Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра вычислительной техники и защиты информации

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.В.Э.2.1 Анализ рисков в системах защиты информации»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки
10.03.01 Информационная безопасность
(код и наименование направления подготовки)

Безопасность автоматизированных систем (информационные технологии и электронная промышленность)
(наименование направленности (профиля) образовательной программы)

Квалификация
Бакалавр

Форма обучения
Очная

Год набора 2023

2058763

Рабочая программа дисциплины «*Б1.Д.В.Э.2.1 Анализ рисков в системах защиты информации*» рассмотрена и утверждена на заседании кафедры

Кафедра радиотехнической техники и защиты информации
наименование кафедры

протокол №8 от 7 марта 2023 г.

Заведующий кафедрой
Кафедра радиотехнической техники и защиты информации
наименование кафедры

подпись Т.З. Аралбаев
расшифровка подписи

Согласовано:
Зав. каф ВТиЗИ
наименование

подпись Т.З. Аралбаев
расшифровка подписи

подпись *расшифровка подписи*

Председатель методической комиссии по направлению подготовки
09.03. Информационная безопасность
код наименование

личная подпись Т.З. Аралбаев
расшифровка подписи

Заведующий отделом формирования фонда и научной обработки документов

личная подпись *расшифровка подписи*

Начальник отдела по качеству факультета

личная подпись И.В. Крючкова
расшифровка подписи

Регистрация

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины: формирование теоретических знаний и практических навыков исследований рисков в системах защиты информации у студентов профиля «Безопасность автоматизированных систем (информационные технологии и электронная промышленность).

Задачи:

– определить актуальность, основные цели и терминологию задач анализа рисков в системах информационной безопасности;

– изучить теоретические основы и модели анализа рисков;

- получить сведения об основных отечественных и международных стандартах по анализу рисков в системах защиты информации;

– освоить методологию и технологии анализа рисков при построении моделей угроз для объектов информатизации, возможных проблем и их решений, рассмотреть примеры разработки методик анализа рисков;

– ознакомиться с основами управления рисками в системах защиты информац**2 Место дисциплины в структуре образовательной программы**

Дисциплина относится к дисциплинам (модулям) по выбору вариативной части блока Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Б1.Д.Б.7 Организационное и правовое обеспечение информационной безопасности, Б1.Д.Б.13 Социокультурная коммуникация, Б1.Д.Б.16 Основы экономики и финансовой грамотности*

Постреквизиты дисциплины: *Отсутствуют*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1-В-1 Применяет философские основы познания и логического мышления, методы научного познания, в том числе методы системного анализа, для решения поставленных задач УК-1-В-2 Осуществляет критический анализ и синтез информации, полученной из разных источников УК-1-В-3 Понимает основные закономерности и главные особенности социально-исторического развития различных культур в этическом и философском контексте УК-1-В-4 Применяет методы сбора, хранения, обработки, передачи, анализа и	**Знать:** основные принципы поиска информации с использованием современных технологий поисковых систем и сопоставления информации от различных источников. **Уметь:** пользоваться нормативными документами и учебно-методическим материалом для определения актуальности

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
	синтеза информации с использованием компьютерных технологий для решения поставленных задач УК-1-В-5 Формулирует и аргументирует выводы и суждения, в том числе с применением философского понятийного аппарата УК-1-В-6 Формулирует собственную гражданскую и мировоззренческую позицию с опорой на системный анализ философских взглядов и исторических закономерностей, процессов, явлений и событий	дисциплины и принципов ее освоения.. **Владеть:** практическими навыками хранения, обработки, передачи, информации для анализа начальных сведений по информационной безопасности и методологии ее изучения.
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2-В-1 Понимает классическую структуру проекта с учетом оптимизации ресурсного обеспечения, способы представления проекта УК-2-В-2 Формулирует цели и задачи проекта, структурирует этапы процесса организации проектной деятельности УК-2-В-3 Применяет элементы анализа, планирования и оценки рисков для выбора оптимальной стратегии развития и обоснования устойчивости проекта УК-2-В-4 В рамках цели проекта опирается на правовые нормы основных отраслей российского законодательства при постановке целей и выборе оптимальных способов их достижения; обладает навыками использования нормативно-правовых ресурсов в разработке и реализации проектов	**Знать:** основы постановки задач и оптимизации проектных решений по управлению информационной безопасностью на основе анализа рисков. **Уметь:** примнять полученные знания в управлении информационной безопасностью на основе анализа рисков.... **Владеть:** практическими навыками решения задач управления информационной безопасностью, исходя из действующих правовых норм, имеющихся ресурсов и ограничений.
ПК*-3 Способен обеспечивать работоспособность систем защиты информации при возникновении нештатных ситуаций	ПК*-3-В-2 Знает теорию управления внештатными ситуациями и инцидентами в автоматизированных системах	**Знать**: основы теории управления автоматизированных систем **Уметь:** принимать эффективные решения в управлении внештатными ситуациями и инцидентами в автоматизированных системах **Владеть:** практическими навыками поиска и принятия эффективных решений в управлении внештатными ситуациями и инцидентами в

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		автоматизированных системах.
ПК*-5 Способен проводить аудит защищенности информации в автоматизированных системах	ПК*-5-В-1 Выбирает и обосновывает рациональные методы и средства аудита защищенности информации	**Знать:** принципы проведения аудита информационной безопасности автоматизированных систем. **Уметь:** выбирать и обосновывать рациональные методы и средства аудита защищенности информации. **Владеть:** инструментальными средствами и методиками проведения аудита защищенности информации в автоматизированных системах.
ПК*-8 Способен проводить анализ уязвимостей внедряемой системы защиты информации	ПК*-8-В-1 Составляет отчеты по аудиту уязвимостей внедряемой системы защиты информации	**Знать:** принципы анализа уязвимостей внедряемой системы защиты информации. **Уметь:** выбирать и обосновывать рациональные методы и средства анализа уязвимостей внедряемой системы защиты информации. **Владеть:** инструментальными средствами и методиками анализа уязвимостей внедряемой системы защиты информации.

