МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины (модуля)

ЭКОНОМИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2024

Форма обучения
очная

Владивосток 2025

Рабочая программа дисциплины (модуля) «Экономические аспекты информационной безопасности» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем (утв. приказом Минобрнауки России от 26.11.2020г. №1457) и Порядком организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (утв. приказом Минобрнауки России от 06.04.2021 г. N245).

Составитель(и):

Шумик Е.Г., кандидат экономических наук, заведующий кафедрой, Кафедра информационной безопасности, Ekaterina.Shumik1@vvsu.ru

Утверждена на заседании кафедры информационной безопасности от 15.05.2025 , протокол № 9

СОГЛАСОВАНО:

Заведующий кафедрой (разработчика)

Шумик Е.Г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат	eg_1575874368
Номер транзакции	0000000000EAB0DA
Владелец	Шумик Е.Г.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

Целью изучения дисциплины является формирование теоретической и практической готовности будущих специалистов к решению комплексных задач в области обеспечения информационной безопасности организаций с учетом экономических факторов и нормативно-правового регулирования.

Для достижения указанных целей ставятся следующие задачи:

обучение созданию предложений по улучшению системы защиты информации с учётом финансовой составляющей.

подготовка студентов к проектированию эффективной системы защиты информации, включающей мониторинг и управление рисками.

приобретение навыков расчёта необходимого финансирования и эффективного распределения ресурсов на нужды информационной безопасности.

Планируемыми результатами обучения по дисциплине (модулю), являются знания, умения, навыки. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы, представлен в таблице 1.

Таблица 1 – Компетенции, формируемые в результате изучения дисциплины (модуля)

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине		
			Код результата	Формулировка результата	
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ПКВ-1 : Способен разрабатывать проекты организационно-распорядительных документов регламентирующих информационную безопасность бизнес- процессов организации	ПКВ-1.2к : Разрабатывает проекты организационно - распорядительных документов, регламентирующих бизнеспроцессы в соответствии с требованиями законодательства в части информационной безопасности	РД1	Знание	положений федерального законодательства и стандартов, определяющих порядок обработки и защиты информации
			РД2	Умение	самостоятельно подготовить и оформить организационно-распорядительную документацию, необходимую для обеспечения информационной безопасности в организации
			РД3	Навык	создавать внутренние документы, определять зоны ответственности сотрудников за выполнение норм информационной безопасности
	ПКВ-2 : Способен разрабатывать модели угроз безопасности и формировать требования к	ПКВ-2.1к : Определяет угрозы безопасности информации, реализация которых может	РД4	Знание	основными источниками угроз информационной безопасности, особенностями их проявления в разных

	защите информации в организации.	привести к нарушениям безопасности в информационных системах			отраслях и оценки ущерба
			РД5	Умение	выявлять наиболее критичные угрозы для конкретных типов информационных систем, оценивать вероятность возникновения инцидентов и степень возможного ущерба
			РД6	Навык	проводить систематизированный анализ угроз информационной безопасности, формировать отчёты по результатам анализа и оценивать эффективность предлагаемых решений

В процессе освоения дисциплины решаются задачи воспитания гармонично развитой, патриотичной и социально ответственной личности на основе традиционных российских духовно-нравственных и культурно-исторических ценностей, представленные в таблице 1.2.

Таблица 1.2 – Целевые ориентиры воспитания

Воспитательные задачи	**Формирование ценностей**	**Целевые ориентиры**
Формирование гражданской позиции и патриотизма		
Воспитание уважения к истории и культуре России	Гражданственность	Внимательность к деталям
Формирование духовно-нравственных ценностей		
Развитие культуры здорового образа жизни	Взаимопомощь и взаимоуважение	Гибкость мышления
Формирование научного мировоззрения и культуры мышления		
Развитие познавательного интереса и стремления к знаниям	Взаимопомощь и взаимоуважение	Дисциплинированность
Формирование коммуникативных навыков и культуры общения		
Воспитание культуры диалога и уважения к мнению других людей	Достоинство	Гибкость мышления

2 Место дисциплины (модуля) в структуре ОПОП

Дисциплина относится в части, формируемая участниками образовательных отношений и опирается на дисциплины:Экономика, Основы информационной безопасности и небходимо для изучения дисциплин: для написания дипломной работы

3. Объем дисциплины (модуля)

Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу с обучающимися (по видам учебных занятий) и на самостоятельную работу, приведен в таблице 2.

