МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Костромской государственный университет»
(КГУ)

УТВЕРЖДЕНО:
На заседании кафедры защиты информации
Протокол заседания № 10 от 15 мая 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ И СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Направление подготовки 10.03.01 Информационная безопасность

Направленность/специализация: Организация и технология защиты информации

Квалификация выпускника: Бакалавр

Кострома 2023

Рабочая программа дисциплины «Моделирование процессов и систем защиты информации» разработана в соответствии с Федеральным государственным образовательным стандартом по направлению подготовки:

10.03.01	Информационная безопасность	ФГОС ВО - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность, утвержденный Минобранауки № 1427 от 17.11.2020

Разработал:	Виноградова Г. Л.	Доцент кафедры защиты информации, к. т. н.
Рецензент:	Щекочихин О.В.	Доцент кафедры защиты информации, к. т. н.

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.

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:

В совокупности с другими базовыми дисциплинами обеспечивает формирование следующих компетенций:

Освоить компетенцию:

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

Код и содержание индикаторов компетенции:

ИК. ОПК-12.1. Способность проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации
ИК. ОПК-12.2. Способность проводить подготовку исходных данных для для технико-экономического обоснования соответствующих проектных решений

ОПК -2.2 - Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы

Код и содержание индикаторов компетенции:

ИК. ОПК -2.2 1. Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы

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.

3. Место дисциплины в структуре ОП ВО

Дисциплина «Моделирование процессов и систем защиты информации» относится к базовой части учебного плана. Изучается в 5 и 6 семестре очной формы обучения.

Изучение дисциплины основывается на ранее освоенных дисциплинах/практиках: «Основы информационной безопасности», «Информационные технологии в информационной безопасности», «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 проектами обеспечения информационной безопасности», «Управление информацией в процессах защиты объектов информатизации».

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	Очно-заочная	Заочная
Общая трудоемкость в зачетных единицах	6	-	-
Общая трудоемкость в часах	216	-	-
Аудиторные занятия в часах, в том числе:		-	-
Лекции	68	-	-
Практические занятия	16	-	-

Лабораторные занятия	68	-	-
Практическая подготовка	-	-	-
Самостоятельная работа в часах	26.4	-	-
Форма промежуточной аттестации	Зачет, Экзамен 36	-	-

4.2. Объем контактной работы на 1 обучающегося

Виды учебных занятий	Очная форма
Лекции	68
Практические занятия	16
Лабораторные занятий	68
Консультации	
Зачет/зачеты	36
Экзамен/экзамены	5.35
Курсовые работы	5,6
Курсовые проекты	-
Всего	153,6

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

5.1 Тематический план учебной дисциплины

№	Название раздела, темы	Всего з.е/час	Аудиторные занятия			Самостоятельная работа
			Лекц.	Практ.	Лаб.	
1	Раздел 1. Базовые понятия методологий моделирования информационных процессов и систем	50	28		28	14
1.1	Задачи моделирования информационных процессов и систем.	10	4		4	2
1.2	Общие принципы моделирования процессов и систем защиты информации	5	4		4	2
1.3	Основные методологии моделирования процессов и систем защиты информации.	5	4		4	2
1.4	Методика моделирования процессов и систем защиты информации.	10	4		4	2
1.5	Классификация функциональных	5	4		4	2

	процессов объекта защиты.					
1.6	Основные функциональные процессы объекта защиты.	10	4		4	2
1.7	Методы совершенствования процессов и систем	5	4		4	2
2	Раздел 2. Модели информационной безопасности	67	26	8	26	17
2.1	Концептуальная модель информационной безопасности	12	4	1	4	3
2.2	Модель нарушителей ИБ	12	4	1	4	3
2.3	Модель угроз ИБ. Методика ФСТЭК по моделям угроз	10	6	2	6	3
2.4	Модели уязвимостей ИБ	13	4	2	4	3
2.5	Аналитические модели ИБ	10	4	2	4	3
2.6	Модели причинно-следственных связей возникновения уязвимостей	10	4	-	4	2
3	Раздел 3. Системы автоматизированного моделирования процессов и систем	63	12	8	12	31
3.1	Основные системы автоматизированного моделирования процессов и систем защиты информации. Классификация	21	4	3	4	10
3.2	Методика оценки экономической эффективности совершенствования процессов и систем защиты информации на основе анализа их моделей	21	4	3	4	10
3.3	Методика разработки тактики защиты объекта и локализации защищаемых элементов на основе анализа их моделей.	21	4	2	4	11

	Зачет, экзамен	36				
	Итого:	6/215	66	16	66	26,4

5.2. Содержание:

Раздел 1. Базовые понятия методологий 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. 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. 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. Описание границ процессов и систем. Методы сбора информации для построения моделей. Описание процессов и систем. Установление контрольных точек в процессах. Показатели процессов. Этапы моделирования. Понятие функциональных процессов объекта защиты. Характеристики функциональных процессов. Виды функциональных процессов. Классификационные признаки. Классификация процессов. 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. 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.