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 академических часов).

Вид работы	Трудоемкость, академических часов	
	6 семестр	всего
Общая трудоёмкость	**108**	**108**
Контактная работа:	**50,25**	**50,25**

Вид работы	Трудоемкость, академических часов	
	6 семестр	всего
Лекции (Л)	34	34
Практические занятия (ПЗ)	16	16
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- подготовка к практическим занятиям;* *- подготовка к рубежному контролю и т.п.)*	**57,75**	**57,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**диф. зач.**	

Разделы дисциплины, изучаемые в 6 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Основные цели и терминология задач анализа рисков в системах информационной безопасности	8	4	-		4
2	Теоретические основы и модели анализа рисков	22	6	4		12
3	Стандарты по анализу рисков в системах ИБ	22	8	2		12
4	Задачи анализа рисков в системах ИБ	28	8	6		14
5	Основы управления рисками в системах защиты информации	28	8	4		16
	Итого:	108	34	16		58
	Всего:	108	34	16		58

4.2 Содержание разделов дисциплины

Раздел № 1. Основные цели и терминология задач анализа рисков в системах информационной безопасности.

1.1. Понятие киберриска, угрозы, уязвимости, понятие и виды ущерба от атак, тотальный и остаточный риск, качественный и количественный риск, предпринимательский риск, цели анализа риска.

1.2. Классификации и характеристики рисков.

Раздел № 2. Теоретические основы и модели анализа рисков.

2.1.Основная концепция анализа рисков в системах защиты информации

2.2. Модели анализа риска

Раздел № 3. Стандарты по анализу рисков в системах ИБ.

3.1. Характеристика отечественных документов по анализу уровня защищенности объектов информатизации.

3.2. Характеристика зарубежных и международных стандартов. Стандарты серии NIST SP 800, стандарты серии ISO/IEC, стандарт IEC 31010:2019.

Раздел № 4. Задачи анализа рисков в системах ИБ.

4.1 Оценка, измерение и прогнозирование рисков.

4.2.Характеристика современных методик анализа рисков. Методики: ГРИФ, FRAP, RiskWatch, CRAMM, OCTAVE.

Документы ФСТЭК по оценке защищенности объектов информатизации.

Раздел № 5. Основы управления рисками в системах защиты информации.

5.1. Основы минимизации рисков. Избегание рисков, передача и принятие рисков, страхование и диверсификация производства.

5.2. Выбор методов и средств защиты информации на основе анализа рисков.

4.3 Практические занятия

№ занятия	№ раздела	Тема	Кол-во часов
1	2	Качественный анализ рисков модели угроз	2
2	2	Количественный анализ рисков модели угроз	2
3	2	Ранжирование угроз по величине рисков	2
4	3	Кластеризация моделей угроз по величинам рисков	2
5	3	Парето-анализ рисков	2
6	4	Прогнозирование рисков	2
7	5	Принятие решений по результатам анализа рисков	4
		Итого:	16

5 Учеб но-методическое обеспечение дисциплины

5.1 Основная литература

1. Девянин, П.Н. Модели безопасности компьютерных систем [Текст] : учеб. пособие для вузов / П. Н. Девянин. - М. : Академия, 2005. - 144 с. - (Высшее профессиональное образование : информационная безопасность). - Библиогр.: с. 139-140. - ISBN 5-7695-2053-1.

5.2 Дополнительная литература

1. Девянин, П.Н. Теоретические основы компьютерной безопасности [Текст] : учеб. пособие для вузов / П. Н. Девянин [и др.]. - М. : Радио и связь, 2000. - 192 с. : ил. - Авт. указаны на обороте тит. л.. - Библиогр. в конце гл. - ISBN 5-256-01413-7.

2. Крышкин, О. Настольная книга по внутреннему аудиту: риски и бизнес-процессы / О. Крышкин ; под ред. В. Ионова. - М. : Альпина Паблишер, 2016. - 477 с. - ISBN 978-5-9614-4449-0 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=279758

5.3 Периодические издания

1 Экономический анализ. Теория и практика: журнал. - М. «Издательский Дом «Финансы и кредит».- 2019

5.4 Интернет-ресурсы

1. https://www.fstec.ru/ - официальный сайт ФСТЭК РФ.
2. https://www.minfin.ru/ru/ - официальный сайт Министерства финансов РФ.
2. http://edu.ru/ - федеральный образовательный портал.

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий

1. Операционная система РЕД ОС.
2. LibreOffice - свободный офисный пакет программ, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.
3. Программная система для организации видео-конференц-связи Webinar.ru.
4. LMS Moodle [Электронный ресурс]: система управления курсами – URL: www.moodle.osu.ru – Режим доступа: для авторизированных пользователей.

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, семинарского типа, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Аудитории оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещение для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к сети "Интернет", и обеспечением доступа в электронную информационно-образовательную среду ОГУ.

К рабочей программе прилагаются:

- Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине;
- Методические указания для обучающихся по освоению дисциплины.