МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ
Декан факультета экономики, менеджмента
и инновационных технологий
_____ С.А. Баркалов
«19» _____ 2024 г.

РАБОЧАЯ ПРОГРАММА

дисциплины
«Информационная безопасность и защита информации»

Направление подготовки 38.04.02 Менеджмент

Магистерская программа Стратегия развития бизнеса

Квалификация выпускника магистр

Нормативный период обучения 2 года / 2 года и 4 м.

Форма обучения очная / очно-заочная

Год начала подготовки 2024

Автор программы _____/ Н.Н. Макаров/

И.о. зав. кафедрой
экономической безопасности _____/ А.В. Красникова /

Руководитель ОПОП _____/ И.Ф. Елфимова /

Воронеж 2024

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины: формирование у обучающихся знаний в области информационной безопасности и защиты информации, а также овладение современными методами обеспечения безопасности информации при разработке стратегии бизнеса.

1.2. Задачи освоения дисциплины:

- изучить основы информационной безопасности;
- овладеть методами защиты информации в организациях
- изучить основные подходы к организации и управлению информационной безопасностью в организации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Информационная безопасность и защита информации» относится к дисциплинам части, формируемой участниками образовательных отношений блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Информационная безопасность и защита информации» направлен на формирование следующих компетенций:

ПК-5 - Способен оценивать риски, разрабатывать мероприятия по их снижению и обеспечению экономической и информационной безопасности, осуществлять мониторинг реализации стратегических решений с учетом возникающих угроз в соответствии со стратегическими целями организации.

Компетенция	**Результаты обучения, характеризующие сформированность компетенции**
ПК-5	Знать - основные понятия и содержание информационной безопасности; - современные методы и инструменты защиты информации; - способы определения угроз информационной безопасности для бизнеса;
	уметь - определять риски информационной безопасности; - организовывать защиту информации на объектах; - осуществлять анализ и разработку политики информационной безопасности;
	владеть - навыками выявления и устранения угроз информационной безопасности; - методами и способами организации и управления защиты

	информации; - навыками безопасной работы с информацией.

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Информационная безопасность и защита информации» составляет 3 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры
		4
Аудиторные занятия (всего)	32	32
В том числе:		
Лекции	8	8
в том числе *в электронной форме*	*4*	*4*
Практические занятия (ПЗ)	24	24
в том числе в форме практической подготовки	6	6
в электронной форме	*8*	*8*
Самостоятельная работа	76	76
Курсовой проект	-	-
Виды промежуточной аттестации - зачет	+	+
Общая трудоемкость: академические часы зач.ед.	 108 3	 108 3

очно-заочная форма обучения

Виды учебной работы	Всего часов	Семестры
		9
Аудиторные занятия (всего)		
В том числе:		
Лекции	6	6
в том числе *в электронной форме*	*2*	*2*
Практические занятия (ПЗ)	24	24
в том числе в форме практической подготовки	6	6
в электронной форме	*8*	*8*
Самостоятельная работа	78	78
Курсовой проект	-	-
Виды промежуточной аттестации - зачет	+	+
Общая трудоемкость: академические часы зач.ед.	 108 3	 108 3

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Практ зан.	СРС	Всего, час
1	Информационная безопасность в системе национальной безопасности РФ	Основные термины и определения. Классификация защищаемой информации. Некоторые проблемы обеспечения информационной безопасности в Российской Федерации. Основные положения документов о стратегии национальной безопасности Российской федерации и «Доктрина информационной безопасности Российской Федерации». Основные составляющие национальных интересов РФ в информационной сфере. Основные направления федерального законодательства в области защиты информации.	2	4	13	19
		в том числе электронная форма обучения		*2*		*2*
		практическая подготовка обучающихся		*2*		*2*
2	Персональные данные	Понятие. Требования закона №152 «О персональных данных». Ответственность за нарушения работы с персональными данными. Классификация персональных данных. Составление документов для разрешения работы с персональными данными.	2	4	13	19
		практическая подготовка обучающихся		*2*		*2*
3	Преступления в сфере компьютерных технологий	Классификация компьютерных преступлений. Статьи УК РФ, связанные с преступлениями в сфере компьютерных технологий, наказание, противодействие атакам злоумышленников.	-	4	13	17
		в том числе электронная форма обучения		*2*		*2*
4	Основные угрозы информационной безопасности	Анализ и классификация угроз информационной безопасности. Причины, виды, каналы утечки и искажения информации. Угрозы программно-математических воздействий и нетрадиционных информационных каналов. Угрозы, основанные на информационных сетевых атаках.	2	4	13	19
		практическая подготовка обучающихся		*2*		*2*
		в том числе электронная форма обучения	*2*			*2*
5	Защита информации	Риски, связанные с информацией (конфиденциальность, целостности,	2	4	10	16

		доступность), методы уменьшения рисков, определение потенциальных и реальных угроз.				
		в том числе электронная форма обучения	*2*	*2*		*4*
6	Антивирусная защита	Антивирусная защита Общие понятия антивирусной защиты. Уязвимости. Классификация вредоносных программ. Признаки присутствия на компьютере вредоносных программ. Методы защиты от вредоносных программ. Основы работы антивирусных программ: Сигнатурный и эвристический анализ. Тестирование работы антивируса. Классификация антивирусов. Режимы работы антивирусов. Антивирусные комплексы	-	*4*	*14*	*18*
\		*в том числе электронная форма обучения*		*2*		
Итого			**8**	**24**	**76**	**108**
Итого по дисциплине			**8**	**24**	**76**	**108**

очно-заочная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Практ зан.	СРС	Всего, час
1	Информационная безопасность в системе национальной безопасности РФ	Основные термины и определения. Классификация защищаемой информации. Некоторые проблемы обеспечения информационной безопасности в Российской Федерации. Основные положения документов о стратегии национальной безопасности Российской федерации и «Доктрина информационной безопасности Российской Федерации». Основные составляющие национальных интересов РФ в информационной сфере. Основные направления федерального законодательства в области защиты информации ограниченного доступа.	2	4	13	19
		в том числе электронная форма обучения		*2*		*2*
		практическая подготовка обучающихся		*2*		*2*
2	Персональные данные	Понятие. Требования закона №152 «О персональных данных». Ответственность за нарушения работы с персональными данными. Классификация персональных данных. Составление документов для разрешения работы с персональными данными.		4	13	17

		практическая подготовка обучающихся		*2*		*2*
3	Преступления в сфере компьютерных технологий	Классификация компьютерных преступлений. Статьи УК РФ, связанные с преступлениями в сфере компьютерных технологий, наказание, противодействие атакам злоумышленников.		4	13	17
		в том числе электронная форма обучения		*2*		*2*
4	Основные угрозы информационной безопасности	Анализ и классификация угроз информационной безопасности. Причины, виды, каналы утечки и искажения информации. Угрозы программно-математических воздействий и нетрадиционных информационных каналов. Угрозы, основанные на информационных сетевых атаках.	2	4	13	19
		в том числе электронная форма обучения		*2*		*2*
5	Защита информации	Риски, связанные с информацией (конфиденциальность, целостности, доступность), методы уменьшения рисков, определение потенциальных и реальных угроз.	2	4	13	19
		в том числе электронная форма обучения	2	*2*		*4*
6	Антивирусная защита	Антивирусная защита Общие понятия антивирусной защиты. Уязвимости. Классификация вредоносных программ. Признаки присутствия на компьютере вредоносных программ. Методы защиты от вредоносных программ. Основы работы антивирусных программ: Сигнатурный и эвристический анализ. Тестирование работы антивируса. Классификация антивирусов. Режимы работы антивирусов. Антивирусные комплексы		*4*	13	*17*
		практическая подготовка обучающихся		*2*		*2*
Итого			**6**	**24**	**78**	**108**
Итого по дисциплине			**6**	**24**	**78**	**108**

Практическая подготовка при освоении дисциплины (модуля) проводится путем непосредственного выполнения обучающимися отдельных элементов работ, связанных с будущей профессиональной деятельностью, способствующих формированию, закреплению и развитию практических навыков и компетенций по профилю соответствующей образовательной программы на практических занятиях.