Раздел 2. Модели информационной безопасности. Концептуальная модель информационной безопасности. Модель нарушителей ИБ. Классификация нарушителей, характеристика видов нарушителей ИБ. Модель угроз ИБ. Методика ФСТЭК по моделям угроз Модели уязвимостей ИБ. Методы определения актуальных угроз ИБ. Метод экспертных оценок. Аналитические модели ИБ. Модели причинно-следственных связей возникновения уязвимостей.

Раздел 3. Системы автоматизированного моделирования 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. 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. 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.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

6.1. Самостоятельная работа обучающихся по дисциплине (модулю)

№ п/п	**Раздел (тема) дисциплины**	**Задание**	**Часы Очная форма**	**Часы очно-заочная, заочная**	**Методические рекомендации по выполнению задания**	**Форма контроля**
1	Раздел 1. Базовые понятия методологий моделирования информационных процессов и систем. .	Изучение литературы и Интернет-источников	7	-	В качестве литературных источников предпочтительнее использовать [1] из списка дополнительной литературы и 3,[4] из списка основной литературы	Проверка
2	Раздел 2. Модели информационной безопасности	Изучение литературы и Интернет-источников	11	-	В качестве литературных источников предпочтительнее использовать [2] из списка дополнительной литературы и [1, 2] из списка основной литературы	Тестирование
3	Раздел 3. Системы автоматизированного моделирования процессов и систем	Разработка моделей	3	-	Для подготовки к составлению программ рекомендуется пользоваться учебными пособиями [3] из списка основной литературы и [3] из списка дополнительной	Проверка

					литературы	
4	Зачет , экзамен	Решение зачетных, экзаменационных заданий	5,6	-	Для подготовки к составлению программ рекомендуется пользоваться учебными пособиями [2] из списка основной литературы и [2] из списка дополнительной литературы	Зачет, экзамен

6.2. Тематика и задания для практических занятий

1. Выбор объекта защиты (организацию, процесс), формулирование цели и задачи моделирования объекта защиты.
2. Формулирование данных и ограничения моделей объекта защиты
3. Описание методов сбора информации для построения моделей процессов объекта защиты. Установление контрольных точек в процессах и разработка системы показателей.
4. Выделение функциональных процессов объекта защиты, дать их классификации
5. Формулирование целей моделирования основных процессов объекта защиты**.**
6. Построение моделей основных процессов объекта защиты в стандартах IDEF0, IDEF 3, DFD с использованием ПП BPWin , Ramus (или аналогов). Модель «как есть».
7. Формулирование цели моделирования вспомогательных процессов объекта защиты**.**
8. Выявление «узких мест» в процессах объекта защиты (уязвимости).
9. Выбор метод совершенствования процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы.
10. Разработка концептуальная модель информационной безопасности организации.
11. Разработка модели нарушителей ИБ.
12. Характеристика видов нарушителей ИБ организации.
13. Разработка модель угроз ИБ.
14. Разработка модели уязвимостей ИБ.
15. Определение активных угроз методом экспертных оценок.
16. Разработать аналитические модели ИБ выбранной организации.
17. Разработать модели причинно-следственных связей возникновения уязвимостей.
18. Выполнение оценки экономической эффективности усовершенствования процессов объекта защиты в CASE-средствах методом АВС, методом затрат.
19. Формулирование цели и разработать план тактических мероприятий защиты объекта на базе моделей его процессов.

Темы курсовых работ

1. Задачи моделирования информационных процессов и систем.
2. Общие принципы моделирования процессов и систем защиты информации.

3. Основные методологии моделирования процессов и систем защиты информации.
4. Методика моделирования процессов и систем защиты информации.
5. Классификация функциональных процессов объекта защиты
6. Основные функциональные процессы объекта защиты.
7. Вспомогательные функциональные процессы объекта защиты.
8. Методы совершенствования процессов и систем.
9. Основные системы автоматизированного моделирования процессов и систем защиты информации. Классификация
10. Методика оценки экономической эффективности совершенствования процессов и систем защиты информации на основе анализа их моделей
11. Методика разработки тактики защиты объекта и локализации защищаемых элементов на основе анализа их моделей.

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

Информация о курсе дисциплины в СДО:
Элемент «Лекции»;
Элемент «Практические занятия», «Лабораторные занятия»;
Элемент «Самостоятельная работа»;
Информационно-образовательные ресурсы:
1. Библиотека ГОСТов. Все ГОСТы, [Электронный ресурс], URL:http://vsegost.com/

Электронные библиотечные системы:

1. ЭБС Университетская библиотека онлайн - http://biblioclub.ru
2. ЭБС «Лань» https://e.lanbook.com
3. ЭБС «ZNANIUM.COM» http://znanium.com
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

Лекционные занятия проводятся в аудиториях с требуемым числом посадочных мест, оборудованные мультимедиа.

Практические занятия проводятся в компьютерных классах.

Лицензионное программное обеспечение:

Не требуется

Свободно распространяемое программное обеспечение:
Офисный пакет, ПП Ramus