Таблица 2 – Общая трудоемкость дисциплины

Название ОПОП ВО	Форма обучения	Часть УП	Семестр (ОФО) или курс (ЗФО, ОЗФО)	Трудоемкость	Объем контактной работы (час)						СРС	Форма аттестации
				(З.Е.)	Всего	Аудиторная			Внеаудиторная			
						лек.	прак.	лаб.	ПА	КСР		
10.05.03 Информационная безопасность автоматизированных систем	ОФО	С1.В	10	4	52	18	18	0	1	15	92	Э

4 Структура и содержание дисциплины (модуля)

4.1 Структура дисциплины (модуля) для ОФО

Тематический план, отражающий содержание дисциплины (перечень разделов и тем), структурированное по видам учебных занятий с указанием их объемов в соответствии с учебным планом, приведен в таблице 3.1

Таблица 3.1 – Разделы дисциплины (модуля), виды учебной деятельности и формы текущего контроля для ОФО

№	Название темы	Код результата обучения	Кол-во часов, отведенное на				Форма текущего контроля
			Лек	Практ	Лаб	СРС	
1	Экономическое обоснование информационной безопасности	РД1, РД2	4	4	0	27	практическое задание
2	Организация управления рисками информационной безопасности	РД1, РД2, РД3, РД4, РД5, РД6	4	4	0	27	практическое задание
3	Информационная безопасность в условиях цифровой трансформации бизнеса	РД1, РД2, РД4, РД5, РД6	4	4	0	27	практическое задание
4	Финансовое обеспечение проектов в области информационной безопасности	РД3, РД4, РД5, РД6	6	6	0	27	практическое задание
Итого по таблице			**18**	**18**	**0**	**108**	

4.2 Содержание разделов и тем дисциплины (модуля) для ОФО

Тема 1 Экономическое обоснование информационной безопасности.

Содержание темы: Определение основных экономических аспектов информационной безопасности. Основные показатели экономической оценки рисков и убытков от утраты или компрометации информации. Оценка стоимости ресурсов и методов защиты информации. Элементы системы расчета ущерба, связанного с нарушением конфиденциальности, целостности и доступности информации. Выбор оптимального уровня инвестиций в средства защиты информации исходя из потенциального экономического эффекта.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 2 Организация управления рисками информационной безопасности.

Содержание темы: Концептуальные основы управления рисками информационной безопасности. Процедуры выявления и классификации потенциальных угроз. Практические методики оценки вероятности реализации угроз и последствий нарушений информационной безопасности. Роль моделирования угроз и уязвимостей в разработке планов реагирования и предотвращения кризисных ситуаций. Применение современных инструментов мониторинга состояния информационной среды и своевременного обнаружения возможных инцидентов.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 3 Информационная безопасность в условиях цифровой трансформации бизнеса.

Содержание темы: Тенденции и направления эволюции информационных технологий, влияющие на экономические аспекты защиты информации. Проблематика повышения информационной устойчивости компаний при переходе на цифровые модели взаимодействия с клиентами и партнерами. Новые виды киберугроз и способов противодействия им в эпоху облачных сервисов и распределенных сетей. Преимущества и риски внедрения новых технологических решений для оптимизации управленческих процессов и снижения расходов на защиту информации. Возможности автоматизации систем защиты информации и интеграции передовых технических средств защиты.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 4 Финансовое обеспечение проектов в области информационной безопасности.

Содержание темы: Процесс формирования бюджета проекта по информационной безопасности. Экономический расчет эффективности внедряемых защитных мер и оценка возврата инвестиций. Специфические особенности планирования финансовых ресурсов для долгосрочных инициатив в области кибербезопасности. Формы финансового стимулирования сотрудников и подразделений, принимающих участие в мероприятиях по защите информации. Контроль качества исполнения запланированных работ и расходования бюджетных средств на мероприятия по информационной безопасности.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

5 Методические указания для обучающихся по изучению и реализации дисциплины (модуля)

5.1 Методические рекомендации обучающимся по изучению дисциплины и по обеспечению самостоятельной работы

Самостоятельная работа студентов (СРС) — это деятельность учащихся, которую они совершают без непосредственной помощи и указаний преподавателя, руководствуясь сформировавшимися ранее представлениями о порядке и правильности выполнения операций. Цель СРС в процессе обучения заключается, как в усвоении знаний, так и в формировании умений и навыков по их использованию в новых условиях на новом учебном материале. Самостоятельная работа призвана обеспечивать возможность осуществления студентами самостоятельной познавательной деятельности в обучении, и является видом учебного труда, способствующего формированию у студентов самостоятельности. В данной учебной программе приведен перечень основных и дополнительных источников, которые предлагается изучить в процессе облучения по дисциплине. Кроме того, для расширения и углубления знаний по данной дисциплине целесообразно использовать: научные публикации в тематических журналах; полнотекстовые базы данных библиотеки; имеющиеся в библиотеках вуза и региона публикаций на электронных и бумажных носителях. Успешное освоение дисциплины предполагает активную работу студентов на всех лекционных занятиях, эффективную самостоятельную работу. В процессе изучения дисциплины студенту необходимо ориентироваться на самостоятельную проработку лекционного материала, выполнение тестов, самостоятельное изучение некоторых разделов курса

5.2 Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости обучающимся из числа лиц с ограниченными возможностями здоровья и инвалидов (по заявлению обучающегося) предоставляется учебная информация в доступных формах с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; индивидуальные задания, консультации и др.

6 Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

В соответствии с требованиями ФГОС ВО для аттестации обучающихся на соответствие их персональных достижений планируемым результатам обучения по дисциплине (модулю) созданы фонды оценочных средств. Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 1.

7 Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература

1. Киселева, О. В., Инвестиционный анализ : учебное пособие / О. В. Киселева, Ф. С. Макеева. — Москва : КноРус, 2022. — 246 с. — ISBN 978-5-406-08881-4. — URL: https://book.ru/book/941752 (дата обращения: 26.10.2025). — Текст : электронный.
2. Козырь, Н. С. Экономические аспекты информационной безопасности : учебник и практикум для вузов / Н. С. Козырь, Л. Л. Оганесян. — Москва : Издательство Юрайт, 2025. — 131 с. — (Высшее образование). — ISBN 978-5-534-17863-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/568708 (дата обращения: 15.10.2025).

7.2 Дополнительная литература

1. Басаргин, А. А. Информационная безопасность и защита информации : практикум : учебное пособие / А. А. Басаргин. — Новосибирск : СГУГиТ, 2024. — 80 с. — ISBN 978-5-907711-75-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/484910 (дата обращения: 27.10.2025). — Режим доступа: для авториз. пользователей.
2. Башин, Ю. Б. Экономика информационного общества : учебное пособие / Ю.Б. Башин, Г.Н. Гринёв, Ю.Г. Дрёмова ; под ред. д-ра техн. наук Ю.Б. Башина. — Москва : ИНФРА-М, 2021. — 302 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1039916. - ISBN 978-5-16-015543-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1039916 (Дата обращения - 22.10.2025)
3. Инвестиционный анализ и финансовое планирование проекта : методические указания / составитель Н. Н. Чепелева. — Омск : СибАДИ, 2023. — 28 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/353756 (дата обращения: 27.10.2025). — Режим доступа: для авториз. пользователей.
4. Косорукова, И. В., Анализ финансово-хозяйственной деятельности : учебник / И. В. Косорукова, О. В. Мощенко, А. Ю. Усанов. — Москва : КноРус, 2024. — 341 с. — ISBN 978-5-406-12713-1. — URL: https://book.ru/book/952155 (дата обращения: 26.10.2025). — Текст : электронный.

7.3 Ресурсы информационно-телекоммуникационной сети "Интернет", включая профессиональные базы данных и информационно-справочные системы (при необходимости):

1. Образовательная платформа "ЮРАЙТ"
2. Электронно-библиотечная система "BOOK.ru"
3. Электронно-библиотечная система "ZNANIUM.COM"

4. Электронно-библиотечная система "ЛАНЬ"

5. Open Academic Journals Index (OAJI). Профессиональная база данных - Режим доступа: http://oaji.net/

6. Президентская библиотека им. Б.Н.Ельцина (база данных различных профессиональных областей) - Режим доступа: https://www.prlib.ru/

7. Информационно-справочная система "Консультант Плюс" - Режим доступа: http://www.consultant.ru/

8 Материально-техническое обеспечение дисциплины (модуля) и перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

Основное оборудование:

- Компьютеры

Программное обеспечение:

- Microsoft Office 2010 Standart

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фонд оценочных средств
для проведения текущего контроля
и промежуточной аттестации по дисциплине (модулю)

ЭКОНОМИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2024

Форма обучения
очная

Владивосток 2025

1 Перечень формируемых компетенций

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ПКВ-1 : Способен разрабатывать проекты организационно-распорядительных документов регламентирующих информационную безопасность бизнес- процессов организации	ПКВ-1.2к : Разрабатывает проекты организационно - распорядительных документов, регламентирующих бизнеспроцессы в соответствии с требованиями законодательства в части информационной безопасности
	ПКВ-2 : Способен разрабатывать модели угроз безопасности и формировать требования к защите информации в организации.	ПКВ-2.1к : Определяет угрозы безопасности информации, реализация которых может привести к нарушениям безопасности в информационных системах

Компетенция считается сформированной на данном этапе в случае, если полученные результаты обучения по дисциплине оценены положительно (диапазон критериев оценивания результатов обучения «зачтено», «удовлетворительно», «хорошо», «отлично»). В случае отсутствия положительной оценки компетенция на данном этапе считается несформированной.

2 Показатели оценивания планируемых результатов обучения

Компетенция ПКВ-1 «Способен разрабатывать проекты организационно-распорядительных документов регламентирующих информационную безопасность бизнес- процессов организации»

Таблица 2.1 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ПКВ-1.2к : Разрабатывает проекты организационно - распорядительных документов, регламентирующих бизнеспроцессы в соответствии с требованиями законодательства в части информационной безопасности	РД 1	Знание	положений федерального законодательства и стандартов, определяющих порядок обработки и защиты информации	выполнение тестовых заданий
	РД 2	Умение	самостоятельно подготовить и оформить организационно-распорядительную документацию, необходимую для обеспечения информационной безопасности в организации	выполнение практических заданий
	РД 3	Навык	создавать внутренние документы, определять зоны ответственности сотрудников за выполнение норм информационной безопасности	решение тестовых заданий

Компетенция ПКВ-2 «Способен разрабатывать модели угроз безопасности и формировать требования к защите информации в организации.»

Таблица 2.2 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ПКВ-2.1к : Определяет угрозы безопасности информации, реализация которых может привести к нарушениям безопасности в информационных системах	РД 4	Знание	основными источниками угроз информационной безопасности, особенностями их проявления в разных отраслях и оценки ущерба	решение тестовых заданий
	РД 5	Умение	выявлять наиболее критичные угрозы для конкретных типов информационных систем, оценивать вероятность возникновения инцидентов и степень возможного ущерба	выполнение практических заданий
	РД 6	Навык	проводить систематизированный анализ угроз информационной безопасности, формировать отчёты по результатам анализа и оценивать эффективность предлагаемых решений	выполнение практических заданий

Таблица заполняется в соответствии с разделом 1 Рабочей программы дисциплины (модуля).

