АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
ИНСТИТУТ СОЦИАЛЬНЫХ НАУК

ДЕПАРТАМЕНТ ЭКОНОМИКИ, УПРАВЛЕНИЯ, МЕНЕДЖМЕНТА И БИЗНЕС-ИНФОРМАТИКИ

УТВЕРЖДАЮ
Ректор _____
Бианкина А.О.
Протокол № 1- от 19.01.2026 г.

ПРОГРАММА БАКАЛАВРИАТ

Бизнес-аналитика
(наименование образовательной программы)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ,

Б1.О.02.02 «Основы национальной безопасности»
(код и наименование РПД)

38.03.05 «Бизнес-информатика»
(код, наименование направления подготовки специальности)

очная форма обучения
(форма обучения)

Год набора – 2026

г. Москва, 2026 г.

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы

1.1. Дисциплина Б1.В.ДВ.04.01 «Основы информационной безопасности» обеспечивает овладение следующими компетенциями:

Код компетенции	Наименование компетенции	Код компонента компетенции	Наименование компонента компетенции
ПКс-10	Способен выполнять технико-экономическое обоснование проектов по совершенствованию и регламентации бизнес-процессов и ИТ-инфраструктуры предприятия		
ПКс-10	Способен выполнять технико-экономическое обоснование проектов по совершенствованию и регламентации бизнес-процессов и ИТ-инфраструктуры предприятия		
ПКс-12	Способен осуществлять планирование и организацию проектной деятельности на основе стандартов управления проектами с учетом информационной безопасности		
ПКс-12	Способен осуществлять планирование и организацию проектной деятельности на основе стандартов управления проектами с учетом информационной безопасности		

1.2. В результате освоения дисциплины у студентов должны быть сформированы:

ОТФ/ТФ *(при наличии профстандарта)*/ трудовые или профессиональные действия	Код компонента компетенции	Результаты обучения

2. Объем и место дисциплины в структуре ОП ВО

Объем дисциплины

3,00 ЗЕ, 36 ак. часа(ов) на контактную работу с преподавателем, 68 ак. часа(ов) на самостоятельную работу обучающихся;

Место дисциплины в структуре ОП ВО

– Б1.В.ДВ.04.01 «Основы информационной безопасности» 4-й курс 8-й семестр

– дисциплина реализуется после изучения дисциплин:

Основы информатики

Операционные среды, системы и оболочки

Введение в анализ данных

– форма промежуточной аттестации – зачет

3. Содержание и структура дисциплины

3.1.Структура дисциплины

очная форма обучения

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), ак. час./ час.						Форма текущего контроля успеваемости*, промежуточной аттестации**
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СРО	
			Л/ДОТ	ЛР/ДОТ	ПЗ/ДОТ	КСР		
Тема 1	Введение. Роль и место информационной безопасности в развитии современного общества	10	2	0	2	0	6	ДЗ
2	Раздел 1. Теоретические основы информационной безопасности	48	8	0	8	0	32	ДЗ
3	Раздел 2. Подготовка и проведение мероприятий по обеспечению информационной безопасности организации (предприятия).	46	8	0	8	0	30	ДЗ

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), ак. час./ час.						Форма текущего контроля успеваемости*, промежуточной аттестации**
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СРО	
			Л/ДОТ	ЛР/ДОТ	ПЗ/ДОТ	КСР		
Промежуточная аттестация		4						Зачет
Всего:		108 / 108	18 / 18	0 / 0	18 / 18	0 / 0	68 / 68	

Используемые сокращения:

Л - занятия лекционного типа (лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях, обучающимся);

ЛР - лабораторные работы (вид занятий семинарского типа);

ПЗ - практические занятия (виды занятий семинарского типа за исключением лабораторных работ);

КСР - индивидуальная работа обучающихся с педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях (в том числе индивидуальные консультации);

ДОТ -занятия, проводимые с применением дистанционных образовательных технологий, в том числе с применением виртуальных аналогов профессиональной деятельности.

СРО - самостоятельная работа, осуществляемая без участия педагогических работников организации и (или) лиц, привлекаемых организацией к реализации образовательных программ на иных условиях.

3.2.Содержание дисциплины

Вводная лекция. Роль и место информационной безопасности в развитии современного общества.

Информация как стратегический ресурс государства и общества. Необходимость изучения вопросов информационной безопасности. Предмет курса, его цели, задачи, структура и порядок изучения.
Исторические аспекты вопроса. Основные факторы, влияющие на процесс обеспечения информационной безопасности в ретроспективе глобального исторического процесса и на современном этапе. Информатизация государства и общества. Эволюция приоритетов угроз информационной безопасности в XXI веке. Теории информационного общества. Концепции информационных войн иностранных государств. Последствия глобализации для информационной безопасности.

Раздел 1. Теоретические основы информационной безопасности.
Тема 1.1. Основные понятия и определения, сущность и содержание информационной безопасности.

Основные понятия и определения теории информационной безопасности в соответствии с действующими нормативно-правовыми документами Российской Федерации и международным правом, а также современными научными взглядами.
Информационная безопасность как составная часть национальной безопасности страны. Составляющие национальных интересов в информационной сфере. Сущность и содержание информационной безопасности с позиций системного подхода.
Цели, задачи, направления (составные части), закономерности и принципы обеспечения информационной безопасности.

Тема 1.2. Угрозы и уровни обеспечения информационной безопасности в условиях глобализации.

Системный подход к построению иерархии последовательно вложенных уровней глобальных угроз информационной безопасности. Особенности форм и содержания угроз на каждом уровне применительно к России. Фасетно-иерархическая классификация угроз информационной безопасности. Специфика информационных угроз на региональном, ведомственном и муниципальном уровнях.
Возможности по нейтрализации угроз информационной безопасности на различных уровнях применительно к существующему состоянию рассматриваемых аспектов в Российской Федерации. Сравнительный анализ проводимых мероприятий по обеспечению информационной безопасности в России и других развитых странах.

Тема 1.3. Нормативно-правовое и концептуальное обеспечение информационной безопасности.

Структура правового обеспечения Российской Федерации в области информационной безопасности: Конституция, Федеральные законы, законы, подзаконные нормативно-правовые акты (Указы Президента, Постановления Правительства, концептуальные и доктринальные документы), государственные стандарты, правовые акты, организационно-распорядительные и методические документы соответствующих федеральных министерств

и ведомств. Концепция национальной безопасности, Доктрина информационной безопасности России. Нормативные документы РФ по стандартизации.
Международная нормативно-правовая база по вопросам информационной безопасности. Международные стандарты обеспечения информационного обмена.

Тема 1.4. Система обеспечения информационной безопасности Российской Федерации (региона, муниципального образования).

Состав и структура системы обеспечения информационной безопасности России. Функции и взаимосвязь системообразующих элементов. Особенности обеспечения информационной безопасности на федеральном, региональном, ведомственном и муниципальном уровнях. Основные механизмы обеспечения информационной безопасности: организационный, нормативно-правовой, методическое и технологическое обеспечение, кадровое и научное обеспечение.

Тема 1.5. Информационная безопасность различных сфер жизнедеятельности общества.

Составляющие национальных интересов в информационной области для различных сфер жизнедеятельности общества: политической, экономической, социальной, духовной. Специфика информационных угроз, особенности решения вопросов обеспечения информационной безопасности в различных сферах жизнедеятельности общества. Субъекты, объекты, цели и задачи, механизмы обеспечения информационной безопасности. Защита интеллектуальной собственности. Роль и место вопросов обеспечения информационной безопасности в ходе реализации Федеральных целевых программ в области информационных технологий.

Тема 1.6. Информационная безопасность отраслей социально-трудовой сферы Российской Федерации.

Система обеспечения информационной безопасности социально-трудовой сферы России. Особенности формирования и развития жизненно-важных интересов и ценностей, угроз и опасностей в информационной области для различных отраслей социально-трудовой сферы: образования, здравоохранения, культуры, рынка труда, процессов обеспечения занятости, жилищно-коммунального хозяйства и др. Специфика рассматриваемых вопросов применительно к проблемам демографии, миграции и эмиграции населения, этническим вопросам. Роль и место вопросов обеспечения информационной безопасности в ходе реализации Приоритетных национальных проектов.

Тема 1.7. Применение методов системных исследований при анализе процессов обеспечения информационной безопасности.

Основные положения современной теории системных исследований. Методология применения системного подхода при анализе процессов обеспечения информационной безопасности, соотношение гуманитарных, естественнонаучных и технических аспектов.
Проблема информационно-аналитического обеспечения в достижении опережающего информационного эффекта при осуществлении реформ. Анализ возможностей использования методов математического моделирования при исследовании проблем обеспечения информационной безопасности.
Особенности прогнозирования информационной обстановки. Основные показатели и критерии обеспечения информационной безопасности. Особенности оценки эффективности мероприятий по обеспечению информационной безопасности. Модель

принятия управленческого решения, вопросы обеспечения его информационной безопасности.

Раздел 2. Подготовка и проведение мероприятий по обеспечению информационной безопасности организации (предприятия).

Тема 2.1. Основы информационной безопасности организации (предприятия).

Роль и место информационной безопасности в системе комплексной безопасности организации (предприятия). Анализ способов нарушения информационной безопасности. Информационные угрозы, цели и задачи обеспечения информационной безопасности. Принципы, методы и способы обеспечения информационной безопасности. Концепция информационной безопасности организации (предприятия). Модели безопасности и их применение.

Тема 2.2. Особенности нормативно-правового обеспечения информационной безопасности в государственном секторе и бизнесе.

Нормативно-правовая база обеспечения информационной безопасности организации (предприятия). Закон РФ “О государственной тайне”. Федеральный закон РФ “О коммерческой тайне”.
Лицензирование деятельности в области информационной безопасности, сертификация средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации.
Структура внутреннего нормативно-правового обеспечения информационной безопасности в организации. Разрабатываемые в организации документы по вопросам информационной безопасности и требования по их корректировке. Содержание руководства по обеспечению информационной безопасности в организации.
Создание защищенного документооборота в организации.

Тема 2.3. Организация мероприятий по обеспечению информационной безопасности предприятия (фирмы).

Основные этапы процесса организации мероприятий по обеспечению информационной безопасности на предприятии (фирме).
Органы обеспечения информационной безопасности организации (предприятия): состав, структура и функции. Порядок действий должностных лиц по вопросам обеспечения информационной безопасности в различных условиях обстановки.

Тема 2.4. Информационный аудит организации (предприятия).

Организация и проведение анализа информационной уязвимости предприятия (фирмы). Роль и место информационного аудита в ходе комплексного аудита организации (предприятия), в процессе информационной санации. Виды информационного аудита, условия их проведения, содержание и взаимосвязь. Нормативно-правовая база проведения аудита.
Этапы алгоритма анализа и оценки информационных рисков. Основные направления управления рисками.

Тема 2.5. Информационно-технические аспекты обеспечения информационной безопасности.

Демаскирующие признаки информационных объектов. Органы, принципы, методы, способы и средства добывания информации. Технические каналы утечки информации. Способы и средства предотвращения утечки информации.
Угрозы и объекты обеспечения информационно-технической безопасности, принципы, методы и способы ее обеспечения. Технология процесса обеспечения информационно-технической безопасности. Контроль состояния технической защиты информации.

Тема 2.6. Методы, способы и средства защиты информации в автоматизированных информационных системах.

Анализ способов нарушений информационной безопасности в сетях и их таксономия. Способы и средства защиты информации от утечки по техническим каналам в автоматизированных информационных системах. Средства программно-математического и программно-технического воздействия. Виды “вирусов” и защита от них.
Использование защищенных компьютерных систем. Системы обнаружения и предотвращения атак. Методы и средства защиты данных, применяемые в сетях. Методы криптографии. Электронная цифровая подпись.

Тема 2.7. Информационно - психологические аспекты обеспечения информационной безопасности.

Теоретические основы межличностной коммуникации, скрытного информационно-психологического управления. Методы и приемы информационно-психологического воздействия на должностных лиц: продуктивного общения, приемы ведения дискуссии, методы и приемы “жесткого” информационно-психологического воздействия. Психологический анализ учебных видеофрагментов. Алгоритмы информационно-психологической защиты: активная защита, пассивная защита.

4. Материалы текущего контроля успеваемости обучающихся

4.1. Формы и методы текущего контроля успеваемости и промежуточной аттестации.

В ходе реализации дисциплины используются следующие методы текущего контроля успеваемости обучающихся: при проведении занятий лекционного типа: беседа (диалог) с обучающимися, при проведении занятий семинарского типа: домашние работы по темам практических заданий

4.2. Материалы текущего контроля успеваемости.

Примерные темы докладов:

1. Роль и место информационной безопасности экономических систем в системе национальной безопасности Российской Федерации.
2. Совершенствование законодательства Российской Федерации в области информационной безопасности.
3. Компьютерная преступность как угроза информационной безопасности и основные направления противодействия ей.
4. Анализ основных положений Доктрины информационной безопасности Российской Федерации.
5. “Информационная революция” и информационная безопасность.
6. Анализ использования моделей управления рисками в области информационной безопасности.

7. Значение обеспечения конкурентоспособности отечественной продукции в области информационных технологий для информационной безопасности.

8. Информационная безопасность и реализация Федеральных целевых программ в области информационных технологий.

9. Проблемы создания информационного общества и обеспечение информационной безопасности.

10. Сравнительный анализ состояния и развития систем обеспечения информационной безопасности России и экономически наиболее развитых зарубежных стран.

11. Организация международного сотрудничества по вопросам информационной безопасности в экономической сфере.

12. Система информационной безопасности организации (конкретная организация может быть выбрана слушателем).

13. Использование программно-аппаратных средств для обеспечения требуемого уровня информационной безопасности предприятия (организации).

14. Роль и место информационно-аналитического компонента в системе обеспечения информационной безопасности организации (предприятии).

15. Лицензирование и сертификация как необходимые условия обеспечения информационной безопасности.

16. Проблемы информационной безопасности в Internet и пути их решения.

17. Угрозы информационной безопасности локальной (корпоративной) сети и возможности по их нейтрализации.

18. Информационная безопасность при использовании электронной цифровой подписи.

19. Значение информационно-психологической безопасности в системе информационной безопасности организации (предприятия).

20. Роль и место СМИ в обеспечении информационной безопасности экономической сферы.

21. Оценка эффективности мероприятий по обеспечению информационной безопасности организации (предприятия).

22. Проекты создания технопарков и обеспечение информационной безопасности.

23. Анализ технологий манипулирования личностью и обществом, направления обеспечения информационно-психологической защиты.

24. Информационная безопасность интеллектуальной собственности в России: состояние и перспективы.

25. Категорирование объектов при обеспечении информационной безопасности предприятия (организации).

26. Основные направления компьютерной вирусологии в современном мире.

27. Информационный терроризм и борьба с ним.

28. Современный “киберконтроль” и защита прав человека.

29. Политика обеспечения информационной безопасности организации.

30. Достижения научно-технической революции и обеспечение информационной безопасности.

Целью подготовки докладов является приобретение студентами знаний в области информационной безопасности путем самостоятельного изучения научной, учебной и методической литературы, нормативно-правовой базы Российской Федерации и международного права по вопросам информационной безопасности.

Доклад выполняется в форме реферата объемом до 20 страниц. Тему доклада и литературу по ней слушатель выбирает самостоятельно, учитывая прилагаемый перечень тем и список литературы.

Результаты выполнения этих работ являются основанием для выставления оценок текущего контроля. Выполнение всех работ является обязательным для всех студентов.

Учитываются также результаты работы на практических занятиях. Обучающиеся не выполнившие в полном объеме все эти работы, не допускаются к сдаче экзамена, как не выполнившие график учебного процесса по данной дисциплине. Студент допускается к экзамену, если у него есть положительные оценки по всем материалам

Шкала оценивания текущего контроля

10-бальная шкала	Традиционная шкала	«Зачтено»/ «Не зачтено»	Определение
10	Отлично	Зачтено	Полные, глубокие и систематические знания, знакомство с дополнительной литературой, полный и правильный ответ, творческий подход в понимании и изложении учебного материала, полное выполнение мероприятий текущего контроля.
9	Отлично	Зачтено	Полные, глубокие и систематические знания, полный и правильный ответ, полное выполнение мероприятий текущего контроля.
8	Отлично	Зачтено	Полные и систематические знания, отсутствие существенных неточностей в ответе, полное выполнение мероприятий текущего контроля.
7	Хорошо	Зачтено	Достаточно полные и систематические знания, отсутствие существенных неточностей в ответе, имеются погрешности при выполнении мероприятий текущего контроля.
6	Хорошо	Зачтено	Достаточно полные и систематические знания, отсутствие существенных неточностей в ответе, имеются погрешности при выполнении мероприятий текущего контроля.
5	Удовлетворительно	Зачтено	Знание основного учебного материала в объеме, необходимом для дальнейшей учебы и работы, имеются погрешности при выполнении мероприятий текущего контроля и при ответе.
4	Удовлетворительно	Зачтено	Знание основного учебного материала в минимальном объеме, необходимом для дальнейшей учебы и работы, имеются погрешности при выполнении мероприятий промежуточного контроля и при ответе.
3	Неудовлетворительно	Не зачтено	Имеются существенные погрешности при выполнении мероприятий текущего контроля, допущены существенные ошибки при ответе, необходима некоторая дополнительная работа.
2	Неудовлетворительно	Не зачтено	Имеются пробелы в знаниях по значительной части учебного материала, допущены существенные ошибки при ответе, необходима значительная дополнительная учебная работа.
1	Неудовлетворительно	Не зачтено	Не выполнены предусмотренные программой задания, не отработаны практические или лабораторные занятия, необходимы дополнительные занятия по соответствующей дисциплине.
0	Неудовлетворительно	Не зачтено	Нарушение академических норм (плагиат и т.п.)

4.3. методы (средства) промежуточной аттестации.

4.3.1. Для контроля усвоения данной дисциплины учебным планом предусмотрен зачет *(в соответствии с учебным планом)*, который проводится в устной форме. Задания содержат вопросы, в которых необходимо использовать теоретические знания и

практическое задание, демонстрирующие способность организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия и умение консультировать заказчиков по вопросам совершенствования управления информационной безопасностью ИТ-инфраструктуры предприятия. На зачет выносятся основные вопросы, рассматриваемые в рамках всего курса. Основой для определения оценки служит объем и уровень усвоения студентами материала, предусмотренного программой данного курса и подведения итогов по результатам выполнения заданий текущего контроля успеваемости

Список вопросов для подготовки к зачету:

1. Основные понятия и определения теории информационной безопасности.
2. Роль и место информационной безопасности в системе национальной безопасности Российской Федерации.
3. Основные положения Доктрины информационной безопасности Российской Федерации.
4. Сущность и содержание информационно-технической безопасности.
5. Сущность и содержание информационно-психологической безопасности.
6. Информационно-аналитическое обеспечение в системе информационной безопасности.
7. Нормативно-правовая база российского законодательства в области информационной безопасности.
8. Международные нормативно-правовые документы по вопросам информационной безопасности.
9. Состояние и перспективы борьбы с компьютерной преступностью в России. Анализ положений Уголовного кодекса Российской Федерации.
10. Основные направления реализации Федеральной целевой программы “Электронная Россия” и информационная безопасность.
11. Интересы личности, общества и государства в информационной сфере.
12. Угрозы жизненно-важным интересам личности, общества и государства в информационной сфере.
13. Система обеспечения информационной безопасности России.
14. Система информационной безопасности региона, ведомства, муниципального образования.
15. Роль и место негосударственных организаций и частных лиц в системе обеспечения информационной безопасности Российской Федерации.
16. Международные стандарты информационного обмена.
17. Виды “нарушителей” режима защиты информации, модели их действий.
18. Основные нормативно-правовые и руководящие документы, касающиеся вопросов соблюдения государственной тайны и их содержание.
19. Основные нормативно-правовые и руководящие документы, касающиеся вопросов соблюдения коммерческой тайны и их содержание.
20. Определение и содержание процессов лицензирования и сертификации.
21. 20. Система информационной безопасности организации (предприятия).
22. Органы обеспечения информационной безопасности организации (предприятия): состав, структура и функции в различных условиях обстановки.
23. Организация мероприятий по обеспечению информационной безопасности предприятия (фирмы).
24. Разрабатываемые в организации документы по вопросам информационной безопасности и требования по их корректировке.
25. Создание и обеспечение защищенного документооборота в организации.
26. 24. Информационный аудит организации (предприятия).
27. Анализа информационных рисков и управление ими.

28. Органы, методы, способы и средства добывания информации по техническим каналам.
29. Способы и средства защиты информации от утечки по техническим каналам в автоматизированных информационных системах.
30. Средства программно-математического и программно-технического воздействия и защита от них.
31. Виды компьютерных “вирусов” и защита от них.
32. Методы и средства защиты данных, применяемые в сетях.
33. Понятие и содержание криптографии, основные методы.
34. Электронная цифровая подпись (понятие, содержание процесса использования ЭЦП, проблемы).
35. Методы и приемы информационно-психологического воздействия на должностных лиц.
36. Алгоритмы информационно-психологической защиты.
37. Использование интернет - технологий и обеспечение информационной безопасности.
38. Основные технологии построения защищенных информационных систем.
39. Формы контроля состояния технической защиты информации.
40. Государственные стандарты, регламентирующие терминологию в области защиты информации.
41. Средства защиты информации от утечки по техническим каналам.
42. Защита интеллектуальной собственности (определение, содержание процесса защиты, проблемы).

4.3. Оценочные средства для промежуточной аттестации.

4.3.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код компетенции	**Наименование компетенции**	**Код этапа освоения компетенции**	**Наименование этапа освоения компетенции**
ПКс-10	Умение выполнять технико-экономическое обоснование проектов по совершенствованию и регламентацию бизнес-процессов и ИТ-инфраструктуры предприятия	ПКс-10.4	
ПКс-12	Умение осуществлять планирование и организацию проектной деятельности на основе стандартов управления проектами	ПКс-12.3	Способен осуществлять организацию проектной деятельности с учетом проблем информационной безопасности

Критерии оценивания уровня формирования компетенций

Этап освоения компетенции	**Показатель оценивания** *Что делает обучающийся (какие действия способен выполнить), подтверждая этап освоения компетенции*	**Критерий оценивания** *Как (с каким качеством) выполняется действие. Соответствует оценке «отлично» в шкале оценивания в РПД.*	**Оценка (баллы)**
ПКс-10.4	Инд. 1 Способен планировать и управлять проектной деятельностью и оформлять результаты на основе	. Определяет тип(ы) ИТ-инфраструктуры предприятия	тест

Этап освоения компетенции	**Показатель оценивания** *Что делает обучающийся (какие действия способен выполнить), подтверждая этап освоения компетенции*	**Критерий оценивания** *Как (с каким качеством) выполняется действие. Соответствует оценке «отлично» в шкале оценивания в РПД.*	**Оценка (баллы)**
	использования логических методов и алгоритмов Инд 2. Использует математические методы для обоснования проектов по совершенствованию и регламентацию бизнес-процессов и ИТ-инфраструктуры предприятия	с учетом стандартов безопасности. Анализ и участие в работе с учетом личностных, социальных и профессиональных интересов1.Оценено качество процесса управления информационной безопасностью 2. Сформирована группа целей, требований и приоритетов управления информационной безопасностью ресурсов ИТ	
ПКс-12.3 Способен осуществлять организацию проектной деятельности с учетом проблем информационной безопасности	Инд. 1 Способность определять и оценивать ресурсы и существующие ограничения проекта и предприятия с качественной и количественной точек зрения Инд. 2 Способность планировать и организовывать проектную деятельность	Осуществлен анализ электронного предприятия по проблемам информационной безопасности. Выражена готовность к сотрудничеству в различных группах (межпредметных) и определена ролевая позиция в группе по совершенствованию ИТ-инфраструктуры и ее безопасности Оптимально распределены обязанности по задачам и подзадачам в рамках инфраструктуры по обеспечению информационной безопасности в условиях риска и неопределенности, вопросах информационно-аналитического обеспечения процессов, принятия решений в области информационной безопасности, с существующими и перспективными возможностями по недопущению возникновения и нейтрализации угроз в информационной сфере;	Промежуточная аттестация

Пересдача зачета (в случае получения студентом оценки "неудовлетворительно") осуществляется в установленном порядке.

4.4. Методические материалы по проведению промежуточной аттестации

Зачет проводится в соответствии с графиком учебного процесса учетом проведения мониторинга уровня освоения компетенции по результатам выполнения самостоятельных заданий. Оценивание осуществляется в соответствии со шкалой оценивания. Студентам, не

выполнившим домашние задания и (или) контрольные задания по уважительным причинам, предоставляется возможность их выполнения и сдачи.

5. Оценочные материалы промежуточной аттестации по дисциплине

5.1. Экзамен (зачет) проводится с применением следующих методов (средств):

Для контроля усвоения данной дисциплины учебным планом предусмотрен зачет (в соответствии с учебным планом), который проводится в устной форме. Задания содержат вопросы, в которых необходимо использовать теоретические знания и практическое задание, демонстрирующие способность организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия и умение консультировать заказчиков по вопросам совершенствования управления информационной безопасностью ИТ-инфраструктуры предприятия. На зачет выносятся основные вопросы, рассматриваемые в рамках всего курса. Основой для определения оценки служит объем и уровень усвоения студентами материала, предусмотренного программой данного курса и подведения итогов по результатам выполнения заданий текущего контроля успеваемости

5.2. Типовые оценочные материалы промежуточной аттестации

Список вопросов для подготовки к зачету:

1. Основные понятия и определения теории информационной безопасности.
2. Роль и место информационной безопасности в системе национальной безопасности Российской Федерации.
3. Основные положения Доктрины информационной безопасности Российской Федерации.
4. Сущность и содержание информационно-технической безопасности.
5. Сущность и содержание информационно-психологической безопасности.
6. Информационно-аналитическое обеспечение в системе информационной безопасности.
7. Нормативно-правовая база российского законодательства в области информационной безопасности.
8. Международные нормативно-правовые документы по вопросам информационной безопасности.
9. Состояние и перспективы борьбы с компьютерной преступностью в России. Анализ положений Уголовного кодекса Российской Федерации.
10. Основные направления реализации Федеральной целевой программы “Электронная Россия” и информационная безопасность.
11. Интересы личности, общества и государства в информационной сфере.
12. Угрозы жизненно-важным интересам личности, общества и государства в информационной сфере.

13. Система обеспечения информационной безопасности России.
14. Система информационной безопасности региона, ведомства, муниципального образования.
15. Роль и место негосударственных организаций и частных лиц в системе обеспечения информационной безопасности Российской Федерации.
16. Международные стандарты информационного обмена.
17. Виды “нарушителей” режима защиты информации, модели их действий.
18. Основные нормативно-правовые и руководящие документы, касающиеся вопросов соблюдения государственной тайны и их содержание.
19. Основные нормативно-правовые и руководящие документы, касающиеся вопросов соблюдения коммерческой тайны и их содержание.
20. Определение и содержание процессов лицензирования и сертификации.
21. 20. Система информационной безопасности организации (предприятия).
22. Органы обеспечения информационной безопасности организации (предприятия): состав, структура и функции в различных условиях обстановки.
23. Организация мероприятий по обеспечению информационной безопасности предприятия (фирмы).
24. Разрабатываемые в организации документы по вопросам информационной безопасности и требования по их корректировке.
25. Создание и обеспечение защищенного документооборота в организации.
26. 24. Информационный аудит организации (предприятия).
27. Анализа информационных рисков и управление ими.
28. Органы, методы, способы и средства добывания информации по техническим каналам.
29. Способы и средства защиты информации от утечки по техническим каналам в автоматизированных информационных системах.
30. Средства программно-математического и программно-технического воздействия и защита от них.
31. Виды компьютерных “вирусов” и защита от них.
32. Методы и средства защиты данных, применяемые в сетях.
33. Понятие и содержание криптографии, основные методы.
34. Электронная цифровая подпись (понятие, содержание процесса использования ЭЦП, проблемы).
35. Методы и приемы информационно-психологического воздействия на должностных лиц.
36. Алгоритмы информационно-психологической защиты.
37. Использование интернет - технологий и обеспечение информационной безопасности.
38. Основные технологии построения защищенных информационных систем.
39. Формы контроля состояния технической защиты информации.
40. Государственные стандарты, регламентирующие терминологию в области защиты информации.
41. Средства защиты информации от утечки по техническим каналам.
42. Защита интеллектуальной собственности (определение, содержание процесса защиты, проблемы).

Шкала оценивания.

Зачтено

Полные, глубокие и систематические знания, знакомство с дополнительной литературой, полный и правильный ответ, творческий подход в понимании и изложении учебного материала, полное выполнение мероприятий текущего контроля.

Полные, глубокие и систематические знания, полный и правильный ответ, полное выполнение мероприятий текущего контроля.

Полные и систематические знания, отсутствие существенных неточностей в ответе, полное выполнение мероприятий текущего контроля.

Достаточно полные и систематические знания, отсутствие существенных неточностей в ответе, имеются погрешности при выполнении мероприятий текущего контроля.

Достаточно полные и систематические знания, отсутствие существенных неточностей в ответе, имеются погрешности при выполнении мероприятий текущего контроля.

Знание основного учебного материала в объеме, необходимом для дальнейшей учебы и работы, имеются погрешности при выполнении мероприятий текущего контроля и при ответе.

Знание основного учебного материала в минимальном объеме, необходимом для дальнейшей учебы и работы, имеются погрешности при выполнении мероприятий промежуточного контроля и при ответе.

Не зачтено

Имеются существенные погрешности при выполнении мероприятий текущего контроля, допущены существенные ошибки при ответе, необходима некоторая дополнительная работа.

Имеются пробелы в знаниях по значительной части учебного материала, допущены существенные ошибки при ответе, необходима значительная дополнительная учебная работа.

Не выполнены предусмотренные программой задания, не отработаны практические или лабораторные занятия, необходимы дополнительные занятия по соответствующей дисциплине.

Нарушение академических норм (плагиат и т.п.)

Компонент компетенции	Промежуточный/ключевой индикатор оценивания	Критерий оценивания
ПКс-12.2	Способность планировать и организовывать проектную деятельность	Осуществлен анализ электронного предприятия по проблемам информационной безопасности. Выражена готовность к сотрудничеству в различных группах (межпредметных) и определена ролевая позиция в группе по совершенствованию ИТ-инфраструктуры и ее безопасности Оптимально распределены обязанности по задачам и подзадачам в рамках инфраструктуры по обеспечению информационной безопасности в условиях риска и неопределенности, вопросах информационно-аналитического обеспечения процессов, принятия решений в области информационной безопасности, с существующими и перспективными возможностями по недопущению возникновения и нейтрализации угроз в информационной сфере
ПКс-10.2	Использует математические методы для обоснования проектов по совершенствованию и регламентацию бизнес-процессов и ИТ-инфраструктуры предприятия	Определяет тип(ы) ИТ-инфраструктуры предприятия с учетом стандартов безопасности. Анализ и участие в работе с учетом личностных, социальных и профессиональных интересов1.Оценено качество процесса

		управления информационной безопасностью 2. Сформирована группа целей, требований и приоритетов управления информационной безопасностью ресурсов ИТ

Оценка	**Баллы БРС**
«не зачтено»	менее 40
«зачтено»	40-100

Оценка	**Баллы БРС**	**Критерии**
Отлично		
Хорошо		
Удовлетворительно		
неудовлетворительно		

6. Методические материалы по освоению дисциплины

В ходе реализации дисциплины используются следующие методы текущего контроля успеваемости обучающихся: при проведении занятий лекционного типа: беседа (диалог) с обучающимися, при проведении занятий семинарского типа: домашние работы по темам практических заданий

7. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

7.1. Основная литература

1. Основы управления информационной безопасностью - Горячая линия-Телеком, 2016 - 244 с. с.

2. Калинин А. Н. Основы информационной безопасности - Национальная компьютерная корпорация, 2005 - 159 с. с.

7.2. Дополнительная литература

1. Мельников, В. П. Информационная безопасность и защита информации: учебное пособие: гриф УМО / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова. - 7-е изд., стер. - М.: Академия, 2012.

2. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2019.

3. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства: учебное пособие : гриф УМО / В. Ф. Шаньгин. - М.: ДМК Пресс, 2008.

7.3. Нормативные правовые документы и иная правовая информация

8. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Требования к аудитории:
- Лекционные
- Семинарские
- Компьютерные

Требования к оборудованию:
- проектор
- Доска

Требования к программному обеспечению:
- Microsoft Office (Word, Excel, Power Point)