МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины (модуля)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

Специальность и специализация
38.05.01 Экономическая безопасность. Экономико-правовое обеспечение экономической безопасности

Год набора на ОПОП
2023

Форма обучения
очная

Владивосток 2025

Рабочая программа дисциплины (модуля) «Информационная безопасность предприятия» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 38.05.01 Экономическая безопасность (утв. приказом Минобрнауки России от 14.04.2021г. №293) 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):

Иванова А.В., старший преподаватель, Кафедра информационной безопасности, Ivanova.A@vvsu.ru

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	0000000000E83E9E
Владелец	Шумик Е.Г.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

Ознакомить студентов с законодательными, административными, организационными, программно-техническими мерами информационной безопасности, с действующими стандартами в этой области.
Задачи дисциплины состоят в том, что в результате ее изучения студенты должны:
– иметь представление об использовании основных положений теории информационной безопасности в различных областях ИС и иметь представление о направлении развития и перспективах защиты информации;
– знать правовые основы защиты компьютерной информации, организационные, технические программные методы защиты информации в ИС, стандарты, модели и методы шифрования, методы идентификации пользователей, методы защиты программ от вирусов;
– уметь применять методы защиты компьютерной информации в различных предметных областях.

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	
38.05.01 «Экономическая безопасность» (ЭБ)	ПКВ-2 : Способен воздействовать на предпринимательские риски и угрозы экономической безопасности организации на основе их мониторинга	ПКВ-2.1к : Оценивает предпринимательские риски и угрозы экономической безопасности организации на основе анализа информации	РД1	Знание	концепции защиты информации и систем безопасности предприятия и их роль в обеспечении экономической безопасности
			РД2	Умение	обосновывать свой выбор при применении методов и приемов защиты от несанкционированного доступа
			РД3	Навык	методами анализ угроз информационной безопасности
		ПКВ-2.2к : Разрабатывает предложения по предупреждению, локализации и нейтрализации предпринимательских рисков и угроз экономической безопасности организации	РД4	Знание	методы предупреждения рисков информационной безопасности, влияющих на экономическую безопасность организации
			РД5	Умение	соблюдать требования, установленные к информационной безопасности организации

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 Конституции и законам Российской Федерации	Гражданственность	Осознание себя членом общества
Формирование духовно-нравственных ценностей		
Воспитание чувства долга и ответственности перед семьей и обществом	Гражданственность	Активная жизненная позиция
Формирование научного мировоззрения и культуры мышления		
Развитие познавательного интереса и стремления к знаниям	Права и свободы человека	Любовь к стране
Формирование коммуникативных навыков и культуры общения		
Воспитание культуры диалога и уважения к мнению других людей	Гражданственность	Коммуникабельность

2 Место дисциплины (модуля) в структуре ОПОП

Дисциплина «Информационная безопасность предприятия» относится к дисциплинам по выбору. Входными требованиями, необходимыми для освоения дисциплины, является наличие у обучающихся компетенций, сформированных при изучении дисциплин и/или прохождении практик «Информатика модуль 1 (Основы информационных технологий)», «Информатика модуль 2 (Информационно-коммуникационные технологии)».

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		

38.05.01 Экономическая безопасность	ОФО	С1.ДВ.А	8	4	55	18	36	0	1	0	89	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	Основные понятия и определения информационной безопасности	РД1, РД5	4	8	0	22	Тестовые задания, практические работы
2	Государственная система информационной безопасности. Законодательный уровень информационной безопасности	РД1, РД3, РД5	4	8	0	15	Тестовые задания, практические работы
3	Угрозы информационной безопасности и их влияние на экономическую безопасность предприятия	РД2, РД3, РД4	4	10	0	24	Тестовые задания, практические работы
4	Методы обеспечения информационной безопасности	РД2, РД3, РД4, РД5	6	10	0	28	Тестовые задания, практические работы
Итого по таблице			**18**	**36**	**0**	**89**	

4.2 Содержание разделов и тем дисциплины (модуля) для ОФО

Тема 1 Основные понятия и определения информационной безопасности.

Содержание темы: Проблемы информационной безопасности в современном обществе. Основные понятия в области защиты информации. Уровни информационной безопасности (личности, общества, государства).

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекция- дискуссия.

Виды самостоятельной подготовки студентов по теме: Изучение рекомендованной литературы.

Тема 2 Государственная система информационной безопасности. Законодательный уровень информационной безопасности.

Содержание темы: Содержание и структура законодательства в области информационной безопасности. Правовое регулирование защиты информации в России. Содержание и структура законодательства в области информационной безопасности. Обзор документов в области обеспечения информационной безопасности по отраслям права.Регуляторы в области информационной безопасности. Изучение нормативных документовв сфере обеспечения информационной безопастности. ФЗ "О персональных данных" Обзор документов в области обеспечения информационной безопасности по отраслям права. Регуляторы в области информационной безопасности. Обзор документов в

области юридической ответственности за правонарушения в области информационной безопасности.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекция- дискуссия.

Виды самостоятельной подготовки студентов по теме: Изучение рекомендованной литературы.

Тема 3 Угрозы информационной безопасности и их влияние на экономическую безопасность предприятия.

Содержание темы: Общий анализ угроз безопасности информации. Пути реализации угроз информационной. Общий анализ угроз безопасности информации. Пути реализации угроз информационной. Классификация угроз безопасности информации. Анализ киберугроз. Методические основы оценки угроз. Влияние угроз информационной безопасности на экономическую безопасность организации.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекция- дискуссия.

Виды самостоятельной подготовки студентов по теме: Изучение рекомендованной литературы.

Тема 4 Методы обеспечения информационной безопасности.

Содержание темы: Управление информационными рисками. Соблюдение режима секретности. Комплексная защита информации. Соблюдение режима секретности. Управление информационными рисками. Соблюдение режима секретности. Комплексная защита информации. Критическая информационная инфраструктура. Категорирование объекта КИИ. Организационные меры обеспечения защиты информации. Аудит информационной безопасности организации. Обзор методических материалов. Организационных мер защиты информации. Критическая информационная инфраструктура. Категорирование объекта КИИ. Организационные меры обеспечения защиты информации. Программно-технические средства защиты информации.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекция- дискуссия.

Виды самостоятельной подготовки студентов по теме: Изучение рекомендованной литературы.

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

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

Успешное освоение дисциплины предполагает активную работу студентов на лекциях и практических занятиях, выполнение аттестационных мероприятий, эффективную самостоятельную работу.

В процессе изучения дисциплины студенту необходимо ориентироваться на самостоятельную проработку лекционного материала, подготовку к практическим занятиям, выполнение рефератов и самостоятельное изучение некоторых вопросов курса. Методические рекомендации по обеспечению самостоятельной работы

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 рамках подготовки к практическим занятиям студенты сначала прорабатывают лекционный материал, презентации по теме работы, знакомятся с целью, задачами и информационными источниками.

При необходимости подбирают дополнительные информационные материалы, необходимую литературу, нормативные и законодательные документы, знакомятся с ними. В случае, если в заданиях работы необходимо написать размышление или эссе, изучают источники, различные данные и др., чтобы иметь представление о вопросах, затрагиваемых в работе.

Задания представляют собой ситуационные практические задания, выполняемые индивидуально или группой студентов - временным творческим коллективом в составе нескольких студентов (2-3 человека).

Самостоятельная работа специалистов предполагает:

1. Изучение материала по теме занятия и подготовка к практическому занятию.

2. Поиск и сбор первичной и вторичной информации по заявленной проблеме в рамках ситуационных заданий к практическим занятиям и подготовка отчета по результатам самостоятельно проведенных исследовании форме презентации (файл с расширением .ppt).

3. Защита ситуационного практического задания проводится на практическом занятии с демонстрацией отчета или презентации, ответы на вопросы, обсуждение.

По результатам проверки студенту выставляется определенное количество баллов, которое входит в общее количество баллов студента, набранных им в течение семестра. При оценке результатов выполнения заданий учитываются четкость структуры работы, умение сбора вторичной информации, умение ставить проблему и анализировать ее, умение логически мыслить, владение профессиональной терминологией, грамотность оформления.

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. Документальное обеспечение информационной безопасности : учебное пособие / составители Е. Е. Смычков [и др.]. — Севастополь : СевГУ, 2022. — 142 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/261899 (дата обращения: 09.09.2025). — Режим доступа: для авториз. пользователей.

2. Правовые основы информационной безопасности : практикум / сост. Х. В. Белогорцева (Пешкова). - Воронеж : Научная книга, 2021. - 80 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1996330 (Дата обращения - 05.09.2025)

7.2 Дополнительная литература

1. Ванюшина, А. В. Основы информационной безопасности : учебно-методическое пособие / А. В. Ванюшина, С. Ю. Рыбаков. — Москва :МТУСИ, 2022. — 22 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/333701 (дата обращения: 09.09.2025). — Режим доступа: для авториз. пользователей.

2. Мельников, В. П., Информационная безопасность. : учебник / В. П. Мельников, А. И. Куприянов, ; под ред. В. П. Мельникова. — Москва : КноРус, 2020. — 267 с. — ISBN 978-5-406-07382-7. — URL: https://book.ru/book/932059 (дата обращения: 09.09.2025). — Текст : электронный.

3. Попов, И. В. Информационная безопасность : практикум / И. В. Попов, Н. И. Улендеева. - Самара : Самарский юридический институт ФСИН России, 2022. - 90 с. - ISBN 978-5-91612-375-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/2016193 (Дата обращения - 05.09.2025)

4. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2023. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1912987 (дата обращения: 01.03.2023). – Режим доступа: по подписке.

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

1. Электронно-библиотечная система "BOOK.ru"
2. Электронно-библиотечная система "ZNANIUM.COM"
3. Электронно-библиотечная система "ZNANIUM.COM" - Режим доступа: https://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:

- Проектор

Программное обеспечение:

- МойОфис

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

Специальность и специализация
38.05.01 Экономическая безопасность. Экономико-правовое обеспечение экономической безопасности

Год набора на ОПОП
2023

Форма обучения
очная

Владивосток 2025

1 Перечень формируемых компетенций

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции
38.05.01 «Экономическая безопасность» (ЭБ)	ПКВ-2 : Способен воздействовать на предпринимательские риски и угрозы экономической безопасности организации на основе их мониторинга	ПКВ-2.1к : Оценивает предпринимательские риски и угрозы экономической безопасности организации на основе анализа информации
		ПКВ-2.2к : Разрабатывает предложения по предупреждению, локализации и нейтрализации предпринимательских рисков и угроз экономической безопасности организации

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-2 «Способен воздействовать на предпринимательские риски и угрозы экономической безопасности организации на основе их мониторинга»

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-2.1к : Оценивает предпринимательские риски и угрозы экономической безопасности организации на основе анализа информации	РД 1	Знание	концепции защиты информации и систем безопасности предприятия и их роль в обеспечении экономической безопасности	ответы на тестовые задания
	РД 2	Умение	обосновывать свой выбор при применении методов и приемов защиты от несанкционированного доступа	корректное выполнение практического задания
	РД 3	Навык	методами анализ угроз информационной безопасности	корректное выполнение практического задания
ПКВ-2.2к : Разрабатывает предложения по предупреждению, локализации и нейтрализации предпринимательских рисков и угроз экономической безопасности организации	РД 4	Знание	методы предупреждения рисков информационной безопасности, влияющих на экономическую безопасность организации	ответы на тестовые задания
	РД 5	Умение	соблюдать требования, установленные к информационной безопасности организации	корректное выполнение практического задания

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 : концепции защиты информации и систем безопасности предприятия и их роль в обеспечении экономической безопасности	1.1. Основные понятия и определения информационной безопасности	Тест	Список вопросов
		1.2. Государственная система информационной безопасности. Законодательный уровень информационной безопасности	Тест	Список вопросов
РД2	Умение : обосновывать свой выбор при применении методов и приемов защиты от несанкционированного доступа	1.3. Угрозы информационной безопасности и их влияние на экономическую безопасность предприятия	Практическая работа	Список вопросов
		1.4. Методы обеспечения информационной безопасности	Практическая работа	Список вопросов
РД3	Навык : методами анализ угроз информационной безопасности	1.2. Государственная система информационной безопасности. Законодательный уровень информационной безопасности	Практическая работа	Список вопросов
		1.3. Угрозы информационной безопасности и их влияние на экономическую безопасность предприятия	Практическая работа	Список вопросов
		1.4. Методы обеспечения информационной безопасности	Практическая работа	Список вопросов
РД4	Знание : методы предупреждения рисков информационной безопасности, влияющих на экономическую безопасность организации	1.3. Угрозы информационной безопасности и их влияние на экономическую безопасность предприятия	Тест	Список вопросов
		1.4. Методы обеспечения информационной безопасности	Тест	Список вопросов
РД5	Умение : соблюдать требования, установленные к информационной безопасности организации	1.1. Основные понятия и определения информационной безопасности	Практическая работа	Список вопросов
		1.2. Государственная система информационной безопасности. Законодательный уровень информационной безопасности	Практическая работа	Список вопросов
		1.4. Методы обеспечения информационной безопасности	Практическая работа	Список вопросов

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	20	40		60
Промежуточная аттестация			20	20
Итого	40	40	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 тестовых заданий

1. К правовым методам, обеспечивающим информационную безопасность, относятся:

- **а)** Разработка аппаратных средств обеспечения правовых данных
- **б)** Разработка и установка во всех компьютерных правовых сетях журналов учета действий
- **в)** Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2. Основными источниками угроз информационной безопасности являются все указанные в списке:

- **а)** Хищение жестких дисков, подключение к сети, инсайдерство

- **б)** Перехват данных, хищение данных, изменение архитектуры системы
- **в)** Хищение данных, подкуп системных администраторов, нарушение регламента работы

3. Виды информационной безопасности:

- **а)** Персональная, корпоративная, государственная
- **б)** Клиентская, серверная, сетевая
- **в)** Локальная, глобальная, смешанная

4. Цели информационной безопасности – своевременное обнаружение, предупреждение:

- **а)** Несанкционированного доступа, воздействия в сети
- **б)** Инсайдерства в организации
- **в)** Чрезвычайных ситуаций

5. Основные объекты информационной безопасности:

- **а)** Компьютерные сети, базы данных
- **б)** Информационные системы, психологическое состояние пользователей
- **в)** Бизнес-ориентированные, коммерческие системы

6. Основными рисками информационной безопасности являются:

- **а)** Искажение, уменьшение объёма, перекодировка информации
- **б)** Техническое вмешательство, выведение из строя оборудования сети
- **в)** Потеря, искажение, утечка информации

7. К основным принципам обеспечения информационной безопасности относится:

- **а)** Экономической эффективности системы безопасности
- **б)** Многоплатформенной реализации системы
- **в)** Усиления защищённости всех звеньев системы

8. Основными субъектами информационной безопасности являются:

- **а)** Руководители, менеджеры, администраторы компаний
- **б)** Органы права, государства, бизнеса
- **в)** Сетевые базы данных, фаерволлы

9. К основным функциям системы безопасности можно отнести всё перечисленное:

- **а)** Установление регламента, аудит системы, выявление рисков
- **б)** Установка новых офисных приложений, смена хостинг-компании
- **в)** Внедрение аутентификации, проверка контактных данных пользователей

10. Принципом информационной безопасности является принцип недопущения:

- **а)** Неоправданных ограничений при работе в сети (системе)
- **б)** Рисков безопасности сети, системы
- **в)** Презумпции секретности

11. Принципом политики информационной безопасности является принцип:

- **а)** Невозможности миновать защитные средства сети (системы)
- **б)** Усиления основного звена сети, системы
- **в)** Полного блокирования доступа при риск-ситуациях

12. Принципом политики информационной безопасности является принцип:

- **а)** Усиления защищённости самого незащищённого звена сети (системы)
- **б)** Перехода в безопасное состояние работы сети, системы
- **в)** Полного доступа пользователей ко всем ресурсам сети, системы

13. Принципом политики информационной безопасности является принцип:

- **а)** Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- **б)** Одноуровневой защиты сети, системы
- **в)** Совместимых, однотипных программно-технических средств сети, системы

14. К основным типам средств воздействия на компьютерную сеть относится:

- **а)** Компьютерный сбой
- **б)** Логические закладки («мины»)
- **в)** Аварийное отключение питания

15. Когда получен спам по e-mail с приложённым файлом, следует:

- **а)** Прочитать приложение, если оно не содержит ничего ценного – удалить
- **б)** Сохранить приложение в папке «Спам», выяснить затем IP-адрес генератора спама
- **в)** Удалить письмо с приложением, не раскрывая (не читая) его

16. Принцип Кирхгофа:

- **а)** Секретность ключа определена секретностью открытого сообщения
- **б)** Секретность информации определена скоростью передачи данных
- **в)** Секретность закрытого сообщения определяется секретностью ключа

17. ЭЦП – это:

- **а)** Электронно-цифровой преобразователь
- **б)** Электронно-цифровая подпись
- **в)** Электронно-цифровой процессор

18. Наиболее распространены угрозы информационной безопасности корпоративной системы:

- **а)** Покупка нелицензионного ПО
- **б)** Ошибки эксплуатации и неумышленного изменения режима работы системы
- **в)** Сознательное внедрение сетевых вирусов

19. Наиболее распространены угрозы информационной безопасности сети:

- **а)** Распределённый доступ клиента, отказ оборудования
- **б)** Моральный износ сети, инсайдерство
- **в)** Сбой (отказ) оборудования, нелегальное копирование данных

20. Наиболее распространены средства воздействия на сеть офиса:

- **а)** Слабый трафик, информационный обман, вирусы в интернет
- **б)** Вирусы в сети, логические мины (закладки), информационный перехват
- **в)** Компьютерные сбои, изменение администрирования, топологии

21. Утечкой информации в системе называется ситуация, характеризуемая:

- **а)** Потерей данных в системе
- **б)** Изменением формы информации
- **в)** Изменением содержания информации

22. Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

- **а)** Целостность
- **б)** Доступность
- **в)** Актуальность

23. Угроза информационной системе (компьютерной сети) – это:

- **а)** Вероятное событие
- **б)** Детерминированное (всегда определённое) событие
- **в)** Периодически повторяющееся событие

24. Информация, которую следует защищать (по нормативам, правилам сети, системы), называется:

- **а)** Регламентированной
- **б)** Правовой
- **в)** Защищаемой

25. Разновидностями угроз безопасности (сети, системы) являются все перечисленные в списке:

- **а)** Программные, технические, организационные, технологические
- **б)** Серверные, клиентские, спутниковые, наземные
- **в)** Личные, корпоративные, социальные, национальные

26. Окончательно, ответственность за защищённость данных в компьютерной сети несёт:

- **а)** Владелец сети
- **б)** Администратор сети
- **в)** Пользователь сети

27. Политика безопасности в системе (сети) – это комплекс:

- **а)** Руководств, требований обеспечения необходимого уровня безопасности
- **б)** Инструкций, алгоритмов поведения пользователя в сети
- **в)** Норм информационного права, соблюдаемых в сети

28. Наиболее важным при реализации защитных мер политики безопасности является:

- **а)** Аудит, анализ затрат на проведение защитных мер
- **б)** Аудит, анализ безопасности
- **в)** Аудит, анализ уязвимостей, риск-ситуаций

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.

Шкала оценки

Оценка	Баллы	Описание
5	3	Студент ответил безошибочно
4	2	Студент совершил от 1 до 2 ошибок в ответах на тест
3	1	Студент совершил от 3 до 4 ошибок в ответах на тест
2	0	Студент совершил от 5 до 6 ошибок в ответах на тест

5.2 Примеры заданий для выполнения практических работ

Разбившись на группу 3-5 человек, придумать организацию и разработать проект внутренней политики информационной безопасности организации с учетом экономических составляющих и действующих федеральных законов и стандартов Российской Федерации.

Краткие методические указания

Разработать проект внутренней политики информационной безопасности организации с учетом экономических составляющих и действующих федеральных законов и стандартов Российской Федерации.

Этапы выполнения задания:

1. **Анализ законодательства РФ** :
    - Изучить федеральный закон №152-ФЗ «О персональных данных», №149-ФЗ «Об информации, информационных технологиях и защите информации» и другие нормативные акты, относящиеся к информационной безопасности.
    - Составить перечень требований, предъявляемых федеральным законодательством к организациям относительно защиты информации.
2. **Ознакомление со стандартами информационной безопасности** :
    - Рассмотреть отраслевые стандарты, такие как СТО БР ИББС-1.1-2007, ГОСТ Р 50922-2006, ГОСТ Р 57580.1-2017, ISO/IEC 27001 и определить их значимость для разработки политики информационной безопасности.
3. **Определение экономического аспекта информационной безопасности** :
    - Оценить экономические риски, возникающие в результате несоблюдения политики информационной безопасности (потеря доходов, штрафы, репутационные издержки).
    - Спланировать расходы на организацию и поддержание необходимых мер защиты информации, учесть затраты на обучение сотрудников, закупку оборудования и лицензий на программное обеспечение.
4. **Проектирование внутренней политики информационной безопасности** :
    - На основании проведенного анализа сформулируйте цель и задачи политики информационной безопасности вашей организации.