3 Перечень оценочных средств

Таблица 3 – Перечень оценочных средств по дисциплине (модулю)

Контролируемые планируемые результаты обучения		Контролируемые темы дисциплины	Наименование оценочного средства и представление его в ФОС	
			Текущий контроль	Промежуточная аттестация
Очная форма обучения				
РД1	Знание : положений федерального законодательства и стандартов, определяющих порядок обработки и защиты информации	1.1. Экономическое обоснование информационной безопасности	Тест	Экзамен в устной форме
		1.2. Организация управления рисками информационной безопасности	Тест	Экзамен в устной форме
		1.3. Информационная безопасность в условиях цифровой трансформации и бизнеса	Тест	Экзамен в устной форме
РД2	Умение : самостоятельно подготовить и оформить организационно-распорядительную документацию, необходимую для обеспечения информационной безопасности в организации	1.1. Экономическое обоснование информационной безопасности	Практическая работа	Экзамен в устной форме
		1.2. Организация управления рисками информационной безопасности	Практическая работа	Экзамен в устной форме
		1.3. Информационная безопасность в условиях цифровой трансформации и бизнеса	Практическая работа	Экзамен в устной форме

РД3	Навык : создавать внутренние документы, определять зоны ответственности сотрудников за выполнение норм информационной безопасности	1.2. Организация управления рисками информационной безопасности	Практическая работа	Экзамен в устной форме
		1.4. Финансовое обеспечение проектов в области информационной безопасности	Практическая работа	Экзамен в устной форме
РД4	Знание : основными источниками угроз информационной безопасности, особенностями их проявления в разных отраслях и оценки ущерба	1.2. Организация управления рисками информационной безопасности	Тест	Экзамен в устной форме
		1.3. Информационная безопасность в условиях цифровой трансформации и бизнеса	Тест	Экзамен в устной форме
		1.4. Финансовое обеспечение проектов в области информационной безопасности	Тест	Экзамен в устной форме
РД5	Умение : выявлять наиболее критичные угрозы для конкретных типов информационных систем, оценивать вероятность возникновения инцидентов и степень возможного ущерба	1.2. Организация управления рисками информационной безопасности	Практическая работа	Экзамен в устной форме
		1.3. Информационная безопасность в условиях цифровой трансформации и бизнеса	Практическая работа	Экзамен в устной форме
		1.4. Финансовое обеспечение проектов в области информационной безопасности	Практическая работа	Экзамен в устной форме
РД6	Навык : проводить систематизированный анализ угроз информационной безопасности, формировать отчёты по результатам анализа и оценивать эффективность предлагаемых решений	1.2. Организация управления рисками информационной безопасности	Практическая работа	Экзамен в устной форме
		1.3. Информационная безопасность в условиях цифровой трансформации и бизнеса	Практическая работа	Экзамен в устной форме
		1.4. Финансовое обеспечение проектов в области информационной безопасности	Практическая работа	Экзамен в устной форме

4 Описание процедуры оценивания

Качество сформированности компетенций на данном этапе оценивается по результатам текущих и промежуточных аттестаций при помощи количественной оценки, выраженной в баллах. Максимальная сумма баллов по дисциплине (модулю) равна 100 баллам.

Вид учебной деятельности	Оценочное средство			
	Тест	Практические задания	Экзамен	Итого
Лекционные занятия	20			20
Практические занятия		60		60
Промежуточная аттестация			20	20
Итого	60	60	20	100

Сумма баллов, набранных студентом по всем видам учебной деятельности в рамках дисциплины, переводится в оценку в соответствии с таблицей.

Сумма баллов по дисциплине	Оценка по промежуточной аттестации	Характеристика качества сформированности компетенции
от 91 до 100	«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций, обнаруживает всестороннее, систематическое и глубокое знание учебного материала, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой, умеет свободно выполнять практические задания, предусмотренные программой, свободно оперирует приобретенными знаниями, умениями, применяет их в ситуациях повышенной сложности.
от 76 до 90	«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
от 61 до 75	«зачтено» / «удовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций: в ходе контрольных мероприятий допускаются значительные ошибки, проявляется отсутствие отдельных знаний, умений, навыков по некоторым дисциплинарным компетенциям, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.
от 41 до 60	«не зачтено» / «неудовлетворительно»	У студента не сформированы дисциплинарные компетенции, проявляется недостаточность знаний, умений, навыков.
от 0 до 40	«не зачтено» / «неудовлетворительно»	Дисциплинарные компетенции не сформированы. Проявляется полное или практически полное отсутствие знаний, умений, навыков.

5 Примерные оценочные средства

5.1 Примеры заданий для выполнения практических работ

Практическая работа №1: Разработка регламента информационной безопасности

Необходимо создать внутренний регламент информационной безопасности организации (например, банка, ИТ-компании или производственного предприятия). Работа должна включать:

определение объектов защиты,

классификацию информации по степени важности и секретности,

описание порядка обращения с конфиденциальной информацией,

разработку форм согласования операций с доступом к данным,

согласование процедур реакции на инциденты.

Практическая работа №2: Оценка риска информационной безопасности

Необходимо провести оценку рисков информационной безопасности конкретного подразделения организации (например, отдела кадров, бухгалтерии или службы технической поддержки).

Практическая работа №3: Проектирование бюджетного плана информационной безопасности

Необходимо составить подробный финансовый план мероприятий по повышению уровня информационной безопасности в организации на ближайший год. План должен учитывать:

стоимость оборудования и программного обеспечения,

расходы на персонал и обучение сотрудников,

издержки на сертификацию и аудит,

инвестиции в резервирование и восстановление работоспособности информационных систем.

Итоговый отчет включает расчеты общей суммы затрат, ожидаемого результата от каждого пункта программы и рекомендации по контролю исполнения бюджета.

Краткие методические указания

Практическая работа может проводится на примере реального предприятия, по итогам работы необходимо предоставить отчет

Шкала оценки

Оценка	Баллы	Описание
5	45-60	Оценка «отлично» выставляется, если студент выполнил задание, правильно применил методы.
4	30-44	Оценка «хорошо» выставляется, если студент выполнил задание, правильно применил методы, но совершил логические ошибки.
3	14-29	Оценка «удовлетворительно» выставляется, если студент выполнил задание, но применил методы не все необходимые методы для его выполнения.
2	0-13	Оценка «неудовлетворительно» выставляется в случае, если студент не выполнил задание и/ или неверно применил методы необходимые его выполнения.

5.2 Контрольный тест

1. Что представляет собой ущерб от потери информации?

a) Прямой убыток, связанный с потерей активов.

b) Косвенный убыток, вызванный снижением доверия клиентов.

c) Ущерб, нанесённый сотрудникам фирмы.

d) Затраты на устранение неполадок.

2. Какие факторы влияют на выбор оптимальной стратегии защиты информации?

a) Размер бюджета компании.

b) Степень воздействия потенциальных угроз.

c) Тип используемых технологий.

d) Все перечисленные варианты верны.

3. Как называется методика оценки рисков, основанная на количественном анализе?

a) Качественный анализ.

b) Экспертный опрос.

c) Вероятностный анализ.

d) Мониторинг угроз.

4. Чем характеризуется качественный анализ рисков?

a) Использование статистических данных.

b) Описание угроз без численных показателей.

c) Количественное измерение частоты и тяжести угроз.

d) Автоматическое выявление угроз.

5. Кто несет ответственность за организацию информационной безопасности в крупных компаниях?

a) Сотрудники среднего звена.

b) Владельцы малого бизнеса.

c) Специалисты служб информационной безопасности.

d) Исполнительный директор.

6. Основной целью страхования рисков информационной безопасности является...

a) Повышение квалификации сотрудников.

b) Получение прибыли страховой компанией.

c) Минимизация финансовых последствий от инцидента.

d) Увеличение налоговых выплат.

7. Что понимается под уровнем зрелости процесса управления информационной безопасностью?

a) Количество внедренных систем защиты.

b) Уровень понимания сотрудниками своей роли в обеспечении безопасности.

c) Эффективность существующих процессов и качество управления ими.

d) Число сертификатов соответствия международным стандартам.

8. Когда рекомендуется проводить повторную оценку рисков информационной безопасности?

a) После обновления корпоративной сети.

b) Только при смене руководства компании.

c) Ежегодно вне зависимости от обстоятельств.

d) По запросу государственных органов.

9. Какова цель регулярной инвентаризации информационных активов?

a) Улучшить производительность серверов.

b) Определить ценность и значимость актива для бизнеса.

c) Повысить квалификацию обслуживающего персонала.

d) Создать новую базу данных.

10. Какой показатель используется для оценки эффективности инвестиций в систему информационной безопасности?

a) Валовая прибыль.

b) Индекс рентабельности.

c) Возврат на инвестиции (ROI).

d) Показатель ликвидности.

11. Какая угроза чаще всего рассматривается как самая опасная для большинства коммерческих организаций?

a) Утрата клиентских баз данных.

b) Потеря бумажных архивов.

c) Атаки хакеров на сайт компании.

d) Физическое повреждение компьютеров сотрудников.

Краткие методические указания

Тестовые задания состоят из вопроса и нескольких вариантов ответа. Решение представляет собой указание номера вопроса и букву, которой обозначен правильный, по мнению студента, вариант ответа. В течение семестра проводится 4 теста по 4 темам на лекционных занятиях, в каждом тесте 16 вопросов.

Шкала оценки

Оценка	Баллы	Описание
5	5	Студент допустил не более 2х ошибок
4	4	Студент совершил от 3 до 6 ошибок в ответах на тест
3	2-3	Студент совершил от 7 до 10 ошибок в ответах на тест
2	0-1	Студент совершил 11 и более ошибок в ответах на тест

5.3 Вопросы к экзамену

1. Перечислите основные компоненты информационной безопасности и дайте характеристику каждому компоненту.
2. Объясните, почему экономический аспект важен при формировании системы информационной безопасности предприятия?
3. Назовите ключевые этапы жизненного цикла информационной системы и охарактеризуйте роль информационной безопасности на каждом этапе.
4. Дайте определение понятия «риск информационной безопасности». Приведите пример расчета риска.
5. Какие типы угроз существуют в современной информационной инфраструктуре и какие меры принимаются для минимизации рисков?
6. Почему важно соблюдать российское законодательство в области информационной безопасности? Приведите конкретные примеры законодательных актов.
7. Охарактеризуйте структуру современного рынка информационно-защитных технологий и определите тенденции его развития.
8. Раскройте смысл термина «экономическая эффективность информационной безопасности». Как определяется эта эффективность?
9. Какие международные стандарты используются для оценки и сертификации систем информационной безопасности?

10. Назовите причины возникновения конфликтных ситуаций в процессе принятия решений по вопросам информационной безопасности и способы их разрешения.

11. В чём заключаются проблемы обеспечения информационной безопасности малых и средних предприятий?

12. Какими факторами обусловлена необходимость непрерывного мониторинга и оценки текущего состояния информационной безопасности организации?

13. Какие методы применяются для измерения уровня информационной безопасности в организации?

14. Что такое система менеджмента информационной безопасности (СМИБ)? В чём заключается её значение для деятельности предприятия?

15. Перечислите и поясните основные элементы типичного комплекса мер по обеспечению информационной безопасности.

Краткие методические указания

Для подготовки к экзамену студенту необходимо изучить лекционный материал, а так же материал представленный в дополнительных источниках.

Шкала оценки

Оценка	Баллы	Описание
5	14-20	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой.
4	8-12	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач.
3	2-6	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки.
2	0-2	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки.