Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет имени В.А. Бондаренко»

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 2026

2240922

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

Кафедра вычислительной техники и защиты информации
наименование кафедры

протокол № 1 от "0" 0 2026 г.

Заведующий кафедрой
Кафедра вычислительной техники и защиты информации В.В. Тугов
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
зав. кафедрой В.В. Тугов
должность *подпись* *расшифровка подписи*

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
10.03.01 Информационная безопасность В.В. Тугов
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом формирования фонда и научной обработки документов
личная подпись *расшифровка подписи*

Уполномоченный по качеству института С.Н. Морозова
личная подпись *расшифровка подписи*

№ регистрации _____

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

формирование у обучающихся знаний о рисках и их классификации, методах анализа риска, технологии управления рисками, овладение общетеоретическими знаниями и практическими навыками проведения анализа в системах защиты информации.

Задачи:

Знать:

- основы поиска, критического анализа и синтеза информации, полученной из различных источников;
- основы формулировки цели и задач проектных решений при организации систем защиты информации с использованием анализа рисков;
- основы проведения аудита защищенности информации в автоматизированных системах.

Уметь:

- применять системный подход для решения поставленных задач;
- применять элементы анализа, планирования и оценки рисков для выбора оптимальной стратегии развития и обоснования устойчивости проекта по защите информации;
- составлять отчеты по аудиту уязвимостей внедряемой системы защиты информации.

Владеть:

- навыками применения методов сбора, хранения, обработки, передачи, анализа и синтеза информации с использованием компьютерных технологий для решения поставленных задач;
- навыками использования нормативно-правовых ресурсов в разработке и реализации проектов по защите информации;
- методиками проведения аудита защищенности информации в автоматизированных системах.

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.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	**Знать:** основы поиска, критического анализа и синтеза информации, полученной из различных источников. **Уметь:** применять системный подход для решения

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
	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 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	поставленных задач. **Владеть:** навыками применения методов сбора, хранения, обработки, передачи, анализа и синтеза информации с использованием компьютерных технологий для решения поставленных задач.
ПК*-5 Способен проводить аудит защищенности информации в автоматизированных системах	ПК*-5-В-1 Выбирает и обосновывает рациональные методы и средства аудита защищенности информации ПК*-5-В-2 Владеет навыками проведения аудита защищенности информации в автоматизированных системах	**Знать:** основы проведения аудита защищенности информации в автоматизированных системах. **Уметь:** выбирать и обосновывать рациональные методы и средства аудита защищенности информации. **Владеть:** 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 ПК*-8-В-2 Знает основные виды уязвимостей системы защиты информации ПК*-8-В-3 Владеет навыками оценки эффективности информационной безопасности автоматизированной системы	**Знать:** основы анализа уязвимостей внедряемой системы защиты информации. **Уметь:** составлять отчеты по аудиту уязвимостей внедряемой системы защиты информации. **Владеть:** методиками проведения аудита уязвимостей внедряемой системы

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		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**
Лекции (Л)	18	18
Практические занятия (ПЗ)	16	16
Лабораторные работы (ЛР)	16	16
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- выполнение индивидуального творческого задания (ИТЗ);* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- изучение разделов курса в системе электронного обучения;* *- подготовка к лабораторным занятиям;* *- подготовка к практическим занятиям;* *- подготовка к рубежному контролю)*	**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	Введение в дисциплину	14	2	2	2	8
2	Анализ рисков в области информационной безопасности	36	6	6	6	18
3	Стандарты управления рисками	14	2	2	2	8
4	Методики и ПО для оценки рисков ИБ	18	4	2	2	10
5	Управление информационными рисками	26	4	4	4	14
	Итого:	108	18	16	16	58
	Всего:	108	18	16	16	58

4.2 Содержание разделов дисциплины

Раздел 1. Введение в дисциплину

Основные понятия, термины и определения. Предмет и задачи дисциплины. Общее описание оценки риска информационной безопасности. Анализ риска. Измерение рисков. Классификация рисков. Понятие аудита информационной безопасности. Основы управления рисками ИБ.

Раздел 2. Анализ рисков в области информационной безопасности

Информационная безопасность бизнеса. Проблемы обоснования стоимости корпоративной системы защиты информации. Службы ИБ. Постановка задачи анализа рисков. Методы анализа рисков. Место анализа рисков в общей схеме управления ИБ. Подходы к оценке рисков ИБ: качественный, количественный. Экономическая модель оценки рисков. Вероятностная модель оценки рисков.

Раздел 3. Стандарты управления рисками

Национальные стандарты управления рисками информационной безопасности: ГОСТ Р ИСО/МЭК семейств 17799, 27000, 13335, 13569, 18044, 18045. Международные стандарты управления рисками: CobiT, ITIL, BSI, COSO, SAS70, NIST-800. Обзор основных стандартов. Ведомственные и корпоративные стандарты управления рисками информационной безопасности.