- Опишите порядок обработки и защиты персональных данных работников и клиентов, установите границы доступа к информационным ресурсам и системам организации.
- Определите мероприятия по управлению рисками информационной безопасности, порядку взаимодействия подразделений, назначению ответственных лиц и санкционированных действий персонала.
- Предусмотрите механизм оценки экономической целесообразности планируемых мер защиты.

5. **Расчет экономической эффективности принятых мер** :
   - Провести предварительную оценку экономической выгоды и расходов, возникающих в результате принятия и реализации разрабатываемых мер информационной безопасности.
   - Привести обоснование оптимальности выбранной стратегии защиты с точки зрения соотношения стоимости внедрения и ожидаемого снижения потерь.
6. **Формализация результата** :
   - Представьте готовый проект внутренней политики информационной безопасности в виде структурированного документа с разделами: общая информация, определение понятий, цели и задачи, экономические обоснования, обязательства сотрудников, ответственность за нарушение политики, контроль и оценка соблюдения требований.
7. **Представление и обсуждение** :
   - Подготовьте краткую презентацию своей политики, обсудив ее преимущества и особенности с преподавателем и группой.

Шкала оценки

Оценка	Баллы	Описание
5	36-40	Оценка «отлично» выставляется при выполнении работы в установленные сроки, в полно м объеме и на высоком теоретическом уровне. Студент свободно владеет теоретическим материалом, умеет применить его при решении кейса; на все вопросы дает правильные и обоснованные ответы, убедительно защищает свою точку зрения.
4	26-35	Оценка «хорошо» выставляется при выполнении работы в установленные сроки, в полно м объеме. Студент достаточно владеет теоретическим материалом, может применять его самостоятельно или по указанию преподавателя. На большинство вопросов даны правиль ные ответы, защищает свою точку зрения достаточно обосновано.
3	16-25	Оценка «удовлетворительно» выставляется при выполнении работы в установленные сро ки, в основном правильно, но без достаточно глубокой проработки некоторых разделов. Студент усвоил только основные разделы теоретического материала и по указанию препо давателя (без инициативы и самостоятельности) применяет его практически; на вопросы отвечает неуверенно или допускает ошибки, неуверенно защищает свою точку зрения.
2	0-15	Оценка «неудовлетворительно» выставляется в случае, если студент не выполняет работу в установленные сроки. Решения кейса не раскрыто, ответы не полные. Студент не может защитить свои выводы, допускает грубые фактические ошибки при ответах на поставлен ные вопросы или не отвечает на них.

5.3 Экзаменационные вопросы

1. Что такое информационная безопасность?
2. Перечислите основные угрозы информационной безопасности.
3. Какие существуют модели информационной безопасности?
4. Какие методы защиты информации выделяют?
5. Право. Источники права.
6. Какие основные законы в области защиты информации в РФ?
7. Охарактеризуйте биометрические данные как персональные данные.
8. Что такое профессиональная тайна?
9. Что такое служебная тайна?
10. Что такое коммерческая тайна?

11. Какие основные международные стандарты в области информационной безопасности?
12. «Оранжевая книга»
13. ISO/IEC 15408.
14. Как связаны международные стандарты и стандарты РФ?
15. СТО БР ИББС-1.1-2007. «Аудит информационной безопасности»
16. РС БР ИББС-2.2-2009. «Методика оценки рисков нарушения информационной безопасности».
17. Что такое политика безопасности?

Краткие методические указания

Подготовка к опросу проводится в ходе самостоятельной работы студентов и включает в себя повторение пройденного материала по вопросам предстоящего опроса. Помимо основного материала студент должен изучить дополнительную рекомендованную литературу и информацию по теме, в том числе с использованием Интернет-ресурсов.

Шкала оценки

Оценка	Баллы	Описание
5	15-20	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	10-14	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	5-9	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки. Не может связать с практическими примерами.
2	0-4	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки.