Министерство сельского хозяйства Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ЛУГАНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ ИМЕНИ К.Е. ВОРОШИЛОВА»

«Утверждаю»
Декан факультета экономики и управления АПК

Шевченко М.Н. _____
«20» июня 2024 г.

РАБОЧАЯ ПРОГРАММА

учебной дисциплины «Информационная безопасность»

для направления подготовки 38.03.05 Бизнес-информатика

направленность (профиль) Бизнес-информатика

Год начала подготовки – 2024

Квалификация выпускника – бакалавр

Луганск, 2024

Рабочая программа составлена с учетом требований:

- порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 06.04.2021 № 245 (с изменениями и дополнениями);
- федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 38.03.05 Бизнес- информатика, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 29.07.2020г. № 838 (с изменениями и дополнениями).

Преподаватели, подготовившие рабочую программу:

старший преподаватель _____ **Ю.А. Горячкова**
кафедры информационных технологий,
математики и физики

Рабочая программа рассмотрена на заседании кафедры информационных технологий, математики и физики (протокол № 10 от «27» мая 2024 г.).

Заведующий кафедрой _____ **В.Ю. Ильин**

Рабочая программа рекомендована к использованию в учебном процессе методической комиссией факультета экономики и управления АПК (протокол № 10/1 от «19» июня 2024 г.).

Председатель методической комиссии _____ **А.В. Худолей**

Руководитель основной профессиональной образовательной программы _____ **В.Ю. Ильин**

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

Предмет дисциплины включает:

– основы правового регулирования отношений в информационной сфере;

– конституционные гарантии прав граждан на получение информации и механизм их реализации;

– понятия и виды защищаемой информации по законодательству РФ;

систему защиты государственной тайны;

– основы правового регулирования отношений в области интеллектуальной собственности и способы защиты этой собственности;

– понятие и виды компьютерных преступлений.

Цель изучения дисциплины: формирование у студентов навыков, связанных с обеспечением защиты информации; творческих подходов при решении сложных научно-технических задач, связанных с обеспечением информационной безопасности объектов информатизации; создание представления об основах информационной безопасности, принципах и методах противодействия несанкционированному информационному воздействию; развитие способностей к логическому и алгоритмическому мышлению.

Задачи изучения дисциплины:

– изучить место и роль информационной безопасности в системе национальной безопасности;

– изучить основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы в данной области; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;

– освоить принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;

– сформировать умения и навыки проведения анализа и оценки угроз информационной безопасности объекта;

– получить навыки работы с современными технологиями обеспечения информационной безопасности.

Место дисциплины в структуре образовательной программы.

Дисциплина «Информационная безопасность» относится к части, формируемой участниками образовательных отношений (Б1.В.08) блока дисциплин подготовки студентов по направлению подготовки 38.03.05 Бизнес-информатика, направление подготовки Бизнес-информатика основой профессиональной образовательной программы высшего образования (далее – ОПОП ВО).

Дисциплина реализуется кафедрой информационных технологий, математики и физики в 6 семестре. Основывается на базе дисциплин: «Современные информационные технологии» и системы искусственного интеллекта», «Базы данных», «Планирование и управление данными». Предшествует дисциплинам: «Системы искусственного интеллекта», «Основы интернет технологий», «Управление информационными ресурсами и контентом».

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

Коды компетенций	Формулировка компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения
ПК-1	Способен формировать возможные решения на основе разработанных для них целевых показателей с учетом имеющихся факторов, условий и рисков и анализа требований заинтересованных сторон с точки зрения выбранных критериев	**ПК–1.1.** Осуществляет выявление, сбор, систематизацию, хранение, поддержание в актуальном состоянии, анализ, определение зависимости между элементами информации бизнес-анализа для формирования возможных решений используя современные методы исследования и применяя информационные технологии	**Знать:** назначение и функции информационных технологий и современных программных продуктов для решения профессиональных задач **иметь:** определять назначение и функции информационных систем и технологий для решения профессиональных задач **иметь навыки:** работы с информационными системами и технологиями для решения профессиональных задач
		ПК-1.4. Составляет описание возможных решений в соответствии с выбранными подходами с учетом имеющихся факторов, условий и рисков	**Знать:** информационные технологии и программные средства для решения профессиональных задач **уметь:** применять информационные технологии и программные средства для решения профессиональных задач **иметь навыки:** применения информационные технологии и программные средства для решения профессиональных задач

3. Объём дисциплины и виды учебной работы

Виды работ	Очная форма обучения		Заочная форма обучения	Очно-заочная форма обучения
	всего	в т.ч. по семестрам	всего часов	всего часов
		6 семестр	–	6 семестр
Общая трудоёмкость дисциплины, зач.ед./часов, в том числе:	3/108	3/108	–	3/108
Контактная работа, часов:	36	36	–	22
- лекции	14	14	–	10
- практические (семинарские) занятия	22	22	–	12
- лабораторные работы	–	–	–	–
Самостоятельная работа, часов	72	72	–	86
Контроль, часов	–	–	–	–
Вид промежуточной аттестации (зачёт, экзамен)	зачет с оценкой	зачет с оценкой	–	зачет с оценкой

4. Содержание дисциплины

4.1. Разделы дисциплины и виды занятий (тематический план)

Раздел дисциплины (тема)	Л	ПЗ	ЛР	СРС
Очная форма обучения				
Тема 1. Введение в информационную безопасность	1	2		8
Тема 2. Правовое обеспечение информационной безопасности	2	2		8
Тема 3. Организационное обеспечение информационной безопасности	2	2		8
Тема 4. Технические средства и методы защиты информации	2	2		8
Тема 5. Программно-аппаратные средства и методы обеспечения информационной безопасности	2	4		8
Тема 6. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	2	2		8
Тема 7. Средства восстановления данных	1	4		8
Тема 8. Средства антивирусной защиты информации	1	2		8
Тема 9. Политика информационной безопасности организации (предприятия)	1	2		8
Всего	**14**	**22**		**72**
Заочная форма обучения				
–	–	–	–	–

Очно-заочная форма обучения				
Тема 1. Введение в информационную безопасность	1	1	–	8
Тема 2. Правовое обеспечение информационной безопасности	1	1	–	10
Тема 3. Организационное обеспечение информационной безопасности	1	1	–	10
Тема 4. Технические средства и методы защиты информации	1	2	–	10
Тема 5. Программно-аппаратные средства и методы обеспечения информационной безопасности	2	2	–	10
Тема 6. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	1	1	–	10
Тема 7. Средства восстановления данных	1	2	–	10
Тема 8. Средства антивирусной защиты информации	1	1	–	10
Тема 9. Политика информационной безопасности организации (предприятия)	1	1	–	8
Всего	**10**	**12**	**–**	**86**

4.2. Содержание разделов учебной дисциплины

Тема 1. Введение в информационную безопасность.

Теоретические аспекты информационной безопасности. Составляющие информационной безопасности. Доступность информации. Целостность информации. Конфиденциальность информации.

Тема 2. Правовое обеспечение информационной безопасности.

Доктрина информационной безопасности Российской Федерации. Концепция информационной безопасности сетей связи общего пользования Российской Федерации. Вопрос правового обеспечения информационной безопасности в Российской Федерации.

Тема 3. Организационное обеспечение информационной безопасности.

Основные понятия организационного обеспечения информационной безопасности. Административный уровень информационной безопасности. Программа безопасности. Уровни детализации политики информационной безопасности.

Тема 4. Технические средства и методы защиты информации.

Оценка безопасности информационных систем. Структура системы информационной безопасности.

Тема 5. Программно-аппаратные средства и методы обеспечения информационной безопасности.

Аппаратные средства защиты информации. Вспомогательные аппаратные средства защиты информации. Основные и вспомогательные программные средства защиты информации.

Тема 6. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности.

Общая структура правового режима информационной безопасности. Нормы и институты правового обеспечения информационной безопасности.

Тема 7.Средства восстановления данных.

Средства резервного копирования, восстановления, защиты данных в операционных системах Windows.

Тема 8. Средства антивирусной защиты информации.

Средства антивирусной защиты информации. Источники вирусов. Признаки заражения и антивирусные программы.

Тема 9. Политика информационной безопасности организации (предприятия).

Анализ структурно-функциональных особенностей предприятия с точки зрения политики безопасности. Теоретические основы построения моделей политики информационной безопасности. Формирование оценки угрозы доступности, целостности, конфиденциальности на предприятии.

4.3. Перечень тем лекций

№ п/п	Тема лекции	Объём, ч		
		форма обучения		
		очная	заочная	очно-заочная
1.	Тема лекционного занятия 1. Введение в информационную безопасность	1	–	1
2.	Тема лекционного занятия 2. Правовое обеспечение информационной безопасности	2	–	1
3.	Тема лекционного занятия 3. Организационное обеспечение информационной безопасности	2	–	1
4.	Тема лекционного занятия 4. Технические средства и методы защиты информации	2	–	1
5.	Тема лекционного занятия 5. Программно-аппаратные средства и методы обеспечения информационной безопасности	2	–	2
6.	Тема лекционного занятия 6. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	2	–	1
7.	Тема лекционного занятия 7. Средства восстановления данных	1	–	1
8.	Тема лекционного занятия 8. Средства антивирусной защиты информации	1	–	1
9.	Тема лекционного занятия 9. Политика информационной безопасности организации (предприятия)	1	–	1
Всего		**14**	**–**	**10**

4.4. Перечень тем практических (семинарских) занятий

№ п/п	Тема практического (семинарского) занятия	Объём, ч		
		форма обучения		
		очная	заочная	очно-заочная
1.	Тема практического занятия 1. Установка и первоначальная настройка VM VirtualBox	2	–	1
2.	Тема практического занятия 2. Разграничение прав доступа системы	2	–	1

3.	Тема практического занятия 3. Файловые подсистемы	2	–	1
4.	Тема практического занятия 4. Обеспечение целостности и доступности данных	2	–	1
5.	Тема практического занятия 5. Восстановление данных	4	–	2
6.	Тема практического занятия 6. Антивирусная защита компьютера	2	–	1
7.	Тема практического занятия 7. Безопасность на уровне операционной системы и приложений	4	–	2
8.	Тема практического занятия 8. Настройки безопасности интернет обозревателей	2	–	1
9	Тема практического занятия 9. Основы информационной безопасности при работе с облачными технологиями	2	–	2
Всего		**22**	**–**	**12**

4.5. Перечень тем лабораторных работ.

Не предусмотрены.

4.6. Виды самостоятельной работы студентов и перечень учебно-методического обеспечения для самостоятельной работы обучающихся

4.6.1. Подготовка к аудиторным занятиям

Материалы лекций являются основой для изучения теоретической части дисциплины и подготовки студента к практическим занятиям.

При подготовке к аудиторным занятиям студент должен:

- изучить рекомендуемую литературу;
- просмотреть самостоятельно дополнительную литературу по изучаемой теме.

Основной целью практических занятий является изучение отдельных наиболее сложных и интересных вопросов в рамках темы, а также контроль за степенью усвоения пройдённого материала и ходом выполнения студентами самостоятельной работы.

4.6.2. Перечень тем курсовых работ (проектов)

Не предусмотрены.

4.6.3. Перечень тем рефератов, расчетно-графических работ и иных видов индивидуальных работ

Не предусмотрены.

4.6.4. Перечень тем и учебно-методического обеспечения для самостоятельной работы обучающихся

№ п/п	Тема самостоятельной работы	Учебно-методическое обеспечение	Объём, ч		
			форма обучения		
			очная	заочная	очно-заочная
1.	Введение в информационную безопасность	1. Башлы, П. Н. Информационная безопасность и защита информации	8	–	8

№	Тема самостоятельной	Учебно-методическое обеспечение	Объём, ч		
2.	Правовое обеспечение информационной безопасности	[Электронный ресурс] : учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва : РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/405000 (дата обращения: 03.09.2024). – Режим доступа: по подписке. 2. Информационная безопасность и зашита информации : учебное пособие для направления подготовки 40.03.01 - Юриспруденция, специальности 40.05.02 - Правоохранительная деятельность, специальности 37.05.02 - Психология служебной деятельности, очной и заочной форм обучения / О. А. Панфилова, Д. Ю. Крюкова, А. Н. Наимов, В. В. Мухин ; Федер. служба исполн. наказаний, Вологод. ин-т права и экономики. - Вологда : ВИПЭ ФСИН России, 2018. - 59 с. - ISBN 978-5-94991-428-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1229037 (дата обращения: 03.09.2024). – Режим доступа: по подписке. 3. Попов, И. В. Информационная безопасность : практикум / И. В. Попов, Н. И. Улендеева. - Самара : Самарский юридический институт ФСИН России, 2022. - 90 с. - ISBN 978-5-91612-375-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/2016193 (дата обращения: 03.09.2024). – Режим доступа: по подписке. 4. Рычаго, М. Е. Основы защиты информации : учебное пособие / М. Е. Рычаго, И. В. Ершова, Р. Н. Тихомиров. - Владимир : ВЮИ ФСИН России, 2017. - 68 с. - ISBN 978-5-93035-622-9. - Текст	8	–	10
3.	Организационное обеспечение информационной безопасности		8	–	10
4.	Технические средства и методы защиты информации		8	–	10
5.	Программно-аппаратные средства и методы обеспечения информационной безопасности		8	–	10
6.	Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности		8	–	10
7.	Средства восстановления данных		8	–	10
8.	Средства антивирусной защиты информации		8	–	10
9.	Политика информационной безопасности организации (предприятия)		8	–	8

№	Тема самостоятельной	Учебно-методическое обеспечение	Объём, ч		
		: электронный. - URL: https://znanium.com/catalog/product/1864501 (дата обращения: 03.09.2024). – Режим доступа: по подписке.			
Всего			**72**	**–**	**86**

4.6.5. Другие виды самостоятельной работы студентов

Не предусмотрены.

4.7. Перечень тем и видов занятий, проводимых в интерактивной форме

№ п/п	Форма занятия	Тема занятия	Интерактивный метод	Объем, ч
1.	Лекция	Правовое обеспечение информационной безопасности	Интерактивная лекция	2

5. Фонд оценочных средств для проведения промежуточной аттестации

Полное описание фонда оценочных средств текущей и промежуточной аттестации обучающихся с перечнем компетенций, описанием показателей и критериев оценивания компетенций, шкал оценивания, типовые контрольные задания и методические материалы представлены в Приложении 3 к настоящей программе.

6. Учебно-методическое обеспечение дисциплины

6.1. Рекомендуемая литература

6.1.1. Основная литература

№ п/п	Автор, название, место издания, изд-во, год издания	Кол-во экз. в библ.
1.	Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва : РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/405000 (дата обращения: 03.09.2024). – Режим доступа: по подписке.	Электронный ресурс
2.	Информационная безопасность и зашита информации : учебное пособие для направления подготовки 40.03.01 - Юриспруденция, специальности 40.05.02 - Правоохранительная деятельность, специальности 37.05.02 - Психология служебной деятельности, очной и заочной форм обучения / О. А. Панфилова, Д. Ю. Крюкова, А. Н. Наимов, В. В. Мухин ; Федер. служба исполн. наказаний, Вологод. ин-т права и экономики. - Вологда : ВИПЭ ФСИН России, 2018. - 59 с. - ISBN 978-5-94991-428-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1229037 (дата обращения: 03.09.2024). – Режим доступа: по подписке.	Электронный ресурс
3.	Попов, И. В. Информационная безопасность : практикум / И. В. Попов, Н. И. Улендеева. - Самара : Самарский юридический институт ФСИН России, 2022. - 90 с. - ISBN 978-5-91612-375-3. - Текст : электронный. - URL:	Электронный ресурс

	https://znanium.com/catalog/product/2016193 (дата обращения: 03.09.2024). – Режим доступа: по подписке.	
4.	Рычаго, М. Е. Основы защиты информации : учебное пособие / М. Е. Рычаго, И. В. Ершова, Р. Н. Тихомиров. - Владимир : ВЮИ ФСИН России, 2017. - 68 с. - ISBN 978-5-93035-622-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1864501 (дата обращения: 03.09.2024). – Режим доступа: по подписке.	Электронный ресурс

6.1.2. Дополнительная литература

№ п/п	Автор, название, место издания, изд-во, год издания, количество страниц
1.	Ерохин, В. В. Безопасность информационных систем : учебное пособие / В. В. Ерохин, Д. А. Погонышева, И. Г. Степченко. - 4-е изд., стер. - Москва : ФЛИНТА, 2022. - 184 с. - ISBN 978-5-9765-1904-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1875457 (дата обращения: 03.09.2024). – Режим доступа: по подписке.
2.	Козьминых, С. И. Организационное и правовое обеспечение информационной безопасности : учебное пособие / С. И. Козьминых. - Тбилиси : Справедливая Грузия, 2020. - 309 с. - ISBN 978-9941-9663-2-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1359091 (дата обращения: 03.09.2024). – Режим доступа: по подписке.

6.1.3. Периодические издания

Не предусмотрены.

6.1.4. Методические указания для обучающихся по освоению дисциплины

Методические указания находятся в стадии разработки

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет»), необходимых для освоения дисциплины

№ п/п	Название интернет-ресурса, адрес и режим доступа
1.	Википедия – свободная энциклопедия. [Электронный ресурс]. URL: https://ru.wikipedia.org/ (дата обращения: 03.09.2024)
2.	Научная электронная библиотека «e-Library». [Электронный ресурс]. URL: https://elibrary.ru/ (дата обращения: 03.09.2024).
3.	Электронно-библиотечная система «Znanium» [Электронный ресурс]. URL: https://znanium.ru/(дата обращения: 03.09.2024).
4.	Anti-Malware.ru — независимый информационно-аналитический портал по информационной безопасности URL: https://www.anti-malware.ru/ (дата обращения: 03.09.2024).
5.	Национальный форум информационной безопасности «ИНФОФОРУМ» — электронное периодическое издание по вопросам информационной безопасности URL: https://infoforum.ru/ (дата обращения: 03.09.2024).

6.3. Средства обеспечения освоения дисциплины

6.3.1. Компьютерные обучающие и контролирующие программы

№ п/п	Вид учебного занятия	Наименование программного обеспечения	Функция программного обеспечения		
			контроль	моделиру-ющая	обучающая
1	Лекционные, практические занятия, самостоятельная работа	http://moodle.lgau.ru	+	+	+

6.3.2. Аудио- и видеопособия

Не предусмотрены.

6.3.3. Компьютерные презентации учебных курсов

Не предусмотрены.

7. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

№ п/п	Наименование оборудованных учебных кабинетов, объектов для проведения занятий	Перечень основного оборудования, приборов и материалов
1.	Г-107 – аудитория для проведения практических занятий, самостоятельной работы	Компьютеры – 7 шт., стол 1 тумб. – 1 шт., стол аудиторн. – 11 шт., стул п/мягкий – 1 шт., стул ученич. – 12 шт., доска для тех.пок. – 1 шт., скамейка ауд. – 6 шт.
2.	Г-109 – аудитория для проведения, лекционных, семинарских лабораторных и практических занятий, групповых и индивидуальных консультаций, текущего контроля, промежуточной аттестации, самостоятельной работы, учебной практики, подготовки и проведение государственной итоговой аттестации	Компьютеры – 10 шт., рециркулятор – 1 шт., мультимедийный проектор - 1 шт., экран – 1 шт., стул мягкий – 1 шт., доска для тех.пок. – 1 шт., стол компьют. – 10 шт., стол аудиторный – 10 шт., стул ученич. – 30 шт.
3.	Г-112 – аудитория для проведения лабораторных и практических занятий, самостоятельной работы	Компьютеры – 7 шт., стол 1 тумб. – 1 шт., доска для тех. пок. – 1 шт., стул ученич. – 19 шт., стол компьют. – 7 шт., скам. аудит. – 2 шт., стол аудиторный – 7 шт.
4.	Г-113 – аудитория для проведения лабораторных и практических занятий, самостоятельной работы	Компьютеры – 6 шт., рециркулятор – 1 шт., стол 1 тумб. – 2 шт., трибуна мал. – 1 шт., стул п/мягкий – 1 шт., стул ученич. – 15 шт., стол компьют. – 6 шт., скамейка аудит. – 9 шт., доска для тех.пок. – 1шт., стол парта – 13 шт.
5.	Г-114 – аудитория для проведения лабораторных и практических	Компьютеры – 8 шт., стол аудит. – 1 шт., доска для тех. пок. – 1 шт., лавка – 3 шт.,

	занятий, самостоятельной работы	скам. аудит. – 5 шт., стол компьют. – 8 шт., стол аудит. – 8 шт., стул ученич. – 14 шт.
6.	Г-115 – аудитория для проведения, семинарских, лабораторных и практических занятий, групповых и индивидуальных консультаций, текущего контроля, промежуточной аттестации, самостоятельной работы	Компьютеры – 3 шт., принтер – 1 шт., МФУ – 2 шт., сейф – 1 шт., стул учен. – 11 шт., стол компьют. – 2 шт., стул мягкий – 1 шт., тумба полиров. – 2 шт., кондиционер – 3 шт., сервер – 1 шт.
7.	Г-116 – аудитория для проведения семинарских занятий	Стул п/мягкий – 1 шт., стул ученич. – 19 шт., стол парта – 8 шт., стол 1 тумб. – 1 шт., доска для тех. пок. – 1 шт.
8.	Г-117 – аудитория дипломного проектирования, самостоятельной работы, индивидуальных и групповых консультаций	Компьютеры – 1 шт., МФУ – 1 шт., стул мягкий – 6 шт., стул ученич. – 1 шт., стол компьют. – 5 шт., доска для тех.пок. – 1 шт., шкаф книжный – 2 шт., кресло – 1 шт., сейф – 1 шт.
9.	Г-120 – аудитория для проведения лабораторных и практических занятий, групповых и индивидуальных консультаций, текущего контроля, промежуточной аттестации, самостоятельной работы	Компьютер – 6 шт., скамейка ауд. – 5 шт., стол 1 тумб. – 2 шт., стол аудит. – 7 шт., стул п/мягкий – 2 шт., стул ученич. – 16 шт., стол компьют. – 7 шт., доска для тех.пок. – 1 шт.

8. Междисциплинарные связи

Протокол
согласования рабочей программы с другими дисциплинами

Наименование дисциплины, с которой проводилось согласование	Кафедра, с которой проводилось согласование	Предложения об изменениях в рабочей программе. Заключение об итогах согласования
Системы искусственного интеллекта	Кафедра информационных технологий, математики и физики	Согласовано
Основы интернет технологий	Кафедра информационных технологий, математики и физики	Согласовано
Управление информационными ресурсами и контентом	Кафедра информационных технологий, математики и физики	Согласовано

Приложение 1

Лист изменений рабочей программы

Номер изменения	Номер протокола заседания кафедры и дата	Страницы с изменениями	Перечень откоррек-тированных пунктов	Подпись заве-дующего кафедрой
1	№ 1 от 03.09.2024г.	8-11	4.6.4, 6.1	

Приложение 2

Лист периодических проверок рабочей программы

Должностное лицо, проводившее проверку Ф.И.О., должность,	Дата	Потребность в корректировке	Перечень пунктов, стр., разделов, требующих изменений

Приложение 3

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ЛУГАНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ ИМЕНИ К.Е. ВОРОШИЛОВА»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

учебной дисциплины «Информационная безопасность»

Направление подготовки: 38.03.05 Бизнес-информатика

Профиль: Бизнес-информатика

Уровень профессионального образования: бакалавр

Год начала подготовки: 2024

Луганск, 2024

1. ПЕРЕЧЕНЬ КОМПЕТЕНЦИЙ, СООТНЕСЕННЫХ С ИНДИКАТОРАМИ ДОСТИЖЕНИЯ КОМПЕТЕНЦИЙ, С УКАЗАНИЕМ ЭТАПОВ ИХ ФОРМИРОВАНИЯ В ПРОЦЕССЕ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код контро-лируемой компе-тенции	Формулировка контролируемой компетенции	Индикаторы достижения компетенции	Этап (уровень) освоения компетенции	Планируемые результаты обучения	Наименование модулей и (или) разделов дисциплины	Наименование оценочного средства	
						Текущий контроль	Промежуточная аттестация
ПК-1	Способен формировать возможные решения на основе разработанных для них целевых показателей с учетом имеющихся факторов, условий и рисков и анализа требований заинтересованных сторон с точки зрения выбранных критериев	**ПК–1.1.** Осуществляет выявление, сбор, систематизацию, хранение, поддержание в актуальном состоянии, анализ, определение зависимости между элементами информации бизнес-анализа для формирования возможных решений используя современные методы исследования и применяя информационные технологии	Первый этап (пороговый уровень)	**Знать:** назначение и функции информационных технологий и современных программных продуктов для решения профессиональных задач	1. Введение в информационную безопасность 2. Правовое обеспечение информационной безопасности 3. Организационное обеспечение информационной безопасности 4. Технические средства и методы защиты информации 5. Программно-аппаратные средства и методы обеспечения информационной безопасности 6. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	Тесты закрытого типа	Зачет с оценкой
			Второй этап (продвинутый уровень)	**Уметь:** определять назначение и функции информационных систем и технологий для решения профессиональных задач		Тесты открытого типа (вопросы для опроса)	Зачет с оценкой
			Третий этап (высокий уровень)	**Иметь навыки:** работы с информационными системами и технологиями для решения профессиональных задач		Практические задания	Зачет с оценкой
		ПК-1.4. Составляет описание	Первый этап (пороговый уровень)	**Знать:** информационные технологии и		Тесты закрытого типа	Зачет с оценкой

		возможных решений в соответствии с выбранными подходами с учетом имеющихся факторов, условий и рисков		программные средства для решения профессиональных задач	7. Средства восстановления данных 8. Средства антивирусной защиты информации 9. Политика информационной безопасности организации (предприятия)		
			Второй этап (продвинутый уровень)	**Уметь:** применять информационные технологии и программные средства для решения профессиональных задач		Тесты открытого типа (вопросы для опроса)	Зачет с оценкой
			Третий этап (высокий уровень)	**Иметь навыки:** применения информационные технологии и программные средства для решения профессиональных задач		Практические задания	Зачет с оценкой

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

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде	Критерии оценивания	Шкала оценивания
1.	**Тест**	Система стандартизированных заданий, позволяющая измерить уровень знаний.	Тестовые задания	В тесте выполнено 90-100% заданий	Оценка «*Отлично*» (5)
				В тесте выполнено более 75-89% заданий	Оценка «*Хорошо*» (4)
				В тесте выполнено 60-74% заданий	Оценка «*Удовлетворительно*» (3)
				В тесте выполнено менее 60% заданий	Оценка «*Неудовлетворительно*» (2)
				Большая часть определений не представлена, либо представлена с грубыми ошибками.	Оценка «*Неудовлетворительно*» (2)
2.	**Опрос**	Форма работы, которая позволяет оценить кругозор, умение логически построить ответ, умение продемонстрировать монологическую речь и иные коммуникативные навыки. Устный опрос обладает большими возможностями воспитательного воздействия, создавая условия для неформального общения.	Вопросы к опросу	Продемонстрированы предполагаемые ответы; правильно использован алгоритм обоснований во время рассуждений; есть логика рассуждений.	Оценка «*Отлично*» (5)
				Продемонстрированы предполагаемые ответы; есть логика рассуждений, но неточно использован алгоритм обоснований во время рассуждений и не все ответы полные.	Оценка «*Хорошо*» (4)
				Продемонстрированы предполагаемые ответы, но неправильно использован алгоритм обоснований во время рассуждений; отсутствует логика рассуждений; ответы не полные.	Оценка «*Удовлетворительно*» (3)
				Ответы не представлены.	Оценка «*Неудовлетворительно*» (2)
3.	**Практические задания**	Направлено на овладение методами и методиками изучаемой дисциплины. Для решения предлагается решить конкретное задание (ситуацию) без применения математических расчетов.	Практические задания	Продемонстрировано свободное владение профессионально-понятийным аппаратом, владение методами и методиками дисциплины. Показаны способности самостоятельного мышления, творческой активности. Задание выполнено в полном объеме.	Оценка «*Отлично*» (5)
				Продемонстрировано владение профессионально-понятийным аппаратом, при применении	Оценка «*Хорошо*» (4)

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде	Критерии оценивания	Шкала оценивания
				методов и методик дисциплины незначительные неточности, показаны способности самостоятельного мышления, творческой активности. Задание выполнено в полном объеме, но с некоторыми неточностями.	
				Продемонстрировано владение профессионально-понятийным аппаратом на низком уровне; допускаются ошибки при применении методов и методик дисциплины. Задание выполнено не полностью.	Оценка «*Удовлетворительно*» (3)
				Не продемонстрировано владение профессионально-понятийным аппаратом, методами и методиками дисциплины. Задание не выполнено.	Оценка «*Неудовлетворительно*» (2)
4.	**Зачет с оценкой**	Контрольное мероприятие, которое проводится по окончании изучения дисциплины.	Вопросы к зачету	Показано знание теории вопроса, понятийно-терминологического аппарата дисциплины; умение анализировать проблему, содержательно и стилистически грамотно излагать суть вопроса; глубоко понимать материал; владение аналитическим способом изложения вопроса, научных идей; навыками аргументации и анализа фактов, событий, явлений, процессов. Выставляется обучающемуся, полно, подробно и грамотно ответившему на вопросы билета и вопросы экзаменатора.	Оценка «*Отлично*» (5)

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде	Критерии оценивания	Шкала оценивания
				Показано знание основных теоретических положений вопроса; умение анализировать явления, факты, действия в рамках вопроса; содержательно и стилистически грамотно излагать суть вопроса, но имеет место недостаточная полнота ответов по излагаемому вопросу. Продемонстрировано владение аналитическим способом изложения вопроса и навыками аргументации. Выставляется обучающемуся, полностью ответившему на вопросы билета и вопросы экзаменатора, но допустив при ответах незначительные ошибки, указывающие на наличие несистемности и пробелов в знаниях.	Оценка «*Хорошо*» (4)
				Показано знание теории вопроса фрагментарно (неполнота изложения информации; оперирование понятиями на бытовом уровне); умение выделить главное, сформулировать выводы, показать связь в построении ответа не продемонстрировано. Владение аналитическим способом изложения вопроса и владение навыками аргументации не продемонстрировано. Обучающийся допустил несущественные ошибки при ответах на вопросы билетов и вопросы экзаменатора.	Оценка «*Удовлетворительно*» (3)
				Знание понятийного аппарата, теории вопроса, не продемонстрировано; умение анализировать учебный материал не продемонстрировано; владение аналитическим способом изложения вопроса и владение навыками аргументации не продемонстрировано. Обучающийся не ответил на один или два вопроса билета и дополнительные вопросы экзаменатора.	Оценка «*Неудовлетворительно*» (2)

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

Оценочные средства для проведения текущего контроля

Текущий контроль осуществляется преподавателем дисциплины при проведении занятий в форме тестовых заданий, устного опроса и практических заданий.

ПК-1. Способен формировать возможные решения на основе разработанных для них целевых показателей с учетом имеющихся факторов, условий и рисков и анализа требований заинтересованных сторон с точки зрения выбранных критериев.

ПК-1.1. Осуществляет выявление, сбор, систематизацию, хранение, поддержание в актуальном состоянии, анализ, определение зависимости между элементами информации бизнес-анализа для формирования возможных решений используя современные методы исследования и применяя информационные технологии.

Первый этап (пороговой уровень) – показывает сформированность показателя компетенции «знать»: назначение и функции информационных технологий и современных программных продуктов для решения профессиональных задач.

Тестовые задания закрытого типа

1. К правовым методам, обеспечивающим информационную безопасность, относятся: (выберите один вариант ответа)

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;

г) обязательная идентификация при входе в информационную систему.

2. Конфиденциальностью называется: (выберите один вариант ответа)

а) описание процедур

б) защита программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов

в) защита от несанкционированного доступа к информации

г) разграничение доступа

3. Кто является основным ответственным за определение уровня классификации информации: (выберите один вариант ответа)

а) высшее руководство

б) руководитель среднего звена

в) владелец

г) системный администратор

4. Таргетированная атака – это: (выберите один вариант ответа)

а) атака на компьютерную систему крупного предприятия

б) атака на конкретный компьютер пользователя

в) атака на сетевое оборудование

г) атака на конкретную учетную запись

5. Основная масса угроз информационной безопасности приходится на: (выберите один вариант ответа)

а) Вирусы-черви
б) Шпионские программы
в) Троянские программы
г) Макровирусы

Ключи

1.	в
2.	в
3.	в
4.	а
5.	в

6. ***Прочитайте текст и установите соответствие***
В таблице приведены базовые понятия в сфере информационной безопасности и их определение. Установите между ними соответствие.

Определение	Понятие
1. Совокупность данных, организованных для получения достоверной информации в самых разных областях знаний и практической деятельности.	а) Информационные технологии
2. Комплекс мер и средств, направленных на защиту конфиденциальности, целостности и доступности информации.	б) Информационная система
3. Совокупность методов, программно-технических и технологических средств, обеспечивающих сбор, накопление, обработку, хранение, представление и распространение информации	в) Информационная безопасность
4. Воздействие на информационную систему с целью повредить её, получить или ограничить к ней доступ, собрать конфиденциальные данные.	г) Информационная война
5. Организационно упорядоченная совокупность программно-аппаратных и других вспомогательных средств, которая обеспечивает надёжное долговременное хранение больших объёмов информации, поиск и обработку данных в соответствии с требованиями предметной области	д) Кибератака
	е) Информационные ресурсы

Запишите в таблицу выбранные буквы под соответствующими цифрами

1	2	3	4	5
е	в	а	д	б

Второй этап (продвинутый уровень) – показывает сформированность показателя компетенции «уметь»: определять назначение и функции информационных систем и технологий для решения профессиональных задач.

Задания открытого типа (вопросы для опроса):

1. Перечислите типы архивации и их возможности, которые можно выполнить с помощью элемента *Панели управления – Архивация и восстановление*.

2. Перечислите основные критерии выбора антивирусного программного обеспечения.
3. Цифровая образовательная платформа, дайте определение, приведите примеры.
4. Перечислите признаки заражения компьютера вирусами.
5. Информационно-правовая система, дайте определение, приведите примеры.

Ключи

1.	Имеются три типа архивирования: 1. Системное архивирование - записывается архивный образ операционной системы 2. Полное архивирование - сохранение всех данных. 3. Нарастающее (инкрементальное) архивирование - записываются только изменения относительно последнего полного архивирования. Этот тип архивирования самый быстрый, но его необходимо проводить очень внимательно.
2.	Основные критерии выбора: обнаружение вредоносных программ с высокой скоростью; высокий процент выявления вирусов; простой и понятный интерфейс; минимальное влияние на производительность устройства.
3.	Цифровая образовательная платформа - информационное пространство, объединяющее участников процесса обучения, которое дает возможность для удаленного образования, обеспечивает доступ к методическим материалам и информации. Например: Moodle, Яндекс Практикум, Stepik, Викиум.
4.	Признаки заражения системы могут быть разными, начиная с появления неожиданных всплывающих окон, самостоятельного запуска программ и их подключения к интернету, отправки сообщений и почты с вашей учетной записи, зависания системы и ее медленной работы, системных ошибок и уведомлений, пропажи файлов и заканчивая тем, что компьютер может и вовсе не грузится.
5.	Информационно-правовая система - класс компьютерных баз данных, направленных на информационное сопровождение работы юристов и специалистов смежных профессий, содержат нормативные правовые акты, судебную практику, постатейные комментарии, профессиональные юридические журналы и прочую профессиональную юридическую литературу. Примеры: «Закон», «КонсультантПлюс», «Гарант».

Третий этап (высокий уровень) – показывает сформированность показателя компетенции «иметь навыки»: работы с информационными системами и технологиями для решения профессиональных задач.

Практические задания:

Задание 1. После переезда на новое место жительства вам для работы необходимо подключить интернет и организовать беспроводную сеть, путем подключения роутера. Какой протокол защиты Wi-Fi лучше выбрать?

Задание 2. . Какая технология разработана для упрощения подключения устройств к сетям Wi-Fi. С ее помощью можно подключиться к роутеру без пароля.

Задание 3. После работы за чужим компьютером папки на вашем USB-накопителе стали «невидимыми». Но по объему занимаемой информации видно, что данные папки есть на USB-накопителе. Как путем использования Total Commander сделать так, чтоб папки снова отображались при открытии USB-накопителя?

Задание 4. Торговое предприятие Retail продают товары через магазины, онлайн-платформы, рынки и другие каналы сбыта, доступные для граждан. Сектор включает в себя широкий спектр товаров и услуг. Как обезопасить имеющуюся на предприятии электронную базу данных от непредвиденной потери данных?

Задание 5. Для работы Вам необходимо найти определенное программное обеспечение, драйвера подключенных устройств. После установки скачанных приложений было установлено дополнительно стороннее программное обеспечение, которое не получается удалить. Как вернуть вернуться к первоначальному состоянию системы?

Ключи

1.	WPA2
2.	технология WPS
3.	Изменить атрибуты папок
4.	Систематическое резервное копирование
5.	Использовать точку восстановления компьютера

ПК-1.4. Составляет описание возможных решений в соответствии с выбранными подходами с учетом имеющихся факторов, условий и рисков.

Первый этап (пороговой уровень) – показывает сформированность показателя компетенции «знать»: информационные технологии и программные средства для решения профессиональных задач.

Тестовые задания закрытого типа

1. Вредоносная программа, которая подменяет собой загрузку некоторых программ при загрузке системы, называется... (выберите один вариант ответа)
а) загрузочный вирус
б) макровирус
в) троян
г) файловый вирус

2. К биометрической системе защиты относятся (выберите один вариант ответа)
а) защита паролем
б) физическая защита данных
в) антивирусная защита
г) идентификация по отпечаткам пальцев

3. Что можно противопоставить взлому системы защиты информации? (выберите один вариант ответа)
а) систему контроля передаваемых сообщений
б) установку дополнительной системы защиты
в) введение специальных паролей
г) создание защищенного домена для системы защиты

4. Как решается проблема защиты каналов передачи данных между головным офисом и филиалами компании? (выберите один вариант ответа)
а) с помощью специального программного обеспечения
б) шифровкой передаваемых сообщений
в) с помощью защищенных частных сетей
г) передачей информации специальными курьерами

5. Что представляют собой средства мониторинга? (выберите один вариант ответа)
а) это набор утилит, отслеживающих операции с файлами, реестром, портами и сетью
б) это набор утилит, используемых для вывода на монитор текстовой информации
в) это набор утилит, защищающих информацию от вирусов

г) это набор утилит, позволяющих сократить время выполнения арифметических операций

Ключи

1.	а
2.	г
3.	г
4.	в
5.	а

6. ***Прочитайте текст и установите соответствие***

В таблице приведены основные методы защиты при доступе к информационной системе и их характеристики. Установите между ними соответствие.

Характеристика	Методы защиты
1. Метод идентификации пользователя в каком-либо сервисе при помощи запроса данных двух разных типов	а) идентификация
2. Предоставление определённых прав доступа и разрешений пользователю на использование ресурсов.	б) авторизация
3. Процесс проверки и подтверждения достоверности чего-либо с использованием различных методов	в) двухфакторная аутентификация
4. Оценка характеристик пользователя для определения его личности	г) аутентификация
5. Процесс идентификации пользователя или устройства, позволяющий установить его подлинность и право доступа к определённым ресурсам или функционалу системы	д) шифрование
	е) верификация

Запишите в таблицу выбранные буквы под соответствующими цифрами

1	2	3	4	5
в	б	е	а	г

Второй этап (продвинутый уровень) – показывает сформированность показателя компетенции «уметь»: применять информационные технологии и программные средства для решения профессиональных задач.

Задания открытого типа (вопросы для опроса):

1. В чем заключается сущность приема, обеспечивающего несанкционированный доступ к конфиденциальной информации и известного как «уборка мусора»?
2. Частью какой, более общей системы, является система обеспечения информационной безопасности Российской Федерации?
3. На кого распространяется действие Закона «О государственной тайне»?
4. Каким образом должен быть организован процесс формирования и потребления информации, составляющей коммерческую тайну предприятия?
5. Аутентификацией называют…

Ключи

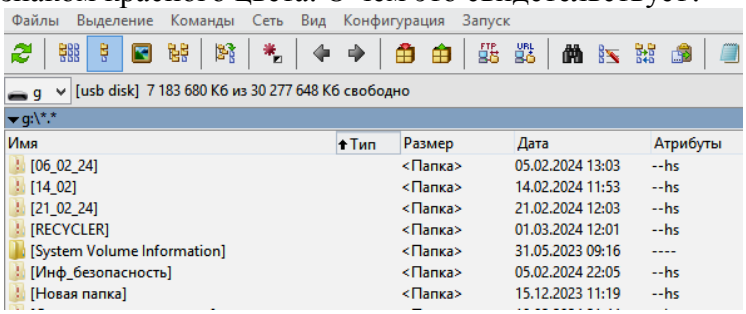
1.	метод получения информации, оставленной пользователем в памяти ПК после окончания работы
2.	системы обеспечения национальной безопасности страны

3.	на всех граждан и должностных лиц, если им предоставили для работы закрытые сведения
4.	он должен быть организован таким образом, чтобы исключить утечку информации
5.	процесс распознавания и проверки подлинности заявлений о себе пользователей и процессов

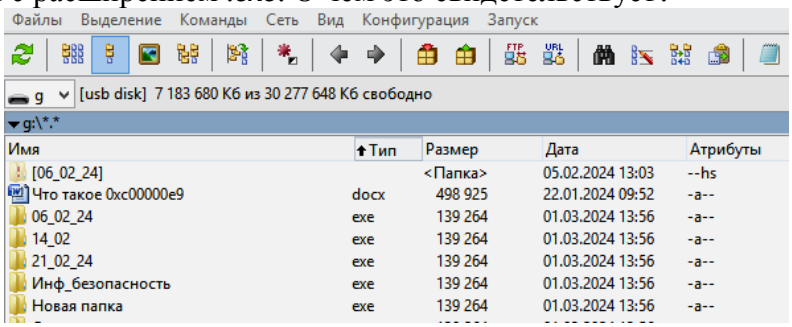
Третий этап (высокий уровень) – показывает сформированность показателя компетенции «иметь навыки»: применения информационные технологии и программные средства для решения профессиональных задач.

Практические задания:

Задание 1. При открытии накопителя часть папок имеют полупрозрачный вид с восклицательным знаком красного цвета. О чем это свидетельствует?



Задание 2. После работы за чужим компьютером часть папок и файлов исчезли и появились папки с расширением *.exe*. О чем это свидетельствует?



Задание 3. В зависимости от среды обитания вирусы можно разделить на сетевые, файловые и загрузочные. Сетевые вирусы распространяются по различным компьютерным сетям. Файловые вирусы внедряются главным образом в исполняемые модули. Куда внедряются загрузочные вирусы?

Задание 4. Запустить ping компьютера: «Пуск»->«Выполнить»->*“cmd”->“ping ip-addr -t”*. Где располагается утилита **ping**?

Задание 5. Методы обеспечения информационной безопасности Российской Федерации направленные на создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи.

Ключи

1.	папки являются скрытыми
2.	накопитель заражен вирусом
3.	в сектор загрузки системного диска (Master Boot Record)
4.	в системной папке Windows (C:\windows\system)
5.	организационно-технические методы

Оценочные средства для проведения промежуточной аттестации

Промежуточная аттестация проводится в виде зачета с оценкой.

Вопросы для зачета

1. Теоретические аспекты информационной безопасности.
2. Составляющие информационной безопасности.
3. Доступность информации.
4. Целостность информации.
5. Конфиденциальность информации.
6. Правовое обеспечение информационной безопасности.
7. Доктрина информационной безопасности Российской Федерации.
8. Концепция информационной безопасности сетей связи общего пользования Российской Федерации.
9. Правовое обеспечение информационной безопасности в Российской Федерации.
10. Основные понятия организационного обеспечения информационной безопасности.
11. Административный уровень информационной безопасности.
12. Программа безопасности.
13. Уровни детализации политики информационной безопасности.
14. Технические средства и методы защиты информации.
15. Оценка безопасности информационных систем. Структура системы информационной безопасности.
16. Аппаратные средства защиты информации.
17. Вспомогательные аппаратные средства защиты информации.
18. Основные и вспомогательные программные средства защиты информации.
19. Ответственность за неправомерный доступ к компьютерной информации.
20. Определение понятия «коммерческая тайна» и «информация, составляющая коммерческую тайну».
21. Основные принципы обработки персональных данных.
22. Общая структура правового режима информационной безопасности.
23. Нормы и институты правового обеспечения информационной безопасности.
24. Система нормативно-правовых актов в области информационной безопасности в РФ.
25. Задачи защиты информации, определенные в ФЗ «Об информации, информационных технологиях и о защите информации».
26. Понятие «политика информационной безопасности».
27. Средства восстановления данных.
28. Средства резервного копирования, восстановления, защиты данных в операционных системах Windows.
29. Средства антивирусной защиты информации.
30. Источники вирусов. Признаки заражения и антивирусные программы.

4. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ

Для выполнения практических заданий студенту необходимы: ручка, листы для черновых подсчетов.

Текущий контроль

Тестирование для проведения текущего контроля проводится в виде тестов или системы дистанционного обучения Moodle.

На тестирование отводится 20 минут. Каждый вариант тестовых заданий включает 10 вопросов. Количество возможных вариантов ответов – 4. Студенту необходимо выбрать один правильный ответ. За каждый правильный ответ на вопрос присваивается 10 баллов. Шкала перевода: 9-10 правильных ответов – оценка «отлично» (5), 7-8 правильных ответов – оценка «хорошо» (4), 6 правильных ответов – оценка «удовлетворительно» (3), 1-5 правильных ответов – оценка «не удовлетворительно» (2).

Опрос как средство текущего контроля проводится в форме устных ответов на вопросы. Студент отвечает на поставленный вопрос сразу, время на подготовку к ответу не предоставляется.

Практические задания как средство текущего контроля проводятся в письменной форме. Студенту выдается задание и предоставляется 10 минут для подготовки к ответу.

Промежуточная аттестация

Зачет проводится путем подведения итогов по результатам текущего контроля. Если студент не справился с частью заданий текущего контроля, ему предоставляется возможность сдать зачет на итоговом контрольном мероприятии в форме ответов на вопросы к зачету или тестовых заданий к зачету, в случае дистанционного обучения.

Если зачет проводится в форме ответов на вопросы, студенту предлагается один или несколько вопросов из перечня вопросов к зачету. Время на подготовку к ответу не предоставляется.

Если зачет проводится в форме тестовых заданий к зачету, и тестирование для проведения текущего контроля проводится с помощью Системы дистанционного обучения Moodle, то на тестирование отводится 20 минут. Каждый вариант тестовых заданий включает 10 вопросов. Количество возможных вариантов ответов – 4. Студенту необходимо выбрать один правильный ответ. За каждый правильный ответ на вопрос присваивается 10 баллов. Шкала перевода: 9-10 правильных ответов – оценка «отлично» (5), 7-8 правильных ответов – оценка «хорошо» (4), 6 правильных ответов – оценка «удовлетворительно» (3), 1-5 правильных ответов – оценка «не удовлетворительно» (2).