№ п/п	Перечень выполняемых обучающимися отдельных элементов работ, связанных с будущей профессиональной деятельностью	Формируемые профессиональные компетенции

Практические занятия		
1	Организация защиты информации организации в соответствии с законодательством РФ	ПК-5
2	Составление документов для разрешения работы с персональными данными.	ПК-5
3	Анализ и выявление угроз информационной безопасности	ПК-5

5.2 Перечень лабораторных работ

Не предусмотрено учебным планом

5.3 Перечень практических занятий

5.3.1 Очная форма обучения

№ п/п	Тема и содержание практического занятия	Объем часов	В т.ч. в электр. форме	Виды контроля
1	Изучение законодательства в сфере защиты информации	2		устный опрос,
2	Организация защиты информации организации на в соответствии с законодательством РФ	2	2	письменные задания, тестовый контроль
3	Правила работы и хранения персональных данных	2		письменные задания
4	Составление документов для разрешения работы с персональными данными.	2		письменные задания, тестовый контроль
5	Изучение практики компьютерных преступлений	2	2	устный опрос, письменные задания
6	Разработка программы противодействия компьютерным преступлениям	2		письменные задания, тестовый контроль
7	Предотвращение угроз, основанных на информационных сетевых атаках	2		устный опрос
8	Анализ и выявление угроз информационной безопасности	2	2	письменные задания, тестовый контроль
9	Разработка программы по борьбе с нарушениями в сфере информационной безопасности в деятельности предприятия	2		устный опрос
10	Выявить угрозы информационной безопасности компании могут нести сотрудники различных возрастных категорий и разработать программу их противодействия	2		письменные задания, тестовый контроль
11	Анализ тренда BYOD (Bring Your Own Device) с точки зрения обеспечения информационной безопасности предприятия	2		письменные задания
12	Применение антивирусных программ	2	2	письменные задания тестовый контроль
	Итого	24	8	

5.3.2 Очно-заочная форма обучения

№ п/п	Тема и содержание практического занятия	Объем часов	В т.ч. в электр. форме	Виды контроля
1	Изучение законодательства в сфере защиты информации	2		устный опрос,
2	Организация защиты информации организации на в соответствии с законодательством РФ	2	2	письменные задания, тестовый контроль
3	Правила работы и хранения персональных данных	2		письменные задания
4	Составление документов для разрешения работы с персональными данными.	2		письменные задания, тестовый контроль
5	Изучение практики компьютерных преступлений	2	2	устный опрос, письменные задания
6	Разработка программы противодействия компьютерным преступлениям	2		письменные задания, тестовый контроль
7	Предотвращение угроз, основанных на информационных сетевых атаках	2		устный опрос
8	Анализ и выявление угроз информационной безопасности	2	2	письменные задания, тестовый контроль
9	Разработка программы по борьбе с нарушениями в сфере информационной безопасности в деятельности предприятия	2		устный опрос
10	Выявить угрозы информационной безопасности компании могут нести сотрудники различных возрастных категорий и разработать программу их противодействия	2		письменные задания, тестовый контроль
11	Анализ тренда BYOD (Bring Your Own Device) с точки зрения обеспечения информационной безопасности предприятия	2		письменные задания
12	Применение антивирусных программ	2	2	письменные задания тестовый контроль
	Итого	24	8	

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ПК-5	Знать - основные понятия и содержание информационной безопасности; - современные методы и инструменты защиты информации; - способы определения угроз информационной безопасности для бизнеса;	Активная работа на практических занятиях, отвечает на теоретические вопросы	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь - определять риски информационной безопасности; - организовывать защиту информации на объектах; - осуществлять анализ и разработку политики информационной безопасности;	Решение заданий по информационной безопасности и защите информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть - навыками выявления и устранения угроз информационной безопасности; - методами и способами организации и управления защиты информации; - навыками безопасной работы с информацией.	Решение заданий по информационной безопасности и защите информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 4 семестре для очной формы обучения, 9 семестре для очно-заочной формы обучения, по четырехбалльной системе:

«зачтено»

«не зачтено».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Зачтено (пороговый уровень)	Не зачтено
ПК-5	Знать - основные понятия и содержание информационной безопасности; - современные	Ответы на тест	Минимально допустимый уровень знаний. Допущены не грубые ошибки. Выполнение теста на 70- 80%	Уровень знаний ниже минимальных требований. Имели место грубые ошибки. В тесте менее 70% правильных ответов

	методы и инструменты защиты информации; - способы определения угроз информационной безопасности для бизнеса;			
	уметь - определять риски информационной безопасности; - организовывать защиту информации на объектах; - осуществлять анализ и разработку политики информационной безопасности;	Решение стандартных практических заданий	Продемонстрированы основные умения. Выполнены типовые задания с не грубыми ошибками. Выполнены все задания, но не в полном объеме (отсутствуют пояснения, неполные выводы)	При выполнении стандартных заданий не продемонстрированы основные умения. Имели место грубые ошибки.
	владеть - навыками выявления и устранения угроз информационной безопасности; - методами и способами организации и управления защиты информации; - навыками безопасной работы с информацией.	Решение прикладных заданий	Имеется минимальный набор навыков для выполнения прикладных заданий с некоторыми недочетами.	При выполнении прикладных заданий не продемонстрированы базовые навыки. Имели место грубые ошибки

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1) К правовым методам, обеспечивающим информационную безопасность, относятся:

一) Разработка аппаратных средств обеспечения правовых данных

二) Разработка и установка во всех компьютерных правовых сетях журналов учета действий

三) Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:

一) Хищение жестких дисков, подключение к сети, инсайдерство

二) Перехват данных, хищение данных, изменение архитектуры системы

三) Хищение данных, подкуп системных администраторов, нарушение регламента

四) работы

3) Виды информационной безопасности:

一) Персональная, корпоративная, государственная

二) Клиентская, серверная, сетевая

三) Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:

一) несанкционированного доступа, воздействия в сети

二) инсайдерства в организации

三) чрезвычайных ситуаций

5) Основные объекты информационной безопасности:

一) Компьютерные сети, базы данных

二) Информационные системы, психологическое состояние пользователей

三) Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:

一) Искажение, уменьшение объема, перекодировка информации

二) Техническое вмешательство, выведение из строя оборудования сети

三) Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:

一) Экономической эффективности системы безопасности

二) Многоплатформенной реализации системы

三) Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:

一) руководители, менеджеры, администраторы компаний

二) органы права, государства, бизнеса

三) сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:

一) Установление регламента, аудит системы, выявление рисков

二) Установка новых офисных приложений, смена хостинг -компании

三) Внедрение аутентификации, проверки контактных данных пользователей

10) Принципом информационной безопасности является принцип недопущения:

一) Неоправданных ограничений при работе в сети (системе)

二) Рисков безопасности сети, системы

三) Презумпции секретности

7.2.2 Примерный перечень стандартных заданий

Задание 1. Назовите виды возможных нарушений информационной системы.

Задание 2. Назовите основные правила защиты от компьютерных вирусов.

Задание 3. Сформулируйте виды противников или «нарушителей» информационной безопасности.

Задание 4. Сформулируйте понятие «Вредоносные программы (вирусы)». Классификация компьютерных вирусов.

Задание 5. Назовите наиболее распространенные угрозы для компьютерной информации.

Задание 6. Назовите наиболее распространенные пути и каналы утечки информации

Задание 7. Назовите виды атак и методы взлома информационных сетей злоумышленниками.

Задание 8. Назовите современные антивирусные программы

Задание 9. Сформулируйте достоинства и недостатки современных антивирусных программ.

Задание 10. Назовите признаки заражения компьютера от вредоносных программ.

7.2.3 Примерный перечень прикладных заданий

Задание 1. Формализуйте требования по обеспечению безопасности ресурсов КИС в соответствии с действующим законодательством.

Политика безопасности «Требования по обеспечению информационной безопасности (ИБ)» для выбранной КИС должна содержать следующие обязательные разделы:

1. Общие положения;
2. Рабочее место пользователя;
3. Парольная политика;
4. Работа с электронной почтой;
5. Работа в сети Интернет;
6. Действия в нестандартных ситуациях;
7. Ответственность.

Задание 2. Определите принципы, порядок и условия обработки персональных данных (ПДн) абонентов, работников организации и иных лиц, чьи ПДн обрабатываются организацией, а также третьими лицами по поручению организации.

Задание 3. Укажите законные основания, на основе которых организация обязана обрабатывать персональные данные. Составьте список угроз безопасности ПДн при их обработке в компании.

Задание 4. Определите порядок организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (ИСПДн), а также установите требования по защите персональных данных в ИСПДн компании.

Задание 5. Продумайте и составьте правила учета машинных носителей ПДн в организации. Продумайте и составьте правила обеспечения безопасности обработки ПДн сотрудников организации.

Задание 6. Проанализируйте данные нарушения?

a) Сотрудники сидят в интернете на развлекательных сайтах по 4 часа. Играют в игры на работе. Перекладывают свои обязанности на других. Сотрудники копируют конфиденциальные данные компании. Сотрудники одновременно работают на другой работе. Сотрудники работают на конкурента. Сотрудник хочет создать собственную конкурентную компанию. Сотрудники распространяют государственную тайну.

b) Используется потенциальное опасное ПО, содержащее уязвимости, позволяющие скрытую передачу данных, дающие возможность деструктивного влияния на ИТ инфраструктуру компании. Выясняется, что административные пароли передаются по открытым каналам. Сотрудники используют средства удаленного управления. Администраторы сделали бреши в межсетевом периметре компании для удобства. Оставлены закладки в самописном программном обеспечении.

2. Как предотвратить потерю информации?
3. Что следует предпринять для устранения данных нарушений?

Задание 7. Для каждого из этих объектов указать не менее 7 угроз, которые могут быть реализованы по отношению к обрабатываемой в них информации, а также методы борьбы с данными угрозами. Обозначить источник каждой из приведенных угроз.

№	Объект защиты	Наименование угрозы	Источник угрозы	Последствия	Как избежать

1	Банкомат				
2	Рабочее место бухгалтера				
3	Домашний компьютер				
4	Рабочее место в налоговой				
5	Строительная компания				
6	Технологический процесс				

Задание 8. Установка и использование антивирусной программы.

1. Скачать и установить антивирус на свое рабочее место
2. Открыть ранее установленное антивирусное программное обеспечение
3. Проверить ПК на наличие вирусного программного обеспечения
4. Устранить последствия заражения вирусом

Задание 9. Ссылаясь на статьи «Уголовного кодекса Российской Федерации» от 13.06.1996 № 63-ФЗ (ред. от 02.08.2019), какую ответственность несут люди в данных ситуациях.

a) Вы пишите на заказ на программы, которые заражает компьютер и подгружают вредоносные программы. При этом сами данным программным обеспечение не пользуетесь.

b) Системный администратор некоторой известной компании без ведома устанавливал по сети всем программу для удаленного администрирования RAdmin.

c) Вы случайно распространили по сети вирус, который шифрует данные на ПК пользователей

Задание 10. Разработайте план организационных и технических мер по технической защите информации для организации, включающий следующие этапы:

1 Анализ угроз и рисков: Проведите анализ возможных угроз безопасности информации, которым подвергается ваша организация. Определите существующие риски и потенциальные последствия инцидентов.

2 Разработка политики безопасности информации: Сформулируйте политику безопасности информации, которая будет служить основой для разработки всех последующих мер по технической защите. Укажите цели, принципы и правила, которые должны быть соблюдены всеми сотрудниками.

3 Защита сети: Разработайте и меры для защиты сетевой инфраструктуры организации. Включите в план использование брандмауэров, систем обнаружения вторжений (Intrusion Detection System – IDS) и систем предотвращения вторжений (Intrusion Prevention System – IPS).

4 Защита данных: Определите методы шифрования данных, которые будут использоваться для защиты конфиденциальной информации. Разработайте план резервного копирования данных и обеспечения их целостности.

5 Управление учетными записями: Создайте стратегию управления учетными записями, включающую разграничение прав доступа, установку сложных паролей, периодическое обновление паролей и мониторинг активности пользователей.

6 Физическая безопасность: Определите организационные меры для обеспечения физической защиты серверных комнат, центров обработки данных и других важных объектов. Рассмотрите использование систем видеонаблюдения, контроля доступа и ограничения зоны доступа.

7 Обучение персонала: Разработайте программу обучения и осведомленности сотрудников о правилах информационной безопасности.

8 Мониторинг и аудит: Разработайте процедуры для анализа журналов событий и реагирования на инциденты.

Ваша задача состоит в том, чтобы разработать подробный план с описанием каждого этапа и соответствующими мерами по технической защите информации. Обоснуйте выбор конкретных мер и инструментов на основе анализа угроз и рисков, а также целей организации в области безопасности информации.

7.2.4 Примерный перечень вопросов для подготовки к зачету

1. Роль информации в современном мире. Понятие о защищаемой информации.
2. Теория информационной безопасности. Основные направления.
3. Обеспечение ИБ и направления защиты.
4. Требования к системе и политике ИБ.
5. Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.
6. Доктрина информационной безопасности РФ.
7. Защита государственной тайны в РФ.
8. Защита коммерческой тайны в РФ.
9. Защита персональных данных в РФ.
10. Защита служебной и профессиональной тайны в РФ.
11. Процедуры сертификации и аттестации в РФ.
12. Понятие о защищаемой информации. Свойства информации.
13. Угрозы информации. Классификация угроз.
14. Угрозы нарушения конфиденциальности информации. Особенности и примеры реализации угроз.
15. Угрозы нарушения целостности информации. Особенности и примеры реализации угроз.
16. Угроза нарушения доступности информации. Особенности и примеры реализации угрозы.
17. Источники угроз. Классификация источников угроз.
18. Идентификация и аутентификация. Использование парольной защиты. Недостатки парольной защиты.
19. Понятие электронной подписи.
20. Организационные меры обеспечения информационной безопасности. Служба безопасности предприятия.
21. Организация внутри объектового режима предприятия. Организация охраны.
22. Криптографические меры обеспечения информационной безопасности.
Классификация криптографических алгоритмов.
23. Программно-аппаратные защиты информации. Межсетевые экраны, их функции и назначения.
24. Программно-аппаратные защиты информации. Антивирусные средства, их функции и назначения.
25. Особенности защиты беспроводных и мобильных подключений.
26. Симметричное и ассиметричное шифрование.
27. Принципы симметричного шифрования.
28. Односторонние функции и их применение.
29. Простейшие методы ассиметричного шифрования.

30. Метод RSA.
31. Электронная подпись и ее применение.

7.2.5 Примерный перечень вопросов для подготовки к экзамену

Не предусмотрено учебным планом.

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Зачет проводится в ЭИОС по билетам, каждый из которых содержит 20 теоретических тестовых вопросов, 1 стандартное задание, 1 прикладное задание. Каждый правильный ответ на тестовый вопрос оценивается в 0,5 балла, стандартные задания в 5 баллов, прикладное задание оцениваются в 5 баллов.

Максимальное количество набранных баллов на зачете – 20.

1. Оценка «Зачтено» ставится в случае, если студент набрал более 15 баллов.
2. Оценка «Не зачтено» ставится в случае, если студент набрал менее 15 баллов.

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Информационная безопасность в системе национальной безопасности РФ	ПК-5	Устный опрос, тест
2	Персональные данные	ПК-5	Тест, выполнение практических заданий
3	Преступления в сфере компьютерных технологий	ПК-5	Тест, выполнение практических заданий
4	Основные угрозы информационной безопасности	ПК-5	Тест, выполнение практических заданий
5	Защита информации	ПК-5	Выполнение практических заданий, тест
6	Антивирусная защита	ПК-5	Выполнение практических заданий, тест

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестовая часть задания на зачете осуществляется в ЭИОС с помощью компьютерного тестирования. Время тестирования 20 мин. Решение стандартных и прикладного задания прикрепляется обучающимся в ЭИОС. Время выполнения практических заданий – 20 минут. Затем осуществляется проверка теста и практических заданий преподавателем и выставляется предварительная оценка согласно методике выставления оценки при проведении промежуточной аттестации. Окончательная оценка выставляется после устной беседы преподавателя с обучающимся в формате видеоконференции в ЭИОС.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная литература

1. Фомин Д.В. Информационная безопасность : учебно-методическое пособие по дисциплине «Информационная безопасность» для студентов экономических специальностей заочной формы обучения / Фомин Д.В.. — Саратов : Вузовское образование, 2018. — 54 c. — ISBN 978-5-4487-0298-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/77320.html — ЭБС «IPRbooks»

2. Костин В.Н. Методы и средства защиты компьютерной информации: информационная безопасность компьютерных сетей : учебное пособие / Костин В.Н.. — Москва : Издательский Дом МИСиС, 2018. — 31 c. — ISBN 978-5-906953-53-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/98200.html — ЭБС «IPRbooks»

Дополнительная литература

1. Фаронов А.Е. Основы информационной безопасности при работе на компьютере : учебное пособие / Фаронов А.Е.. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 154 c. — ISBN 978-5-4497-2418-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/133957.html — ЭБС «IPRbooks»

2. Мирошников А.И. Основы информационной безопасности и защита информации : учебное пособие / Мирошников А.И., Сысоев А.С.. — Липецк : Липецкий государственный технический университет, ЭБС АСВ, 2022. — 107 c. — ISBN 978-5-00175-160-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/128718.html — ЭБС «IPRbooks»

3. Мартынов А.П. Информационная безопасность и защита информации : учебное пособие / Мартынов А.П., Мартынова И.А., Русаков А.А.. — Москва : Ай Пи Ар Медиа, 2024. — 130 c. — ISBN 978-5-4497-2349-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/134185.html — ЭБС «IPRbooks»

4. Сычев Ю.Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Сычев Ю.Н.. — Саратов : Вузовское образование, 2018. — 195 c. — ISBN 978-5-4487-0128-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/72345.html — ЭБС «IPRbooks»

5. Бахаров, Л. Е. Информационная безопасность и защита информации : сборник тестов / Л. Е. Бахаров. — Москва : Издательский Дом МИСиС, 2015. — 43 c. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/98858.html — ЭБС «IPRbooks»

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

Комплект лицензионного программного обеспечения:

1. Академическая лицензия на использование программного обеспечения Microsoft Office;

Ресурсы информационно-телекоммуникационной сети «Интернет»:

– Министерство экономического развития http://www.economy.gov.ru/minec/main

– Госкомстат России– http://www.gks.ru

– Территориальный орган Федеральной службы государственной статистики по Воронежской области – http://voronezhstat.gks.ru

– Федеральный образовательный портал: Экономика, Социология, Менеджмент – http://ecsocman.ru

– журнал «Эксперт» http://www.expert.ru

Информационно-справочные системы:

– Электронный периодический справочник «Система ГАРАНТ».

– http://window.edu.ru

– https://wiki.cchgeu.ru/

Современные профессиональные базы данных:

– Информационная система «Единое окно доступа к образовательным ресурсам» – http://window.edu.ru

– База данных «Библиотека управления» - Корпоративный менеджмент - https://www.cfin.ru

– База данных Научной электронной библиотеки eLIBRARY.RU - https://elibrary.ru/defaultx.asp

– Единое окно доступа к образовательным ресурсам. Раздел Информатика и информационные технологии http://window.edu.ru/catalog/?p_rubr=2.2.75.6

– Портал об информационной безопасности - bugtraq.ru

– Информационная безопасность: новости, журнал - itsec.ru

– Информационный портал, оперативно и ежедневно рассказывающий о событиях в области защиты информации, интернет права и новых технологиях. securitylab.ru - SecurityLab.ru -

– Искусство управления информационной безопасностью - iso27000.ru

– Документы по информационной безопасности - securitypolicy.ru-SecurityPolicy.ru

– Компания «СёрчИнформ» – ведущий российский разработчик средств информационной безопасности - searchinform.ru

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Лекционная аудитория / виртуальная аудитория, оснащённая мультимедийным демонстрационным оборудованием (проектор, экран, звуковоспроизводящее оборудование), обеспечивающим демонстрацию мультимедиаматериалов и обеспечивающая проведение занятия в ЭИОС.

Аудитория для практических занятий / виртуальная аудитория, оснащённые мультимедийным демонстрационным оборудованием (проектор, экран, звуковоспроизводящее оборудование), обеспечивающим проведение занятия в ЭИОС, демонстрацию мультимедиаматериалов и представляющая возможность синхронного взаимодействия с обучающимися.

Виртуальная аудитория для консультаций в виде комнаты на платформе видеоконференции в ЭИОС, доступ к которой обеспечивается с использованием персональных средств идентификации обучающихся посредством сети Интернет, обеспечивающая возможность демонстрации экрана всех участников, а также организации диалога.

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Информационная безопасность и защита информации» читаются лекции, проводятся практические занятия.

Основой изучения дисциплины являются дистанционные лекции в ЭИОС, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе. Часть лекционного материала предоставляется обучающемуся в виде видеолекции и изучаются самостоятельно. Такой формат позволяет в режиме паузы просмотра изучить более детально схемы и иллюстрации, определения, вызывающие затруднения.

Практические занятия направлены на приобретение практических навыков обеспечения информационной безопасности и защиты информации. Занятия проводятся путем решения конкретных заданий на занятиях, проводимых дистанционно в ЭИОС. Часть практических заданий выполняется обучающимися самостоятельно на основе поясняющих видеоматериалов и прикрепляются в ЭИОС для контроля преподавателем.

Каждая тема курса содержит контрольный тест по теме.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Практическое занятие	Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Решение задач по алгоритму, разбор

	хозяйственных ситуаций.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоению учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, просмотр видеолекций и других обучающих видеоматериалов, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Время на подготовку к экзамену в течении трех дней эффективнее всего использовать для повторения и систематизации материала.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Перечень вносимых изменений	Дата внесения изменений	Подпись заведующего кафедрой, ответственной за реализацию ОПОП