



Федеральное государственное бюджетное образовательное учреждение
высшего образования

САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
АРХИТЕКТУРНО-СТРОИТЕЛЬНЫЙ УНИВЕРСИТЕТ

Кафедра Экономической безопасности

УТВЕРЖДАЮ
Начальник учебно-методического управления

«31» октября 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Анализ и оценка информационной составляющей экономической безопасности

направление подготовки/специальность 38.04.05 Бизнес-информатика

направленность (профиль)/специализация образовательной программы Бизнес-анализ систем
управления строительной организацией

Форма обучения очная

Санкт-Петербург, 2024

1. Цели и задачи освоения дисциплины (модуля)

Цели освоения дисциплины

1. Освоить методы управления рисками информационной безопасности.
2. Получить базовые знания в области защиты данных в информационных системах.
3. Получить первичные навыки по использованию специализированного программного обеспечения для защиты информационных активов и решения профессиональных задач в области информационной и экономической безопасности.

Задачи дисциплины

1. Изучение источников угроз информационной безопасности. Место рисков информационной безопасности в структуре рисков бизнеса.
2. Изучение требований стандартов и нормативных документов в области информационной безопасности.
3. Изучение основных видов систем информационной безопасности и способов защиты.
4. Знакомство с возможностями использования программных продуктов информационной безопасности для решения задач информационной и экономической безопасности.
5. Изучение функционала DLP-систем.
6. Получение навыков использования DLP-систем для решения задач информационной и экономической безопасности.
7. Изучение организационных аспектов информационной безопасности.
8. Знакомство с системами защиты электронного документооборота.

2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов освоения ОПОП
ОПК-1 Способен разрабатывать стратегию развития информационных технологий инфраструктуры предприятия и управлять ее реализацией	ОПК-1.1 Проводит анализ бизнес-процессов и ИТ-инфраструктуры предприятия	знает Источники угроз информационной безопасности. Последствия реализации угроз информационной безопасности для предприятия. Способы сбора информации об информационных активах предприятия. Состав компонентов информационных систем предприятия. Назначение и функции основных классов систем информационной безопасности. умеет Применять криптографические системы защиты для обеспечения безопасности данных. Использовать системы противодействия утечкам данных для снижения рисков информационной и экономической безопасности. владеет Навыком использования общедоступных сервисов для выявления угроз информационной безопасности.

3. Указание места дисциплины (модуля) в структуре образовательной программы

Данная дисциплина (модуль) включена в Блок «Дисциплины, модули» Б1.О.07 основной профессиональной образовательной программы 38.04.05 Бизнес-информатика и относится к обязательной части учебного плана.

Для успешного освоения дисциплины обучающемуся необходимы следующие знания, умения, навыки:

Организация и управление строительным производством:

знает распределение обязанностей между подразделениями строительной организации и основные бизнес-процессы;

Проектный менеджмент:

знает теоретические основы управления проектами;

Методы научных исследований:

умеет анализировать научную и научно-практическую литературу по теме;

Информационные технологии

владеет навыком поиска информационных ресурсов, сбора и обработки информации о проблемной ситуации.

№ п/п	Последующие дисциплины	Код и наименование индикатора достижения компетенции
1	Подготовка к процедуре защиты и защита выпускной квалификационной работы	УК-1.1, УК-1.2, УК-1.3, УК-1.4, УК-1.5, УК-1.6, УК-2.1, УК-2.2, УК-2.3, УК-2.4, УК-2.5, УК-3.1, УК-3.2, УК-3.3, УК-3.4, УК-4.1, УК-4.2, УК-4.3, УК-4.4, УК-5.1, УК-5.2, УК-5.3, УК-6.1, УК-6.2, УК-6.3, ОПК-1.1, ОПК-1.2, ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-5.1, ОПК-5.2, ПК(Ц)-1.1, ПК(Ц)-1.2, ПК(Ц)-1.3, ПК(Ц)-1.4, ПК(Ц)-1.5, ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4
2	Практика по управлению бизнес-процессами в строительной организации	ПК-1.1, ПК-1.2, ПК-1.3
3	Управление жизненным циклом информационных систем	ОПК-2.2, ОПК-2.3, ОПК-3.3
4	Цифровая трансформация бизнеса в ИТ-сфере	ПК(Ц)-1.1, ПК(Ц)-1.2, ПК(Ц)-1.3, ПК(Ц)-1.4, ПК(Ц)-1.5, ПК-2.1, ПК-2.2

2.1.	Криптография как основа защиты данных при хранении и передаче по каналам связи	1	2		6				28,7 5	36,75	ОПК-1.1
2.2.	Системы защиты данных от утечек	1	4		8				5	17	ОПК-1.1
3.	3 раздел. Мониторинг инцидентов информационной безопасности. Оценка системы информационной безопасности организации										
3.1.	Стандарты информационной безопасности	1	4		2				20	26	ОПК-1.1
3.2.	Работа с инцидентами информационной безопасности. Платформа реагирования на инциденты (IRP). Security Operational Center (SOC)	1	2		8				15	25	ОПК-1.1
4.	4 раздел. Иная контактная работа										
4.1.	Курсовой проект	1								1,25	ОПК-1.1
5.	5 раздел. Контроль										
5.1.	Зачет с оценкой	1								9	ОПК-1.1

5.1. Лекции

№ разд	Наименование раздела и темы лекций	Наименование и краткое содержание лекций
1	Экономическая и информационная безопасность как необходимые условия существования предприятия	Информационная сущность бизнеса Понятие и составляющие экономической безопасности. Информационная сущность бизнеса. Информационная безопасность. Связь материальных и информационных процессов. Структура информационных потоков компании. Локальная нормативная база организации по информационной безопасности. Риски информационной безопасности в структуре рисков бизнеса.
2	Управление информационной безопасностью бизнеса	Управление информационной безопасностью организации Модели непрерывного совершенствования и процессного подхода. Гибкие модели менеджмента и международные стандарты. Этапы создания системы менеджмента информационной безопасности предприятия (СМИБ). Определение области действия СМИБ. Идентификация информационных активов. Выбор средств противодействия рискам информационной безопасности.
3	Криптография как основа защиты данных при хранении и передаче по каналам связи	Возможности современных криптографических систем в обеспечении безопасности данных Обзор основных классов систем информационной безопасности. Системы шифрования. Функции современных криптографических систем. Инфраструктура безопасности электронного документооборота. Основы блокчейн-технологии и ее использование для обеспечения целостности и доступности данных.
4	Системы защиты данных от утечек	Назначение и функции систем защиты данных от утечек (DLP-систем) Примеры, причины и последствия утечки конфиденциальных данных

		организации. Функции DLP-систем. Обзор рынка DLP-систем в РФ. Критерии выбора DLP-системы. Состав затрат на внедрение и эксплуатацию DLP-системы. Источники экономического эффекта от внедрения DLP-системы
5	Стандарты информационной безопасности	Требования международных и российских стандартов информационной безопасности Стандарты Банка России. PCI DSS. Особенности оценки системы информационной безопасности организации. Модель угроз. Модель нарушителя
6	Работа с инцидентами информационной безопасности. Платформа реагирования на инциденты (IRP). Security Operational Center (SOC)	Реагирование на инциденты информационной безопасности Особенности рисков информационной безопасности. Модель управления рисками информационной безопасности. Incident Responce Platform. Security Operational Center

5.2. Практические занятия

№ разд	Наименование раздела и темы практических занятий	Наименование и содержание практических занятий
1	Экономическая и информационная безопасность как необходимые условия существования предприятия	Риски информационной безопасности Распределение ресурсов организации в условиях риска. Риск-ориентированный подход к обеспечению информационной безопасности. Идентификация рисков. Зависимость качества оценки рисков и идентификации событий информационной безопасности от степени документированности информационных процессов компании. Накопление знаний по рискам. Модель Деминга-Шухарта. Модель обеспечения информационной безопасности бизнеса. Требования к модели информационной безопасности. Понятия риска, угрозы, ущерба и уязвимости. Анализ и оценка рисков информационной безопасности: примеры, задания.
2	Управление информационной безопасностью бизнеса	Распределение функций по информационной безопасности между подразделениями организации Организационная структура информационной безопасности. Распределение полномочий и обязанностей между подразделениями организации по обеспечению информационной безопасности. Место информационной безопасности в структуре подразделений, отвечающих за комплексную безопасность организации. Обсуждение кейсов распределения функций ИБ между подразделениями организации.
3	Криптография как основа защиты данных при хранении и передаче по каналам связи	Системы безопасности электронного документооборота Возможности криптографических систем. Использование криптографии для защиты данных при передаче по каналам связи и при хранении. Индивидуальные задания на получение умений и отработку навыков использования криптографических средств защиты
3	Криптография как основа защиты данных при хранении и передаче по каналам связи	Криптография как одна из ключевых технологий блокчейн Технология блокчейн - принципы и механизмы работы. Возможности использования для защиты данных
4	Системы защиты данных от утечек	Использование систем защиты данных от утечек для снижения рисков информационной и экономической безопасности

		Освоение работы с DLP-системой: функции, параметры, отчеты. Выполнение заданий
4	Системы защиты данных от утечек	Решение задач экономической безопасности с использованием систем мониторинга информационных потоков и противодействия утечкам данных Виды и особенности систем противодействия утечкам данных. Задачи учета использования рабочего времени и контроль соответствующих рисков кадровой безопасности; продуктивность использования рабочего времени сотрудниками; решение кейсов мошенничества, нецелевого использования сотрудниками ресурсов организации, др.
5	Стандарты информационной безопасности	Ключевые требования стандартов информационной безопасности Банка России Система документов Банка России по информационной безопасности. Содержание и структура. Основные требования. Назначение и основные требования стандартов информационной безопасности.
6	Работа с инцидентами информационной безопасности. Платформа реагирования на инциденты (IRP). Security Operational Center (SOC)	Система реагирования на инциденты информационной безопасности Организационная и техническая составляющая систем мониторинга и реагирования на инциденты
6	Работа с инцидентами информационной безопасности. Платформа реагирования на инциденты (IRP). Security Operational Center (SOC)	Аутсорсинг услуг информационной безопасности vs собственные подразделения Состав затрат на собственную систему информационной безопасности, преимущества и недостатки. Состав затрат на аутсорсинга информационной безопасности. Преимущества и недостатки. Расчет экономической целесообразности аутсорсинга. Сравнение с расходами на собственные подразделения информационной безопасности.

5.3. Самостоятельная работа обучающихся

№ разд	Наименование раздела дисциплины и темы	Содержание самостоятельной работы
1	Экономическая и информационная безопасность как необходимые условия существования предприятия	Управление рисками информационной безопасности Подготовка к практическим занятиям по теме. Выполнение заданий, подготовка к тестированию. Выполнение заданий курсового проекта.
2	Управление информационной безопасностью бизнеса	Распределение обязанностей по обеспечению информационной безопасности организации Подготовка к практическим занятиям, подготовка докладов, подготовка к тестированию
3	Криптография как основа защиты данных при хранении и передаче по каналам связи	Блокчейн Подготовка к практическим занятиям, подготовка докладов. Выполнение заданий курсового проекта.

3	Криптография как основа защиты данных при хранении и передаче по каналам связи	Системы электронного документооборота Изучение возможностей систем электронного документооборота по документации производителей. Подготовка к практическим занятиям. Выполнение заданий курсового проекта.
3	Криптография как основа защиты данных при хранении и передаче по каналам связи	История развития криптографических систем Подготовка к практическим занятиям. Выполнение заданий курсового проекта.
4	Системы защиты данных от утечек	Системы противодействия утечкам данных Подготовка к практическим занятиям, выполнение заданий, подготовка к тестированию
5	Стандарты информационной безопасности	Стандарты информационной безопасности Содержание стандартов информационной безопасности. Подготовка к практическим занятиям и тестированию. Выполнение заданий курсового проекта. Выполнение заданий курсового проекта.
6	Работа с инцидентами информационной безопасности. Платформа реагирования на инциденты (IRP). Security Operational Center (SOC)	Управление инцидентами информационной безопасности Выполнение заданий, подготовка к практическим занятиям и тестированию. Выполнение заданий курсового проекта.

6. Методические материалы для самостоятельной работы обучающихся по дисциплине (модулю)

Самостоятельную работу необходимо выполнять по всем разделам программы дисциплины в форме:

- изучения рекомендуемой основной и дополнительной литературы;
 - самостоятельных занятий по подбору и анализу литературных источников;
 - выполнению полученных на практических занятиях заданий, включая задания проектной работы;
 - поиска источников, сбора и анализа данных, расчетов, написания текста курсового проекта.
- Задания самостоятельной работы направлены в том числе на подготовку курсового проекта.

7. Оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине (модулю)

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины

№ п/п	Контролируемые разделы дисциплины (модуля)	Код и наименование индикатора контролируемой компетенции	Вид оценочного средства
1	Экономическая и информационная безопасность как необходимые условия существования предприятия	ОПК-1.1	Устный опрос, тесты, задания, доклады
2	Управление информационной безопасностью бизнеса	ОПК-1.1	Устный опрос, тесты, задания, доклады
3	Криптография как основа защиты данных при хранении и передаче по каналам связи	ОПК-1.1	Устный опрос, тесты, задания
4	Системы защиты данных от утечек	ОПК-1.1	Устный опрос, тесты, задания
5	Стандарты информационной безопасности	ОПК-1.1	Устный опрос, тесты
6	Работа с инцидентами информационной безопасности. Платформа реагирования на инциденты (IRP). Security Operational Center (SOC)	ОПК-1.1	Устный опрос, тесты, задания
7	Курсовой проект	ОПК-1.1	Курсовой проект. Устная защита
8	Зачет с оценкой	ОПК-1.1	Вопросы промежуточной аттестации (устный опрос)

7.2. Типовые контрольные задания или иные материалы текущего контроля успеваемости, необходимые для оценки знаний, умений и навыков и (или) опыта профессиональной деятельности, характеризующих этапы формирования компетенций в процессе освоения дисциплины

Групповые задания (проекты) для проверки сформированности индикаторов достижения компетенции ОПК-1.1.

Оцениваются знания, умения, навыки по разделам курса и наличие знаний для подготовки курсового проекта.

Групповое (индивидуальное по выбору студента) творческое задание для проверки сформированности индикаторов достижения компетенции ОПК-1.1.

Оцениваются знания, умения, навыки по разделам курса.

Вариант 1

Вы руководитель предприятия. Вам необходимо организовать процесс формирования «Перечня сведений конфиденциального характера». Сделайте описание бизнес-процесса.

Вариант 2

Вы руководитель предприятия. Вам необходимо организовать конфиденциальное делопроизводство. Сделайте описание бизнес-процесса.

Вариант 3

Вы руководитель предприятия. Вам необходимо организовать защиту коммерческой тайны. Сделайте описание бизнес-процесса.

Тестовые задания

(примеры тестовых заданий для проверки сформированности индикаторов достижения компетенции ОПК-1.1).

Оцениваются знания по разделам курса.

1. Безопасность информации (в соответствии с Руководящим документом "Защита от несанкционированного доступа к информации Термины и определения") — это:

- а) состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз;
- б) система управления защитой информации;
- в) последовательность действий по защите от угроз?

2. Какой документ является базовым в системе локальной документации компании по информационной безопасности:

- а) политика информационной безопасности;
- б) правила разделения доступа;
- в) регламент мониторинга инцидентов безопасности?

3. К какому типу рисков относятся риски информационной безопасности по классификации Базельского комитета по банковскому надзору:

- а) стратегический;
- б) операционный;
- в) ликвидности;
- г) рыночный?

4. Какое из перечисленных действий является первым этапом разработки системы информационной безопасности предприятия:

- а) выбор средств защиты;
- б) идентификация событий информационной безопасности;
- в) мониторинг событий информационной безопасности?

5. DLP системы предназначены для:

- а) выявления и предотвращения утечек данных;
- б) выявления и предотвращения заражения вирусами;
- в) выявления и предотвращения сетевых атак?

6. Совокупность правил, определяющих разрешения и запреты доступа к информационным ресурсам — это:

- а) уровень полномочий субъекта доступа;
- б) правила разделения доступа;
- в) модель защиты информационных ресурсов?

7. Возможность возникновения ущерба в результате нарушения информационной безопасности — это:

- а) уязвимость;
- б) атака;
- в) риск?

8. Какое свойство защищенной информации было нарушено, если вы видите

приблизительно следующий текст ошибки «сервис временно не работает, обратитесь . . .»:

- a) целостность;
- b) доступность;
- c) конфиденциальность;
- d) авторство документа?

9. Целью федерального закона о персональных данных является:

- обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;
- обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных.

10. Персональными данными, согласно закону о персональных данных, являются:

- любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), за исключением информации открытого доступа (общедоступные информационные ресурсы).

11. Трансграничная передача персональных данных — это:

- передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;
- передача персональных данных на территорию иностранного государства органу власти иностранного государства или иностранному юридическому лицу;
- передача персональных данных на территорию иностранного государства органу власти иностранного государства.

12. Доступность данных — это:

- состояние данных, при котором они могут быть беспрепятственно использованы любым сотрудником организации;
- состояние данных, при котором они могут быть беспрепятственно использованы любым сотрудником организации, имеющим соответствующее право доступа;
- отсутствие ошибок в данных.

13. Уязвимость информационной системы или программного продукта — это:

- слабое место;
- начавшая реализовываться атака;
- характеристика уровня безопасности информационной системы.

14. Наличие процесса управления уязвимостями, включая управление жизненным циклом программного обеспечения, patch management, pentesting является:

- необходимым, но недостаточным условием обеспечения безопасности персональных данных;
- необходимым и достаточным условием обеспечения безопасности персональных данных;
- не является необходимым и достаточным условием обеспечения безопасности персональных данных.

15. Неизменность информации в процессе ее передачи или хранения — это:

- целостность;
- конфиденциальность;
- аутентичность.

16. Федеральный закон «О персональных данных» принят:

- 27 июля 2006 года;
- 27 июня 2003 года;
- 19 мая 2010 года.

Проект «Построение концепции информационной безопасности предприятия»
(для проверки сформированности индикаторов достижения компетенции ОПК-1.1).
Оцениваются знания, умения по разделам курса.

1. Цель работы

Знакомство с основными принципами построения концепции ИБ предприятия с учетом особенностей его информационной инфраструктуры.

2. Краткие теоретические сведения

До начала создания систем информационной безопасности ряд отечественных нормативных документов (ГОСТ Р ИСО/МЭК 15408 ГОСТ Р ИСО/МЭК 27000 ГОСТ Р ИСО/МЭК 17799) и международных стандартов (ISO 27001/17799) прямо требуют разработки основополагающих документов – Концепции и Политики информационной безопасности. Если Концепция ИБ в общих чертах определяет, ЧТО необходимо сделать для защиты информации, то Политика детализирует положения Концепции, и говорит КАК, какими средствами и способами они должны быть реализованы.

Концепция информационной безопасности используется для:

- принятия обоснованных управленческих решений по разработке мер защиты информации;
- выработки комплекса организационно-технических и технологических мероприятий по выявлению угроз информационной безопасности и предотвращению последствий их реализации;
- координации деятельности подразделений по созданию, развитию и эксплуатации информационной системы с соблюдением требований обеспечения безопасности информации;
- и, наконец, для формирования и реализации единой политики в области обеспечения информационной безопасности.

3. Задание

Разработать концепцию информационной безопасности компании, содержащую следующие основные разделы. Приведен примерный план, который корректируется в зависимости от темы проекта и выбранного предприятия.

1. Общие положения

Назначение Концепции по обеспечению информационной безопасности.

1.2. Цели системы информационной безопасности

1.3. Задачи системы информационной безопасности.

2. Проблемная ситуация в сфере информационной безопасности

2.1. Объекты информационной безопасности.

2.2. Определение вероятного нарушителя.

2.3. Описание особенностей (профиля) каждой из групп вероятных нарушителей.

2.4. Основные виды угроз информационной безопасности Предприятия.

• Классификации угроз.

• Основные непреднамеренные искусственные угрозы.

• Основные преднамеренные искусственные угрозы.

2.5. Общестатистическая информация по искусственным нарушениям информационной безопасности.

2.6. Оценка потенциального ущерба от реализации угрозы.

3. Механизмы обеспечения информационной безопасности Предприятия

3.1. Принципы, условия и требования к организации и функционированию системы информационной безопасности.

3.2. Основные направления политики в сфере информационной безопасности.

3.3. Планирование мероприятий по обеспечению информационной безопасности

Предприятия.

3.4. Критерии и показатели информационной безопасности Предприятия.

4. Мероприятия по реализации мер информационной безопасности Предприятия

4.1. Организационное обеспечение информационной безопасности.

- Задачи организационного обеспечения информационной безопасности.
- Подразделения, занятые в обеспечении информационной безопасности.
- Взаимодействие подразделений, занятых в обеспечении информационной безопасности.

4.2. Техническое обеспечение информационной безопасности Предприятия.

- Общие положения.
- Защита информационных ресурсов от несанкционированного доступа.
- Средства комплексной защиты от потенциальных угроз.
- Обеспечение качества в системе безопасности.
- Принципы организации работ обслуживающего персонала.

4.3. Правовое обеспечение информационной безопасности Предприятия.

- Правовое обеспечение юридических отношений с работниками Предприятия.
- Правовое обеспечение юридических отношений с партнерами Предприятия.
- Правовое обеспечение применения электронной цифровой подписи.

4.4. Оценивание эффективности системы информационной безопасности Предприятия.

5. Программа создания системы информационной безопасности Предприятия

Задание по использованию системы противодействия утечкам данных

(для проверки сформированности индикаторов достижения компетенции ОПК-1.1).

2.1. Изменение расписания. Отчеты по учету рабочего времени.

2.1.1. Сделать отчет "Комбинированный отчет", меню "Учет рабочего времени.

2.1.2. Сделать развернутый отчет по одному из пользователей (левая кнопка мыши на имени компьютера).

Зафиксировать продуктивность или непродуктивность работы в каком-либо приложении или на сайте.

2.1.3. Изменить категорию продуктивности приложения или сайта (Фильтры - Политики - Политики продуктивности - категории приложений или категории веб-ресурсов).

2.1.4. Проявить активность в приложении / веб-ресурсе, по которому была изменена категория продуктивности (новая категория продуктивности применяется только для новых событий).

2.1.5. Сделать отчет "Комбинированный отчет", меню "Учет рабочего времени, убедившись в изменении категоризации активности с продуктивной на непродуктивную или наоборот.

2.1.6. Создать рабочее расписание (Админ - Рабочее расписание).

2.1.7. Назначить созданное рабочее расписание компьютеру, за которым Вы работаете (Админ - Назначение расписания).

2.1.8. Сделать отчет "Комбинированный отчет", меню "Учет рабочего времени, убедившись в изменении параметров расписания.

В отчет:

- отчет до изменения категории продуктивности и расписания;
- отчет после изменения категории продуктивности;
- отчет после изменения расписания.

Темы докладов

(для проверки сформированности индикаторов достижения компетенции ОПК-1.1).

Оцениваются знания, умения по разделам курса.

1. Информация как правовая категория: понятие и основные критерии классификации.
2. Правовые режимы информации: понятие и виды.
3. Правовые режимы ограниченного доступа к информации: понятие и общая характеристика.
4. Тайна и ее разновидности.
5. Понятие и виды конфиденциальной информации.
6. Государственная тайна.
7. Признаки сведений, составляющих государственную тайну.
8. Гриф секретности: понятие и порядок использования.
9. Правовой режим носителей сведений, составляющих государственную тайну.
10. Допуск к государственной тайне.

11. Доступ к сведениям, составляющим государственную тайну.
12. Основания и порядок отнесения сведений к государственной тайне.
13. Основания и порядок рассекречивания сведений, составляющих государственную тайну.
14. Коммерческая тайна.
15. Особенности правовой охраны конфиденциальности информации в рамках трудовых отношений.
16. Банковская тайна.
17. Служебная тайна.
18. Адвокатская тайна.
19. Аудиторская тайна.
20. Врачебная тайна.
21. Медицинская тайна.
22. Налоговая тайна.
23. Нотариальная тайна.
24. Тайна связи.
25. Тайна совещания судей.
26. Тайна совещания присяжных заседателей.
27. Тайна страхования.
28. Тайна усыновления (удочерения).
29. Правовой режим инсайдерской информации.
30. Правовой режим данных предварительного расследования.
31. Правовой режим сведений о государственной регистрации актов гражданского состояния.
32. Правовой режим сведений о защищаемом лице.
33. Признаки сведений, составляющих тайну завещания.
34. Признаки сведений, составляющих профессиональную тайну ломбардов.
35. Правовой режим сведений о сущности изобретения.
36. Особенности правового режима сведений, составляющих секретное изобретение.
37. Правовой режим сведений о сущности полезной модели.
38. Правовой режим сведений о сущности промышленного образца.
39. Особенности правового режима сведений, составляющих секрет производства (ноу-хау).
40. Особенности правового режима сведений, составляющих секрет производства (ноу-хау).
41. Особенности правового режима сведений, составляющих служебный секрет производства (ноу-хау).
42. Ответственность за нарушение законодательства Российской Федерации о государственной тайне.
43. Ответственность за нарушение законодательства Российской Федерации о коммерческой тайне.
44. Ответственность за разглашение сведений, составляющих банковскую тайну.
45. Правовой режим массовой информации.
46. Средства массовой информации: понятие и виды.
47. Особенности правового статуса информационного агентства.
48. Правовой статус учредителя средства массовой информации.
49. Правовой статус главного редактора.
50. Правовой статус журналиста.
51. Правовой статус зарубежного корреспондента.
52. Ответственность за нарушение законодательства о средствах массовой информации.
53. Правовой режим персональных данных.
54. Условия обработки персональных данных.
55. Биометрические персональные данные.
56. Права субъекта персональных данных.
57. Ответственность за нарушение законодательства Российской Федерации о персональных данных.

58. Правовой статус библиотеки.
59. Особенности правового режима библиотечных фондов.
60. Архив: понятие и виды.
61. Архивный документ: понятие и виды.
62. Правовые режимы доступа к архивным документам.
63. Особенности правового регулирования использования сети «Интернет».
64. Правовой статус владельца сайта в сети "Интернет".
65. Правовой статус провайдера хостинга.
66. Понятие информационной безопасности Российской Федерации.
67. Система обеспечения информационной безопасности Российской Федерации.
68. Государственный надзор в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию.
69. Уголовная ответственность за преступления в информационной сфере.
70. Административно-правовая ответственность за правонарушения в информационной сфере.
71. Качество управления информационными активами как существенный фактор обеспечения прибыльности бизнеса.
72. Место информационной безопасности в иерархии рисков бизнеса.
73. Влияние качества информации на результаты работы предприятия и качество его администрирования.
74. Роль высшего руководства компании в обеспечении информационной безопасности. Связь системы менеджмента информационной безопасности с системой менеджмента компании.
75. Роль мониторинга в обеспечении информационной безопасности.
76. Процедура проведения аудита на соответствие регуляторным требованиям в области защиты персональных данных.
77. Понятие и классификация информационных систем персональных данных.
78. Инвентаризация информационных ресурсов.
79. Обзор систем защиты информационных активов.
80. Системы защиты данных от утечек.
81. Средства защиты конфиденциальных данных от несанкционированного доступа при передаче и хранении.
82. Обезличивание данных: причины и способы.
83. Выявление актуальных угроз безопасности конфиденциальных данных.
84. Методы оценки экономической целесообразности внедрения средств защиты данных.
85. Каналы утечки конфиденциальных данных: анализ современной ситуации.
86. Организация системы защиты данных на предприятии.
87. Разработка требований к системе информационной безопасности.
88. Состав затрат на разработку (приобретение) и внедрение системы защиты данных.

7.3. Система оценивания результатов обучения по дисциплине (модулю) при проведении текущего контроля успеваемости

<p>Оценка «отлично» (зачтено)</p>	<p>знания: - систематизированные, глубокие и полные знания по всем разделам дисциплины, а также по основным вопросам, выходящим за пределы учебной программы; - точное использование научной терминологии, систематически грамотное и логически правильное изложение ответа на вопросы; - полное и глубокое усвоение основной и дополнительной литературы, рекомендованной рабочей программой по дисциплине (модулю)</p> <p>умения: - умеет ориентироваться в теориях, концепциях и направлениях дисциплины и давать им критическую оценку, используя научные достижения других дисциплин</p> <p>навыки: - высокий уровень сформированности заявленных в рабочей программе компетенций; - владеет навыками самостоятельно и творчески решать сложные проблемы и нестандартные ситуации; - применяет теоретические знания для выбора методики выполнения заданий; - грамотно обосновывает ход решения задач; - безупречно владеет инструментарием учебной дисциплины, умение его эффективно использовать в постановке научных и практических задач; - творческая самостоятельная работа на практических/семинарских/лабораторных занятиях, активно участвует в групповых обсуждениях, высокий уровень культуры исполнения заданий</p>
<p>Оценка «хорошо» (зачтено)</p>	<p>знания: - достаточно полные и систематизированные знания по дисциплине; - усвоение основной и дополнительной литературы, рекомендованной рабочей программой по дисциплине (модулю)</p> <p>умения: - умеет ориентироваться в основных теориях, концепциях и направлениях дисциплины и давать им критическую оценку; - использует научную терминологию, лингвистически и логически правильно излагает ответы на вопросы, умеет делать обоснованные выводы; - владеет инструментарием по дисциплине, умение его использовать в постановке и решении научных и профессиональных задач</p> <p>навыки: - самостоятельная работа на практических занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий; - средний уровень сформированности заявленных в рабочей программе компетенций; - без затруднений выбирает стандартную методику выполнения заданий; - обосновывает ход решения задач без затруднений</p>

<p>Оценка «удовлетворительно» (зачтено)</p>	<p>знания: - достаточный минимальный объем знаний по дисциплине; - усвоение основной литературы, рекомендованной рабочей программой; - использование научной терминологии, стилистическое и логическое изложение ответа на вопросы, умение делать выводы без существенных ошибок умения: - умеет ориентироваться в основных теориях, концепциях и направлениях по дисциплине и давать им оценку; - владеет инструментарием учебной дисциплины, умение его использовать в решении типовых задач; - умеет под руководством преподавателя решать стандартные задачи навыки: - работа под руководством преподавателя на практических занятиях, допустимый уровень культуры исполнения заданий; - достаточный минимальный уровень сформированности заявленных в рабочей программе компетенций; - испытывает затруднения при обосновании алгоритма выполнения заданий</p>
<p>Оценка «неудовлетворительно» (не зачтено)</p>	<p>знания: - фрагментарные знания по дисциплине; - отказ от ответа (выполнения письменной работы); - знание отдельных источников, рекомендованных рабочей программой по дисциплине; умения: - не умеет использовать научную терминологию; - наличие грубых ошибок навыки: - низкий уровень культуры исполнения заданий; - низкий уровень сформированности заявленных в рабочей программе компетенций; - отсутствие навыков самостоятельной работы; - не может обосновать алгоритм выполнения заданий</p>

7.4. Теоретические вопросы и практические задания для проведения промежуточной аттестации обучающихся, необходимые для оценки знаний, умений и навыков и (или) опыта профессиональной деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

7.4.1. Теоретические вопросы для проведения промежуточной аттестации обучающихся

Примерный перечень вопросов по разделу 1

1. Предмет и методы информационного права.
2. Принципы информационного права.
3. Система и источники информационного права.
4. Информация как правовая категория: понятие и основные критерии классификации.
5. Информационные правоотношения: понятие, признаки и виды.
6. Содержание информационных правоотношений.
7. Понятие и виды документов.
8. Нормы информационного права и их действие в пространстве и во времени.
9. Правовые режимы информации: понятие и виды.
10. Правовые режимы ограниченного доступа к информации: понятие и общая характеристика.
11. Тайна и ее разновидности.
12. Средства защиты информации.
13. Понятие и виды конфиденциальной информации.
14. Государственная тайна.
15. Признаки сведений, составляющих государственную тайну.

16. Степени секретности сведений, составляющих государственную тайну.
17. Гриф секретности: понятие и порядок использования.
18. Правовой режим носителей сведений, составляющих государственную тайну.
19. Допуск к государственной тайне.
20. Доступ к сведениям, составляющим государственную тайну.
21. Основания и порядок отнесения сведений к государственной тайне.
22. Основания и порядок рассекречивания сведений, составляющих государственную тайну.
23. Коммерческая тайна.
24. Признаки сведений, составляющих коммерческую тайну.
25. Гриф «Коммерческая тайна»: понятие и порядок использования.
26. Сведения, которые не могут составлять коммерческую тайну.
27. Понятие разглашения информации, составляющей коммерческую тайну.
28. Особенности правовой охраны конфиденциальности информации в рамках трудовых отношений.
29. Банковская тайна.
30. Признаки сведений, составляющих банковскую тайну.
31. Служебная тайна.
32. Адвокатская тайна.
33. Аудиторская тайна.
34. Врачебная тайна.
35. Медицинская тайна.
36. Налоговая тайна.
37. Нотариальная тайна.
38. Тайна связи.
39. Тайна совещания судей.
40. Тайна совещания присяжных заседателей.
41. Тайна страхования.
42. Тайна усыновления (удочерения).
43. Правовой режим инсайдерской информации.
44. Правовой режим данных предварительного расследования.
45. Правовой режим сведений о государственной регистрации актов гражданского состояния.
46. Правовой режим сведений о защищаемом лице.
47. Признаки сведений, составляющих тайну завещания.
48. Признаки сведений, составляющих профессиональную тайну ломбардов.
49. Правовой режим сведений о сущности изобретения.
50. Особенности правового режима сведений, составляющих секретное изобретение.
51. Правовой режим сведений о сущности полезной модели.
52. Правовой режим сведений о сущности промышленного образца.
53. Особенности правового режима сведений, составляющих секрет производства (ноу-хау).
54. Понятие электронного документа.
55. Электронная подпись и ее виды.
56. Ответственность за нарушение законодательства Российской Федерации о государственной тайне.
57. Ответственность за нарушение законодательства Российской Федерации о коммерческой тайне.
58. Ответственность за непредоставление органам государственной власти и органам местного самоуправления информации, составляющей коммерческую тайну.
59. Ответственность за разглашение сведений, составляющих банковскую тайну.
60. Правовой режим массовой информации.
61. Понятие массовой информации.
62. Цензура массовой информации.
63. Средства массовой информации: понятие и виды.
64. Особенности правового статуса информационного агентства.

65. Правовой статус учредителя средства массовой информации.
66. Правовой статус главного редактора.
67. Правовой статус журналиста.
68. Правовой статус зарубежного корреспондента.
69. Аккредитация журналиста.
70. Понятие злоупотребления свободой массовой информации.
71. Ответственность за нарушение законодательства о средствах массовой информации.
72. Правовой режим персональных данных.
73. Понятие обработки персональных данных.
74. Принципы обработки персональных данных.
75. Условия обработки персональных данных.
76. Биометрические персональные данные.
77. Права субъекта персональных данных.
78. Обязанности оператора при сборе персональных данных.
79. Ответственность за нарушение законодательства Российской Федерации о персональных данных.
80. Правовой статус библиотеки.
81. Особенности правового режима библиотечных фондов.
82. Архив: понятие и виды.
83. Архивный документ: понятие и виды.
84. Правовые режимы доступа к архивным документам.
85. Особенности правового регулирования использования сети «Интернет».
86. Понятие сайта в сети "Интернет".
87. Понятие страницы сайта в сети "Интернет".
88. Понятие доменного имени.
89. Правовой статус владельца сайта в сети "Интернет".
90. Правовой статус провайдера хостинга.
91. Понятие информационной безопасности Российской Федерации.
92. Национальные интересы Российской Федерации в информационной сфере.
93. Виды угроз информационной безопасности Российской Федерации.
94. Правовые методы обеспечения информационной безопасности Российской Федерации.
95. Система обеспечения информационной безопасности Российской Федерации.
96. Понятие информационной безопасности детей.
97. Государственный надзор в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию.
98. Защита информации как правовая категория.
99. Уголовная ответственность за преступления в информационной сфере.
100. Административно-правовая ответственность за правонарушения в информационной сфере.

Примерный перечень вопросов по разделу 2

1. Бизнес и информация. Информационная сущность бизнеса.
2. Риск-ориентированный подход к обеспечению информационной безопасности бизнеса.
3. Назначение и общая характеристика DLP-систем.
4. Назначение и общая характеристика SIEM-систем.
5. Назначение и общая характеристика Threat Intelligence.
6. Системы шифрования как средство обеспечения защиты от несанкционированного доступа при хранении и передаче данных.
7. Электронно-цифровая подпись. Обеспечение целостности и подтверждения авторства.
8. Алгоритм формирования и проверки электронной цифровой подписи на примере системы PGP.
9. Комплексный подход к обеспечению информационной безопасности.
10. Безопасность как специфическая совокупность условий деятельности.
11. Основные положения стандарта Банка России СТО/РС БР ИББС.

12. Основные положения стандарта PCI DSS.
13. Организация системы безопасности и субъекты обеспечения безопасности предприятия.
14. Основные виды угроз безопасности. Обстоятельства, способы и субъекты их реализации.
15. Организация мониторинга информационной безопасности.
16. Безопасность мобильных приложений.
17. Особенности обеспечения безопасности облачных сервисов.
18. Модель непрерывного совершенствования информационной безопасности.
19. Реализация процессного подхода к обеспечению информационной безопасности.
20. Характеристика системы стандартов СМИБ.
21. Этапы разработки системы менеджмента информационной безопасности.
22. Структура частных менеджментов информационной безопасности.
23. Взаимосвязь менеджмента инцидентов и мониторинга информационной безопасности.
24. Основные положения методологии ITIL.
25. Спецификация процессов комплекса документов стандарта COBIT.
26. Экономическая эффективность внедрения средств обеспечения информационной безопасности.
27. SOC. Понятие. Назначение. Общая характеристика.
28. Цикл Деминга-Шухарта в управлении информационной безопасностью.
29. Система рисков предприятия и место рисков информационной безопасности в данной системе.
30. Понятие процессов и проектов применительно к информационной безопасности.
31. Подразделения, участвующие в реализации функций информационной безопасности и их взаимодействие.
32. Организация взаимодействия подразделений информационных технологий и информационной безопасности.
33. Адаптивные технологии управления информационной безопасностью.
34. Причины мотивации сотрудников предприятия к нарушению информационной безопасности.
35. Мотивация сотрудников предприятия к активному участию в разработке и поддержанию эксплуатации мер информационной безопасности.
36. Влияние корпоративной культуры на мотивацию сотрудников в области информационной безопасности.
37. Процесс отбора претендентов на должности офицеров информационной безопасности.
38. Требования к офицерам информационной безопасности.
39. Организация обучения сотрудников компании по информационной безопасности.
40. Взаимодействие компании с регулирующими органами по информационной безопасности.
41. Проектирование SOC.
42. Мониторинг событий информационной безопасности.
43. Организация работы с инцидентами информационной безопасности.
44. Аутсорсинг информационной безопасности.
45. Расчет затрат на внедрение SOC.
46. Текущие тенденции и перспективы развития систем обеспечения информационной безопасности.
47. Профессиональные сообщества в области информационной безопасности: характеристика, функции.
48. Обзор наиболее значимых в РФ компаний, оказывающих услуги в области информационной безопасности.
49. Анализ статистики по наиболее актуальным угрозам информационной безопасности.
50. Наиболее значимые хакерские преступные группировки: характеристика деятельности, примеры инцидентов.
51. Примеры веерных атак на информационные ресурсы.
52. Примеры целевых атак на информационные ресурсы.
53. Международное сотрудничество в области информационной безопасности.

54. Особенности финансовых организаций при обеспечении информационной безопасности.
55. Особенности защиты объектов критической информационной инфраструктуры.
56. Особенности защиты государственных и муниципальных предприятий.
57. Требования к средствам криптографической защиты информации.
58. Информационная безопасность как фактор повышения операционной эффективности компании.
59. Регулирование информационной безопасности — обзор нормативно-правовой базы.
60. Место информационной безопасности в процессах цифровизации предприятий.

Примерный перечень вопросов по разделу 3

1. Функции оператора персональных данных.
2. Ответственность за нарушения в области информационной безопасности
3. Условия обработки персональных данных (согласно закону о персональных данных).
4. Состав внутренних документов компании по организации защиты конфиденциальных данных.
5. Особенности обработки персональных данных уволенных работников.
6. Особенности обработки персональных данных соискателей на замещение вакантных должностей.
7. Избыточность обработки персональных данных.
8. Назначение и характеристика модели угроз.
9. Расчет затрат на внедрение и использование системы защиты данных.
10. Направления сокращения затрат на создание системы защиты данных.
11. Особенности защиты данных от утечек.
12. Методика выбора мер по обеспечению безопасности данных.
13. Характеристика видов угроз безопасности данных.
14. Классификация средств защиты данных.
15. Обязанности оператора при обработке персональных данных.
16. Меры обеспечения безопасной обработки данных.
17. Уведомление об обработке персональных данных.
18. Права субъектов персональных данных.
19. Согласие субъекта персональных данных на обработку персональных данных.
20. Специальные категории персональных данных.
21. Характеристика биометрических персональных данных.
22. Принципы обработки конфиденциальных данных.
23. Требования к обучению сотрудников в области защиты персональных данных.
24. Цикл Деминга в организации защиты персональных данных.
25. Интеграция системы защиты персональных данных в систему информационной безопасности компании.
26. Документы ФСТЭК в области защиты персональных данных.
27. Проверки Роскомнадзора в области защиты данных.
28. Управление инцидентами информационной безопасности.
29. Банк данных угроз информационной безопасности персональных данных.
30. Политика обработки персональных данных — содержание документа.
31. Модель угроз информационной безопасности — содержание документа.
32. Методические указания Роскомнадзора по защите персональных данных (для субъектов персональных данных).
33. Конфликт требований законодательства по защите персональных данных и использования систем мониторинга работы сотрудников.
34. Положения Конституции РФ, связанные с защитой персональных данных.
35. Основные положения GDPR.
36. Способы незаконного использования персональных данных. Примеры.
37. Кибербуллинг: характеристика, примеры.
38. Источники утечек персональных данных.
39. История развития законодательной базы защиты персональных данных в РФ.
40. Зарубежное законодательство по защите персональных данных.

41. Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных.
42. Определение персональных данных: 152 ФЗ, Трудовой Кодекс, GDPR, др.
43. Документы Правительства РФ в области защиты персональных данных.
44. Обезличивание персональных данных — понятие, требования законодательства, методы обезличивания.
45. Характеристика рынка персональных данных: участники, цели приобретения персональных данных.
46. Примеры утечек персональных данных в РФ.
47. Примеры утечек персональных данных за пределами РФ.
48. Трансграничная передача персональных данных.
49. Особенности обработки персональных данных в государственных и муниципальных системах персональных данных.
50. Биометрические персональные данные.
51. Характеристика правовых (нормативных), организационных и технических мер защиты конфиденциальных данных. Примеры.
52. Уровни защищенности персональных данных.
53. Обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных (статья 21 главы 4 ФЗ-152).
54. Обязанности лица, ответственного за организацию обработки персональных данных.
55. Государственный контроль и надзор в области защиты персональных данных.
56. Ответственность, предусмотренная за нарушение законодательства в области защиты персональных данных.
57. Роскомнадзор — цели, задачи, функции.
58. Значение персонала компании как субъекта угроз безопасности персональных данных.

7.4.2. Практические задания для проведения промежуточной аттестации обучающихся

Примеры практических заданий

1. Разработать схему бизнес-процесса управления инцидентами информационной безопасности для предприятия. В описании задания привести характеристику предприятия: вид деятельности, масштаб, географическая распределенность подразделений, подразделения, участвующие в управлении инцидентами.
2. Продемонстрировать последовательность действий в интерфейсе StaffCop по созданию фильтра для поиска событий, связанных с определенным документом. Ограничить период времени (по датам), каналы передачи информации.
3. Создать интеллектуальную карту в сервисе Miro по теме "Управление операционными рисками".
4. Создать интеллектуальную карту в сервисе Miro по классификации угроз информационной безопасности. В описании задания привести характеристику предприятия.
5. Определить уровень защищенности и требования к защите для выбранного Вами предприятия. В описании задания привести характеристику предприятия.

7.4.3. Примерные темы курсовой работы (проекта) (при наличии)

Примерные темы курсового проекта

1. Идентификация и аутентификация пользователей, не являющихся сотрудниками организации.
2. Управление доступом к конфиденциальным данным.
3. Нормативно-правовые основы защиты персональных данных в РФ.
4. Протокол Европейского союза по защите персональных данных.
5. Законодательство США по защите персональных данных.
6. Использование блокчейн для защиты конфиденциальных данных.
7. Управление информационной безопасностью на базе ISO/IEC 27001.
8. Меры защиты информации согласно ISO/IEC 27002.
9. Политика информационной безопасности как ключевой локальный нормативный акт по защите данных.

10. Организация защиты персональных данных на предприятии.
11. Данные как основной ресурс цифровой экономики.
12. Политика Facebook (другой социальной сети по выбору студента) в области защиты персональных данных.
13. Анализ мировой индустрии торговли персональными данными.
14. Управление инцидентами информационной безопасности.
15. Назначение и функции DLP-систем.
16. Анализ российского рынка DLP-систем.
17. Характеристика основных угроз информационной безопасности в 2020 году.
18. Способы обезличивания персональных данных.
19. Брокеры данных - Data Brokers (Acxiom, Equifax, CoreLogic, др.).
20. Характеристика действующих в РФ хакерских группировок.
21. Характеристика индустрии защиты данных в РФ.
22. Мошенничество с электронной подписью в РФ.
23. Судебная практика по преступлениям, связанным с компрометацией конфиденциальных данных.
24. Последствия реализации рисков информационной безопасности для предприятия.
25. Последствия компрометации персональных данных для гражданина.
26. Рекомендации для гражданина по защите персональных данных.
27. Цифровой профиль гражданина РФ.
28. Цифровые государственные сервисы (на примере любой страны по выбору обучающегося).
29. Единая система биометрической идентификации в РФ.
30. Локальная нормативная база предприятия в области обеспечения безопасности персональных данных (состав и структура документов).

7.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта профессиональной деятельности, характеризующие этапы формирования компетенций

Процедура проведения промежуточной аттестации и текущего контроля успеваемости регламентируется локальным нормативным актом, определяющим порядок организации и проведения текущего контроля успеваемости и промежуточной аттестации обучающихся. Процедура оценивания формирования компетенций при проведении текущего контроля приведена в п. 7.3. Типовые контрольные задания или иные материалы текущего контроля приведены в п. 7.2. Промежуточная аттестация по дисциплине проводится в форме зачета с оценкой. Зачет с оценкой проводится в устной форме.

7.6. Критерии оценивания сформированности компетенций при проведении промежуточной аттестации

Критерии оценивания	Уровень освоения и оценка			
	Оценка «неудовлетворительно»	Оценка «удовлетворительно»	Оценка «хорошо»	Оценка «отлично»
	«не зачтено»	«зачтено»		

	<p>Уровень освоения компетенции «недостаточный». Компетенции не сформированы. Знания отсутствуют, умения и навыки не сформированы</p>	<p>Уровень освоения компетенции «пороговый». Компетенции сформированы. Сформированы базовые структуры знаний. Умения фрагментарны и носят репродуктивный характер. Демонстрируется низкий уровень самостоятельности практического навыка.</p>	<p>Уровень освоения компетенции «продвинутый». Компетенции сформированы. Знания обширные, системные. Умения носят репродуктивный характер, применяются к решению типовых заданий. Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка.</p>	<p>Уровень освоения компетенции «высокий». Компетенции сформированы. Знания аргументированные, всесторонние. Умения успешно применяются к решению как типовых, так и нестандартных творческих заданий. Демонстрируется высокий уровень самостоятельности, высокая адаптивность практического навыка</p>
знания	<p>Обучающийся демонстрирует: -существенные пробелы в знаниях учебного материала; -допускаются принципиальные ошибки при ответе на основные вопросы билета, отсутствует знание и понимание основных понятий и категорий; -непонимание сущности дополнительных вопросов в рамках заданий билета.</p>	<p>Обучающийся демонстрирует: -знания теоретического материала; -неполные ответы на основные вопросы, ошибки в ответе, недостаточное понимание сущности излагаемых вопросов; -неуверенные и неточные ответы на дополнительные вопросы.</p>	<p>Обучающийся демонстрирует: -знание и понимание основных вопросов контролируемого объема программного материала; - знания теоретического материала -способность устанавливать и объяснять связь практики и теории, выявлять противоречия, проблемы и тенденции развития; -правильные и конкретные, без грубых ошибок, ответы на поставленные вопросы.</p>	<p>Обучающийся демонстрирует: -глубокие, всесторонние и аргументированные знания программного материала; -полное понимание сущности и взаимосвязи рассматриваемых процессов и явлений, точное знание основных понятий, в рамках обсуждаемых заданий; -способность устанавливать и объяснять связь практики и теории, -логически последовательные, содержательные, конкретные и исчерпывающие ответы на все задания билета, а также дополнительные вопросы экзаменатора.</p>

<p>умения</p>	<p>При выполнении практического задания билета обучающийся продемонстрировал недостаточный уровень умений. Практические задания не выполнены. Обучающийся не отвечает на вопросы билета при дополнительных наводящих вопросах преподавателя.</p>	<p>Обучающийся выполнил практическое задание билета с существенными неточностями. Допускаются ошибки в содержании ответа и решении практических заданий. При ответах на дополнительные вопросы было допущено много неточностей.</p>	<p>Обучающийся выполнил практическое задание билета с небольшими неточностями. Показал хорошие умения в рамках освоенного учебного материала. Предложенные практические задания решены с небольшими неточностями. Ответил на большинство дополнительных вопросов.</p>	<p>Обучающийся правильно выполнил практическое задание билета. Показал отличные умения в рамках освоенного учебного материала. Решает предложенные практические задания без ошибок. Ответил на все дополнительные вопросы.</p>
<p>владение навыками</p>	<p>Не может выбрать методику выполнения заданий. Допускает грубые ошибки при выполнении заданий, нарушающие логику решения задач. Делает некорректные выводы. Не может обосновать алгоритм выполнения заданий.</p>	<p>Испытывает затруднения по выбору методики выполнения заданий. Допускает ошибки при выполнении заданий, нарушения логики решения задач. Испытывает затруднения с формулированием корректных выводов. Испытывает затруднения при обосновании алгоритма выполнения заданий.</p>	<p>Без затруднений выбирает стандартную методику выполнения заданий. Допускает ошибки при выполнении заданий, не нарушающие логику решения задач. Делает корректные выводы по результатам решения задачи. Обосновывает ход решения задач без затруднений.</p>	<p>Применяет теоретические знания для выбора методики выполнения заданий. Не допускает ошибок при выполнении заданий. Самостоятельно анализирует результаты выполнения заданий. Грамотно обосновывает ход решения задач.</p>

Оценка по дисциплине зависит от уровня сформированности компетенций, закрепленных за дисциплиной, и представляет собой среднее арифметическое от выставленных оценок по отдельным результатам обучения (знания, умения, владение навыками).

Оценка «отлично»/«зачтено» выставляется, если среднее арифметическое находится в интервале от 4,5 до 5,0.

Оценка «хорошо»/«зачтено» выставляется, если среднее арифметическое находится в интервале от 3,5 до 4,4.

Оценка «удовлетворительно»/«зачтено» выставляется, если среднее арифметическое находится в интервале от 2,5 до 3,4.

Оценка «неудовлетворительно»/«не зачтено» выставляется, если среднее арифметическое находится в интервале от 0 до 2,4.

8. Учебно-методическое и материально-техническое обеспечение дисциплины (модуля)

8.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины (модуля)

№ п/п	Автор, название, место издания, издательство, год издания учебной и учебно-методической литературы	Количество экземпляров/электронный адрес ЭБС
<u>Основная литература</u>		
1	Суворова Г. М., Информационная безопасность, Москва: Юрайт, 2024	https://urait.ru/bcode/544029
<u>Дополнительная литература</u>		
1	Зенков А. В., Информационная безопасность и защита информации, Москва: Юрайт, 2024	https://urait.ru/bcode/544290
<u>Учебно-методическая литература</u>		
1	Сафонова Л. А., Экономические аспекты информационной безопасности, Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2019	http://www.iprbookshop.ru/90606.html

Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечиваются печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

8.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Наименование ресурса сети «Интернет»	Электронный адрес ресурса
Российская газета	http://www.rg.ru
Информационная безопасность: рынок России	https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_(%D1%80%D1%8B%D0%BD%D0%BE%D0%BA_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8)
Курс "Основы информационной безопасности"	https://intuit.ru/studies/courses/10/10/info
Официальный сайт компании "Атом-безопасность"	https://www.staffcop.ru/

8.3. Перечень современных профессиональных баз данных и информационных справочных систем

Наименование	Электронный адрес ресурса
Образовательные интернет-ресурсы СПбГАСУ	https://www.spbgasu.ru/university/obrazovatelnye-internet-resursy/
Журналы издательства Sage. В настоящее время доступны статьи из 320 журналов по 36 предметным рубрикам: гуманитарные и общественные науки, информатика, инженерные дисциплины, экономика, здоровье и образование.	www.sagepublications.com
Библиотека по Естественным наукам Российской Академии наук (РАН)	www.ras.ru

Аналитический портал по экономическим дисциплинам	www.economicus.ru
Научная электронная библиотека eLIBRARY.RU	https://www.elibrary.ru/
Электронно-библиотечная система издательства "Консультант студента"	https://www.studentlibrary.ru/
Электронно-библиотечная система издательства "IPRsmart"	http://www.iprbookshop.ru/
Электронно-библиотечная система издательства "ЮРАЙТ"	https://www.biblio-online.ru/
Электронно-библиотечная система издательства "Лань"	https://e.lanbook.com/
Электронная библиотека Ирбис 64	http://ntb.spbgasu.ru/irbis64r_plus/
Система дистанционного обучения СПбГАСУ Moodle	https://moodle.spbgasu.ru/
Информационно-правовая база данных Кодекс	http://gasudata.lan.spbgasu.ru/docs/
Информационно-правовая система Консультант	https://student2.consultant.ru/cgi/online.cgi?req=home;rnd=0.34403827862102354
Информационно-правовая система Гарант	https://www.garant.ru/products/ipo/

8.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного и свободно распространяемого программного обеспечения

Наименование	Способ распространения (лицензионное или свободно распространяемое)
LibreOffice	Свободно распространяемое

8.5. Материально-техническое обеспечение дисциплины

Сведения об оснащённости учебных аудиторий и помещений для самостоятельной работы

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащённость оборудованием и техническими средствами обучения
68. Учебные аудитории для проведения лекционных занятий	Учебная аудитория для проведения занятий лекционного типа, комплект мультимедийного оборудования (персональный компьютер, мультимедийный проектор, экран, аудиосистема), доска, экран, комплект учебной мебели, подключение к компьютерной сети СПбГАСУ, выход в Интернет
68. Помещения для самостоятельной работы	Помещение для самостоятельной работы (читальный зал библиотеки, ауд. 217): ПК-23 шт., в т.ч. 1 шт.- ПК для лиц с ОВЗ (системный блок, монитор, клавиатура, мышь) с подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду СПбГАСУ.
68. Компьютерный класс	Рабочие места с ПК (стол компьютерный, системный блок, монитор, клавиатура, мышь), стол рабочий, подключение к компьютерной сети СПбГАСУ, выход в Internet.
68. Учебные аудитории для проведения практических занятий, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Комплект мультимедийного оборудования (персональный компьютер, мультимедийный проектор, экран, аудиосистема), доска, комплект учебной мебели, подключение к компьютерной сети СПбГАСУ, выход в Интернет.

Для инвалидов и лиц с ОВЗ обеспечиваются специальные условия для получения образования в соответствии с требованиями нормативно-правовых документов.

Рабочая программа составлена на основе ФГОС ВО - магистратура по направлению подготовки 38.04.05 Бизнес-информатика (приказ Минобрнауки России от 12.08.2020 № 990).

Программу составил:

доцент ЭБ, к. э. н. Дурандина Анна Павловна

Программа обсуждена и рекомендована на заседании кафедры Экономической безопасности 26.08.2024, протокол № 01

Заведующий кафедрой к.ю.н., д.э.н., профессор А. К. Моденов

Программа одобрена на заседании учебно-методической комиссии факультета 19.09.2024, протокол № 02.

Председатель УМК д.э.н., профессор Г.Ф. Токунова