорев Павел Борисович. - 4-е изд., стер. - Москва : ИЦ "Академия", 2008. - 256 с. - (Высш. проф. образов. Информ. и выч. техн.). - УМО. - ЕН, ОПД, СД. - ISBN 978-5-7695-5118-5 : 116.82.

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Информационно-образовательные ресурсы:
1. www.atlas.Krasnodar.ru -КФ НТЦ «Атлас»: защита информации.

Электронные библиотечные системы:
1. Университетская библиотека онлайн http://biblioclub.ru
2. «Лань» http://e.lanbook.com/
3. ЭБС «Znanium»
4. Справочно-информационная система (СИС) «Гарант».
5. Справочно-информационная система «Консультант».
6.Электронно-библиотечная система (ЭБС) «Инфра-М».

9. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционная аудитория, оснащенная проектором, компьютером.
Компьютерный класс с выходом в интернет
Программное обеспечение:
BP-WIN
T-Flex