

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гнатюк Сергей Иванович
Должность: Первый проректор
Дата подписания: 20.05.2025 08:58:53
Уникальный программный ключ:
5ede28fe5b714e680817c5c132d4ba793a6b442

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. _____

« 30 » _____ июня _____ 2023 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине «Информационная безопасность»
для специальности 38.05.01 Экономическая безопасность
специализация Экономико-правовое обеспечение экономической безопасности

Год начала подготовки – 2023

Квалификация выпускника – экономист

Луганск, 2023

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;
- Федерального государственного образовательного стандарта высшего образования по специальности 38.05.01 Экономическая безопасность (уровень специалитета), утвержденный приказом Министерства науки и высшего образования Российской Федерации от «14» апреля 2021 г. № 293.

Преподаватели, подготовившие рабочую программу:

ассистент _____ **Ю.А. Горячкова**

Рабочая программа рассмотрена на заседании кафедры информационных технологий, математики и физики (протокол № 11 от 20.06.2023 г.).

Заведующий кафедрой _____ **Г.В. Колтакова**

Рабочая программа рекомендована к использованию в учебном процессе методической комиссией факультета экономики и управления АПК (протокол № 11 от 26.06.2023 г.).

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

Руководитель основной профессиональной образовательной программы _____ **В.Г. Ткаченко**

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 вариативной части (Б1.В.11) блока дисциплин подготовки студентов по специальности 38.05.01 Экономическая безопасность, специализация Экономико-правовое обеспечение экономической безопасности основной профессиональной образовательной программы высшего образования (далее – ОПОП ВО).

Дисциплина реализуется кафедрой информационных технологий, математики и физики.

Последующие читаемые дисциплины: «Безопасность электронного документооборота».

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
ПК-3	Способен составлять прогнозы динамики основных экономических показателей деятельности хозяйствующих субъектов с учетом возможных экономических рисков и угроз экономической безопасности	ПК-3.1. Разрабатывает и обосновывает финансово-экономические показатели характеризующие деятельность хозяйствующих субъектов, и методики их расчёта	Знать информационные технологии решения экономических задач
			Уметь применять информационные технологии для обработки экономической информации
		ПК-3.2. Анализирует и составляет прогнозы динамики основных экономических показателей деятельности хозяйствующих субъектов с учетом возможных экономических рисков и угроз экономической безопасности	Владеть навыками использования информационных технологий и систем для решения экономических задач
			Знать программные средства решения экономических задач
			Уметь применять программные средства для обработки экономической информации
			Владеть навыками использования программных средств для решения экономических задач

3. Объём дисциплины и виды учебной работы

Виды работ	Очная форма обучения		Заочная форма обучения
	всего зач.ед./ часов	объём часов	всего часов
		2 семестр	2 семестр
Общая трудоёмкость дисциплины	2/108	2/108	2/108
Аудиторная работа:	34	34	12
Лекции	18	18	6
Практические занятия	16	16	6
Лабораторные работы	–	–	–
Другие виды аудиторных занятий	–	–	–
Предэкзаменационные консультации	–	–	–
Самостоятельная работа обучающихся, час	74	74	96
Вид промежуточной аттестации (зачёт, экзамен)	зачет	зачет	зачет

4. Содержание дисциплины

4.1. Разделы дисциплины и виды занятий (тематический план)

№ п/п	Раздел дисциплины	Л	ПЗ	ЛР	СРС
очная форма обучения					
1	Введение в информационную безопасность	2	-		8
2	Правовое обеспечение информационной безопасности	2	2		10
3	Организационное обеспечение информационной безопасности	2	2		8
4	Технические средства и методы защиты информации	2	2		8
5	Программно-аппаратные средства и методы обеспечения информационной безопасности	2	2		8
6	Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	2	2		8
7	Средства восстановления данных	2	2		8
8	Средства антивирусной защиты информации	2	2		8
9	Политика информационной безопасности организации (предприятия)	2	2		8
Итого		18	16		74
заочная форма обучения					
1	Введение в информационную безопасность	0,5	0,5		10
2	Правовое обеспечение информационной безопасности	0,5	0,5		12
3	Организационное обеспечение информационной безопасности	0,5	0,5		10

4	Технические средства и методы защиты информации	0,5	0,5		10
5	Программно-аппаратные средства и методы обеспечения информационной безопасности	1	1		12
6	Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	1	1		10
7	Средства восстановления данных	1	1		12
8	Средства антивирусной защиты информации	0,5	0,5		10
9	Политика информационной безопасности организации (предприятия)	0,5	0,5		10
Итого		6	6		96

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 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
1.	Введение в информационную безопасность	2	0,5
2.	Правовое обеспечение информационной безопасности	2	0,5
3.	Организационное обеспечение информационной безопасности	2	0,5
4.	Технические средства и методы защиты информации	2	0,5
5.	Программно-аппаратные средства и методы обеспечения информационной безопасности	2	1
6.	Применение информационных технологий для изучения вопросов организационно-правового	2	1
7.	Средства восстановления данных	2	1
8.	Средства антивирусной защиты информации	2	0,5
9.	Политика информационной безопасности организации (предприятия)	2	0,5
Итого		18	6

4.4. Перечень тем практических занятий (семинаров)

№ п/п	Тема практических занятий	Объём, ч	
		форма обучения	
		очная	заочная
1.	Установка и первоначальная настройка VM VirtualBox	2	0,5
2.	Разграничение прав доступа системы	2	0,5
3.	Файловые подсистемы	2	0,5
4.	Обеспечение целостности и доступности данных	2	0,5
5.	Восстановление данных	2	1
6.	Антивирусная защита компьютера	2	1
7.	Безопасность на уровне операционной системы и приложений	2	1
8.	Настройки безопасности интернет обозревателей	2	1
Итого		16	6

4.5. Перечень тем лабораторных работ.

Лабораторные работы 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)

Курсовые работы (проекты) не предусмотрены.

4.6.3. Перечень тем рефератов, расчетно-графических работ

Рефераты, расчетно-графические работы 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
1.	Введение в информационную безопасность	Бондаренко, И. С. Информационная безопасность: учебник / И. С. Бондаренко. — Москва : МИСИС, 2023. — 254 с. — ISBN 978-5-907560-71-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/360344 (дата обращения: 20.03.2023). — Режим доступа: для авториз. пользователей.	8	10
2.	Правовое обеспечение информационной безопасности		10	12
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	12
6.	Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	Капгер, И. В. Управление информационной безопасностью : учебное пособие / И. В. Капгер, А. С. Шабуров. — Пермь : ПНИПУ, 2023. — 91 с. — ISBN 978-5-398-02866-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/328889 (дата обращения: 20.03.2023). — Режим доступа: для авториз. пользователей.	8	10
7.	Средства восстановления данных		8	12
8.	Средства антивирусной защиты информации	Моргунов, А. В. Информационная безопасность : учебно-методическое пособие / А. В. Моргунов. — Новосибирск : НГТУ, 2019. — 83 с. — ISBN 978-	8	10
9.	Политика информационной		8	10

№	Тема самостоятельной	Учебно-методическое обеспечение	Объём, ч	
	безопасности организации (предприятия)	5-7782-3918-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/152227 (дата обращения: 20.03.2023). — Режим доступа: для авториз. пользователей.		
Итого			74	96

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 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.	Басыня, Е. А. Сетевая информационная безопасность : учебник / Е. А. Басыня. — Москва : НИЯУ МИФИ, 2023. — 224 с. — ISBN 978-5-7262-2949-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/355511 (дата обращения: 20.03.2023). — Режим доступа: для авториз. пользователей.	Электронный ресурс
2.	Бондаренко, И. С. Информационная безопасность: учебник / И. С. Бондаренко. — Москва: МИСИС, 2023. — 254 с. — ISBN 978-5-907560-71-0. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/360344 (дата обращения: 20.03.2023). — Режим доступа: для авториз. пользователей.	Электронный ресурс
3.	Гродзенский, Я. С. Информационная безопасность : учебное пособие / Я. С. Гродзенский. — Москва : Проспект, 2020. — 142 с. — ISBN 978-5-9988-0845-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/181193 (дата обращения: 20.03.2023). — Режим доступа: для авториз. пользователей.	Электронный ресурс
4.	Информационная безопасность : учебное пособие / В. И. Лойко, В. Н. Лаптев, Г. А. Аршинов, С. Н. Лаптев. — Краснодар: КубГАУ, 2020. — 332 с. — ISBN 978-5-907346-50-5. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/254168 (дата обращения: 27.03.2024). —	Электронный ресурс

	Режим доступа: для авториз. пользователей.	
5.	Ярочкин, В. И. Информационная безопасность: учебник / В. И. Ярочкин. — 5-е изд. — Москва : Академический Проект, 2020. — 544 с. — ISBN 978-5-8291-3031-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/132242 (дата обращения: 20.03.2023). — Режим доступа: для авториз. пользователей.	Электронный ресурс

6.1.2. Дополнительная литература

№ П/П	Автор, название, место издания, изд-во, год издания, количество страниц
1.	Зырянова, Т. Ю. Управление информационной безопасностью : учебное пособие / Т. Ю. Зырянова. — Екатеринбург : , 2023. — 96 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/369482 (дата обращения: 27.03.2024). — Режим доступа: для авториз. пользователей. Зырянова, Т. Ю. Управление информационной безопасностью : учебное пособие / Т. Ю. Зырянова. — Екатеринбург : , 2023. — 96 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/369482 (дата обращения: 20.03.2023). — Режим доступа: для авториз. пользователей.
2.	Капгер, И. В. Управление информационной безопасностью : учебное пособие / И. В. Капгер, А. С. Шабуров. — Пермь : ПНИПУ, 2023. — 91 с. — ISBN 978-5-398-02866-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/328889 (дата обращения: 20.03.2023). — Режим доступа: для авториз. пользователей.

6.1.3. Периодические издания

Периодические издания при изучении дисциплины 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: 20.03.2023)
2.	Фундаментальная электронная библиотека «Лань». [Электронный ресурс]. Режим доступа: https://e.lanbook.com/
3.	http://vlad-ezhov.narod.ru/zor/pbaa1.html Учебные материалы по информатике

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	http://moodle.lnau.su	+	+	+

6.3.2. Аудио- и видеопособия

Аудио- и видеопособия не предусмотрены.

6.3.3. Компьютерные презентации учебных курсов

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 – 5 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 – 8 шт., рециркулятор – 1 шт., стул мягкий – 1 шт., доска для тех.пок. – 1 шт., стол компьют. – 25 шт., стул ученич. – 29 шт.
3.	Г-112 – аудитория для проведения лабораторных и практических занятий, самостоятельной работы	Компьютеры – 5 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 – 6 шт.
4.	Г-113 – аудитория для проведения лабораторных и практических занятий, самостоятельной работы	Компьютеры – 5 шт., рециркулятор – 1 шт., стол 1 тумб. – 2 шт., трибуна мал. – 1 шт., стул п/мягкий – 1 шт., стул ученич. – 15 шт., стол компьют. – 5 шт., скамейка аудит. – 9 шт., доска для тех.пок. – 1шт., стол парта – 11 шт.
5.	Г-114 – аудитория для проведения лабораторных и практических занятий, самостоятельной работы	Компьютеры – 7 шт., стол аудит. – 1 шт., доска для тех. пок. – 1 шт., лавка – 3 шт., скам. аудит. – 5 шт., стол компьют. – 1 шт., стол аудит. – 13 шт., стул ученич. – 14 шт.
6.	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.
7.	Г-120 – аудитория для проведения лабораторных и практических занятий, групповых и индивидуальных консультаций, текущего контроля, промежуточной аттестации, самостоятельной работы	Компьютер – 5 шт., скамейка ауд. – 5 шт., стол 1 тумб. – 2 шт., стол аудит. – 6 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
Современные информационные технологии	Кафедра информационных технологий, математики и физики	согласовано
Информационные технологии в профессиональной деятельности	Кафедра информационных технологий, математики и физики	согласовано
Безопасность электронного документооборота	Кафедра информационных технологий, математики и физики	согласовано

МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ЛУГАНСКИЙ ГОСУДАРСТВЕННЫЙ
АГРАРНЫЙ УНИВЕРСИТЕТ ИМЕНИ К.Е. ВОРОШИЛОВА»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине (модулю) «Информационная безопасность»

Специальность: 38.05.01 Экономическая безопасность

Специализация: Экономика-правовое обеспечение экономической безопасности

Уровень профессионального образования: специалитет

Год начала подготовки: 2023

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
ПК-3	Способен составлять прогнозы динамики основных экономических показателей деятельности хозяйствующих субъектов с учетом возможных экономических рисков и угроз экономической безопасности	ПК-3.1. Разрабатывает и обосновывает финансово-экономические показатели характеризующие деятельность хозяйствующих субъектов, и методики их расчёта	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)	Владеть навыками использования информационных технологий и систем для решения экономических задач		Практические задания	Зачет

					7. Средства восстановления данных 8. Средства антивирусной защиты информации 9. Политика информационной безопасности организации (предприятия)		
		ПК-3.2. Анализирует и составляет прогнозы динамики основных экономических показателей деятельности хозяйствующих субъектов с учетом возможных экономических рисков и угроз экономической безопасности	Первый этап (пороговый уровень)	Знать программные средства решения экономических задач	1. Введение в информационную безопасность	Тесты закрытого типа	Зачет
			Второй этап (продвинутый уровень)	Уметь применять программные средства для обработки экономической информации	2. Правовое обеспечение информационной безопасности 3. Организационное обеспечение информационной безопасности	Тесты открытого типа (вопросы для опроса)	Зачет
			Третий этап (высокий уровень)	Владеть навыками использования программных средств для решения экономических задач	4. Технические средства и методы защиты информации 5. Программно-аппаратные средства и методы обеспечения информационной безопасности 6. Применение информационных технологий для изучения вопросов	Практические задания	Зачет

					организационно- правового обеспечения информационной безопасности 7. Средства восстановления данных 8. Средства антивирусной защиты информации 9. Политика информационной безопасности организации (предприятия)		
--	--	--	--	--	---	--	--

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	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.

ПК-3. Способен составлять прогнозы динамики основных экономических показателей деятельности хозяйствующих субъектов с учетом возможных экономических рисков и угроз экономической безопасности.

ПК-3.1. Разрабатывает и обосновывает финансово-экономические показатели характеризующие деятельность хозяйствующих субъектов, и методики их расчёта

Первый этап (пороговой уровень) – показывает сформированность показателя компетенции «знать»: информационные технологии решения экономических задач

Тестовые задания закрытого типа

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

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

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

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

4. Защита информации: (выберите один правильный 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 правильный 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

Установите соответствие основных понятий и их формулировки

<i>Основные понятия</i>	<i>Формулировка</i>
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) Информационная платформа
	ж) Информационные ресурсы

Запишите в таблицу выбранные буквы под соответствующими цифрами

1	2	3	4	5
ж)	в)	а)	д)	б)

Второй этап (продвинутый уровень) – показывает сформированность показателя компетенции «уметь»: применять информационные технологии для обработки экономической информации

Задания открытого типа (вопросы для опроса):

1. Каким главным требованиям должен отвечать надёжный 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 ping ip отправляет серию небольших пакетов данных на указанное устройство, а затем показывает время ответа.

Третий этап (высокий уровень) – показывает сформированность показателя компетенции «владеть»: навыками использования информационных технологий и систем для решения экономических задач

Практические задания:

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

Задание 2. Для передачи сообщения используется код, состоящий из прописных латинских букв и цифр (всего используется 30 различных символов). При этом все символы кодируются одним и тем же (минимально возможным) количеством битов. Определите информационный объём сообщения длиной в 100 символов.

Задание 3. Метеорологическая станция ведет наблюдение за влажностью воздуха. Результатом одного наблюдения является целое число от 0 до 100%, записываемое при помощи минимально возможного количества бит. Станция сделала 300 измерений. Определите информационный объём результатов наблюдений.

Задание 4. В течение двух минут производилась четырёхканальная звукозапись с частотой дискретизации 16 КГц и 32-битным разрешением без сжатия. В ответе укажите целое количество мегабайт, необходимых для хранения такой аудиозаписи.

Задание 5. 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?

Ключи

1.	в системной папке Windows (C:\windows\system)
2.	62,5 байта
3.	262,5 байта
4.	30 Мб
5.	в сектор загрузки системного диска (Master Boot Record)

ПК-3.2. Анализирует и составляет прогнозы динамики основных экономических показателей деятельности хозяйствующих субъектов с учетом возможных экономических рисков и угроз экономической безопасности.

Первый этап (пороговой уровень) – показывает сформированность показателя компетенции «знать»: программные средства решения экономических задач.

Тестовые задания закрытого типа

1. К правовым методам, обеспечивающим информационную безопасность, относятся: (выбрать 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 правильный 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. Основными источниками угроз информационной безопасности являются: (выберите один правильный вариант ответа)

- а) хищение жестких дисков, подключение к сети, инсайдерство
- б) Перехват данных, хищение данных, изменение архитектуры системы
- в) Хищение данных, подкуп системных администраторов, нарушение регламента работы
- г) все указанное в списке

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

- а) Черви
- б) Шпионские программы
- в) Троянские программы
- г) Макровирусы

Ключи

1.	в)
2.	в)
3.	б)
4.	а)
5.	в)

6. Прочитайте текст и установите соответствие

Установите соответствие основных понятий и их формулировки

<i>Основные понятия</i>	<i>Формулировка</i>
1. Специализированная программа для обнаружения вредоносными программ и восстановления заражённых (модифицированных) такими программами файлов и профилактики — предотвращения заражения	а) Компьютерный вирус

(модификации) файлов или операционной системы вредоносным кодом.	
2. Вид вредоносных программ, способных внедряться в код других программ, системные области памяти, загрузочные секторы и распространять свои копии по разнообразным каналам связи.	б) Антивирусная программа
3. Защищённость информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации.	в) Сетевой вирус
4. Противоборство сторон посредством распространения специально подготовленной информации и противодействия аналогичному внешнему воздействию на себя.	г) Макровирус
5. Вредоносный код, специально разработанный злоумышленником с использованием макроязыка (языка, который используется для создания таких приложений, как Microsoft Word, Excel или PowerPoint).	д) Информационная безопасность
	е) Вирусная атака
	ж) Информационная война

Запишите в таблицу выбранные буквы под соответствующими цифрами

1	2	3	4	5
б)	а)	д)	ж)	г)

Второй этап (продвинутый уровень) – показывает сформированность показателя компетенции «уметь»: применять программные средства для обработки экономической информации

Задания открытого типа (вопросы для опроса):

1. Перечислите типы архивации и их возможности, которые можно выполнить с помощью элемента *Панель управления – Архивация и восстановление*.
2. Перечислите основные виды сетевых атак.
3. Перечислите основные каналы несанкционированного доступа.
4. Признаки заражения компьютера вирусами.
5. Раскройте понятие «фишинг».

Ключи

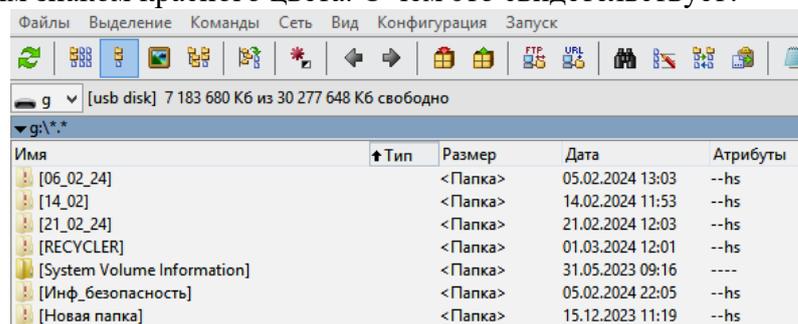
1.	Имеются три типа архивирования: 1. Системное архивирование - записывается архивный образ операционной системы 2. Полное архивирование - сохранение всех данных. 3. Нарастающее (инкрементальное) архивирование - записываются только изменения относительно последнего полного архивирования. Этот тип архивирования самый быстрый, но его необходимо проводить очень внимательно.
2.	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;

	<ul style="list-style-type: none"> – прослушивание речевой конфиденциальной информации; – визуальный съём конфиденциальной информации; – перехват электромагнитных излучений.
4.	<p>Некоторые признаки заражения компьютера вирусами:</p> <ul style="list-style-type: none"> – 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.	<p>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.</p>

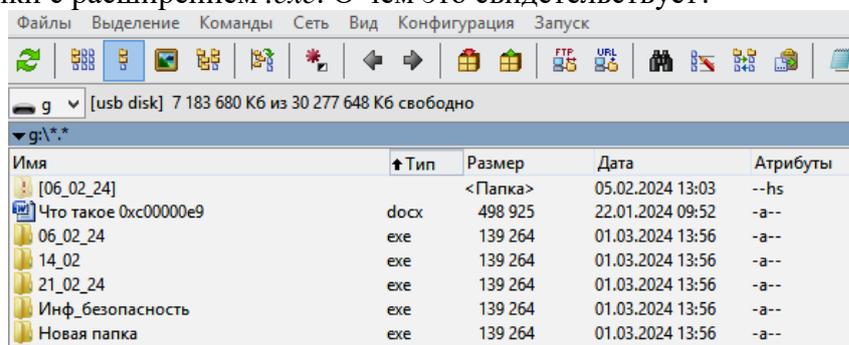
Третий этап (высокий уровень) – показывает сформированность показателя компетенции «владеть»: навыками использования программных для решения экономических задач.

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. 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 объём 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

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. Уровень 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

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 выставляется преподавателем в конце изучения дисциплины 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.