	Министерство сельского хозяйства Российской Федерации
	федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный аграрный университет»
	ФГБОУ ВО Уральский ГАУ
	Рабочая программа учебной дисциплины «Информационная безопасность в бизнес-аналитике»
Б1.О.39	Кафедра менеджмента и экономической теории

РАБОЧАЯ ПРОГРАММА
учебной дисциплины

Информационная безопасность в бизнес-аналитике

Направления подготовки
38.03.02 Менеджмент

Направленность (профиль) программы
«Бизнес-аналитика в управленческой деятельности»

Уровень подготовки
бакалавриат

Форма обучения
очная, очно-заочная, заочная

Екатеринбург, 2023

	Должность	***Фамилия***	***Дата № протокола***
Разработал:	*Ст.преподаватель*	*А.В. Фетисова*	11.04.2023 Протокол №8 кафедры менеджмента и экономической теории
Версия: 2.0			***Стр** 1 **из** 15*

Содержание

1.Цели и задачи дисциплины, место дисциплины в структуре образовательной программы……3

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы 3

3. Объем дисциплины и виды учебной работы ..... …….4

4. Содержание дисциплины..... 4

5. Перечень учебно-методического обеспечения и программного обеспечения дисциплины..... 8

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине..... 8

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины: 10

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины..... 10

9. Методические указания для обучающихся по освоению дисциплины 11

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем..... 11

11. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине……12

12. Особенности обучения студентов с различными нозологиями 14

1. Цели и задачи дисциплины, место дисциплины в структуре образовательной программы

Цель изучения дисциплины - получение студентами целостного представления о современных методах обеспечения информационной безопасности на базе терминологического фундамента, грамотного проведения анализа угроз информационной безопасности в бизнес-аналитике, знакомства с методами нарушения доступности, конфиденциальности и целостности информации, общеметодологических принципов теории информационной безопасности.

Задачи изучения дисциплины:

– освоение основных понятий и терминологии информационной безопасности;

– знакомство с угрозами, которым подвергается информация, а также классификацией этих угроз и их анализом;

– изучение нормативно-законодательной базы и стандартов информационной безопасности и защиты информации в бизнес-аналитике;

– изучение методов обеспечения информационной безопасности, в том числе в бизнес-аналитике.

Дисциплина Б1.О.39 «Информационная безопасность в бизнес - аналитике» относится к числу дисциплин обязательной части.

Траектория формирования компетенций выделяет этапы формирования в соответствии с учебным планом, при этом соблюдается принцип нарастающей сложности.

Основными этапами формирования компетенций при изучении дисциплины «Информационная безопасность в бизнес-аналитике» является последовательное изучение содержательно связанных между собой разделов (тем) дисциплины. Изучение каждого раздела (темы) предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Изучение дисциплины «Информационная безопасность в бизнес-аналитике» основывается на знаниях, полученных студентами при изучении дисциплин «Основы проектного менеджмента», «Информационные технологии в бизнес-аналитике», «Цифровой маркетинг и социальные сети», «Методы принятия управленческих решений». Полученные знания, умения, навыки используются студентами в процессе изучения таких дисциплин, как «Теория систем и системный анализ», государственная итоговая аттестация.

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

В процессе изучения дисциплины студент должен приобрести следующие компетенции:

ОПК-2. Способен осуществлять сбор, обработку и анализ данных, необходимых для решения поставленных управленческих задач, с использованием современного инструментария и интеллектуальных информационно-аналитических систем;

ОПК-5. Способен использовать при решении профессиональных задач современные информационные технологии и программные средства, включая управление крупными массивами данных и их интеллектуальный анализ.

В результате изучения дисциплины «Информационная безопасность в бизнес-аналитике» обучающийся должен

Знать:

- основные понятия и терминологию информационной безопасности в бизнес-аналитике, современные информационные технологии и программные средства;
- способы сбора, обработки и анализа данных для решения управленческих задач;
- методы обеспечения информационной безопасности, в том числе в бизнес-аналитике.

Уметь:

- применять на практике современный инструментарий и интеллектуальные информационно-аналитические системы в бизнес-аналитике, а также обеспечивать их информационную безопасность;
- проводить интеллектуальный анализ данных в по бизнес-аналитике в управленческой деятельности.

Владеть:

- навыками управления крупными массивами данных

3. Объем дисциплины и виды учебной работы

Общая трудоёмкость дисциплины составляет 5 зачетных единиц.

Вид учебной работы	Всего часов **очное**	Очная форма обучения	Всего часов **очно-заочное**	Очно-заочная форма обучения	Всего часов **заочное**	заочная форма обучения
		4 курс		4 курс		5 курс
		7 семестр		8 семестр		9 семестр
Контактная работа* (всего)	58,25	58,25	58,25	58,25	22,75	22,75
В том числе:						
Лекции	24	24	24	24	10	10
Практические занятия (ПЗ)	24	24	24	24	10	10
Групповые консультации	10	10	10	10	2,5	2,5

Вид учебной работы	Всего часов **очное**	Очная форма обучения	Всего часов **очно-заочное**	Очно-заочная форма обучения	Всего часов **заочное**	заочная форма обучения
		4 курс		4 курс		5 курс
		7 семестр		8 семестр		9 семестр
Промежуточная аттестация (зачет, экзамен)	0,25	0,25	0,25	0,,25	0,25	0,25
Самостоятельная работа (всего)	121,75	121,75	121,75	121,75	157,25	157,25
В том числе:						
Общая трудоёмкость, час	180	180	180	180	180	180
зач.ед.	5	5	5	5	5	5
Вид промежуточной аттестации	Зачет с оценкой	Зачет с оценкой	Зачет с оценкой	Зачет с оценкой	Зачет с оценкой	Зачет с оценкой

4.Содержание дисциплины

Основные понятия и определения информационной безопасности. Информационная безопасность в системе национальной безопасности РФ. Нормативно-законодательная база и стандарты в области информационной безопасности в бизнес-аналитике. Угрозы информационной безопасности, их классификация и анализ. Общие сведения о методах и средствах обеспечения информационной безопасности в бизнес-аналитике. Информационная безопасность автоматизированных систем на предприятии. Информационная безопасность компьютеров и компьютерных сетей на предприятии.

4.1 Модули (разделы) дисциплин и виды занятий

Очная форма обучения

№ п.п	Наименование раздела дисциплин	Лекции	Практ. занятия	СРС	Всего часов
1.	Раздел 1. Основы информационной безопасности в бизнес -аналитике				
	Тема 1.1. Основные понятия и определения.	2	2	12	16
	Тема 1.2. Задачи информационной безопасности в бизнес -аналитике.	2	2	12	16
	Тема 1.3. Угрозы информационной безопасности в бизнес -аналитике.	2	2	12	16
	Тема 1.4. Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере.	2	2	12	16

№ п.п	Наименование раздела дисциплин	Лекции	Практ. занятия	СРС	Всего часов
	Тема 1.5. Понятие и виды защищаемой информации в бизнес –аналитике.	2	2	12	16
	Итого по разделу 1:	***10***	***10***	***60***	***80***
2.	Раздел 2. Защита информации в бизнес -анализе				
	Тема 2.1. Общая характеристика способов и средств защиты информации в бизнес -аналитике.	2	2	12	16
	Тема 2.2. Криптографические методы защиты информации в бизнес –аналитике.	3	3	12	18
	Тема 2.3. Методы организации безопасного доступа	3	3	12	18
	Тема 2.4. Электронная цифровая подпись и цифровые сертификаты	3	3	12	18
	Тема 2.5. Программно-аппаратные средства защиты информации в бизнес -аналитике	3	3	13,75	19,75
	Итого по разделу 2:	***14***	***14***	***61,75***	***89,75***
3.	Групповые консультации				10
4.	Промежуточная аттестация (зачет с оценкой)				0,25
	ИТОГО:	***24***	***24***	***121,75***	***180***

Очно-заочная форма обучения

№ п.п	Наименование раздела дисциплин	Лекции	Практ. занятия	СРС	Всего часов
1.	Раздел 1. Основы информационной безопасности в бизнес -аналитике				
	Тема 1.1. Основные понятия и определения.	2	2	12	16
	Тема 1.2. Задачи информационной безопасности в бизнес -аналитике.	2	2	12	16
	Тема 1.3. Угрозы информационной безопасности в бизнес -аналитике.	2	2	12	16
	Тема 1.4. Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере.	2	2	12	16
	Тема 1.5. Понятие и виды защищаемой информации в бизнес –аналитике.	2	2	12	16
	Итого по разделу 1:	***10***	***10***	***60***	***80***
2.	Раздел 2. Защита информации в бизнес -анализе				
	Тема 2.1. Общая характеристика способов и средств защиты информации в бизнес -аналитике.	2	2	12	16
	Тема 2.2. Криптографические методы защиты информации в бизнес –аналитике.	3	3	12	18
	Тема 2.3. Методы организации безопасного доступа	3	3	12	18
	Тема 2.4. Электронная цифровая подпись и цифровые сертификаты	3	3	12	18
	Тема 2.5. Программно-аппаратные средства защиты информации в бизнес -аналитике	3	3	13,75	19,75
	Итого по разделу 2:	***14***	***14***	***61,75***	***89,75***
3.	Групповые консультации				10

№ п.п	Наименование раздела дисциплин	Лекции	Практ. занятия	СРС	Всего часов
4.	Промежуточная аттестация (зачет с оценкой)				0,25
	ИТОГО:	***24***	***24***	***121,75***	***180***

Заочная форма обучения

№ п.п	Наименование раздела дисциплин	Лекции	Практ. занятия	СРС	Всего часов
1.	Раздел 1. Основы информационной безопасности в бизнес -аналитике				
	Тема 1.1. Основные понятия и определения.	1	1	15	17
	Тема 1.2. Задачи информационной безопасности в бизнес -аналитике.	1	1	15	17
	Тема 1.3. Угрозы информационной безопасности в бизнес -аналитике.	1	1	15	17
	Тема 1.4. Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере.	1	1	16	18
	Тема 1.5. Понятие и виды защищаемой информации в бизнес –аналитике.	1	1	16	18
	Итого по разделу 1:	***5***	***5***	***77***	***87***
2.	Раздел 2. Защита информации в бизнес -анализе				
	Тема 2.1. Общая характеристика способов и средств защиты информации в бизнес -аналитике.	1	1	16	18
	Тема 2.2. Криптографические методы защиты информации в бизнес –аналитике.	1	1	16	18
	Тема 2.3. Методы организации безопасного доступа	1	1	16	18
	Тема 2.4. Электронная цифровая подпись и цифровые сертификаты	1	1	16	18
	Тема 2.5. Программно-аппаратные средства защиты информации в бизнес -аналитике	1	1	16,25	18,25
	Итого по разделу 2:	***5***	***5***	***80,25***	***90,25***
3.	Групповые консультации				2,5
4.	Промежуточная аттестация (зачет с оценкой)				0,25
	ИТОГО:	***10***	***10***	***157,25***	***180***

4.2 Содержание модулей (разделов) дисциплин

п.п	Наименование модуля (раздела)	Содержание раздела	Трудоёмкость (час.)	Формируемые компетенции	Формы контроля	Технологии интерактивного обучения
1	2	3	4 Очн., очн.-заочн., Заоч.	5	6	7
1.	Раздел 1. Основы информационной безопасности в бизнес -аналитике	Тема 1.1. Основные понятия и определения. Тема 1.2. Задачи информационной безопасности в бизнес -аналитике. Тема 1.3. Угрозы информационной безопасности в бизнес -аналитике. Тема 1.4. Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере. Тема 1.5. Понятие и виды защищаемой информации в бизнес –аналитике.	87/87/ 87	ОПК-2 ОПК-5	Письменная работа, практические задания, тест	Презентации лекций, работа в группах
2.	Раздел 2. Защита информации в бизнес -анализе	Тема 2.1. Общая характеристика способов и средств защиты информации в бизнес -аналитике. Тема 2.2. Криптографические методы защиты информации в бизнес –аналитике. Тема 2.3. Методы организации безопасного доступа Тема 2.4. Электронная цифровая подпись и цифровые сертификаты Тема 2.5. Программно-аппаратные средства защиты информации в бизнес -аналитике	89,75/89,75/ 90,25	ОПК-2 ОПК-5	Письменная работа, практические задания	Презентации лекций, работа в группах

4.3 Детализация самостоятельной работы

№ п/п	Наименование модуля дисциплины	Тематика самостоятельной работы	Формы самостоятельной работы	Трудоемкость, часы		
				очное	заочное	очно-заочное
1	Раздел 1. Основы информационной безопасности в бизнес - аналитике	Тема 1.1. Основные понятия и определения.	Подготовка к лекционным и практическим занятиям, работа в библиотеке	12	15	12
		Тема 1.2. Задачи информационной безопасности в бизнес -аналитике.		12	15	12
		Тема 1.3. Угрозы информационной безопасности в бизнес -аналитике.		12	15	12
		Тема 1.4. Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере.		12	16	12
		Тема 1.5. Понятие и виды защищаемой информации в бизнес –аналитике.		12	16	12
2	Раздел 2. Защита информации в бизнес - анализе	Тема 2.1. Общая характеристика способов и средств защиты информации в бизнес -аналитике.	Подготовка к лекционным и практическим занятиям, работа в библиотеке	12	16	12
		Тема 2.2. Криптографические методы защиты информации в бизнес –аналитике.		12	16	12
		Тема 2.3. Методы организации безопасного доступа		12	16	12
		Тема 2.4. Электронная цифровая подпись и цифровые сертификаты		12	16	12
		Тема 2.5. Программно-аппаратные средства защиты информации в бизнес - аналитике		13,75	16,25	13,75
6	**ИТОГО:**			***121,75***	***157,25***	***121,75***

5. Перечень учебно-методического обеспечения и программного обеспечения дисциплины

Методические указания к самостоятельной работе для студентов по дисциплине «Информационная безопасность в бизнес-аналитике»/ сост. Фетисова А.В. – Екатеринбург: Изд-во Уральский ГАУ, 2023.

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

6.1. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины (ФОС)

Приложение к рабочей программе

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины:

а) основная литература:

1. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2022. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496741

2. В. Л Шульц, В. Л. Безопасность предпринимательской деятельности : учебник для вузов / В. Л. Шульц, А. В. Юрченко, А. Д. Рудченко ; под редакцией В. Л. Шульца. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 585 с. — (Высшее образование). — ISBN 978-5-534-12368-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496303

б) дополнительная литература:

1. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/530927

2. Фомчёв, Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2022. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489745

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1) *интернет-ресурсы библиотеки:*
- электронные учебно-методические ресурсы (ЭУМР),
- электронный каталог Web ИРБИС;

электронные библиотечные системы:

- ЭБС «Лань» – Режим доступа: http://e.lanbook.com
- ЭБС «Юрайт» - Режим доступа: https://biblio-online.ru;
- ЭБС «Руконт» - Режим доступа: http://lib.rucont.ru
- ЭБС «IPR BOOX» - Режим доступа: http://www.iprbookshop.ru

– доступ к информационным ресурсам «eLIBRARY», «УИС РОССИЯ» и «Polpred.com».

2) Справочная правовая система «Консультант Плюс»

3) система ЭИОС на платформе Moodle.

4) Профессиональные базы данных:

– официальный сайт Федеральной службы государственной статистики - http://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/accounts/ (Рынок труда, занятость и заработная плата);

– международная информационная система по сельскому хозяйству и смежным с ним отраслям – AGRIS http://agris.fao.org/agris-search/index.do

– базы данных официального сайта ФГБУ «Центр агроаналитики» Министерства сельского хозяйства Российской Федерации - http://www.specagro.ru

9. Методические указания для обучающихся по освоению дисциплины

Учебным планом при изучении дисциплины предусмотрены практические занятия, а также самостоятельная работа обучающихся.

Практические занятия проводятся с целью закрепления и более тщательной проработки материала по основным разделам дисциплины.

Чтобы получить необходимое представление о дисциплине и о процессе организации её изучения, целесообразно в первые дни занятий ознакомиться с рабочей программой дисциплины на платформе MOODLE или на сайте университета.

В процессе изучения дисциплины, обучающиеся должны самостоятельно изучить теоретическую часть материала, для чего необходимо ознакомиться с конспектом лекций, литературой, указанной в списке основной и дополнительной литературы.

Основные понятия и определения, используемые в курсе, можно эффективно закрепить, обратившись к тексту глоссария.

Проверить степень овладения дисциплиной помогут вопросы для самопроверки и самоконтроля (вопросы к зачету), ответы на которые позволят студенту систематизировать свои знания, а также тесты, выложенные на платформе MOODLE в фонде оценочных средств по дисциплине.

Применение электронного обучения: обучение возможно с применением электронных и дистанционных технологий.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

Для формирования этапов компетенций у обучающихся в процессе изучения данной дисциплины применяются традиционные (пассивные) и инновационные (активные) технологии обучения в зависимости от учебных целей с учетом различного сочетания форм организации образовательной деятельности и методов ее активизации с приоритетом на самостоятельную работу обучающихся.

Для успешного овладения дисциплиной используются следующие информационные технологии обучения:

При проведении лекций используются презентации материала в программе Microsoft Office (Power Point), выход на профессиональные сайты, использование видеоматериалов различных интернет-ресурсов.

Практические занятия по дисциплине проводятся с использованием платформы MOODLE, Справочной правовой системы «Консультант Плюс».

В процессе изучения дисциплины учебными целями являются восприятие учебной информации, ее усвоение, запоминание, а также структурирование полученных знаний и развитие интеллектуальных умений, ориентированных на способы деятельности репродуктивного характера. Посредством использования этих интеллектуальных умений достигаются узнавание ранее усвоенного материала в новых ситуациях, применение абстрактного знания в конкретных ситуациях.

Для достижения этих целей используются в основном традиционные информативно-развивающие технологии обучения с учетом различного сочетания пассивных форм (практическое занятие, консультация, самостоятельная работа) и репродуктивных методов обучения (повествовательное изложение учебной информации, объяснительно- иллюстративное изложение, чтение информативных текстов) и лабораторно-практических методов обучения (упражнение, инструктаж, проектно-организованная работа).

Для организации учебного процесса используется программное обеспечение, обновляемое согласно лицензионным соглашениям.

Программное обеспечение:

- Microsoft WinHome 10 RUS OLP NL Acdm Legalizatiom get Genuine (объем 168); Лицензия бессрочная. Контракт № ЭА - 103 от 17.05.2018.

- Kaspersky Total Security для бизнеса Russian Edition. 250-499. Node 2 year Educational Renewal License: Лицензионный сертификат 24342003031146291531071

Информационная справочная система:

Справочная правовая система «Консультант Плюс» Договор об информационной поддержке от 02.08.2011 г. (с ежегодным автоматическим продлением).

- Справочная правовая система «Консультант Плюс» Договор об информационной поддержке от 02.08.2011 г. (с ежегодным автоматическим продлением).

11. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Наименование специальных* помещений и помещений для самостоятельной работы	**Оснащенность специальных помещений и помещений для самостоятельной работы**	**Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа**
Учебная лаборатория «Информационные технологии профессиональной деятельности» для проведения лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации – 620075, Свердловская область, г. Екатеринбург, ул. Тургенева, д. 23 Литер А, ауд. № 4412	Аудитория, оснащенная столами и стульями. Переносные: - мультимедийное оборудование (ноутбук, экран, проектор); - комплект электронных учебно-наглядных материалов (презентаций) на флеш-носителях, обеспечивающих тематические иллюстрации. Рабочие места, оснащенные компьютерами с выходом в сеть Интернет и электронно - образовательную среду. Оборудование и программное обеспечение - в соответствие с паспортом лаборатории	Microsoft WinHome 10 RUS OLP NL Acdm Legalizatiom get Genuine (объем 168); Лицензия бессрочная. Контракт № ЭА - 103 от 17.05.2018. Kaspersky Total Security для бизнеса Russian Edition. 250-499. Node 2 year Educational Renewal License: Лицензионный сертификат 24342003031146291531071 1С: Предприятие 8. Комплект для обучения в высших и средних учебных заведениях (рег. № 800908077); Сельское хозяйство (рег. № 10380733). Лицензия бессрочная. Лицензионный договор 000287682/ЛД-12 от 15 марта 2012. Справочная правовая система «Консультант Плюс» Договор об информационной поддержке от 02.08.2011 г. (с ежегодным автоматическим продлением).
Самостоятельная работа		
Помещение для самостоятельной работы – 620075, Свердловская область, г. Екатеринбург, ул. Тургенева, д. 23 Литер А, ауд. № 4412, 4420 620075, Свердловская область, г. Екатеринбург, ул. Карла Либкнехта, д. 42	Аудитория, оснащенная столами и стульями; Переносным демонстрационным мультимедийным оборудованием (ноутбук, экран, проектор); рабочими местами, оснащенными компьютерами с выходом в сеть Интернет и электронно-образовательную среду	Microsoft WinHome 10 RUS OLP NL Acdm Legalizatiom get Genuine (объем 168); Лицензия бессрочная. Контракт № ЭА - 103 от 17.05.2018. Kaspersky Total Security для бизнеса Russian Edition. 250-499. Node 2 year Educational Renewal

Литер Е читальный зал - № 5104, 5208		License: Лицензионный сертификат 243420030311462915310 71

Помещение для хранения и профилактического обслуживания учебного оборудования: к. 4412а

12. Особенности обучения студентов с различными нозологиями

Для инвалидов и лиц с ограниченным возможностями здоровья предъявляются особые требования к организации образовательного процесса и выбору методов и форм обучения при изучении данной дисциплины, в случаи зачисления таких обучающихся.

Для обучения студентов с нарушением слуха предусмотрены следующие методы обучения:

- объяснительно-иллюстративный метод (лекция, работа с литературой);
- репродуктивный (студенты получают знания в готов виде);
- программированный или частично-поисковый (управление и контроль познавательной деятельности по схеме, образцу).

Для повышения эффективности занятия используются следующие средства обучения:

- учебная, справочная литература, работа с которой позволяет развивать речь, логику, умение обобщать и систематизировать информацию;
- словарь понятий, способствующих формированию и закреплению терминологии;
- структурно-логические схемы, таблицы и графики, концентрирующие и обобщающие информацию, опорные конспекты, активирующие различные виды памяти;
- раздаточный материал, позволяющий осуществить индивидуальный и дифференцированный подход, разнообразить приемы обучения и контроля;
- технические средства обучения.

Во время лекции используются следующие приемы:

- наглядность;
- использование различных форм речи: устной или письменной – в зависимости от навыков, которыми владеют студенты;
- разделение лекционного материала на небольшие логические блоки.

Учитывая специфику обучения слепых и слабовидящих студентов, соблюдаются следующие условия:

- дозирование учебных нагрузок;
- применение специальных форм и методов обучения, оригинальных учебников и наглядных пособий;

Во время проведения занятий происходит частое переключение внимания обучающихся с одного вида деятельности на другой. Также учитываются

продолжительность непрерывной зрительной нагрузки для слабовидящих. Учет зрительной работы строго индивидуален.

Искусственная освещенность помещения, в которых занимаются студенты с пониженным зрением, оставляет от 500 до 1000 лк. На занятиях используются настольные лампы.

Формы работы со студентами с нарушениями опорно-двигательного аппарата следующие:

- лекции групповые (проблемная лекция, лекция-презентация, лекция-диалог, лекция с применением дистанционных технологий и привлечением возможностей интернета).
- индивидуальные беседы;
- мониторинг (опрос, анкетирование).

Конкретные виды и формы самостоятельной работы обучающихся лиц с ограниченными возможностями здоровья и инвалидов устанавливаются преподавателем самостоятельно. Выбор форм и видов самостоятельной работы обучающихся с ОВЗ и инвалидов осуществляются с учетом их способностей, особенностей восприятия и готовности к освоению учебного материала. При необходимости обучающимся предоставляется дополнительное время для консультаций и выполнения заданий.

Приложение 1

1. ПЕРЕЧЕНЬ КОМПЕТЕНЦИЙ С УКАЗАНИЕМ ЭТАПОВ ИХ ФОРМИРОВАНИЯ В ПРОЦЕССЕ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код компетенции	Формулировка	Разделы дисциплины	
		1	2
ОПК-2	Способен осуществлять сбор, обработку и анализ данных, необходимых для решения поставленных управленческих задач, с использованием современного инструментария и интеллектуальных информационно-аналитических систем;	+	+
ОПК-5	Способен использовать при решении профессиональных задач современные информационные технологии и программные средства, включая управление крупными массивами данных и их интеллектуальный анализ	+	+

2. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ НА РАЗЛИЧНЫХ ЭТАПАХ ИХ ФОРМИРОВАНИЯ, ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

2.1 Шкала академических оценок освоения дисциплины

Виды оценок	Оценки			
Академическая оценка по 4-х балльной шкале (зачет с оценкой)	отлично,	хорошо	удовлетворительно,	неудовлетворительно

2.2 Текущий контроль

Код	Планируемые результаты	Раздел дисциплины	Содержание требования в разрезе разделов дисциплины	Технология формирования	Форма оценочного средства (контроля)	№ задания		
						Пороговый уровень (удовл.)	Повышенный уровень (хорошо)	Высокий уровень (отлично)
ОПК-2	Знать: - основные понятия и терминологию информационной безопасности в бизнес-аналитике, современные информационные технологии и программные средства; - способы сбора, обработки и анализа данных для решения управленческих задач.	1	Тема 1.1. Основные понятия и определения Тема 1.2. Задачи информационной безопасности в бизнес -аналитике	Лекция Практические занятия Самостоятельная работа	Письменная работа, практические задания, тест	пункт 3.3., пункта 3.2., пункт 3.4.	пункт 3.3., пункта 3.2., пункт 3.4.	пункт 3.3., пункта 3.2., пункт 3.4.
	Уметь: - проводить интеллектуальный анализ данных в по бизнес-аналитике в управленческой деятельности.	1	Тема 1.3. Угрозы информационной безопасности в бизнес –аналитике Тема 1.4. Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере	Лекция Практические занятия Самостоятельная работа				
	Владеть: - навыками управления крупными массивами данных.	1	Тема 1.5. Понятие и виды защищаемой информации в бизнес –аналитике.	Лекция Практические занятия Самостоятельн				

				ая работа				
ОПК-5	Знать: - методы обеспечения информационной безопасности, в том числе в бизнес-аналитике.	2	Тема 2.1. Общая характеристика способов и средств защиты информации в бизнес –аналитике	Лекция Практические занятия Самостоятельная работа	Письменная работа, практические задания	пункт 3.3., пункта 3.2.,	пункт 3.3., пункта 3.2.,	пункт 3.3., пункта 3.2.,
	Уметь: - применять на практике современный инструментарий и интеллектуальные; информационно-аналитические системы в бизнес-аналитике, а также обеспечивать их информационную безопасность.	2	Тема 2.2. Криптографические методы защиты информации в бизнес –аналитике Тема 2.3. Методы организации безопасного доступа Тема 2.4. Электронная цифровая подпись и цифровые сертификаты	Лекция Практические занятия Самостоятельная работа				
	Владеть: - навыками работы с программно-аппаратными средства защиты информации.	2	Тема 2.5. Программно-аппаратные средства защиты информации в бизнес -аналитике	Лекция Практические занятия Самостоятельная работа				

2.3 Промежуточная аттестация

Код	Планируемые результаты	Технология формирования	Форма оценочного средства (контроля)	№ задания		
				Пороговый уровень (удовл.)	Повышенный уровень (хорошо)	Высокий уровень (отлично)
ОПК-2 ОПК-5	**Знать:** - основные понятия и терминологию информационной безопасности в бизнес-аналитике, современные информационные технологии и программные средства; - способы сбора, обработки и анализа данных для решения управленческих задач; - методы обеспечения информационной безопасности, в том числе в бизнес-аналитике.	Лекция Практические занятия Самостоятельная работа	Зачет с оценкой	Из пункта 3.1.		
	Уметь: - применять на практике современный инструментарий и интеллектуальные информационно-аналитические системы в бизнес-аналитике, а также обеспечивать их информационную безопасность; - проводить интеллектуальный анализ данных в по бизнес-аналитике в управленческой деятельности.					
	Владеть: - навыками управления крупными массивами данных.					

2.4. Критерии оценки на зачете (вопросы к зачету)

Результат экзамена	Критерии оценки	Показатель оценки сформированности компетенции
Отлично (повышенный)	- ставится в том случае, когда студент обнаруживает систематическое и глубокое знание программного материала по дисциплине, умеет свободно ориентироваться в вопросе. Ответ полный и правильный на основании изученного материала. Выдвинутые положения аргументированы и иллюстрированы примерами. Материал изложен в определенной логической последовательности, осознанно, литературным языком, с использованием современных научных терминов; ответ самостоятельный. Студент уверенно отвечает на дополнительные вопросы.	Не менее 86-100% В результате оценки студент показал сформированность компетенций
Хорошо (базовый)	- ставится в том случае, когда студент обнаруживает полное знание учебного материала, демонстрирует систематический характер знаний по дисциплине. Ответ полный и правильный, подтвержден примерами; но их обоснование не аргументировано, отсутствует собственная точка зрения. Материал изложен в определенной логической последовательности, при этом допущены 2-3 несущественные погрешности, исправленные по требованию экзаменатора. Студент испытывает незначительные трудности в ответах на дополнительные вопросы. Материал изложен осознанно, самостоятельно, с использованием современных научных терминов, литературным языком.	Не менее 71-85% В результате оценки студент показал частично сформированность компетенций
Удовлетворительно (пороговый)	- ставится в том случае, когда студент обнаруживает знание основного программного материала по дисциплине, но допускает погрешности в ответе. Ответ недостаточно логически выстроен, самостоятелен. Основные понятия употреблены правильно, но обнаруживается недостаточное раскрытие теоретического материала. Выдвигаемые положения недостаточно аргументированы и не подтверждены примерами; ответ носит преимущественно описательный характер. Студент испытывает достаточные трудности в ответах на вопросы. Научная терминология используется недостаточно.	. Не менее 55-70% В результате оценки студент показал частично сформированность компетенций

Неудовлетворительно	- ставится в том случае, когда студент демонстрирует пробелы в знаниях основного учебного материала по дисциплине. При ответе обнаружено непонимание студентом основного содержания теоретического материала или допущен ряд существенных ошибок, которые студент не может исправить при наводящих вопросах экзаменатора, затрудняется в ответах на вопросы. Студент подменил научное обоснование проблем рассуждением бытового плана. Ответ носит поверхностный характер; наблюдаются неточности в использовании научной	Менее 45-55% В результате оценки студент не показал сформированность компетенций

2.5. Критерии оценки письменной работы

Ступени уровней освоения компетенций	Критерии
Повышенный уровень (отлично)	Содержание ответа в целом соответствует теме задания. Продемонстрировано знание фактического материала, отсутствуют фактические ошибки. Продемонстрировано уверенное владение понятийно-терминологическим аппаратом дисциплины (уместность употребления, аббревиатуры, толкование и т.д.), отсутствуют ошибки в употреблении терминов. Показано умелое использование категорий и терминов дисциплины в их ассоциативной взаимосвязи.
Базовый уровень (хорошо)	1) недостаточно полное, по мнению преподавателя, раскрытие темы; 2) несущественные ошибки в определении понятий, категорий и т.п., кардинально не меняющих суть изложения; 3) использование устаревшей учебной литературы и других источников; 4) неспособность осветить проблематику учебной дисциплины и др.
Пороговый уровень (удовлетворительно)	1) отражение лишь общего направления изложения лекционного материала и материала современных учебников; 2) наличие достаточного количества несущественных или одной-двух существенных ошибок в определении понятий и категорий и т.п.; 3) неспособность осветить проблематику учебной дисциплины и др.

2.6. Критерии оценки практического задания

Ступени уровней освоения компетенций	Критерии
Повышенный уровень (отлично)	1)задача решена правильно. 2)сделаны полные, соответствующие задаче выводы
Базовый уровень (хорошо)	1) задача решена правильно, есть некоторые неточности 2) сделаны краткие выводы
Пороговый уровень (удовлетворительно)	1) задача решена не полностью 2) нет выводов

2.7. Критерии оценки теста

Ступени уровней освоения компетенций	Отличительные признаки	Показатель оценки сформированности компетенции
Пороговый (удовлетвори-тельно)	Обучающийся воспроизводит термины, основные понятия, способен узнавать методы, процедуры, свойства.	Обучающийся воспроизводит термины, основные понятия, способен узнавать методы, процедуры, свойства - не менее 70% правильных ответов на тестовые задания
Базовый (хорошо)	Обучающийся выявляет взаимосвязи, классифицирует, упорядочивает, интерпретирует.	Обучающийся выявляет взаимосвязи, классифицирует, упорядочивает, интерпретирует.- не менее 80% правильных ответов
Повышенный (отлично)	Обучающийся анализирует, диагностирует, оценивает, прогнозирует, конструирует.	Обучающийся анализирует, оценивает, прогнозирует- 90% и более правильных ответов
Компетенция не сформирована	-	Обучающийся набрал менее 70% правильных ответов на задания

2.8. Процедура оценка

2.8.1 Работа в семестре

В течение семестра в ходе выполнения заданий в виде устного опроса, письменной работы, ситуационных задач студент получает допуск к экзамену

№ п/п	Измерители обученности текущего контроля	Ступени уровней освоения компетенций		
1.	Практическое задание	Пороговый уровень (удовлетворительно)	Базовый уровень (хорошо)	Повышенный уровень (отлично)
2.	Письменная работа	Пороговый уровень (удовлетворительно)	Базовый уровень (хорошо)	Повышенный уровень (отлично)
3.	Тест	Пороговый уровень (удовлетворительно)	Базовый уровень (хорошо)	Повышенный уровень (отлично)

Студент, выполнивший задания не ниже порогового (удовлетворительно) допускается до экзамена.

2.8.2 Промежуточная аттестация

Зачет с оценкой проводится в форме ответов на вопросы

Для формирования итоговой оценки знаний, умений и навыков сформированности компетенций студент отвечает на экзаменационные вопросы.

№ п/п	Измерители обученности текущего контроля	Ступени уровней освоения компетенций		
1.	Зачет с оценкой (вопросы)	Пороговый уровень (удовлетворительно)	Базовый уровень (хорошо)	Повышенный уровень (отлично)

3. ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ В ПРОЦЕССЕ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

3.1 Вопросы к зачету

1. Назовите основные направления обеспечения безопасности предприятия.
2. Определите цели и задачи системы безопасности предприятия.
3. Представьте возможную структуру службы безопасности предприятия.
4. Что такое и зачем необходима концепция безопасности предприятия?
5. Что такое «угроза» безопасности предприятия?
6. Приведите основные параметры концептуальной модели безопасности предприятия.
7. Прокомментируйте организацию информационного процесса в компании.
8. Перечислите классические объекты наблюдения и информационные источники фактографических данных.
9. Охарактеризуйте основные каналы получения информации.
10. Назовите и прокомментируйте основные положения правовых документов (Законов РФ),
регламентирующих законную основу сбора информации о предприятиях сторонними субъектами.
11. Назовите основные легальные, полулегальные и нелегальные методы сбора информации.
12. Почему качественный подбор и расстановка кадров является условием обеспечения безопасности организации.
13. Предложите перечень сведений при проверке личности кандидата на работу.
14. Назовите качества и особенности личности, могущие способствовать вовлечению в деятельность, направленную на нанесение ущерба организации.
15. Прокомментируйте мошенничество как угрозу безопасности предприятию (причины, способы и формы проявления).
16. Определите сущность финансовой составляющей экономической безопасности предприятия.
17. Назовите составные части обеспечения финансовой составляющей экономической безопасности предприятия.
18. Приведите вид карты расчета эффективности принимаемых мер по обеспечению финансовой составляющей экономической безопасности предприятия.
19. Определите объекты и субъекты информационной безопасности предприятия.
20. Охарактеризуйте понятие угрозы информационной безопасности предприятия и прокомментируйте ее основные свойства.
21. Что понимают под ущербом, наносимым предприятию в результате воздействия угроз информационной безопасности.
22. Систематизируйте и проанализируйте организационные каналы передачи и обмена информацией.
23. Охарактеризуйте основные методы, силы и средства, используемые для организации системы защиты информации.
24. Как обеспечить безопасность компании при найме персонала? Критерии пригодности, этапы отбора кандидатов.
25. Как обеспечить проверку работника на лояльность фирме, на честность в работе, на

возможные связи с криминальными структурами, на соблюдение коммерческой тайны.
26. Какие новые психотехнологии работы с персоналом могут обеспечить безопасность предприятия.
27. Недобросовестная конкуренция, ее место в современной экономики.
28. Основные методы противодействия недобросовестной конкуренции.
29. Назовите признаки компьютерных преступлений в интернет технологиях
30. Перечислите основные технологии и методы компьютерных преступлений.
31. Какие существуют модели информационной безопасности?
32. Какие методы защиты информации выделяют?
33. Что такое правовые методы защиты информации?
34. Что такое организационные методы защиты информации?
35. Что такое технические методы защиты информации?
36. Что такое программно-аппаратные методы защиты информации?
37. Что такое криптографические методы защиты информации?
38. Что такое физические методы защиты информации?
39. Какие главные государственные органы в области обеспечения информационной безопасности?
40. Перечислите виды защищаемой информации.

3.2. Практическое задание

Задание 1.

Понятие об информационном рынке (рынке информационных продуктов и информационных услуг). Этапы развития ЮИС..Роль и место информационных технологий в развитии современных юридических систем. Роль и место ЮИС в управлении. Технология работы в ЮИС Понятие технологического процесса обработки юридической информации. Основные этапы технологического процесса и составляющие их операции. Основные функции, реализуемые с применением информационных технологий: сбор, накопление, ввод, обработка, генерация, хранение, поиск, передача и предоставление юридической информации пользователю

Задание 2.

Информационно-поисковые справочные и консультационные юридические системы и их использование в юриспруденции.. Справочно-правовые информационные системы. Характеристика справочно -правовых информационных систем. Обзор существующих СПИС. Сетевые и локальные СПИС. Универсальные и специализированные СПИС Понятие, назначение, отличительные черты АИС констатирующего типа. Обзор современных программных продуктов в области тестирования юридического состояния предприятий Понятие, назначение, отличительные черты АИС моделирующего типа. Обзор современных программных продуктов, поддерживающих указанную технологию: интегрированные пакеты Project Expert.

3.3 Письменная работа

Письменная работа студента – это самостоятельная письменная работа на тему, предложенную преподавателем (тема может быть предложена и студентом, но обязательно должна быть согласована с преподавателем). Цель письменной работы состоит в развитии навыков самостоятельного творческого мышления и письменного изложения собственных мыслей.

Письменная работа должно содержать: четкое изложение сути поставленной проблемы, включать самостоятельно проведенный анализ этой проблемы с

использованием концепций и аналитического инструментария, рассматриваемого в рамках дисциплины, выводы, обобщающие авторскую позицию по поставленной проблеме.

Структура письменной работы:

1. Титульный лист;
2. Введение – суть и обоснование выбора данной темы, состоит из ряда компонентов, связанных логически и стилистически.

На этом этапе очень важно правильно сформулировать вопрос, на который вы собираетесь найти ответ в ходе своего исследования.

3. Основная часть – теоретические основы выбранной проблемы и изложение основного вопроса. Данная часть предполагает развитие аргументации и анализа, а также обоснование их, исходя из имеющихся данных, других аргументов и позиций по этому вопросу, свидетельствовать о наличии или отсутствии логичности в освещении темы.

Заключение – обобщения и аргументированные выводы по теме с указанием области ее применения и т.д.

Темы письменных работ

1. Основные концептуальные положения системы защиты информации
2. Концептуальная модель информационной безопасности
3. Угрозы конфиденциальной информации
4. Действия, приводящие к неправомерному овладении конфиденциальной информацией
5. Общие положения способов защиты информации
6. Характеристика основных защитных действий
7. Правовая защита информации
8. Организационная защита информации
9. Общие положения по инженерно-технической защите информации в таможенном деле
10. Физические средства защиты информации в таможенном деле
11. Аппаратные средства защиты информации в таможенном деле
12. Программные средства защиты информации в таможенном деле
13. Криптографические средства защиты информации в таможенном деле
14. Общие положения о способах защиты информации
15. Характеристика защитных действий
16. Защита информации от утечки по визуально оптическим каналам
17. Защита информации от утечки по акустическим каналам
18. Защита информации от утечки за счет микрофонного эффекта
19. Защита от утечки за счет электромагнитного излучения
20. Защита от утечки за счет паразитной генерации

3.4.Тест

1) К правовым методам, обеспечивающим информационную безопасность, относятся:
а. Разработка аппаратных средств обеспечения правовых данных
б. Разработка и установка во всех компьютерных правовых сетях журналов учета действий
в. Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:
а. Хищение жестких дисков, подключение к сети, инсайдерство
б. Перехват данных, хищение данных, изменение архитектуры системы
в. Хищение данных, подкуп системных администраторов, нарушение регламента работы
3) Виды информационной безопасности:
а. Персональная, корпоративная, государственная
б. Клиентская, серверная, сетевая
в. Локальная, глобальная, смешанная
4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
а. несанкционированного доступа, воздействия в сети
б. инсайдерства в организации
в. чрезвычайных ситуаций
5) Основные объекты информационной безопасности:
а. Компьютерные сети, базы данных
б. Информационные системы, психологическое состояние пользователей
в. Бизнес-ориентированные, коммерческие системы
6) Основными рисками информационной безопасности являются:
а. Искажение, уменьшение объема, перекодировка информации
б. Техническое вмешательство, выведение из строя оборудования сети
в. Потеря, искажение, утечка информации
7) К основным принципам обеспечения информационной безопасности относится:
а. Экономической эффективности системы безопасности
б. Многоплатформенной реализации системы
в. Усиления защищенности всех звеньев системы
8) Основными субъектами информационной безопасности являются:
а. руководители, менеджеры, администраторы компаний
б. органы права, государства, бизнеса
в. сетевые базы данных, фаерволлы
9) К основным функциям системы безопасности можно отнести все перечисленное:
а. Установление регламента, аудит системы, выявление рисков
б. Установка новых офисных приложений, смена хостинг-компании
в. Внедрение аутентификации, проверки контактных данных пользователей
10) Принципом информационной безопасности является принцип недопущения:
а. Неоправданных ограничений при работе в сети (системе)
б. Рисков безопасности сети, системы
в. Презумпции секретности
11) Принципом политики информационной безопасности является принцип:
а. Невозможности миновать защитные средства сети (системы)
б. Усиления основного звена сети, системы
в. Полного блокирования доступа при риск-ситуациях
12) Принципом политики информационной безопасности является принцип:
а. Усиления защищенности самого незащищенного звена сети (системы)
б. Перехода в безопасное состояние работы сети, системы
в. Полного доступа пользователей ко всем ресурсам сети, системы
13) Принципом политики информационной безопасности является принцип:
а. Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
б. Одноуровневой защиты сети, системы

в. Совместимых, однотипных программно-технических средств сети, системы
14) К основным типам средств воздействия на компьютерную сеть относится:
а. Компьютерный сбой
б. Логические закладки («мины»)
в. Аварийное отключение питания
15) Когда получен спам по e-mail с приложенным файлом, следует:
а. Прочитать приложение, если оно не содержит ничего ценного – удалить
б. Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
в. Удалить письмо с приложением, не раскрывая (не читая) его
16) Принцип Кирхгофа:
а. Секретность ключа определена секретностью открытого сообщения
б. Секретность информации определена скоростью передачи данных
в. Секретность закрытого сообщения определяется секретностью ключа
17) ЭЦП – это:
а. Электронно-цифровой преобразователь
б. Электронно-цифровая подпись
в. Электронно-цифровой процессор
18) Наиболее распространены угрозы информационной безопасности корпоративной системы:
а. Покупка нелицензионного ПО
б. Ошибки эксплуатации и неумышленного изменения режима работы системы
в. Сознательного внедрения сетевых вирусов
19) Наиболее распространены угрозы информационной безопасности сети:
а. Распределенный доступ клиент, отказ оборудования
б. Моральный износ сети, инсайдерство
в. Сбой (отказ) оборудования, нелегальное копирование данных
20) Наиболее распространены средства воздействия на сеть офиса:
а. Слабый трафик, информационный обман, вирусы в интернет
б. Вирусы в сети, логические мины (закладки), информационный перехват
в. Компьютерные сбои, изменение администрирования, топологии
21) Утечкой информации в системе называется ситуация, характеризуемая:
а. Потерей данных в системе
б. Изменением формы информации
в. Изменением содержания информации
22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
а. Целостность
б. Доступность
в. Актуальность
23) Угроза информационной системе (компьютерной сети) – это:
а. Вероятное событие
б. Детерминированное (всегда определенное) событие
в. Событие, происходящее периодически
24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
а. Регламентированной
б. Правовой
в. Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:
а. Программные, технические, организационные, технологические
б. Серверные, клиентские, спутниковые, наземные
в. Личные, корпоративные, социальные, национальные
26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:
а. Владелец сети
б. Администратор сети
в. Пользователь сети
27) Политика безопасности в системе (сети) – это комплекс:
а. Руководств, требований обеспечения необходимого уровня безопасности
б. Инструкций, алгоритмов поведения пользователя в сети
в. Нормы информационного права, соблюдаемые в сети
28) Наиболее важным при реализации защитных мер политики безопасности является:
а. Аудит, анализ затрат на проведение защитных мер
б. Аудит, анализ безопасности
в. Аудит, анализ уязвимостей, риск-ситуаций

4. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРУ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ

4.1 Методические указания по проведению текущего контроля

4.1.1. Решение практических заданий

1.	Сроки проведения текущего контроля	После изучения соответствующих тем дисциплины
2.	Место и время проведения текущего контроля	В учебной аудитории во время занятия
3.	Требование к техническому оснащению аудитории	В соответствии с паспортом аудитории
4.	Ф.И.О. преподавателя (ей), проводящих процедуру контроля	
5.	Вид и форма заданий	Практическая задача
6.	Время решения практических задач	Во время практических занятий
7.	Возможность использования дополнительных материалов:	Обучающийся может пользоваться дополнительными материалами
8.	Ф.И.О. преподавателя (ей), обрабатывающих результаты	
9.	Методы оценки результатов	Экспертный
10.	Предъявление результатов	Оценка выставляется в журнал и доводится до сведения обучающихся после решения практической задачи
11.	Апелляция результатов	В порядке, установленном нормативными документами, регулирующими образовательный процесс в ФГБОУ ВО Уральский ГАУ

4.1.2 Тест

1.	Сроки проведения текущего контроля	После изучения соответствующих тем дисциплины
2.	Место и время проведения текущего контроля	В учебной аудитории во время занятия
3.	Требование к техническому оснащению аудитории	В соответствии с паспортом аудитории
4.	Вид и форма заданий	Тест
5.	Время проведения опроса	30-40 минут
6.	Возможность использования дополнительных материалов:	Обучающийся не может пользоваться дополнительными материалами
7.	Методы оценки результатов	Экспертный
8.	Предъявление результатов	Оценка выставляется в журнал и доводится до сведения обучающихся в конце опроса

9.	Апелляция результатов	В порядке, установленном нормативными документами, регулирующими образовательный процесс в ФГБОУ ВО Уральский ГАУ

4.1.3 Письменная работа

12.	Сроки проведения текущего контроля	После изучения соответствующих тем дисциплины
13.	Место и время проведения текущего контроля	В учебной аудитории во время занятия
14.	Требование к техническому оснащению аудитории	В соответствии с паспортом аудитории
15.	Ф.И.О. преподавателя (ей), проводящих процедуру контроля	
16.	Вид и форма заданий	Письменная работа
17.	Время проведения опроса	30 минут
18.	Возможность использования дополнительных материалов:	Обучающийся не может пользоваться дополнительными материалами
19.	Ф.И.О. преподавателя (ей), обрабатывающих результаты	
20.	Методы оценки результатов	Экспертный
21.	Предъявление результатов	Оценка выставляется в журнал и доводится до сведения обучающихся в конце опроса
22.	Апелляция результатов	В порядке, установленном нормативными документами, регулирующими образовательный процесс в ФГБОУ ВО Уральский ГАУ

4.2 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций

Оценка знаний, умений, навыков, характеризующая этапы формирования компетенций проводится в форме текущей и промежуточной аттестации.

Контроль текущей успеваемости обучающихся – текущая аттестация – проводится в ходе семестра с целью определения уровня усвоения обучающимися знаний; формирования у них умений и навыков; своевременного выявления преподавателем недостатков в подготовке обучающихся и принятия необходимых мер по ее корректировке; совершенствованию методики обучения; организации учебной работы и оказания обучающимся индивидуальной помощи.

К контролю текущей успеваемости относятся проверка знаний, умений и навыков обучающихся:

- на занятиях (опрос, тестирования, круглый стол, решение задач, творческие задания, деловая игра);

▪ по результатам выполнения индивидуальных заданий ;
▪ по результатам проверки качества конспектов лекций и иных материалов;
▪ по результатам отчета обучающихся в ходе индивидуальной консультации преподавателя, проводимой в часы самоподготовки, по имеющимся задолженностям.

Промежуточная аттестация по дисциплине проводится с целью выявления соответствия уровня теоретических знаний, практических умений и навыков по дисциплине требованиям ФГОС ВО в форме предусмотренной учебным планом.

Промежуточная аттестация проводится после завершения изучения дисциплины в объеме рабочей учебной программы. Форма определяется кафедрой (устный – по билетам, либо путем собеседования по вопросам; письменная работа, тестирование и др.). Оценка по результатам экзамена – «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» (оценка по результатам зачета – «зачтено» или «не зачтено»).

Каждая компетенция (или ее часть) проверяется теоретическими вопросами, позволяющими оценить уровень освоения обучающимися знаний и практическими заданиями, выявляющими степень сформированности умений и навыков.

Процедура оценивания компетенций обучающихся основана на следующих стандартах:

1. Периодичность проведения оценки (на каждом занятии).

2. Многоступенчатость: оценка (как преподавателем, так и обучающимися группы) и самооценка обучающегося, обсуждение результатов и комплекса мер по устранению недостатков.

3. Единство используемой технологии для всех обучающихся, выполнение условий сопоставимости результатов оценивания.

4. Соблюдение последовательности проведения оценки: предусмотрено, что развитие компетенций идет по возрастанию их уровней сложности, а оценочные средства на каждом этапе учитывают это возрастание.