Раздел 4. Методики и ПО для оценки рисков ИБ

Вопросы политики безопасности. Стандарты, процедуры, метрики и анализ рисков. Методики стратегического планирования построения системы защиты. Модель многоуровневой защиты. Инструментарии базового уровня. Средства полного анализа рисков. Комплекс оценки рисков «ГРИФ». Методики и инструменты CORAS, CRAMM, Babel Enterprise, RiskWatch. Экспертная система «АванГард». Анализ существующих подходов.

Раздел 5. Управление информационными рисками

Основные элементы управления рисками в системах защиты информации. Особенности внедрения системы управления информационными рисками (СУИР). Документация. Начальные условия для внедрения СУИР. Организационная структура управления рисками.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	1	Организация компании по проведению аудита информационной безопасности предприятия	2
2	2	Табличные методы оценки и анализа информационных рисков	2
3	2	Расчет рисков информационной безопасности	2
4	2	Обоснование рисковых решений методом «Дерева решений»	2
5	3	Анализ требований и стандартов в области управления рисками информационной безопасности	2
6	4	Инструментальные средства анализа и управления рисками. Анализ рисков на основе модели угроз и уязвимостей	2
7	5	Разработка системы управления информационными рисками	2
8	5	Разработка рекомендаций по информационной безопасности	2
		Итого:	16

4.4 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Информационная безопасность автоматизированных систем. Основные понятия.	2
2	2	Реализация модели информационной безопасности	4
3	2	Анализ и оценка рисков предприятия	2
4	3	Основные стандарты в области обеспечения информационной безопасности	2
5	4	Оценка рисков в организации с применением существующих методик и программных средств	2

№ занятия	№ раздела	Тема	Кол-во часов
6	5	Сравнение результатов оценки рисков	2
7	5	Составление плана действий по повышению уровня ИБ	2
		Итого:	16

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1 Аверченков, В.И. Аудит информационной безопасности: учебное пособие / В. И. Аверченков. – 4-е изд., стер. – Москва: ФЛИНТА, 2021. – 269 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=93245 (дата обращения: 28.04.2026). – Библиогр. в кн. – ISBN 978-5-9765-1256-6.

2 Никитин, И. А. Процессы анализа и управления рисками в области ИТ / И.А. Никитин, М. Т. Цулая. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 167 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=429089 . (дата обращения: 28.04.2026).

5.2 Дополнительная литература

1 Фомичев, А. Н. Риск-менеджмент: учебник / А. Н. Фомичев. – 11-е изд. – Москва: Дашков и К°, 2025. – 366 с.: схем. – (Учебные издания для бакалавров). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=720241 (дата обращения: 28.04.2026). – Библиогр. в кн. – ISBN 978-57394-05980-3. – Текст: электронный.

2 Веселов, Г. Е. Менеджмент риска информационной безопасности: учебное пособие / Г. Е. Веселов, Е. С. Абрамов, А. К. Шилов; Южный федеральный университет, Инженерно-технологическая академия. – Таганрог: Южный федеральный университет, 2016. – 109 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=493331 (дата обращения: 28.04.2026). – ISBN 978-5-9275-2327-5.

5.3 Периодические издания

1 Информационные технологии: журнал. - Москва: Агентство "Роспечать", 2017-2021.

2 Вестник компьютерных и информационных технологий: журнал. - Москва: ИД "Спектр", 2017-2021.

5.4 Интернет-ресурсы

1 http://www.fsb.ru - Федеральная служба безопасности [официальный сайт]

2 http://fstec.ru - Федеральная служба по техническому и экспортному контролю [официальный сайт]

3 http://rsl.ru/ - Российская государственная библиотека.

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1. Операционная система РЕД ОС.
2. Пакет офисных приложений «МойОфис Образование»
3. Для работы с ресурсами Интернет - веб-браузер Яндекс https://yandex.ru/..

4. ГАРАНТ Платформа F1 [Электронный ресурс]: справочно-правовая система. / Разработчик ООО НПП «ГАРАНТ-Сервис», 119992, Москва, Воробьевы горы, МГУ, [1990–2026]. – Режим доступа в сети ОГУ http://garant.net.osu.ru

5. Автоматизированная интерактивная система сетевого тестирования - АИССТ (зарегистрирована в РОСПАТЕНТ, Свидетельство о государственной регистрации программы для ЭВМ №2011610456, правообладатель – Оренбургский государственный университет), режим доступа - http://aist.osu.ru.

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.

Для проведения лабораторных занятий используется компьютерный класс, оснащенный компьютерной техникой.

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