Минобрнауки России

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

Кафедра вычислительной техники и защиты информации

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б.1.В.ДВ.1.1 Анализ рисков в системах защиты информации»

Уровень высшего образования

БАКАЛАВРИАТ

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

№ 3 «Комплексная защита объектов информатизации»
(наименование направленности (профиля) образовательной программы)

Квалификация
Бакалавр

Форма обучения
Очная

Год набора 2020

1701200

Рабочая программа дисциплины «*Б.1.В.ДВ.1.1 Анализ рисков в системах защиты информации*» рассмотрена и утверждена на заседании кафедры

Кафедра вычислительной техники и защиты информации
наименование кафедры

протокол № 1 от 27.08.2020 г.

Заведующий кафедрой
Кафедра вычислительной техники и защиты информации _____ Т.З. Аралбаев
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
Зав.каф. ВТиЗИ _____ Т.З. Аралбаев
должность *подпись* *расшифровка подписи*

_____
должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
10.03.01 Информационная безопасность _____ Т.З. Аралбаев
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом комплектования научной библиотеки
_____ Н.Н. Бигалиева
личная подпись *расшифровка подписи*

Уполномоченный по качеству факультета
_____ И.В. Крючкова
личная подпись *расшифровка подписи*

№ регистрации _____

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 «№ 3 «Комплексная защита объектов информатизации».

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 информации.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам (модулям) по выбору вариативной части блока 1 «Дисциплины (модули)»

Пререквизиты дисциплины: *Б.1.Б.6 Экономическая теория, Б.1.Б.9 Социокультурная коммуникация, Б.1.Б.16 Организационное и правовое обеспечение информационной безопасности*

Постреквизиты дисциплины: *Отсутствуют*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
Знать: основы экономической теории защиты информации **Уметь:** использовать основы экономических знаний в области управления рисками **Владеть:** практическими навыками использования основ экономических знаний в задачах управления информационной безопасностью	ОК-2 способностью использовать основы экономических знаний в различных сферах деятельности
Знать: специфику совместной работы в подразделениях защиты информации, принципы толерантности в вопросах культурного и иного взаимодействия в коллективе. **Уметь:** толерантно воспринимать социальные, культурные и иные различия сотрудников подразделения. **Владеть:** навыками производственного общения с персоналом на месте работы.	ОК-6 способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия
Знать: принципы подбора, изучения и обобщения научно - технической литературы, нормативных и методических материалов. **Уметь:** составлять обзор по вопросам обеспечения информационной **Владеть:** практическими навыками обобщения научно - технической литературы.	ПК-9 способностью осуществлять подбор, изучение и обобщение научно - технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
	безопасности по профилю своей профессиональной деятельности
Знать: принципы организации технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. **Уметь:** организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами. **Владеть: практическими навыками** организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами.	ПК-15 способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
Знать: принципы организации и управлении мероприятиями по комплексной защите информационно-вычислительных систем и телекоммуникаций. **Уметь:** организовывать и управлять мероприятиями по комплексной защите информационно-вычислительных систем и телекоммуникаций. **Владеть**: практическими навыками организации и управления мероприятиями по комплексной защите информационно-вычислительных систем и телекоммуникаций.	ПСК*-4 способностью принимать участие в организации и управлении мероприятиями по комплексной защите информационно-вычислительных систем и телекоммуникаций

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:	**34,25**	**34,25**
Лекции (Л)	18	18
Практические занятия (ПЗ)	16	16
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: **Самостоятельная работа:** **-** *анализ лекционного материала;* - *подготовка к практическим занятиям;* - *подготовка к рубежному контролю*	**73,75**	**73,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**диф. зач.**	

Разделы дисциплины, изучаемые в 6 семестре

№	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	2	-	-	6
2	Теоретические основы и модели анализа рисков	20	4	4	-	12
3	Стандарты по анализу рисков в системах ИБ	24	2	4	-	18
4	Задачи анализа рисков в системах ИБ	32	4	4	-	24
5	Основы управления рисками в системах защиты информации	24	6	4	-	14
	Итого:	108	18	16	-	74
	Всего:	108	18	16	-	74

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 (семинары)

№ 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 Учебно-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 : информаци-онная безопасность). - Библиогр.: с. 139-140. - ISBN 5-7695-2053-1.

2. Плотников А.Н. Учет факторов риска и неопределенности при оценке эффективности инвестиционных проектов / Плотников А.Н. - М.:НИЦ ИНФРА-М, 2016. - 80 с.: 60х90 1/16 ISBN 978-5-16-105472-7 http://znanium.com/bookread2.php?book=754387

5.2 Дополнительная литература

1. Антонов, Г.Д. Управление рисками организации: Учебное пособие / Г.Д. Антонов, О.П. Иванова, В.М. Тумин. - М.: НИЦ ИНФРА-М, 2015. - 153 с.: 60х90 1/16 -. ISBN 978-5-16-010203-0 http://znanium.com/bookread2.php?book=475625

2. Авдийский, В.И. Риски хозяйствующих субъектов: теоретические основы, методологии анализа, прогнозирования и упр.: Уч.пос. / В.И.Авдийский, В.М.Безденежных. -М.: Альфа-М: НИЦ ИНФРА-М,2013 - 368 с.: 60х90 1/16. - (Магистратура). (п) ISBN 978-5-98281-333-6 http://znanium.com/bookread2.php?book=394136

3. 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.

4. 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.
3. http://edu.ru/ - федеральный образовательный портал.

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1. Операционная система Microsoft Windows
2. Пакет настольных приложений Microsoft Office (Word, Excel, PowerPoint, OneNote, Outlook, Publisher, Access)
3. ГАРАНТ Платформа F1 [Электронный ресурс]: справочно-правовая система. / Разработчик ООО НПП «ГАРАНТ-Сервис», 119992, Москва, Воробьевы горы, МГУ, [1990–2019]. – Режим доступа в сети ОГУ для установки системы: \\fileserver1\GarantClient\garant.exe
4. КонсультантПлюс [Электронный ресурс]: электронное периодическое издание справочная правовая система. / Разработчик ЗАО «Консультант Плюс», [1992–2019]. – Режим доступа к системе в сети ОГУ для установки системы: \\fileserver1\!CONSULT\cons.exe

5. Аралбаев, Т.З. Метод оценки затрат на защиту информации на основе анализа рисков: прикладная программа / Д.А. Горбунова, Т.З. Аралбаев. – Оренбург.: УФЭР. – 2017. - №1407.

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.