

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гнатюк Сергей Иванович
Должность: Первый проректор
Дата подписания: 07.08.2025 12:15:08
Уникальный программный ключ:
5ede28fe5b714e680817c5c132d4ba793a6b4421

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 38.03.01 Экономика
направленность (профиль) Бухгалтерский учет, анализ и аудит

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 38.03.01 Экономика, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 12.08.2020 № 954 (с изменениями и дополнениями).

Преподаватели, подготовившие рабочую программу:

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

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 2024г.)

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

Руководитель основной профессиональной образовательной программы _____ **И.П. Житная**

1. Предмет. Цели и задачи дисциплины, её место в структуре основной 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 обязательной части (Б1.О.33) блока дисциплин подготовки студентов по направлению подготовки 38.03.01 Экономика, направление подготовки Бухгалтерский учет, анализ и аудит основной профессиональной образовательной программы высшего образования (далее – ОПОП ВО).

Дисциплина реализуется кафедрой информационных технологий, математики и физики во 2 семестре.

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

Коды компетенций	Формулировка компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
ОПК-5	Способен использовать современные информационные технологии и программные средства при решении профессиональных задач	ОПК-5.1. Определяет назначение и функции информационных систем в экономике и современных программных продуктов для решения профессиональных задач	Знать: назначение и функции информационных систем в экономике и современных программных продуктов для решения профессиональных задач; уметь: определять назначение и функции информационных систем в экономике и современных программных продуктов для решения профессиональных задач; иметь навыки: определения назначений и функции информационных систем в экономике и современных программных продуктов для решения профессиональных задач
		ОПК-5.2. Применяет информационные технологии и программные средства для решения профессиональных задач	Знать: информационные технологии и программные средства для решения профессиональных задач; уметь: применять информационные технологии и программные средства для решения профессиональных задач; иметь навыки: применения информационных технологий и программные средства для решения профессиональных задач
ОПК-6	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-6.1. Обладает базовыми знаниями о современных информационных технологиях и принципах их работы для решения задач профессиональной деятельности	Знать: основные принципы работы, модели и методы в области информационных технологий; уметь: решать задачи профессиональной деятельности с помощью современных информационных технологий

			иметь навыки: использования современных информационных технологий для решения общенаучных задач в своей профессиональной деятельности и для организации своего труда
		ОПК-6.2. Осуществляет поиск, анализ и отбор современных информационных технологий, с учетом принципов их работы, необходимых для решения задач профессиональной деятельности	Знать: методики поиска, сбора и отбора информационных технологий в сфере профессиональной деятельности; уметь: ориентируясь на задачи профессиональной деятельности, обоснованно выбирать современные информационные технологии; иметь навыки: поиска, анализа, выбора и эффективного применения современных информационных технологий при решении задач профессиональной деятельности
		ОПК-6.3. Применяет современные информационные технологии при решении задач профессиональной деятельности	Знать: современные информационные технологии и программные средства, применяемые для решения задач профессиональной деятельности; уметь: применять современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности; иметь навыки: применения на практике современных информационных технологий для решения общенаучных задач в своей профессиональной деятельности и для организации своего труда

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	всего
		2 семестр		2 семестр
Общая трудоёмкость дисциплины, зач.ед./часов, в том числе:	4/144	4/144	—	4/144
Контактная работа, часов:	40	40	—	30
- лекции	20	20	—	14
- практические (семинарские) занятия	20	20	—	16
- лабораторные работы	—	—	—	—
Самостоятельная работа, часов	104	104	—	114
Контроль, часов	—	—	—	—
Вид промежуточной аттестации (зачёт, экзамен)	зачет	зачет	—	зачет

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	2	-		10
Тема 2. Правовое обеспечение информационной безопасности	2	2		10
Тема 3. Организационное обеспечение информационной безопасности	2	2		12
Тема 4. Технические средства и методы защиты информации	2	2		12
Тема 5. Программно-аппаратные средства и методы обеспечения информационной безопасности	2	4		12
Тема 6. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	2	4		12
Тема 7. Средства восстановления данных	2	2		12
Тема 8. Средства антивирусной защиты информации	2	2		12
Тема 9. Политика информационной безопасности организации (предприятия)	4	2		12
Всего	20	20		104
Заочная форма обучения				
—	—	—	—	—
Очно-заочная форма обучения				
Тема 1. Введение в информационную безопасность	1	1		12
Тема 2. Правовое обеспечение информационной	2	2		12

безопасности				
Тема 3. Организационное обеспечение информационной безопасности	1	1		12
Тема 4. Технические средства и методы защиты информации	2	2		12
Тема 5. Программно-аппаратные средства и методы обеспечения информационной безопасности	2	2		12
Тема 6. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	2	2		12
Тема 7. Средства восстановления данных	1	2		14
Тема 8. Средства антивирусной защиты информации	1	2		14
Тема 9. Политика информационной безопасности организации (предприятия)	2	2		14
Всего	14	16		114

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	2	—	1
2.	Тема лекционного занятия 2. Правовое	2	—	2
3.	Тема лекционного занятия 3. Организационное обеспечение информационной безопасности	2	—	1
4.	Тема лекционного занятия 4. Технические	2	—	2
5.	Тема лекционного занятия 5. Программно-аппаратные средства и методы обеспечения	2	—	2
6.	Тема лекционного занятия 6. Применение информационных технологий для изучения	2	—	2
7.	Тема лекционного занятия 7. Средства	2	—	1
8.	Тема лекционного занятия 8. Средства	2	—	1
9.	Тема лекционного занятия 9. Политика информационной безопасности организации	4	—	2
Всего		20	—	14

4.4. Перечень тем практических занятий (семинаров)

№ 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	—	2
2.	Тема практического занятия 2. Разграничение прав доступа системы	2	—	2
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	2	—	2
6.	Тема практического занятия 6. Антивирусная защита компьютера	2	—	2
7.	Тема практического занятия 7. Безопасность на уровне операционной системы и приложений	4	—	2
8.	Тема практического занятия 8. Настройки безопасности интернет обозревателей	2	—	2

9	Тема практического занятия 9. Основы информационной безопасности при работе с облачными технологиями	2	–	2
Всего		20	–	16

44.5. 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 пройденного 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 [Электронный ресурс] : учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова.	10	–	12
2.	Правовое обеспечение информационной безопасности	2. Информационная безопасность и защита информации : учебное пособие для направления подготовки 40.03.01	10	–	12
3.	Организационное обеспечение информационной безопасности	3. Попов, И. В. Информационная безопасность : практикум / И. В. Попов, Н. И. Улендеева.	12	–	12
4.	Технические средства и методы защиты информации		12	–	12
5.	Программно-		12	–	12

№	Тема самостоятельной	Учебно-методическое	Объём, ч		
	аппаратные средства и методы обеспечения информационной безопасности	4. Рычаго, М. Е. Основы защиты информации : учебное пособие / М. Е. Рычаго, И. В. Ершова, Р. Н. Тихомиров. 1. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : учебник / П. Н. Башлы, А. В. Бабащ, Е. К. Баранова.			
6.	Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	2. Информационная безопасность и защита информации : учебное пособие для направления подготовки 40.03.01 3. Попов, И. В. Информационная безопасность : практикум / И. В. Попов, Н. И. Улендеева.	12	—	12
7.	Средства восстановления данных		12	—	14
8.	Средства антивирусной защиты информации	4. Рычаго, М. Е. Основы защиты информации : учебное пособие / М. Е. Рычаго, И. В. Ершова, Р. Н. Тихомиров.	12	—	14
9.	Политика информационной безопасности организации (предприятия)		12	—	14
Всего			104	—	114

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	Объём, ч
1.	Лекция	Правовое обеспечение информационной безопасности	Интерактивная лекция	2

5. Фонд оценочных средств для текущего контроля и 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.
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 защита 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: https://znanium.com/catalog/product/2016193 (дата обращения: 03.09.2024). – Режим доступа: по подписке.	Электронный ресурс
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. Погonyшева, 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: 20.04.2024)
2.	Научная электронная библиотека «e-Library». [Электронный ресурс]. URL: https://elibrary.ru/ (дата обращения: 20.04.2024).
3.	Электронно-библиотечная система «Znanium» [Электронный ресурс]. URL: https://znanium.ru/
4.	Anti-Malware.ru — независимый информационно-аналитический портал по информационной безопасности URL: https://www.anti-malware.ru/ (дата обращения: 20.04.2024).
5.	Национальный форум информационной безопасности «ИНФОФОРУМ» — электронное периодическое издание по вопросам информационной безопасности URL: https://infoforum.ru/ (дата обращения: 20.04.2024).

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	моделирующая	обучающая
1	Лекционные, практические занятия, самостоятельная работа	https://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 занятий, самостоятельной работы	Компьютеры – 8 шт., стол аудит. – 1 шт., доска для тех. пок. – 1 шт., лавка – 3 шт., 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	Компьютер – 6 шт., скамейка ауд. – 5 шт.,

лабораторных и практических занятий, групповых и индивидуальных консультаций, текущего контроля, промежуточной аттестации, самостоятельной работы	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

Лист изменений рабочей программы

[illegible]

Лист периодических проверок рабочей программы

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

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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
учебной дисциплины «Информационная безопасность»

Направление подготовки: 38.03.01 Экономика

Профиль: Бухгалтерский учет, анализ и аудит

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 контролируемой компетенции	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
ОПК-5	Способен использовать современные информационные технологии и программные средства при решении профессиональных задач	ОПК-5.1. Определяет назначение и функции информационных систем в экономике и современных программных продуктов для решения профессиональных задач	Первый этап (пороговый уровень)	Знать информационные технологии решения экономических 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
			Второй этап (продвинутый уровень)	Уметь применять информационные технологии для обработки экономической информации		Тесты открытого типа (вопросы для опроса)	Зачет
			Третий этап (высокий уровень)	Иметь навыки использования информационных технологий и систем для решения экономических задач		Практические задания	Зачет
		ОПК-5.2. Применяет информационные технологии и программные средства для решения профессиональных задач	Первый этап (пороговый уровень)	Знать программные средства решения экономических задач		Тесты закрытого типа	Зачет
			Второй этап (продвинутый уровень)	Уметь применять программные средства для обработки экономической информации		Тесты открытого типа (вопросы для опроса)	Зачет
			Третий этап (высокий уровень)	Иметь навыки использования программных средств для решения		Практические задания	Зачет
			Первый этап (пороговый уровень)				
			Второй этап (продвинутый уровень)				
			Третий этап (высокий уровень)				

