МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины (модуля)

БИЗНЕС-ПРОЦЕССЫ ПРЕДПРИЯТИЯ И ИХ ЗАЩИТА

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

Год набора на ОПОП
2022

Форма обучения
очная

Владивосток 2025

Рабочая программа дисциплины (модуля) «Бизнес-процессы предприятия и их защита» 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	0000000000EA7C51
Владелец	Шумик Е.Г.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

Целью освоения дисциплины является приобретение студентами теоретических знаний и практических навыков в области организационного проектирования бизнес-процессов организаций и эффективного построения системы защиты информации в условиях современной экономики.

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-1.1к : идентифицирует бизнес-процессы происходящие в организации, определяет возможные угрозы информационной безопасности	РД1	Знание	угрозы информационной безопасности, присущие различным этапам и звеньям бизнес-процессов
			РД2	Умение	выделять значимые элементы и шаги бизнес-процессов, влияющие на общий уровень информационной безопасности
			РД3	Навык	анализа и синтеза полученной информации о процессах и процедурах предприятия с целью установления возможных точек риска и уязвимостей

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	Справедливость	Внимательность к деталям
Формирование духовно-нравственных ценностей		

Воспитание чувства долга и ответственности перед семьей и обществом	Служение Отечеству и ответственность за его судьбу	Дисциплинированность
Формирование научного мировоззрения и культуры мышления		
Развитие познавательного интереса и стремления к знаниям	Взаимопомощь и взаимоуважение	Самообучение
Формирование коммуникативных навыков и культуры общения		
Воспитание культуры диалога и уважения к мнению других людей	Созидательный труд	Гибкость мышления

2 Место дисциплины (модуля) в структуре ОПОП

Дисциплина «Бизнес-процессы предприятия и их защита» относится к вариативной части дисциплин учебного плана направления «Информационная безопасность автоматизированных систем».

Входными требованиями, необходимыми для освоения дисциплины, является наличие у обучающихся компетенций, сформированных при изучении дисциплин и/или прохождении практик «Аудит информационной безопасности», «Основы информационной безопасности». На данную дисциплину опираются «Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты», «Производственная преддипломная практика»

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 обуче-ния	Часть УП	Семестр (ОФО) или курс (ЗФО, ОЗФО)	Трудо-емкость	Объем контактной работы (час)						СРС	Форма аттес-тации
				(З.Е.)	Всего	Аудиторная			Внеауди-торная			
						лек.	прак.	лаб.	ПА	КСР		
10.05.03 Информационная безопасность автоматизированных систем	ОФО	С1.В	11	3	47	12	24	0	1	10	61	3

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	Основы анализа бизнес-процессов	РД1, РД2, РД3	2	4	0	18	практическое задание
2	Моделирование и документирование бизнес-процессов	РД1, РД2, РД3	2	4	0	18	практическое задание
3	Безопасность бизнес-процессов	РД1, РД2, РД3	4	8	0	18	практическое задание
4	Практическое построение защиты информации	РД1, РД2, РД3	4	8	0	18	практическое задание
Итого по таблице			**12**	**24**	**0**	**72**	

4.2 Содержание разделов и тем дисциплины (модуля) для ОФО

Тема 1 Основы анализа бизнес-процессов.

Содержание темы: Что такое бизнес-процесс?Определение понятия «бизнес-процесс», характеристика основных элементов и свойств бизнес-процессов. Понятия первичного и вспомогательного процессов, горизонтального и вертикального уровней управления. Методы анализа бизнес-процессов.Рассмотрение традиционных и современных методик анализа бизнес-процессов: SWOT-анализ, ABC-анализ, Benchmarking, Six Sigma, Lean Management и другие. Примеры успешного применения данных методов в практике отечественных компаний.

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 Моделирование и документирование бизнес-процессов.

Содержание темы: Основы графического моделирования.Описание наиболее распространённых стандартов и нотаций (IDEF, BPMN, UML, EPC). Описание принципов составления диаграмм потоков работ и IDEF-диаграмм. Методики документирования бизнес-процессов.Стандарты ISO 9001, методики регламентирования процедур и инструкций, разработка документации для поддержки бизнес-процессов. Правила оформления технологических карт и схем процессов.

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 Безопасность бизнес-процессов.

Содержание темы: Виды угроз информационной безопасности в бизнесе.Выявление внутренних и внешних угроз безопасности, классификация и характеристика угроз (неправомерный доступ, утечка информации, вирусные атаки, сбои оборудования и программного обеспечения). Организационно-технические меры защиты информации.Обзор ключевых организационных и технических мер защиты информации в бизнес-процессах: политика паролей, регулярное обучение персонала, резервное копирование, шифрование, использование межсетевых экранов и антивирусных программ.
.

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 Практическое построение защиты информации.

Содержание темы: Средства и методы защиты информации в бизнеспроцессах.Современные технологические решения для защиты информации: PKI-инфраструктура, криптографические системы, SIEM-решения, Firewall и IDS/IPS. Рассматривается практика внедрения систем защиты информации и опыт российских компаний. Организация внутреннего контроля и мониторинга безопасности.Система постоянного мониторинга информационной безопасности: назначение служб, обязанности сотрудников, ведение журналов регистрации инцидентов, порядок действий при обнаружении нарушений. .

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 занятиях аудиторной формы: лекций и практических занятий, выполнение аттестационный мероприятий, эффективную самостоятельную работу. В процессе изучения дисциплины студенту необходимо ориентироваться на самостоятельную проработку лекционного материала, подготовку к практическим занятиям, выполнение тестов, самостоятельное изучение некоторых разделов курса Для проведения занятий лекционного типа используются учебно-наглядные пособия в форме презентационных материалов, обеспечивающих тематические иллюстрации, соответствующие темам лекций, представленным в пункте 4 настоящей РПД

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. Аверченков, В. И. Аудит информационной безопасности : учебное пособие : [16+] / В. И. Аверченков. – 4-е изд., стер. – Москва : ФЛИНТА, 2021. – 269 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=93245 (дата обращения: 20.10.2025). – Библиогр. в кн. – ISBN 978-5-9765-1256-6. – Текст : электронный.
2. Елиферов, В. Г. Бизнес-процессы: регламентация и управление : учебник / В.Г. Елиферов, В.В. Репин. — Москва : ИНФРА-М, 2025. — 319 с. — (Учебники для программы MBA). - ISBN 978-5-16-001825-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2174078 (Дата обращения - 22.10.2025)
3. Козырь, Н. С. Аудит информационной безопасности : учебник для вузов / Н. С. Козырь. — Москва : Издательство Юрайт, 2025. — 36 с. — (Высшее образование). — ISBN 978-5-534-20647-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/581505 (дата обращения: 15.10.2025).
4. Организация и порядок функционирования бизнеса и бизнес-процессы : учебное пособие / составители Н. В. Пучкова, Н. А. Масюк. — Сургут : СурГУ, 2024. — 38 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/422384 (дата обращения: 27.10.2025). — Режим доступа: для авториз. пользователей.

7.2 Дополнительная литература

1. Щербак, А. В. Информационная безопасность : учебник для вузов / А. В. Щербак. — 2-е изд. — Москва : Издательство Юрайт, 2025. — 252 с. — (Высшее образование). — ISBN 978-5-9916-4299-6. — Текст : электронный // Образовательная

платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/569267 (дата обращения: 15.10.2025).

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 "ZNANIUM.COM"
3. Электронно-библиотечная система "ЛАНЬ"
4. Электронно-библиотечная система "УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН"
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 Professional Plus 2010

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

БИЗНЕС-ПРОЦЕССЫ ПРЕДПРИЯТИЯ И ИХ ЗАЩИТА

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

Год набора на ОПОП
2022

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-1.1к : идентифицирует бизнес-процессы происходящие в организации, определяет возможные угрозы информационной безопасности

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-1.1к : идентифицирует бизнес-процессы происходящие в организации, определяет возможные угрозы информационной безопасности	РД 1	Знание	угрозы информационной безопасности, присущие различным этапам и звеньям бизнес-процессов	решение тестовых заданий
	РД 2	Умение	выделять значимые элементы и шаги бизнес-процессов, влияющие на общий уровень информационной безопасности	выполнение практических заданий
	РД 3	Навык	анализа и синтеза полученной информации о процессах и процедурах предприятия с целью установления возможных точек риска и уязвимостей	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 ат тестация
Очная форма обучения				
РД1	Знание : угрозы информ ационной безопасности, присущие различным эт апам и звеньям бизнес-п роцессов	1.1. Основы анализа биз нес-процессов	Тест	Зачет в письменно й форме
		1.2. Моделирование и д окументирование бизне с-процессов	Тест	Зачет в письменно й форме
		1.3. Безопасность бизнес -процессов	Тест	Зачет в письменно й форме
		1.4. Практическое постр оение защиты информац ии	Тест	Зачет в письменно й форме
РД2	Умение : выделять знач имые элементы и шаги б изнес-процессов, влияю щие на общий уровень и нформационной безопас ности	1.1. Основы анализа биз нес-процессов	Практическая рабо та	Зачет в письменно й форме
		1.2. Моделирование и д окументирование бизне с-процессов	Практическая рабо та	Зачет в письменно й форме
		1.3. Безопасность бизнес -процессов	Практическая рабо та	Зачет в письменно й форме
		1.4. Практическое постр оение защиты информац ии	Практическая рабо та	Зачет в письменно й форме
РД3	Навык : анализа и синте за полученной информа ции о процессах и проце дурах предприятия с цел ью установления возмо жных точек риска и уязв имостей	1.1. Основы анализа биз нес-процессов	Практическая рабо та	Зачет в письменно й форме
		1.2. Моделирование и д окументирование бизне с-процессов	Практическая рабо та	Зачет в письменно й форме
		1.3. Безопасность бизнес -процессов	Практическая рабо та	Зачет в письменно й форме
		1.4. Практическое постр оение защиты информац ии	Практическая рабо та	Зачет в письменно й 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 1-5	Практическая р абота	Зачет	Ито го
Лекционные занятия	20			80
Практические занятия		60		
Промежуточная аттестация			20	20
Итого	20	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 Контрольный тест

Какой из перечисленных ниже элементов относится к основным составляющим любого бизнес-процесса?

A) Финансовое положение предприятия

B) Совокупность последовательных шагов и операций

C) Наличие большого количества клиентов

D) Высокий объем производства продукции

Какие из приведенных методов применяются для анализа и улучшения бизнес-процессов?

A) SWOT-анализ, PESTLE-анализ

B) Benchmarking, ABC-анализ

C) All of the above (Все вышеперечисленные)

D) Только SWOT-анализ

Какие виды бизнес-процессов выделяют в зависимости от характера выполняемой деятельности?

A) Первичные и вторичные

B) Внутренние и внешние

C) Производственные и обслуживающие

D) Горизонтальные и вертикальные

Какие основные формы угроз информационной безопасности характерны для большинства организаций?

A) Утрата данных, кража интеллектуальной собственности

B) Физическое повреждение имущества, износ техники

C) Недостаточная квалификация сотрудников

D) Отсутствие маркетинговых исследований

Какой термин обозначает документально зафиксированную последовательность шагов и действий, обеспечивающих достижение поставленной цели?

A) План развития

B) Политика информационной безопасности

C) Карта бизнес-процесса

D) Инструкция по охране труда

Какие стандартные нотации используются для визуализации бизнес-процессов?

A) IDEFO, BPMN, EPC

B) HTML, CSS, JavaScript

C) Microsoft Word, Excel

D) Linux, Windows, Mac OS

Что понимается под внутренним контролем информационной безопасности?

A) Постоянный мониторинг информационной безопасности силами самой организации

B) Внешняя аудиторская проверка систем безопасности

C) Государственное регулирование в области информационной безопасности

D) Обязательные тренировки сотрудников по действиям в чрезвычайных ситуациях

Какие факторы влияют на выбор средств защиты информации в конкретном бизнес-процессе?

A) Стоимость оборудования и программного обеспечения

B) Специфичность самого процесса и возможные угрозы

C) Уровень квалификации сотрудников

D) Все перечисленные факторы имеют значение

Что означает аббревиатура «PKI»?

A) Public Key Infrastructure (Инфраструктура открытых ключей)

B) Private Key Interface (Интерфейс закрытых ключей)

C) Personal Knowledge Integration (Интеграция персональных знаний)

D) Policy for Key Issues (Политика по ключевым вопросам)

Какие категории угроз относятся к внешним угрозам информационной безопасности?

A) Атака вирусов и вредоносных программ

B) Недовольство среди сотрудников компании

C) Несоблюдение правил сотрудниками компании

D) Устаревшие компьютерные системы

Что включает в себя система внутреннего контроля информационной безопасности?

A) Периодические отчёты руководителей отделов

B) Мониторинг активности пользователей и контроль доступа

C) Повышение заработной платы сотрудникам отдела безопасности

D) Запрет на использование социальных сетей в рабочее время

Что является задачей мониторинга информационной безопасности?

A) Улучшение финансовых показателей компании

B) Повышение мотивации сотрудников

C) Своевременное выявление и устранение угроз и инцидентов

D) Сокращение затрат на обслуживание компьютерных систем

Что входит в организационные меры защиты информации?

A) Установка антивирусных программ

B) Настройка брандмауэра

C) Разработанные инструкции и правила поведения сотрудников

D) Резервное копирование данных

Что называется угрозой информационной безопасности?

A) Любое событие, приводящее к финансовым потерям компании

B) Потеря конкурентоспособности вследствие неудачной рекламной кампании

C) Возможность несанкционированного доступа к данным или их уничтожения

D) Неблагоприятные погодные условия

Какие методы применяют для уменьшения рисков, связанных с нарушением информационной безопасности?

A) Проверка кредитной истории сотрудников

B) Страхование транспортных средств

C) Постановка четких ролей и обязанностей сотрудников

D) Ограничение свободы передвижения сотрудников по территории предприятия

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

5.2 Примеры заданий для выполнения практических работ

Практическое занятие 1. Анализ готовой модели бизнес-процесса, выявляются потенциальные проблемные места и предлагаются изменения, повышающие эффективность.

Практическое занятие 2. Оценка потенциальных угроз и анализ действующей системы безопасности бизнес-процесса учёта финансов торговой компании.

Практическое задание 3. Разработка перечня рекомендаций по устранению недостатков системы защиты информации на примере выбранного учебного бизнес-процесса.

Практическое задание 4. Проведение мини-аудит внутренней системы защиты информации условного предприятия, включая обсуждение полученных выводов и предложений по совершенствованию системы.

Краткие методические указания

На выполнение одной практической работы отводится не менее трех двухчасовых занятий. После выполнения каждой практической работы студент должен представить отчет о ее выполнении, а также, по указаниям преподавателя, выполнить дополнительные задания по теме

Шкала оценки

Оценка	Баллы	Описание
5	12-15	Оценка «отлично» выставляется, если студент выполнил задание, правильно применил методы.
4	8-11	Оценка «хорошо» выставляется, если студент выполнил задание, правильно применил методы, но совершил логические ошибки.
3	4-7	Оценка «удовлетворительно» выставляется, если студент выполнил задание, но применил методы не все необходимые методы для его выполнения.
2	0-3	Оценка «неудовлетворительно» выставляется в случае, если студент не выполнил задание и/ или неверно применил методы необходимые его выполнения.

5.3 Вопросы к зачету (письменная форма)

1. Что такое бизнес-процесс? Какие бывают виды бизнес-процессов?
2. Назовите основные этапы анализа бизнес-процесса.
3. Перечислите известные вам методы анализа и оптимизации бизнес-процессов.
4. Чем отличаются производственный и административный бизнес-процессы?
5. Какие существуют методы моделирования бизнес-процессов?
6. Что такое карта бизнес-процесса и зачем она необходима?
7. Какой вид документации помогает зафиксировать последовательность шагов бизнес-процесса?

8. Какие элементы входят в нотацию BPMN?
9. Почему важно своевременно обновлять документы, отражающие бизнес-процессы?
10. Какие внутренние и внешние угрозы чаще всего возникают в бизнес-процессах?
11. Какие организационные меры защиты информации необходимы в любом предприятии?
12. Каким образом техника резервного копирования способствует повышению безопасности?
13. Зачем необходим внутренний контроль информационной безопасности?
14. Что такое угроза информационной безопасности и как она проявляется?
15. Какие инструменты помогают обнаружить и предотвратить угрозы информационной безопасности?
16. Какие признаки указывают на возможное нарушение безопасности бизнес-процесса?
17. Какие правовые нормы определяют ответственность за нарушение информационной безопасности?
18. Что включает в себя проведение аудита информационной безопасности?
19. Какие преимущества даёт внедрение автоматизированных систем управления бизнес-процессами?
20. Какую роль играет квалифицированный персонал в обеспечении информационной безопасности?

Краткие методические указания

Для подготовки к зачету 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.