				экономических задач	7. Средства восстановления данных 8. Средства антивирусной защиты информации 9. Политика информационной безопасности организации (предприятия)		
ОПК-6	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.	ОПК-6.1. Обладает базовыми знаниями о современных информационных технологиях и принципах их работы для решения задач профессиональной деятельности	Первый этап (пороговый уровень)	Знать программные средства решения экономических 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	Тесты закрытого типа	Зачет
			Второй этап (продвинутый уровень)	Уметь применять программные средства для обработки экономической информации		Тесты открытого типа (вопросы для опроса)	Зачет
			Третий этап (высокий уровень)	Иметь навыки использования программных средств для решения экономических задач		Практические задания	Зачет
		ОПК-6.2. Осуществляет поиск, анализ и отбор современных информационных технологий, с учетом	Первый этап (пороговый уровень)	Знать программные средства решения экономических задач		Тесты закрытого типа	Зачет
			Второй этап (продвинутый уровень)	Уметь применять программные средства для обработки экономической		Тесты открытого типа (вопросы для опроса)	Зачет

		принципов их работы, необходимых для решения задач профессиональной деятельности		информации	изучения вопросов организационно-правового обеспечения информационной безопасности 7. Средства восстановления данных 8. Средства антивирусной защиты информации 9. Политика информационной безопасности организации (предприятия)		
			Третий этап (высокий уровень)	Иметь навыки использования программных средств для решения экономических задач		Практические задания	Зачет
		ОПК-6.3. Применяет современные информационные технологии при решении задач профессиональной деятельности	Первый этап (пороговый уровень)	Знать программные средства решения экономических задач		Тесты закрытого типа	Зачет
			Второй этап (продвинутый уровень)	Уметь применять программные средства для обработки экономической информации		Тесты открытого типа (вопросы для опроса)	Зачет
			Третий этап (высокий уровень)	Иметь навыки использования программных средств для решения экономических задач		Практические задания	Зачет

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	Представлен ие 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.	
				Продemonстрировано 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	Зачет выставляется в результате подведения итогов текущего контроля. Зачет в форме итогового контроля проводится для обучающихся, которые не справились с частью заданий текущего контроля.	Вопросы к зачету	Показано знание теории вопроса, понятийного аппарата; умение содержательно излагать суть вопроса; владение навыками аргументации и анализа фактов, явлений, процессов в их взаимосвязи. Выставляется обучающемуся, который освоил не менее 60% программного материала дисциплины.	«Зачтено»
				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 освоил менее 60% программного материала дисциплины.	«Не зачтено»

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.

ОПК-5. Способен использовать современные информационные технологии и программные средства при решении профессиональных задач.

ОПК-5.1. Определяет назначение и функции информационных систем в экономике и современных программных продуктов для решения профессиональных задач.

Первый этап (пороговой уровень) – показывает сформированность показателя компетенции «знать»: назначение и функции информационных систем в экономике 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) разработка программных средств обеспечения правовых данных

2. Виды информационной безопасности: (выберите один вариант ответа)

- а) персональная, корпоративная, государственная
- б) клиентская, серверная, сетевая
- в) локальная, глобальная, смешанная
- г) локальная, государственная, персональная

3. Цели информационной безопасности – своевременное обнаружение, предупреждение: (выберите один вариант ответа)

- а) несанкционированного доступа, воздействия в сети
- б) инсайдерства в организации
- в) чрезвычайных ситуаций
- г) некомпетентности персонала

4. Основные объекты информационной безопасности: (выберите один вариант ответа)

- а) персональные компьютерные сети
- б) компьютерные сети, базы данных
- в) информационные системы, психологическое состояние пользователей
- г) бизнес-ориентированные, коммерческие системы

5. Основными рисками информационной безопасности являются: (выберите один вариант ответа)

- а) искажение, уменьшение объема, перекодировка информации
- б) техническое вмешательство, выведение из строя оборудования сети
- в) потеря, искажение, утечка информации
- г) информационная неграмотность

Ключи

1.	в
2.	а
3.	а
4.	б
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 в экономике и современных программных продуктов для решения профессиональных задач.

Задания открытого типа (вопросы для опроса):

1. Перечислите основные источники угроз целостности информации.
2. Что предполагает понятие «информационная война»?
3. Что предполагает понятие «информационное оружие»?
4. Как можно классифицировать информационное оружие по основным видам воздействия?
5. Перечислите характерные черты для информационного оружия.

Ключи

1.	Источники можно разделить на следующие группы: люди; технические устройства; модели, алгоритмы, программы; технологические схемы обработки; внешняя среда
2.	«Информационная война» – конфликты, где информационные ресурсы используются для достижения целей (политических, экономических, военных, социальных и др.) государствами, организациями, отдельными субъектами. Они базируются на манипуляции информацией и создании определенного восприятия реальности, что может оказывать значительное влияние на общественное мнение и принятие решений.
3.	Информационное оружие — это совокупность средств и методов, позволяющих похищать, искажать или уничтожать информацию, ограничивать или прекращать доступ к ней законных пользователей, нарушать работу или выводить из строя телекоммуникационные сети и компьютерные системы, используемые в обеспечении жизнедеятельности общества и государства.
4.	Информационно-психологическое. Нацелено на осуществление психологических атак на сферу психики человека, групповое или общественное сознание посредством информационных раздражителей. Информационно-техническое. Основано на применении средств радиоэлектронной борьбы, предназначенных для выявления и электронного подавления систем управления войсками и оружием противника, его систем разведки, навигации и целеуказания, а также средств специального программно-технического воздействия.
5.	Для информационного оружия характерны: – скрытность (достижение поставленных целей без видимой и фиксируемой подготовки и объявления войны). – масштабность (нанесение критического ущерба в различных сферах жизнедеятельности общества и государства без пространственных и временных ограничений). – универсальность (многовариантность использования информационных структур двойного назначения для достижения поставленных целей).

Третий этап (высокий уровень) – показывает сформированность показателя компетенции «иметь навыки»: определения назначений и функции информационных систем в экономике и современных программных продуктов для решения профессиональных задач.

Практические задания:

Задание 1. Анализируя возможные пути воздействия на информацию, представляемую как совокупность n информационных элементов, связанных между собой логическими связями, можно выделить основные нарушения. Что предполагает уничтожение, разрушение информационных элементов?

Задание 2. Анализируя возможные пути воздействия на информацию, представляемую как совокупность n информационных элементов, связанных между собой логическими связями, можно выделить основные нарушения. Что предполагает изменение блоков информации, внешнее навязывание ложной информации?

Задание 3. Физическая нехватка одного или нескольких элементов системы обработки, вызывающая нарушения технологического процесса обработки или перегрузку имеющихся элементов определяется как...

Задание 4. Несовершенство конструкции (организации) элементов системы, в силу чего может появляться возможность случайного или преднамеренного негативного воздействия на обрабатываемую или хранимую информацию определяется как...

Задание 5. Что предполагает негласная деятельность отечественных и зарубежных промышленных организаций (фирм), направленная на по лучение незаконным путем

конфиденциальной информации, используемой для достижения промышленных, коммерческих, политических или подрывных целей?

Ключи

1.	нарушение физической целостности
2.	нарушение содержания
3.	количественная недостаточность
4.	качественная недостаточность
5.	промышленный шпионаж

ОПК-5.2. Применяет информационные технологии и программные средства для решения профессиональных задач.

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

Тестовые задания закрытого типа

1. К основным принципам обеспечения информационной безопасности относится: (выберите один вариант ответа)

- а) экономической эффективности системы безопасности
- б) многоплатформенной реализации системы
- в) усиления защищенности всех звеньев системы
- г) усиления защищенности одного звена системы

2. Основными субъектами информационной безопасности являются: (выберите один вариант ответа)

- а) руководители, менеджеры, администраторы компаний
- б) органы права, государства, бизнеса
- в) сетевые базы данных, фаерволлы
- г) браузеры, брандмауэры

3. Принципом информационной безопасности является принцип недопущения: (выберите один вариант ответа)

- а) неоправданных ограничений при работе в сети (системе)
- б) рисков безопасности сети, системы
- в) презумпции секретности
- г) автоматизации процессов

4. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности? (выберите один вариант ответа)

- а) сотрудники
- б) хакеры
- в) атакующие
- г) контрагенты (лица, работающие по договору)

5. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству? (выберите один вариант ответа)

- а) снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
- б) требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
- в) улучшить контроль за безопасностью этой информации
- г) снизить уровень классификации этой информации

Ключи

1.	а
2.	б
3.	а
4.	а
5.	в

6. Прочитайте текст и установите соответствие

В таблице приведены основные виды компьютерных сетей и их характеристики. Установите между ними соответствие.

Характеристика компьютерной сети	Вид компьютерной сети
1. Сеть, которая позволяет объединить во всемирную информационную инфраструктуру ЛВС и компьютеры в разных регионах и странах.	а) локальная сеть
2. Сеть, которая может объединять множество абонентов и действовать в радиусе до 2 км. К данной категории относятся корпоративные и частные сети, которые объединяют компьютерное, серверное оборудование и периферийные устройства	б) глобальная сеть
3. Сеть, которая работает поверх общественных сетей и за счёт зашифрованных соединений даёт возможность пользователям безопасно обмениваться данными.	в) виртуальная частная сеть
4. Внутренняя сеть, предназначенная для объединения компьютеров, серверов, баз данных и других устройств внутри компании или организации.	г) корпоративная сеть
5. Сеть, которая объединяет личное пользовательское компьютерное и вспомогательное оборудование. В её состав могут входить ноутбуки, смартфоны, музыкальное оборудование, NAS-серверы, игровые консоли, наушники, камеры.	д) региональная сеть
	е) персональная сеть

Запишите в таблицу выбранные буквы под соответствующими цифрами

1	2	3	4	5
б	а	в	г	е

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. Файлы cookie, дайте определение.
2. Основные задачи файлов cookie.
3. Какие выделяют типы файлов cookie?
4. Что обозначает понятие «кибергигиена»?
5. Один из самых важных инструментов обеспечения информационной безопасности – кодирование. Что входит в это понятие?

Ключи

1.	Файлы cookie — это небольшие текстовые файлы, которые веб-сайты отправляют и хранят на компьютере пользователя. Они содержат практически любую
----	--

	информацию о взаимодействии пользователя с веб-ресурсом, например, идентификаторы сеансов, параметры входа в личный кабинет, время сеанса.
2.	Основные задачи файлов cookie: – сохранение настроек (помогают узнать и запомнить предпочтения пользователя) – управление сеансами (позволяют отслеживать активность пользователя во время одной сессии, что полезно, например, при онлайн-покупках) – аутентификация. Используются для того, чтобы оставаться залогиненным на своих аккаунтах и не вводить логины и пароли повторно. – сбор сведений. Собирают аналитику о том, как пользователь использует ресурс, что помогает персонализировать контент, улучшить функциональность и устранять проблемы. – маркетинг и реклама. Позволяют показывать рекламу на основе интересов и предпочтений пользователя в интернете и в соцсетях.
3.	Выделяют два типа файлов cookie: – cookie сеансов. Используются только во время работы с сайтом. Они никогда не записываются на жёсткий диск, а хранятся в оперативной памяти устройства. После завершения сеанса они автоматически удаляются. – постоянные cookie. Могут оставаться на компьютере долго. У некоторых есть срок действия, и когда он истекает, файлы удаляются автоматически.
4.	Кибергигиена – это полезные привычки обращения с информационными системами – некоторые правила, соблюдение которых уменьшает риски информационной безопасности.
5.	Кодирование – это процесс преобразования данных из формы, удобной для непосредственного использования, в форму, удобную для передачи, хранения, автоматической переработки и сохранения от несанкционированного доступа.

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

Практические задания:

Задание 1. Сколько бит информации мы получим при наступлении события: «дважды подкинули игральный кубик, оба раза выпало 6»?

Задание 2. Сколько бит информации мы получим при наступлении события: «трижды подкинули игральный кубик, сумма всех выпавших граней равна 4»?

Задание 3. Известно, что, придумывая пароль, Аня взяла свое имя (полную форму) и поменяла в нем буквы местами. Сколько бит информации содержит сообщение «пароль Ани начинается с буквы А»?

Задание 4. Известно, что, придумывая пароль, Боря взял свое имя (полную форму) и поменял в нем буквы местами. Сколько бит информации содержит сообщение «пароль Бори начинается с буквы С»?

Задание 5. 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?

Ключи

1.	6 бит
2.	7 бит
3.	1 бит
4.	3 бита
5.	WPA2

ОПК-6. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

ОПК-6.1. Обладает базовыми знаниями о современных информационных технологиях и принципах их работы для решения задач профессиональной деятельности.

Первый этап (пороговой уровень) – показывает сформированность показателя компетенции «знать»: основные принципы работы, модели и методы в области информационных технологий.

Тестовые задания закрытого типа

1. Первоочередным при реализации защитных мер политики безопасности является: (выберите один вариант ответа)

- а) анализ затрат на проведение защитных мер
- б) анализ безопасности
- в) аудит, анализ уязвимостей, риск-ситуаций
- г) проверка персонала

2. Политика безопасности в системе (сети) – это комплекс: (выберите один вариант ответа)

- а) руководств, требований обеспечения необходимого уровня безопасности
- б) инструкций, алгоритмов поведения пользователя в сети
- в) нормы информационного права, соблюдаемые в сети
- г) должностных инструкций

3. Ответственность за защищенность данных в компьютерной сети несет: (выберите один вариант ответа)

- а) владелец сети
- б) администратор сети
- в) пользователь сети
- г) администратор сети и пользователи

4. Принципом политики информационной безопасности является принцип: (выберите один вариант ответа)

- а) разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- б) одноуровневой защиты сети (системы)
- в) совместимых, однотипных программно-технических средств сети (системы)
- г) отсутствия ограничений системы (сети)

5. Какие уровни защиты информации существуют? (выберите один вариант ответа)

- а) организационно-правовой
- б) организационно-технический
- в) правовой, организационный, технический
- г) юридический, методический, технический

Ключи

1.	в
2.	а
3.	а
4.	а
5.	в

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»: решать задачи профессиональной деятельности с помощью современных информационных технологий.

Задания открытого типа (вопросы для опроса):

1. Перечислите главные недостатки использования парольных систем.
2. Цель разграничения доступа к данным в операционной системе?
3. Главная задача концептуального плана защиты.
4. Что характерно для административного уровня защиты информации?
5. Приведите пример определенного вида атак на каналы передачи данных.

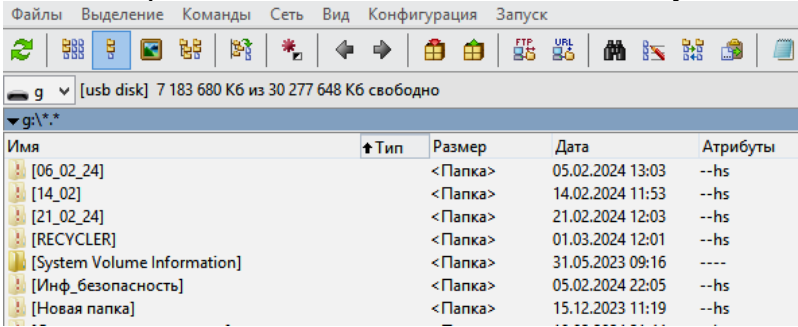
Ключи

1.	– уязвимость к взлому (слабые пароли легко подобрать) – сложность запоминания (надежные пароли часто трудно запомнить) – риск повторного использования (один и тот же пароль для разных сайтов) – уязвимость к фишингу
2.	Основная цель – предотвращение нежелательного использования данных и информации. Разграничение доступа позволяет предоставлять легальным пользователям именно те права, которые были определены администратором, и контролировать возможность выполнения ими различных системных функций.
3.	Главная задача – обеспечение заданного уровня защиты от различных угроз при минимизации затрат на охрану и безопасность.
4.	Административный уровень защиты информации включает комплекс скоординированных мероприятий и технических мер, реализующих практические механизмы защиты в процессе создания и эксплуатации систем защиты информации.
5.	Например, Спуффинг. Полученный пакет данных видоизменяется и отправляется адресату. Адресат принимает видоизменённый пакет за легальный, который может содержать вредоносный «груз».

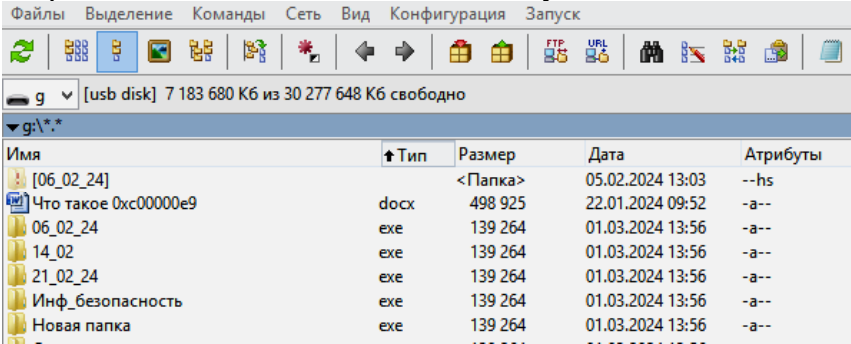
Третий этап (высокий уровень) – показывает сформированность показателя компетенции «иметь навыки»: владения современными информационными технологиями для решения общенаучных задач в своей профессиональной деятельности и для организации своего труда.

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. Максимальная скорость передачи данных в локальной сети 100 Мбит/с. Сколько страниц текста можно передать за 1 сек, если 1 страница текста содержит 50 строк и на каждой строке - 70 символов?

Задание 4. Для передачи сообщения используется код, состоящий из прописных латинских букв (всего используется 20 различных символов). При этом все символы кодируются одним и тем же (минимально возможным) количеством битов. Определите информационный объем сообщения длиной в 200 символов.

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.	3571,43 страниц
4.	125 байт
5.	организационно-технические методы

ОПК-6.2. Применяет современные информационные технологии при решении задач профессиональной деятельности.

Первый этап (пороговой уровень) – показывает сформированность показателя компетенции «знать»: методики поиска, сбора и отбора информационных технологий в сфере профессиональной деятельности.

Тестовые задания закрытого типа

1. Основными рисками информационной безопасности являются: (выберите один вариант ответа)

- а) искажение, уменьшение объема, перекодировка информации
- б) техническое вмешательство, выведение из строя оборудования сети
- в) потеря, искажение, утечка информации
- г) модификация информации

2. К основным принципам обеспечения информационной безопасности относится: (выберите один вариант ответа)

- а) экономическая эффективность системы безопасности
- б) многоплатформенная реализация системы
- в) усиленная защищенность всех звеньев системы
- г) многопользовательский режим работы системы

3. Основными субъектами информационной безопасности являются: (выберите один вариант ответа)

- а) руководители, менеджеры, администраторы компаний
- б) органы права, государства, бизнеса
- в) сетевые базы данных
- г) фаерволлы

4. В случае получения спама по e-mail с приложенным файлом, следует: (выберите один вариант ответа)

- а) прочитать вложение, если оно не содержит ничего ценного – удалить
- б) сохранить вложение в папке «Спам», выяснить затем IP-адрес генератора спама
- в) удалить письмо с вложением, не раскрывая его
- г) отправить коллеге

5. Наиболее распространены угрозы информационной безопасности корпоративной системы: (выберите один вариант ответа)

- а) покупка нелегального ПО
- б) ошибки эксплуатации и неумышленного изменения режима работы системы
- в) сознательного внедрения сетевых вирусов
- г) недостаток компьютерной грамотности

Ключи

1.	в
2.	а
3.	б
4.	в
5.	б

6. Прочитайте текст и установите соответствие

В таблице приведены понятия в сфере информационной безопасности и их характеристики. Установите между ними соответствие.

Характеристика	Понятия
1. Программа, которая запускается при определённых временных или информационных условиях для осуществления вредоносных действий	а) анализ уязвимостей

2. Процесс определения личности или объекта в системе	б) утечка информации
3. Процесс проверки пользователя, который подтверждает его личность при доступе к сайту, приложению, аккаунту в социальной сети.	в) информационный перехват
4. Процесс оценки уровня безопасности информационной системы, направленный на обнаружение угроз и рисков вероятного несанкционированного проникновения третьих лиц в систему	г) идентификация
5. Ситуация, характеризующая потерей данных в системе	д) аутентификация
	е) логическая бомба

Запишите в таблицу выбранные буквы под соответствующими цифрами

1	2	3	4	5
е	г	д	а	б

Второй этап (продвинутый уровень) – показывает сформированность показателя компетенции «уметь»: ориентируясь на задачи профессиональной деятельности, обоснованно выбирать современные информационные технологии.

Задания открытого типа (вопросы для опроса):

1. Каким главным требованиям должен отвечать надежный пароль?
2. Опишите алгоритм задания пароля на открытие книги в MS Excel.
3. Перечислите виды атак на пароль.
4. Брандмауэр – это...
5. Опишите утилиту *ping*.

Ключи

1.	– пароль должен состоять не менее чем из восьми знаков; – должен содержать знаки, относящиеся к каждой из следующих трех групп: прописные и строчные буквы латинского алфавита, цифры (от 0 до 9) и символы; – должен значительно отличаться от паролей, использовавшихся ранее; – не должен содержать фамилию или имя пользователя.
2.	Перейти по вкладке <i>Файл</i> на панели инструментов. В меню слева выбрать <i>Сведения – Защитить книгу</i> –. Зашифровать с использованием пароля. В новом окне задать пароль к файлу, подтвердить введенный пароль. Сохраните файл. При повторном открытии файла программа затребует пароль.
3.	Различают два вида атак: Online: атаки, в которых единственным способом для атакующего проверить, является ли данный пароль корректным, есть взаимодействие с сервером. Offline: атаки, когда атакующий имеет возможность проверить все допустимые пароли, не нуждаясь при этом в обратной связи с сервером.
4.	Брандмауэр (фаервол, межсетевой экран) — это фильтр между компьютером и сетью, который проверяет безопасность входящих и исходящих данных.
5.	Ping – утилита командной строки, которая нужна для проверки подключения к другому компьютеру на уровне IP. Принцип работы очень простой: команда <i>ping ip</i> отправляет серию небольших пакетов данных на указанное устройство, а затем показывает время ответа.

Третий этап (высокий уровень) – показывает сформированность показателя компетенции «иметь навыки»: поиска, анализа, выбора и эффективного применения

современные информационные технологии при решении задач профессиональной деятельности.

Практические задания:

Задание 1. После установки программного обеспечения из непроверенного источника, значительно уменьшился объем оперативной памяти. А также появилось множество пустых папок. О чем это свидетельствует?

Задание 2. Вы являетесь пользователем кроссплатформенного мессенджера Telegram. Ваш аккаунт взломали. Каким должно быть первое ваше действие?

Задание 3. Пароль от вашей учетной записи стал известен посторонним лицам. Что необходимо предпринять в первую очередь?

Задание 4. При определенных условиях вами была утеряна банковская карта. Каким должно быть ваше первое действие?

Задание 5. Какая технология разработана для упрощения подключения устройств к сетям Wi-Fi. С ее помощью можно подключиться к роутеру без пароля.

Ключи

1.	о загрузке вируса на ПК
2.	завершить сеанс на всех устройствах
3.	сменить пароль
4.	заблокировать карту
5.	технология WPS

ОПК-6.3. Применяет современные информационные технологии при решении задач профессиональной деятельности.

Первый этап (пороговой уровень) – показывает сформированность показателя компетенции «знать»: знает современные информационные технологии и программные средства, применяемые для решения задач профессиональной деятельности.

Тестовые задания закрытого типа

1. Заключительным этапом построения системы защиты является: (выберите один вариант ответа)

- а) сопровождение
- б) планирование
- в) анализ уязвимых мест
- г) утверждение сметы работ

2. Информационная безопасность зависит от: (выберите один вариант ответа)

- а) информации
- б) компьютеров, поддерживающей инфраструктуры
- в) пользователей
- г) сотрудников

3. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности: (выберите один вариант ответа)

- а) контрагенты
- б) сотрудники
- в) хакеры
- г) администратор сети предприятия

4. Защита информации: (выберите один вариант ответа)

- а) комплекс мероприятий, направленных на обеспечение информационной безопасности
- б) небольшая программа для выполнения определенной задачи
- в) процесс разработки структуры базы данных в соответствии с требованиями пользователей
- г) антивирусное программное обеспечение

5. Какие вирусы активизируются в самом начале работы с операционной системой:
(выберите один вариант ответа)

- а) загрузочные вирусы
- б) троянцы
- в) черви
- г) макровирусы

Ключи

1.	а
2.	б
3.	б
4.	а
5.	а

6. Прочитайте текст и установите соответствие

В таблице приведены основные виды компьютерных вирусов и их характеристики. Установите между ними соответствие.

Основные характеристики вируса	Виды компьютерных вирусов
1. Вирус способный копировать себя и распространяться с одного устройства на другое через сеть, заражая все попавшиеся на её путь устройства.	а) Загрузочный вирус
2. Разновидность компьютерных вирусов, разработанных на макроязыках, встроенных в такие прикладные пакеты программного обеспечения, как Microsoft Office.	б) Полиморфный вирус
3. Компьютерный вирус, записывающийся в первый сектор гибкого или жёсткого диска и выполняющийся при загрузке компьютера. Данный вирус может контролировать загрузку операционной системы и перехватывать управление перед передачей его операционной системе.	в) Сетевой вирус
4. Компьютерный вирус, прикрепляющий себя к файлу или программе и активизирующийся при каждом использовании файла. Для своего размножения использует файловую систему, внедряясь в исполняемые файлы практически любой операционной системы.	г) Макровирус
5. Вирус, полностью или частично скрывающий своё присутствие в системе путём перехвата обращений к операционной системе.	д) Файловый вирус
	е) Стелс-вирус

Запишите в таблицу выбранные буквы под соответствующими цифрами

1	2	3	4	5
в	г	а	д	е

Второй этап (продвинутый уровень) – показывает сформированность показателя компетенции «уметь»: применять современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности.

Задания открытого типа (вопросы для опроса):

1. Брандмауэр, его понятие и главная задача.
2. Перечислите основные виды сетевых атак.
3. Перечислите основные каналы несанкционированного доступа.
4. Признаки заражения компьютера вирусами.
5. Раскройте понятие «фишинг».

Ключи

1.	Брандмауэр (файрвол, межсетевой экран) — это система защиты компьютерной сети, которая ограничивает прохождение входящего, исходящего и внутрисетевого трафика. Основная функция брандмауэра — блокировать вредоносную активность и предотвращать несанкционированные действия пользователей.
2.	Существует два основных типа сетевых атак: пассивные и активные. При пассивных сетевых атаках злоумышленники входят в сети без разрешения, контролируют и крадут личную информацию без внесения каких-либо изменений. Активные сетевые атаки включают изменение, шифрование или повреждение данных.
3.	Основные каналы несанкционированного доступа к информации могут включать: – установление контакта с лицами, имеющими или имевшими доступ к конфиденциальной информации; – вербовка и внедрение агентов; – физическое проникновение к носителям конфиденциальной информации; – подключение к средствам отображения, хранения, обработки, воспроизведения и передачи информации, средства связи; – прослушивание речевой конфиденциальной информации; – визуальный съём конфиденциальной информации; – перехват электромагнитных излучений.
4.	Некоторые признаки заражения компьютера вирусами: – снижение производительности (медленная работа и долгий запуск программ) – проблемы с жёстким диском (например, длительная запись или копирование данных) – всплывающие окна – проблемы с доступом к учётным записям (внезапная потеря доступа к учётной записи по старому паролю или уведомления о попытке смены пароля) – некорректная работа браузера – появление новых и незнакомых программ, файлов, ярлыков – долгое выключение или перезагрузка компьютера.
5.	Фишинг (от англ. fishing — рыбачить, выуживать) — вид кибератаки, при которой злоумышленник пытается получить доступ к личной информации пользователя. Например, к логину и паролю от электронной почты или данным банковской карты.

Третий этап (высокий уровень) – показывает сформированность показателя компетенции «иметь навыки»: владения современными информационными технологиями для решения общенаучных задач в своей профессиональной деятельности и для организации своего труда.

Практические задания:

Задание 1. 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 2. Запустить ping компьютера: «Пуск»->«Выполнить»->“cmd”->“ping ip-addr -t”. Где располагается утилита **ping**?

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.	в сектор загрузки системного диска (Master Boot Record)
2.	в системной папке Windows (C:\windows\system)
3.	изменить атрибуты папок
4.	систематическое резервное копирование
5.	использовать точку восстановления компьютера

Оценочные средства для проведения промежуточной аттестации

Промежуточная аттестация проводится в виде зачета.

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).