МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Пензенский государственный аграрный университет»

СОГЛАСОВАНО	**УТВЕРЖДАЮ**
Председатель методической комиссии экономического факультета	Декан экономического факультета
И.Е. Шпагина	И.А. Бондин
«20» февраля 2023 г.	«20» февраля 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.25

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки
09.03.03 Прикладная информатика

Направленность (профиль) программы
Прикладная информатика в экономике

Квалификация
«Бакалавр»

Форма обучения – очная

Пенза – 2023

Рабочая программа дисциплины «Информационная безопасность» составлена на основании федерального государственного образовательного стандарта высшего образования - бакалавриат по направлению подготовки 09.03.03 Прикладная информатика, утверждённого приказом Минобрнауки РФ от 19 сентября 2017 года № 922.

Составитель рабочей программы:

канд. экон. наук, доцент	_____	Е.В. Фудина
(уч. степень, ученое звание)	(подпись)	(инициалы, Ф.)

Рецензент:

канд. техн. наук, доцент		В.В. Шумаев
(уч. степень, ученое звание)	(подпись)	(инициалы, Ф.)

Рабочая программа одобрена на заседании кафедры «Финансы и информатизация бизнеса»

«20» февраля 2023 года, протокол № 6

Заведующий кафедрой:

канд. экон. наук, доцент		О.А. Тагирова
(уч. степень, ученое звание)	(подпись)	(инициалы, Ф.)

Рабочая программа одобрена на заседании методической комиссии экономического факультета
«20» февраля 2023 года, протокол № 7

Председатель методической комиссии

экономического факультета		И.Е. Шпагина

РЕЦЕНЗИЯ

на рабочую программу дисциплины *Информационная безопасность*
Направление подготовки 09.03.03 Прикладная информатика
Направленность (профиль) программы Прикладная информатика в экономике
Квалификация (степень) выпускника *бакалавр*
разработанную доцентом кафедры «Финансы и информатизация бизнеса»
Е.В. Фудиной

Структура рабочей программы соответствует нормативным требованиям, разработанным и утвержденным в ФГБОУ ВО Пензенский ГАУ. РП включает в себя: титульный лист, тематику лекций и лабораторных занятий, вопросы для самостоятельного изучения, методические рекомендации студентам по изучению дисциплины, перечень учебно-методических материалов, словарь терминов (глоссарий).

Представленный курс охватывает следующие разделы:

1. Правовые и организационные аспекты защиты информации
2. Угрозы информационной безопасности и методы их реализации
3. Защита от разрушающих программных воздействий

Содержание дисциплины в рабочей программе соответствует Федеральному государственному образовательному стандарту высшего образования по направлению подготовки 09.03.03 Прикладная информатика.

Рабочая программа отражает базовые сведения об информационной безопасности как о научной дисциплине. Позволяет сформировать комплексное представление об основных целях, задачах и методах защиты информации, а также о теоретических основах построения системы защиты информации в информационных системах.

Для осмысления разделов и тем предусмотрено выполнение лабораторных работ, что позволяет не только закрепить теоретические знания, но и обеспечить возможность проведения промежуточного контроля знаний по теоретической и практической части дисциплины.

Преподавателем разработан список рекомендуемой основной и дополнительной литературы, который способствует более глубокому изучению дисциплины.

Содержание программы с дидактической стороны соответствует требованиям научности и доступности (количество часов, выделенных на изучение тем, адаптировано под возможный темп усвоения, связанный с общим уровнем подготовленности студентов данного направления).

В целом, рецензируемая РП, соответствует всем предъявляемым требованиям, изложенным в нормативных документах к рабочей программе дисциплины, утвержденных в ФГБОУ ВО Пензенский ГАУ и может быть рекомендован к использованию в обучающем процессе для студентов направления подготовки 09.03.03 Прикладная информатика в экономике.

Рецензент:
канд. техн. наук, доцент
кафедры «Механизация
технологических процессов в АПК»  В.В. Шумаев

ВЫПИСКА

из протокола № 7 заседания методического комиссии
экономического факультета
от «20» февраля 2023 г.

Присутствовали члены методической комиссии:

Бондин И.А., Лаврина О.В., Позубенкова Э.И., Шпагина И.Е., Бондина Н.Н., Тагирова О.А., Столярова О.А., Захарова Г.К.

Повестка дня:

Вопрос 1 Рассмотрение и утверждение рабочей программы дисциплины «Информационная безопасность» для студентов направления подготовки 09.03.03 Прикладная информатика (профиль) Прикладная информатика в экономике, разработанных доцентом кафедры «Финансы и информатизация бизнеса» Фудиной Е.В.

Слушали: Фудину Е.В., которая представила рабочую программу дисциплины «Информационная безопасность» для студентов направления подготовки 09.03.03 Прикладная информатика (профиль) Прикладная информатика в экономике на рассмотрение методической комиссии и отметила, что данная рабочая программа разработана в соответствии с федеральным государственным образовательным стандартом высшего образования - бакалавриат по направлению подготовки 09.03.03 Прикладная информатика, Минобрнауки РФ от 19 сентября 2017 года № 922, отвечает предъявляемым требованиям, рассмотрена на заседании кафедры «Финансы и информатизация бизнеса» (протокол № 6 от 20 февраля 2023 г.) и может быть использованы в учебном процессе экономического факультета.

Постановили: утвердить рабочую программу дисциплины «Информационная безопасность» для студентов направления подготовки 09.03.03 Прикладная информатика направленность (профиль) Прикладная информатика в экономике.

Председатель методической комиссии

экономического факультета /И.Е. Шпагина/

Лист регистрации изменений и дополнений к рабочей программе дисциплины «Информационная безопасность»

№ п/п	Раздел	Изменения и дополнения	Дата, № протокола, виза зав. кафедрой	Дата, № протокола, виза председателя методической комиссии	С какой даты вводятся
1	10 Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине	Новая редакция таблицы 10.1 «Материально-техническое обеспечение дисциплины»	Протокол № 12 от 30.08.23	Протокол № 9 от 30.08.2023	01.09.2023

Лист регистрации изменений и дополнений к рабочей программе

дисциплины «Информационная безопасность»

№ п/п	Раздел	Изменения и дополнения	Дата, № протокола, виза зав. кафедрой	Дата, № протокола, виза председателя методической комиссии	С какой даты вводятся
1	9 Учебно-методическое и информационное обеспечение дисциплины	Новая редакция таблиц 9.1.1 «Основная литература» и 9.1.2 «Дополнительная литература»	28.08.2024 протокол № 12	28.08.2024 протокол № 8	01.09.2024
2	9 Учебно-методическое и информационное обеспечение дисциплины	Новая редакция таблицы 9.2.3 «Перечень информационных технологий (перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине»			
3	10 Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине	Новая редакция таблицы 10.1 «Материально-техническое обеспечение дисциплины»			

Лист регистрации изменений и дополнений к рабочей программе дисциплины «Информационная безопасность»

№ п/п	Раздел	Изменения и дополнения	Дата, № протокола, виза зав. кафедрой	Дата, № протокола, виза председателя методической комиссии	С какой даты вводятся
1	9 Учебно-методическое и информационное обеспечение дисциплины	Новая редакция таблиц 9.1.1 «Основная литература» и 9.1.2 «Дополнительная литература»	23.06.2025 протокол № 11	29.08.2025 протокол № 6	01.09.2025
2	9 Учебно-методическое и информационное обеспечение дисциплины	Новая редакция таблицы 9.2.1 «Перечень информационных технологий (перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине»			
3	10 Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине	Новая редакция таблицы 10.1 «Материально-техническое обеспечение дисциплины»			

1 Цель и задачи дисциплины

Целью дисциплины «Информационная безопасность» является формирование у студентов устойчивых навыков работы в сложной сетевой информационной среде современной организации, получение сведений о современном состоянии проблем обеспечения информационной безопасности компьютерных систем.

Задачи дисциплины: изучение основных теоретических принципов информационной безопасности; ознакомление с существующими технологиями защиты информации в областях операционных систем, баз данных и компьютерных сетей; изучение основ сетевых технологий и формирование навыков работы в среде сетевых информационных систем; освоение средств защиты информации и приобретение навыков их применения; получение навыков эксплуатации систем с позиций информационной безопасности; изучение основ правового регулирования отношений в информационной сфере.

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

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

ОПК-4: Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью.

Индикаторы и дескрипторы части соответствующей компетенции, формируемой в процессе изучения дисциплины «Информационная безопасность», оцениваются при помощи контрольных мероприятий, приведенных в таблице 2.1.

Таблица 2.1 – Планируемые результаты обучения по дисциплине «Информационная безопасность», индикаторы достижения компетенций ОПК-3, ОПК-4, перечень контрольных мероприятий

№ пп	Код индикатора достижения компетенции	Наименование индикатора достижения компетенции	Код планируемого результата обучения	Планируемые результаты обучения	Наименование контрольных мероприятий *
1	ИД-2$_{ОПК-3}$	Решает стандартные задачи профессиональной деятельности с соблюдением требований информационной безопасности	З1 (ИД-2$_{ОПК-3}$)	Знать: способы решения стандартных задач для обеспечения информационной безопасности	Собеседование, индивидуальная (контрольная) работа, экзамен
			У1 (ИД-2 $_{ОПК-3}$)	Уметь: формировать массив необходимой информации для оценки и интерпретации информации, в том числе с позиции обеспечения информационной безопасности организаций	
			В1 (ИД-2 $_{ОПК-3}$)	Владеть: навыками решения профессиональных задач с позиции защиты информации от несанкционированного доступа	
2	ИД-1$_{ОПК-4}$	Участвует в разработке стандартов, норм и правил на различных стадиях проектирования и поддержки жизненного цикла информационной системы	З1 (ИД-1$_{ОПК-4}$)	Знать: стандарты, нормы и правила на различных этапах проектирования жизненного цикла в контексте защиты информационной системы	Собеседование, индивидуальная (контрольная) работа, экзамен
			У1 (ИД-1 $_{ОПК-4}$)	Уметь: выбирать инструментальные средства при проектировании жизненного цикла информационной системы в контексте реализации политики информационной безопасности	
			В1 (ИД-1 $_{ОПК-4}$)	Владеть: навыками разработки стандартов, норм и правил на различных стадиях проектирования жизненного цикла информационной системы и экономико-правового обеспечения информационной безопасности	

* Оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине, в т.ч. в форме заданий тестового типа, представлены в Приложении.

Задания тестового типа могут быть использованы при проведении диагностических процедур, в т.ч. диагностической работы, в рамках НОКО.

3 Место учебной дисциплины в структуре программы бакалавриата

Дисциплина «Информационная безопасность» включена в Блок Б1 «Дисциплины (модули)», обязательная часть (Б1.О.25).

Для изучения дисциплины необходимы компетенции, сформированные при изучении дисциплин «Информационные системы и технологии», «Право».

Освоение дисциплины «Информационная безопасность» является необходимой основой для последующего изучения дисциплин «Проектирование информационных систем», «Проектный практикум в ИТ-сфере».

4 Структура дисциплины

Общая трудоёмкость дисциплины «Информационная безопасность» составляет 5 зачётных единицы, 180 ч.

Таблица 4.1 – Распределение общей трудоемкости дисциплины «Информационная безопасность организации» по формам и видам учебной работы

№ п/п	Форма и вид учебной работы	Условное обозначение по учебному плану	Трудоёмкость, ч/з.е.
			очная форма обучения
			3 семестр
1	Контактная работа – всего	Контакт часы	89,95/2,5
1.1	Лекции	Лек	32/0,89
1.2	Семинары и практические занятия	Пр	
1.3	Лабораторные работы	Лаб	54/1,50
1.4	Текущие консультации, руководство и консультации курсовых работ (курсовых проектов)	КТ	1,6/0,04
1.5	Сдача зачета (зачёта с оценкой), защита курсовой работы (курсового проекта)	КЗ	
1.7	Предэкзаменационные консультации по дисциплине	КПЭ	2/0,06
1.8	Сдача экзамена	КЭ	0,35/0,01
2	Общий объем самостоятельной работы		90,05/2,5
2.1	Самостоятельная работа	СР	56,4/1,57
2.2	Контроль (самостоятельная подготовка к сдаче экзамена)	Контроль	33,65/0,93
	Всего	По плану	180/5

Форма промежуточной аттестации –экзамен, 6 семестр.

5 Содержание дисциплины

Таблица 5.1 – Наименование разделов дисциплины «Информационная безопасность» и их содержание

№ раздела	Наименование раздела дисциплины	Содержание раздела	Код планируемого результата обучения
1	Правовые и организационные аспекты защиты информации	Программа информационной безопасности России и пути ее реализации. Обзор состояния систем защиты информации в России и в ведущих зарубежных странах. Роль и место системы обеспечения информационной безопасности в системе национальной безопасности РФ. Современное состояние правового регулирования в информационной сфере. Правовое обеспечение информационной безопасности. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Компьютерные преступления. Организационное обеспечение информационной безопасности	З1 (ИД-2$_{ОПК-3}$) У1 (ИД-2 $_{ОПК-3}$) В1 (ИД-2 $_{ОПК-3}$)
2	Угрозы информационной безопасности и методы их реализации	Понятие угрозы. Анализ угроз безопасности информации. Причины, виды, каналы утечки и искажения информации. Основные методы реализации угроз информационной безопасности: методы нарушения секретности, целостности и доступности информации. Информационная безопасность в условиях функционирования в России глобальных сетей. Основные технологии построения защищенных экономических информационных систем (ЭИС). Защита информации от несанкционированного доступа. Компьютерные средства	З1 (ИД-2$_{ОПК-3}$) У1 (ИД-2 $_{ОПК-3}$) В1 (ИД-2 $_{ОПК-3}$)

		реализации защиты в информационных системах	
3	Защита от разрушающих программных воздействий	Политика безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных систем. Использование защищенных компьютерных систем. Стандарты по оценке защищенных систем. Понятие разрушающего программного воздействия Методы перехвата и навязывания информации. Общие подходы к построению парольных систем. Выбор паролей. Хранение паролей. Передача пароля по сети. Особенности криптографического и стеганографического преобразования информации. Типы алгоритмов шифрования. Примеры криптографических алгоритмов. Особенности применения криптографических методов. Особенности реализации систем с симметричными и несимметричными ключами. Электронная подпись. Виды уязвимости и атак на ОС. Классификация угроз безопасности операционной системы. Способы противодействия несанкционированному сетевому и межсетевому доступу. Противодействие несанкционированному межсетевому доступу. Защита информации для электронной коммерции в Интернет.	З1 (ИД-1$_{ОПК-4}$) У1 (ИД-1 $_{ОПК-4}$) В1 (ИД-1 $_{ОПК-4}$)

Таблица 5.2.1 − Наименование тем лекций и их объём в часах с указанием рассматриваемых вопросов (очная форма обучения)

№ п/п	№ раздела дисциплины	Тема лекции	Рассматриваемые вопросы	Время, час.
1	2	3	4	5
1	1	Информационная безопасность организации: основные понятия и терминология	1. Роль и место системы обеспечения информационной безопасности в системе национальной безопасности РФ. 2. Концепция информационной безопасности. 3. Основные понятия и определения защиты информации	2
2	1	Правовые и организационные аспекты защиты информации	1. Современное состояние правового регулирования в информационной сфере. 2. Правовое обеспечение информационной безопасности 3. Организационное обеспечение информационной безопасности.	4
3	1	Угрозы информационной безопасности и методы их реализации	1. Понятие угрозы. Анализ угроз безопасности информации 2. Основные методы реализации угроз информационной безопасности 3. Информационная безопасность в условиях функционирования в России глобальных сетей	2
4	2	Методы и средства обеспечения информационной безопасности информационных систем	1. Защита информации при реализации информационных процессов 2. Защита информации от несанкционированного доступа 3. Компьютерные средства реализации защиты в информационных системах	4
5	2	Использование защищенных компьютерных систем	1. Политика безопасности 2. Критерии и классы защищенности средств вычислительной техники и автоматизированных систем 3. Стандарты по оценке защищенных систем	4

6	2	Защита от разрушающих программных воздействий	1. Понятие разрушающего программного воздействия 2. Методы перехвата и навязывания информации 3. Компьютерные вирусы	4
7	3	Парольные системы	1. Общие подходы к построению парольных систем 2. Выбор паролей 3. Хранение паролей 4. Передача пароля по сети	4
8	3	Шифрование данных	1. Особенности криптографического и стеганографического преобразования информации 2. Типы алгоритмов шифрования 3. Особенности реализации систем с симметричными и несимметричными ключами. Электронная подпись	4
9	3	Особенности защиты в операционных системах и сетях	1. Подходы к построению защищенной операционной системы 2. Классификация угроз безопасности операционной системы 3. Классификация способов несанкционированного доступа и жизненный цикл атак 4. Аутентификация пользователя локальной сети 5. Разграничение доступа к локальной сети 6. Противодействие несанкционированному межсетевому доступу	4
Всего				32

5.3.1 Наименование тем практических и семинарских занятий, их объем в часах и содержание (очная форма обучения)

№ п/п	№ раздела дисциплины	Тема работы	Время, ч.
1	2	3	4
1.	1	Информационная безопасность организации**:** основные понятия и терминология	4
2.	1	Правовые и организационные аспекты защиты информации	6
3.	2	Угрозы информационной безопасности и методы их реализации	6
4.	2	Методы и средства обеспечения информационной безопасности информационных систем	6
5.	3	Защита от разрушающих программных воздействий	6
6.	3	Парольные системы	4
7.	3	Шифрование данных	4
8.	3	Защита программ и данных	4
9.	3	Особенности защиты в операционных системах	6
10.	3	Особенности защиты информации в компьютерных сетях	6
Итого			54

Таблица 5.4.1 − Распределение трудоёмкости самостоятельной работы (СР) по видам работ (очная форма обучения)*

№п/п	Вид работы	Время, ч
1	Подготовка к практическим и семинарским занятиям	20
1.1	Информационная безопасность организации**:** основные понятия и терминология	2
1.2	Правовые и организационные аспекты защиты информации	2
1.3	Угрозы информационной безопасности и методы их реализации	2
1.4	Методы и средства обеспечения информационной безопасности информационных систем	2
1.5	Защита от разрушающих программных воздействий	2
1.6	Парольные системы	2
1.7	Шифрование данных	2
1.8	Защита программ и данных	2
1.9	Особенности защиты в операционных системах	2
1.10	Особенности защиты информации в компьютерных сетях	2
2	Изучение вопросов не рассматриваемых в лекционном курсе	16,4
3	Выполнение индивидуальной (контрольной) работы №1 и №2	20
Итого:		56,4

**35,25 = 36 ч – 0,5 ч консультации – 0,25 ч защита*

6 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине «Информационная безопасность»

Таблица 6.1 − Тема, задания и вопросы для самостоятельного изучения (очная форма обучения)

№ п/п	№ раздела дисциплины	Тема, вопросы, задание	Время, час.	Рекомендуемая литература
1	1	Программа информационной безопасности России и пути ее реализации Роль и место системы обеспечения информационной безопасности в системе национальной безопасности РФ Обзор состояния систем защиты информации в России и в ведущих зарубежных странах Международные стандарты информационного обмена Основные принципы защиты информации в компьютерных системах Основные понятия и определения защиты информации З1 (ИД-2$_{ОПК-3}$)	4	1, с.43-55, с.94-99
2	1	Современное состояние правового регулирования в информационной сфере Правовое обеспечение информационной безопасности Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства Компьютерные преступления Организационное обеспечение информационной безопасности З1 (ИД-2$_{ОПК-3}$)	4	1, с.23-31, с.99-101
3	2	Понятие угрозы Анализ угроз безопасности информации Причины, виды, каналы утечки и искажения информации Основные методы реализации угроз информационной безопасности: методы нарушения секретности, целостности и	4	1, с. 124-270

		доступности информации У1 (ИД-2 $_{ОПК-3}$)		
4	2	Общая проблема информационной безопасности информационных систем Основные технологии построения защищенных экономических информационных систем (ЭИС) Защита информации от несанкционированного доступа Математические и методические средства защиты У1 (ИД-2 $_{ОПК-3}$)	4	1, с.283-320
5	3	Политика безопасности Критерии и классы защищенности средств вычислительной техники и автоматизированных систем Использование защищенных компьютерных систем. Стандарты по оценке защищенных систем Понятие разрушающего программного воздействия Методы перехвата и навязывания информации Общие подходы к построению парольных систем. Выбор паролей. Хранение паролей. Передача пароля по сети Особенности криптографического и стеганографического преобразования информации Типы алгоритмов шифрования. Примеры криптографических алгоритмов Особенности применения криптографических методов. Особенности реализации систем с симметричными и несимметричными ключами Электронная подпись З1 (ИД-1$_{ОПК-4}$)	4	1, с.34-56
6	3	Подходы к построению защищенной операционной системы. Административные меры защиты. Стандарты защищенности операционных систем. Виды уязвимости и атак на ОС. Классификация угроз безопасности операционной системы	4	1, с.324-350

		Классификация способов несанкционированного доступа и жизненный цикл атак. Нападения на политику безопасности и процедуры административного управления. Нападения на постоянные и сменные компоненты системы защиты. Нападения на протоколы информационного взаимодействия. Нападения на функциональные элементы компьютерных сетей. Способы противодействия несанкционированному сетевому и межсетевому доступу. Противодействие несанкционированному межсетевому доступу. Использование межсетевых экранов (Firewall). Критерии их оценки. Защита виртуальных потоков на различных сетевых уровнях. Защита удаленного доступа к локальной сети. Безопасная доставка E-mail сообщений. Использование ключей и цифровых подписей. Безопасность работы в Интернет с использованием браузера. Защита информации для электронной коммерции в Интернет. З1 (ИД-1$_{ОПК-4}$), У1 (ИД-1 $_{ОПК-4}$), В1 (ИД-1 $_{ОПК-4}$)		
7	1-3	Подготовка к практическим и семинарским занятиям З1 (ИД-2$_{ОПК-3}$), У1 (ИД-2 $_{ОПК-3}$), В1 (ИД-2 $_{ОПК-3}$) З1 (ИД-1$_{ОПК-4}$), У1 (ИД-1 $_{ОПК-4}$), В1 (ИД-1 $_{ОПК-4}$)	12,4	
8	1-3	Выполнение индивидуальной работы З1 (ИД-2$_{ОПК-3}$), У1 (ИД-2 $_{ОПК-3}$), В1 (ИД-2 $_{ОПК-3}$) З1 (ИД-1$_{ОПК-4}$), У1 (ИД-1 $_{ОПК-4}$), В1 (ИД-1 $_{ОПК-4}$)	20	
Итого			56,4	

7 Образовательные технологии

Таблица 7.1.1 – Образовательные технологии, обеспечивающие развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (очная форма обучения)

№раздела	Вид занятия (Л, ПЗ, ЛР)	Используемые технологии и рассматриваемые вопросы	Время, ч
1	*Лек*	Информационная безопасность организации: основные понятия и терминология (лекция-диалог) В1 (ИД-2 $_{ОПК-3}$), У1 (ИД-2 $_{ОПК-3}$), З1 (ИД-2$_{ОПК-3}$)	2
1	*Лек*	Правовые и организационные аспекты защиты информации (лекция-диалог) З1 (ИД-1$_{ОПК-4}$), У1 (ИД-1 $_{ОПК-4}$), В1 (ИД-1 $_{ОПК-4}$)	4
Всего часов по лекциям			6
1	*Лаб*	*Угрозы информационной безопасности и методы их реализации* Занятие проводится в виде лабораторной работы с обсуждением и анализом полученных результатов в малых группах.	6
2	*Лаб*	*Методы и средства обеспечения информационной безопасности информационных систем* Занятие проводится в виде лабораторной работы с обсуждением и анализом полученных результатов в малых группах.	6
3	*Лаб*	*Защита от разрушающих программных воздействий* Занятие проводится в виде лабораторной работы с обсуждением и анализом полученных результатов в малых группах.	6
4	*Лаб*	*Защита программ и данных* Занятие проводится в виде лабораторной работы с обсуждением и анализом полученных результатов в малых группах.	4
5	*Лаб*	*Особенности защиты в операционных системах* Занятие проводится в виде лабораторной работы с обсуждением и анализом полученных результатов в малых группах.	6
6	*Лаб*	*Особенности защиты информации в компьютерных сетях* Занятие проводится в виде лабораторной работы с обсуждением и анализом полученных результатов в малых группах.	6
Всего часов по лабораторным занятиям			34
Итого			40

8 Оценочные материалы по дисциплине «Информационная безопасность»

Оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине, в т.ч. в форме заданий тестового типа, представлены в Приложении.

Задания тестового типа могут быть использованы при проведении диагностических процедур, в т.ч. диагностической работы, в рамках НОКО.

9 Учебно-методическое и информационное обеспечение дисциплины

9.1 Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» необходимых для освоения дисциплины

Таблица 9.1 – Основная литература по дисциплине «Информационная безопасность»

№ п/п	Наименование	Количество, экз.	
		всего	в расчете на 100 обучающихся
1	*Суворова, Г. М.* Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2022. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496741	–	–

Таблица 9.2 – Дополнительная литература по дисциплине «Информационная безопасность»

№ п/п	Наименование	Количество, экз.	
		всего	в расчете на 100 обучающихся
1	*Зенков, А. В.* Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497002	–	–

Таблица 9.1.1 – Основная литература по дисциплине «Информационная безопасность» (*редакция от 01.09.2024 г.*)

№ п/п	Наименование	Количество, экз.	
		всего	в расчете на 100 обучающихся
1	Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544029	–	–

Таблица 9.1.2 – Дополнительная литература по дисциплине «Информационная безопасность» (*редакция от 01.09.2024 г.*)

№ п/п	Наименование	Количество, экз.	
		всего	в расчете на 100 обучающихся
1	Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544290	–	–

Таблица 9.1.1 – Основная литература по дисциплине «Информационная безопасность» (*редакция от 01.09.2025 г.*)

№ п/п	Наименование	Количество, экз.	
		всего	в расчете на 100 обучающихся
1	Зенков, А. В. Информационная безопасность и защита информации : учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/	–	–

Таблица 9.1.2 – Дополнительная литература по дисциплине «Информационная безопасность» (*редакция от 01.09.2025 г.*)

№ п/п	Наименование	Количество, экз.	
		всего	в расчете на 100 обучающихся
1	Суворова, Г. М. Информационная безопасность : учебник для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567672	–	–

Таблица 9.3 –Собственные методические издания кафедры по дисциплине

№ п/п	Наименование	Количество, экз.	
		всего	в расчете на 100 обучающихся

Таблица 9.1.4 – Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

№ п/п	Наименование	Условия доступа
1	Информационно-коммуникационные технологии в образовании // Электронный ресурс	Свободный http://ict.edu.ru/
2	ФГУ ГНИИ ИТТ «Информика» // Электронный ресурс	Свободный http://www.informika.ru/
3	Электронно-библиотечная система «Znanium.com» // Электронный ресурс	С любого компьютера локальной сети университета по IP-адресам; с личных ПК, мобильных устройств по индивидуальному аутентификатору (логин/пароль) Номер Абонента 25751
4	Библиотека «Книгосайт» // Электронный ресурс	[Режим доступа: свободный] http://knigosite.ru/
5	Единое окно информационных ресурсов window.edu.ru	Свободный http://window.edu.ru/

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

Таблица 9.2.1 – Перечень информационных технологий (перечень современных профессиональных баз данных и информационных справочных систем), используемых при осуществлении образовательного процесса по дисциплине

№ п/п	Наименование	Условия доступа
1	*Образовательная платформа «Юрайт» Электронно-библиотечная система «ЮРАЙТ»*	***https://urait.ru/*** *(доступ с любого компьютера локальной сети университета по IP-адресам; с личных ПК, мобильных устройств по индивидуальному аутентификатору (логин/пароль), через личный кабинет)* помещения для самостоятельной работы: аудитория № 5202 *Читальный зал гуманитарных наук, электронный читальный зал* аудитория № 1237 *Читальный зал сельскохозяйственной, естественнонаучной литературы и периодики, электронный читальный зал научных работников; специальная библиотека*
2	*Электронно-библиотечная система «Национальный цифровой ресурс «Руконт»*	***https://lib.rucont.ru/search*** *(доступ с любого компьютера локальной сети университета по IP-адресам; с личных ПК, мобильных устройств по коллективному или индивидуальному аутентификатору (логин/пароль); возможность регистрации для удаленной работы по IP)* помещения для самостоятельной работы: аудитория № 5202 *Читальный зал гуманитарных наук, электронный читальный зал* аудитория № 1237 *Читальный зал сельскохозяйственной, естественнонаучной литературы и периодики, электронный читальный зал научных работников; специальная библиотека*
3	Научная электронная библиотека eLIBRARY.RU	**http://elibrary.ru** *(доступны поиск, просмотр и загрузка полнотекстовых лицензионных материалов через Интернет (в том числе по электронной почте) по IP адресам университета без ограничения количества пользователей; неограниченный доступ с личных компьютеров для библиографического поиска, просмотра оглавления журналов)* помещения для самостоятельной работы: аудитория № 5202 *Читальный зал гуманитарных наук, электронный читальный зал* аудитория № 1237 *Читальный зал сельскохозяй-*

		ственной, естественнонаучной литературы и периодики, электронный читальный зал научных работников; специальная библиотека
4	*Научная электронная библиотека «КИБЕРЛЕНИНКА»*	***https://cyberleninka.ru/*** *(доступ свободный)* помещения для самостоятельной работы: аудитория № 5202 *Читальный зал гуманитарных наук, электронный читальный зал* аудитория № 1237 *Читальный зал сельскохозяйственной, естественнонаучной литературы и периодики, электронный читальный зал научных работников; специальная библиотека*
5	*Федеральный образовательный портал «Экономика. Социология. Менеджмент» (НИУ «Высшая школа экономики»)*	***http://ecsocman.hse.ru/*** *(доступ свободный)* помещения для самостоятельной работы: аудитория № 5202 *Читальный зал гуманитарных наук, электронный читальный зал* аудитория № 1237 *Читальный зал сельскохозяйственной, естественнонаучной литературы и периодики, электронный читальный зал научных работников; специальная библиотека*
6	*Национальная платформа «Открытое образование»*	***https://openedu.ru/*** *(доступ свободный)* помещения для самостоятельной работы: аудитория № 5202 *Читальный зал гуманитарных наук, электронный читальный зал* аудитория № 1237 *Читальный зал сельскохозяйственной, естественнонаучной литературы и периодики, электронный читальный зал научных работников; специальная библиотека*
7	*Открытый образовательный видеопортал Univertv.ru*	***http://univertv.ru/*** *(доступ свободный)* помещения для самостоятельной работы: аудитория № 5202 *Читальный зал гуманитарных наук, электронный читальный зал* аудитория № 1237 *Читальный зал сельскохозяйственной, естественнонаучной литературы и периодики, электронный читальный зал научных работников; специальная библиотека*

Таблица 9.2.1 – Перечень информационных технологий (перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине «Информационная безопасность» (редакция от 01.09.2024)

№ п/п	Наименование	Условия доступа
1	Справочно-правовая система «КОНСУЛЬТАНТ+»	(https://www.consultant.ru/) – сторонняя *без пароля* помещения для самостоятельной работы: аудитория № 5202 *Зал обеспечения цифровыми ресурсами и сервисами, коворкинга* *Помещение для научно-исследовательской работы* аудитория № 1237 *Зал обслуживания научными ресурсами, автоматизации RFID-технологий, коворкинга* *Отдел учета и хранения фондов*
2	Образовательная платформа Юрайт. Для вузов и ссузов.	(https://urait.ru/) – сторонняя *(Доступ с любого компьютера локальной сети университета по IP-адресам; с личных ПК, мобильных устройств по индивидуальному аутентификатору (логин/пароль), через Личный кабинет)* помещения для самостоятельной работы: аудитория № 5202 *Зал обеспечения цифровыми ресурсами и сервисами, коворкинга* *Помещение для научно-исследовательской работы* аудитория № 1237 *Зал обслуживания научными ресурсами, автоматизации RFID-технологий, коворкинга* *Отдел учета и хранения фондов*
3	Электронно-библиотечная система «Национальный цифровой ресурс «Руконт»	(https://lib.rucont.ru/search) – сторонняя *(Доступ с любого компьютера локальной сети университета по IP-адресам; с личных ПК, мобильных устройств по индивидуальному аутентификатору (логин/пароль), через Личный кабинет)* помещения для самостоятельной работы: аудитория № 5202 *Зал обеспечения цифровыми ресурсами и сервисами, коворкинга* *Помещение для научно-исследовательской работы* аудитория № 1237 *Зал обслуживания научными ресурсами, автоматизации RFID-технологий, коворкинга* *Отдел учета и хранения фондов*
4	Электронная библиотека полнотекстовых документов Пензенского ГАУ	(https://pgau.ru/strukturnye-podrazdeleniya/nauchnaya-biblioteka/elektronnaya-biblioteka-pgau.html) - собственная генерация *(Доступ с любого компьютера локальной сети университета по IP-адресам; с личных ПК, мобильных устройств по коллективному или индивидуальному аутентификатору (логин/пароль), через Личный кабинет; возможность регистрации для удаленной работы по IP.)* помещения для самостоятельной работы: аудитория № 5202 *Зал обеспечения цифровыми ресурсами и сервисами, коворкинга* *Помещение для научно-исследовательской работы* аудитория № 1237 *Зал обслуживания научными ресурсами, автоматизации RFID-технологий, коворкинга* *Отдел учета и хранения фондов*
5	Федеральная служба государственной статистики	(https://rosstat.gov.ru/) – сторонняя *(доступ свободный)* помещения для самостоятельной работы: аудитория № 5202 *Зал обеспечения цифровыми ресурсами и сервисами, коворкинга*

		Помещение для научно-исследовательской работы аудитория № 1237 *Зал обслуживания научными ресурсами, автоматизации RFID-технологий, коворкинга* *Отдел учета и хранения фондов*
6	Территориальный орган Федеральной службы государственной статистики по Пензенской области	(https://58.rosstat.gov.ru/) – сторонняя *(доступ свободный)* помещения для самостоятельной работы: аудитория № 5202 *Зал обеспечения цифровыми ресурсами и сервисами, коворкинга* *Помещение для научно-исследовательской работы* аудитория № 1237 *Зал обслуживания научными ресурсами, автоматизации RFID-технологий, коворкинга* *Отдел учета и хранения фондов*
7	Национальная платформа открытого образования	(https://npoed.ru/)- сторонняя *(доступ свободный)* помещения для самостоятельной работы: аудитория № 5202 *Зал обеспечения цифровыми ресурсами и сервисами, коворкинга* *Помещение для научно-исследовательской работы* аудитория № 1237 *Зал обслуживания научными ресурсами, автоматизации RFID-технологий, коворкинга* *Отдел учета и хранения фондов*

Таблица 9.2.1 – Перечень информационных технологий (перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (редакция от 01.09.2025)

№ п/п	Наименование	Условия доступа
1	Справочно-правовая система «КОНСУЛЬТАНТ+»	(https://www.consultant.ru/) – сторонняя *без пароля* помещения для самостоятельной работы: аудитория № 5202 *Зал обеспечения цифровыми ресурсами и сервисами, коворкинга* *Помещение для научно-исследовательской работы* аудитория № 1237 *Зал обслуживания научными ресурсами, автоматизации RFID-технологий, коворкинга* *Отдел учета и хранения фондов*
2	Образовательная платформа Юрайт. Для вузов и ссузов.	(https://urait.ru/) – сторонняя *(Доступ с любого компьютера локальной сети университета по IP-адресам; с личных ПК, мобильных устройств по индивидуальному аутентификатору (логин/пароль), через Личный кабинет)* помещения для самостоятельной работы: аудитория № 5202 *Зал обеспечения цифровыми ресурсами и сервисами, коворкинга* *Помещение для научно-исследовательской работы* аудитория № 1237 *Зал обслуживания научными ресурсами, автоматизации RFID-технологий, коворкинга* *Отдел учета и хранения фондов*
3	Электронно-библиотечная система «Национальный цифровой ресурс «Руконт»	(https://lib.rucont.ru/search) – сторонняя *(Доступ с любого компьютера локальной сети университета по IP-адресам; с личных ПК, мобильных устройств по индивидуальному аутентификатору (логин/пароль), через Личный кабинет)* помещения для самостоятельной работы: аудитория № 5202 *Зал обеспечения цифровыми ресурсами и сервисами, коворкинга* *Помещение для научно-исследовательской работы* аудитория № 1237 *Зал обслуживания научными ресурсами, автоматизации RFID-технологий, коворкинга* *Отдел учета и хранения фондов*
4	Электронная библиотека полнотекстовых документов Пензенского ГАУ	(https://pgau.ru/strukturnye-podrazdeleniya/nauchnaya-biblioteka/elektronnaya-biblioteka-pgau.html) - собственная генерация *(Доступ с любого компьютера локальной сети университета по IP-адресам; с личных ПК, мобильных устройств по коллективному или индивидуальному аутентификатору (логин/пароль), через Личный кабинет; возможность регистрации для удаленной работы по IP.)* помещения для самостоятельной работы: аудитория № 5202 *Зал обеспечения цифровыми ресурсами и сервисами, коворкинга* *Помещение для научно-исследовательской работы*

		аудитория № 1237 *Зал обслуживания научными ресурсами, автоматизации RFID-технологий, коворкинга* *Отдел учета и хранения фондов*
5	Федеральная служба государственной статистики	(https://rosstat.gov.ru/) – сторонняя *(доступ свободный)* помещения для самостоятельной работы: аудитория № 5202 *Зал обеспечения цифровыми ресурсами и сервисами, коворкинга* *Помещение для научно-исследовательской работы* аудитория № 1237 *Зал обслуживания научными ресурсами, автоматизации RFID-технологий, коворкинга* *Отдел учета и хранения фондов*
6	Территориальный орган Федеральной службы государственной статистики по Пензенской области	(https://58.rosstat.gov.ru/) – сторонняя *(доступ свободный)* помещения для самостоятельной работы: аудитория № 5202 *Зал обеспечения цифровыми ресурсами и сервисами, коворкинга* *Помещение для научно-исследовательской работы* аудитория № 1237 *Зал обслуживания научными ресурсами, автоматизации RFID-технологий, коворкинга* *Отдел учета и хранения фондов*
7	Национальная платформа открытого образования	(https://npoed.ru/)- сторонняя *(доступ свободный)* помещения для самостоятельной работы: аудитория № 5202 *Зал обеспечения цифровыми ресурсами и сервисами, коворкинга* *Помещение для научно-исследовательской работы* аудитория № 1237 *Зал обслуживания научными ресурсами, автоматизации RFID-технологий, коворкинга* *Отдел учета и хранения фондов*
8	Электронно-библиотечная система Znanium	(https://znanium.ru/) – сторонняя С любого компьютера локальной сети университета по IP-адресам; с личных ПК, мобильных устройств по индивидуальным ключам доступа

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

Таблица 10.1 – Материально-техническое обеспечение дисциплины «Информационная безопасность»

№ п/п	Наименование дисциплины в соответствии с учебным планом	Наименование учебных аудиторий и помещений для самостоятельной работы	Перечень оборудования и технических средств обучения, наличие возможности подключения к сети «Интернет»	Перечень лицензионного и свободно распространяемого программного обеспечения, в т.ч. отечественного производства. Реквизиты подтверждающего документа
1	Информационная безопасность	**Учебная аудитория для проведения учебных занятий** 440014, Пензенская область, г. Пенза, ул. Ботаническая, д. 30; аудитория 1121	**Специализированная мебель:** столы аудиторные 4-х местные со скамьей, скамьи аудиторные 4-х местные, скамьи 2-х местные, столы аудиторные 4-х местные, стол преподавательский (3 части), трибуны напольные, доска аудиторная. **Оборудование и технические средства обучения, наборы демонстрационного оборудования и учебно-наглядных пособий:** плакаты. **Набор демонстрационного оборудования (стационарный):** персональный компьютер, проектор, колонки звуковые, микрофон, экран.	**Комплект лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:** • MS Windows 10 (9879093834, 2020); • MS Office 2019 (9879093834, 2020).
2	Информационная безопасность	**Учебная аудитория для проведения учебных занятий** 440014, Пензенская область, г. Пенза, ул. Ботаническая, д. 30; аудитория 5101	**Специализированная мебель:** парты, стол аудиторный, стул, трибуна, шкаф, доски. **Оборудование и технические средства обучения, наборы демонстрационного оборудования и учебно-наглядных пособий:** плакаты. **Набор демонстрационного оборудования (стационарный):** проектор, персональный компьютер, колонки, экран.	**Комплект лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:** • MS Windows 10 (9879093834, 2020); • MS Office 2019 (9879093834, 2020); • СПС «КонсультантПлюс»* («Договор об информационной поддержке» от 03 мая 2018 года (бессрочный)).
3	Информационная безопасность	**Учебная аудитория для проведения учебных занятий Помещение для самостоятельной работы** 440014, Пензенская область, г. Пенза,	**Специализированная мебель:** столы аудиторные 2-х местные, скамьи аудиторные 2-х местные, компьютерные столы, стол компьютерный двух тумбовый, стулья жесткие, стул мягкий, кресло офисное, шкаф угловой, доска маркерная, стол СИ-1 (стол рабочий для инвалидов колясочников детей и взрослых), парта для слабовидящих.	**Комплект лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:** • MS Windows 10 (V9414975, 2021); • MS Office 2019

		ул. Ботаническая, д. 30; аудитория 1102 *Кабинет информатики (компьютерный класс)*	**Оборудование и технические средства обучения, набор учебно-наглядных пособий:** персональные компьютеры; видеоувеличитель портативный HV-MVC; ресивер для беспроводной связи; клавиатура адаптированная с крупными кнопками + пластиковая накладка, разделяющая клавиши, беспроводная; джойстик компьютерный адаптированный беспроводной; выносные компьютерные кнопки: большая беспроводная, малая беспроводная; компьютерный комплекс для слабовидящего, включающий в себя программу экранного доступа, ноутбук с наклейками на клавиатуру шрифтом Брайля; радиокласс (радиомикрофон) «Сонет-РСМ» РМ-1-1 (заушный индуктор и индукционная петля); плакаты «Компьютер и безопасность»; плакаты. Доступ в электронную информационно-образовательную среду университета; Выход в Интернет.	(V9414975, 2021); • CorelDRAW Graphics Suite 2021 Education License (Windows) (single User) Лицензия № 731078 (бессрочная) от 03 февраля 2022 года; • Yandex Browser **(GNU Lesser General Public License) • Oracle VM + образ (Windows Server 2008 R, Linux) (Freeware) • MS SQL SERVER Express(Freeware) • 1С: Предприятие (Договор поставки № 3 от 03.12.2021). • СПС Консультант +*(«Договор об информационной поддержке» от 03 мая 2018 года (бессрочный)). • SciLAB (Freeware) • MS Visual Studio 2020 Community (Freeware) • BPMN.Studio (Freeware) • Project Expert (договор № 0003/1КУ-01 от 15.03.2023)
4	Информационная безопасность	**Учебная аудитория для проведения учебных занятий** **Помещение для самостоятельной работы** 440014, Пензенская область, г. Пенза, ул. Ботаническая, д. 30; аудитория 1114	**Специализированная мебель:** столы аудиторные 2-х местные, стулья офисные, столы компьютерные, доска маркерная, трибуна настольная, шкафы со стеклом, тумбочка, стол однотумбовый с тумбой приставкой, кресло офисное. **Оборудование и технические средства обучения, наборы демонстрационного оборудования и учебно-наглядных пособий:** персональные компьютеры, телевизор. Доступ в электронную информационно-образовательную среду университета; Выход в Интернет.	**Комплект лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:** • MS Windows 10 (9879093834, 2020) или MS Windows 10 (87550822, 2019); • MS Office 2019 (9879093834, 2020) или MS Office 2019 (87550822, 2019); • Yandex Browser **(GNU Lesser General Public License); • 1С: Предприятие (Договор поставки № 3 от 03.12.2021); • СПС «Консультант-Плюс»* («Договор об информационной поддержке» от 03 мая 2018 года (бессрочный)). • Oracle VM + образ (Windows Server 2008 R, Linux) (Freeware) • MS SQL SERVER Express(Freeware)

				• SciLAB (Freeware) • MS Visual Studio 2020 Community (Freeware) • BPMN.Studio (Freeware)
5	Информационная безопасность	**Учебная аудитория для проведения учебных занятий** 440014, Пензенская область, г. Пенза, ул. Ботаническая, д. 30; аудитория 4435 *Компьютерный класс*	**Специализированная мебель:** столы для студентов, стол для преподавателя, лавки, компьютерные столы, стулья. **Оборудование и технические средства обучения, наборы демонстрационного оборудования и учебно-наглядных пособий:** персональные компьютеры, плакаты. Доступ в электронную информационно-образовательную среду университета; Выход в Интернет. **Набор демонстрационного оборудования (мобильный)**	**Комплект лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:** • MS Windows 10 (9879093834, 2020); • MS Office 2019 (9879093834, 2020); • Yandex Browser **(GNU Lesser General Public License); • 1С: Предприятие (Договор поставки № 3 от 03.12.2021); • СПС «КонсультантПлюс»* («Договор об информационной поддержке» от 03 мая 2018 года (бессрочный)); • Oracle VM + образ (Windows Server 2008 R (на 180 дней), Linux) (Freeware) • MS SQL SERVER Express(Freeware) • SciLAB (Freeware) • MS Visual Studio 2020 Community (Freeware) • BPMN.Studio (Freeware) • Государственная информационная система в области ветеринарии. Учебная (демо) версия подсистемы «Меркурий.ХС» Demoware (бесплатная демонстрационная версия с урезанным функционалом); • Комплекс программ по животноводству на ПК («СЕЛЭКС») (Договор с ООО «РЦ «ПЛИНОР» о предоставлении неисключительной (простой) лицензии № 434/58 от 30 апреля 2019 года).
6	Информационная безопасность	**Помещение для самостоятельной работы** 440014, Пензенская область, г. Пенза, ул. Ботаническая,	**Специализированная мебель:** столы читательские, столы компьютерные, стол однотумбовый, стулья, шкафы-витрины для выставок. **Оборудование и технические средства обучения:** персональные компьютеры.	**Комплект лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:**

		д. 30; аудитория 1237 *Зал обслуживания научными ресурсами, автоматизации RFID-технологий, коворкинга* *Отдел учета и хранения фондов*	Доступ в электронную информационно-образовательную среду университета; Выход в Интернет.	• MS Windows 7 (46298560, 2009); • MS Office 2010 (61403663, 2013); • Yandex Browser **(GNU Lesser General Public License); • СПС «КонсультантПлюс»* («Договор об информационной поддержке» от 03 мая 2018 года (бессрочный)).
7	Информационная безопасность	**Помещение для самостоятельной работы** 440014, Пензенская область, г. Пенза, ул. Ботаническая, д. 30; аудитория 5202 *Зал обеспечения цифровыми ресурсами и сервисами, коворкинга* *Помещение для научно-исследовательской работы*	**Специализированная мебель:** парты треугольные, столы компьютерные, стол сотрудника, витрина для книг, стулья. **Оборудование и технические средства обучения:** персональные компьютеры, телевизор, экранизированное устройство книговыдачи, считыватели электронных читательских билетов/банковских карт. Доступ в электронную информационно-образовательную среду университета; Выход в Интернет.	**Комплект лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:** • MS Windows 10 (V9414975, 2021); • MS Office 2019 (V9414975, 2021). • Yandex Browser **(GNU Lesser General Public License); • СПС «КонсультантПлюс»* («Договор об информационной поддержке» от 03 мая 2018 года (бессрочный)); • НЭБ РФ.

* – лицензионное программное обеспечение отечественного производства;

** − свободно распространяемое программное обеспечение отечественного производства.

Таблица 10.1 – Материально-техническое обеспечение дисциплины (редакция от 01.09.2023)

№ п/п	Наименование дисциплины в соответствии с учебным планом	Наименование учебных аудиторий и помещений для самостоятельной работы	Перечень оборудования и технических средств обучения, наличие возможности подключения к сети «Интернет»	Перечень лицензионного и свободно распространяемого программного обеспечения, в т.ч. отечественного производства. Реквизиты подтверждающего документа
1	Информационная безопасность	**Учебная аудитория для проведения учебных занятий** 440014, Пензенская область, г. Пенза, ул. Ботаническая, д. 30; аудитория 1121	**Специализированная мебель:** столы аудиторные 4-х местные со скамьей, скамьи аудиторные 4-х местные, скамьи 2-х местные, столы аудиторные 4-х местные, стол преподавательский (3 части), трибуны напольные, доска аудиторная. **Оборудование и технические средства обучения. Набор демонстрационного оборудования (стационарный):** персональный компьютер, проектор, колонки звуковые, микрофон, экран.	MS Windows 10 (9879093834, 2020); MS Office 2019 (9879093834, 2020).
2	Информационная безопасность	**Учебная аудитория для проведения учебных занятий** 440014, Пензенская область, г. Пенза, ул. Ботаническая, д. 30; аудитория 5101	**Специализированная мебель:** парты, стол аудиторный, стул, трибуна, шкаф, доски. **Оборудование и технические средства обучения. Набор демонстрационного оборудования (стационарный):** проектор, персональный компьютер, колонки, экран.	• MS Windows 10 (9879093834, 2020); • MS Office 2019 (9879093834, 2020); • СПС «Консультант-Плюс»* («Договор об информационной поддержке» от 03 мая 2018 года (бессрочный)).
3	Информационная безопасность	**Учебная аудитория для проведения учебных занятий Помещение для самостоятельной работы** 440014, Пензенская область, г. Пенза, ул. Ботаническая, д. 30; аудитория 1102 *(компьютерный класс)*	**Специализированная мебель:** столы аудиторные 2-х местные, скамьи аудиторные 2-х местные, компьютерные столы, стол компьютерный двух тумбовый, стулья жесткие, стул мягкий, кресло офисное, шкаф угловой, доска маркерная, стол СИ-1 (стол рабочий для инвалидов колясочников детей и взрослых), парта для слабовидящих. **Оборудование и технические средства обучения:** персональные компьютеры; видеоувеличитель портативный HV-MVC; ресивер для беспроводной связи; клавиатура адаптированная с крупными кнопками + пластиковая накладка, разделяющая клавиши, беспроводная; джойстик компьютерный адаптированный беспроводной; выносные компьютерные	• MS Windows 10 (V9414975, 2021); • MS Office 2019 (V9414975, 2021); • CorelDRAW Graphics Suite 2021 Education License (Windows) (single User) Лицензия № 731078 (бессрочная) от 03 февраля 2022 года; • Yandex Browser (GNU Lesser General Public License); • VirtualBox (Windows Server 2008 R (Demoware), Linux openSUSE (GNU General Public License (GPL))) (GNU General Public License (GPL); • MS SQL SERVER Express (Free edition); • SciLAB (GNU General Public License); • MS Visual Studio 2020 Community (Free edition);

			кнопки: большая беспроводная, малая беспроводная; компьютерный комплекс для слабовидящего, включающий в себя программу экранного доступа, ноутбук с наклейками на клавиатуру шрифтом Брайля; радиокласс (радиомикрофон) «Сонет-РСМ» РМ-1-1 (заушный индуктор и индукционная петля); плакаты «Компьютер и безопасность»; Доступ в электронную информационно-образовательную среду университета; Выход в Интернет.	• BPMN.Studio (Free edition); • 1С:Предприятие* (Договор поставки № 3 от 03.12.2021); • СПС «Консультант-Плюс»* («Договор об информационной поддержке» от 03 мая 2018 года (бессрочный)); • Project Expert (Договор на передачу программы для ЭВМ № 0716/2П-01 от 01.12.2005; Договор консультационного сопровождения № 0003/1КУ-01 от 15.03.2023).
4	Информационная безопасность	**Учебная аудитория для проведения учебных занятий** **Помещение для самостоятельной работы** 440014, Пензенская область, г. Пенза, ул. Ботаническая, д. 30; аудитория 1114	**Специализированная мебель:** столы аудиторные 2-х местные, стулья офисные, столы компьютерные, доска маркерная, трибуна настольная, шкафы со стеклом, тумбочка, стол однотумбовый с тумбой приставкой, кресло офисное. **Оборудование и технические средства обучения:** персональные компьютеры, телевизор. Доступ в электронную информационно-образовательную среду университета; Выход в Интернет.	• MS Windows 10 (9879093834, 2020) или MS Windows 10 (87550822, 2019); • MS Office 2019 (9879093834, 2020) или MS Office 2019 (87550822, 2019); • Yandex Browser** (GNU Lesser General Public License); • 1С:Предприятие* (Договор поставки № 3 от 03.12.2021); • СПС «Консультант-Плюс»* («Договор об информационной поддержке» от 03 мая 2018 года (бессрочный)); • VirtualBox (Windows Server 2008 R (Demoware), Linux openSUSE (GNU General Public License (GPL))) (GNU General Public License (GPL); • MS SQL SERVER Express (Free edition); • SciLAB (GNU General Public License); • MS Visual Studio 2020 Community (Free edition); • BPMN.Studio (Free edition).
5	Информационная безопасность	**Учебная аудитория для проведения учебных занятий** 440014, Пензенская область, г. Пенза, ул. Ботаническая, д. 30; аудитория 4435 *Компьютерный класс*	**Специализированная мебель:** столы для студентов, стол для преподавателя, лавки, компьютерные столы, стулья. **Оборудование и технические средства обучения:** персональные компьютеры. Доступ в электронную информационно-образовательную среду университета;	• MS Windows 10 (9879093834, 2020); • MS Office 2019 (9879093834, 2020); • Yandex Browser** (GNU Lesser General Public License); • 1С:Предприятие* (Договор поставки № 3 от 03.12.2021); • СПС «Консультант-Плюс»* («Договор об ин-

			Выход в Интернет.	формационной поддержке» от 03 мая 2018 года (бессрочный)); • VirtualBox (Windows Server 2008 R (Demoware), Linux openSUSE (GNU General Public License (GPL))) (GNU General Public License (GPL); • MS SQL SERVER Express (Free edition); • SciLAB (GNU General Public License); • MS Visual Studio 2020 Community (Free edition); • BPMN.Studio (Free edition); • Государственная информационная система в области ветеринарии. Учебная (демо) версия подсистемы «Меркурий.ХС»** Demoware (бесплатная демонстрационная версия с урезанным функционалом); • Комплекс программ по животноводству на ПК («СЕЛЭКС») (Договор с ООО «РЦ «ПЛИНОР» о предоставлении неисключительной (простой) лицензии № 434/58 от 30 апреля 2019 года).
6	Информационная безопасность	**Помещение для самостоятельной работы** 440014, Пензенская область, г. Пенза, ул. Ботаническая, д. 30; аудитория 1237 *Зал обслуживания научными ресурсами, автоматизации RFID-технологий, коворкинга* *Отдел учета и хранения фондов*	**Специализированная мебель:** столы читательские, столы компьютерные, стол однотумбовый, стулья, шкафы-витрины для выставок. **Оборудование и технические средства обучения:** персональные компьютеры. Доступ в электронную информационно-образовательную среду университета; Выход в Интернет.	MS Windows 7 (46298560, 2009); • MS Office 2010 (61403663, 2013); • Yandex Browser** (GNU Lesser General Public License); • СПС «Консультант-Плюс»* («Договор об информационной поддержке» от 03 мая 2018 года (бессрочный)).
7	Информационная безопасность	**Помещение для самостоятельной работы** 440014, Пензенская область, г. Пенза, ул. Ботаническая, д. 30; аудитория 5202 *Зал обеспечения цифровыми ресурсами и сервисами, коворкинга* *Помещение для научно-исследовательской работы*	**Специализированная мебель:** парты треугольные, столы компьютерные, стол сотрудника, витрина для книг, стулья. **Оборудование и технические средства обучения:** персональные компьютеры, телевизор, экранизированное устройство книговыдачи, считыватели электронных читательских билетов/банковских карт. Доступ в электронную информационно-образовательную среду уни-	MS Windows 10 (V9414975, 2021); • MS Office 2019 (V9414975, 2021). • Yandex Browser** (GNU Lesser General Public License); • СПС «Консультант-Плюс»* («Договор об информационной поддержке» от 03 мая 2018 года (бессрочный)); • НЭБ РФ.

			верситета; Выход в Интернет.	

* − лицензионное программное обеспечение отечественного производства;
** − свободно распространяемое программное обеспечение отечественного производства.

Таблица 10.1 – Материально-техническое обеспечение дисциплины (редакция от 01.09.2025)

№ п/п	Наименование дисциплины в соответствии с учебным планом	Наименование учебных аудиторий и помещений для самостоятельной работы	Перечень оборудования и технических средств обучения, наличие возможности подключения к сети «Интернет»	Перечень лицензионного и свободно распространяемого программного обеспечения, в т.ч. отечественного производства. Реквизиты подтверждающего документа
1	Информационная безопасность	**Учебная аудитория для проведения учебных занятий** 440014, Пензенская область, г. Пенза, ул. Ботаническая, д. 30; аудитория 1121	**Специализированная мебель:** столы аудиторные 4-х местные со скамьей, скамьи аудиторные 4-х местные, скамьи 2-х местные, столы аудиторные 4-х местные, стол преподавательский (3 части), трибуны напольные, доска аудиторная. **Оборудование и технические средства обучения:** плакаты. **Набор демонстрационного оборудования (стационарный):** персональный компьютер, проектор, колонки звуковые, микрофон, экран.	• MS Windows 10 (9879093834, 2020); • MS Office 2019 (9879093834, 2020).
2	Моделирование экономических процессов	**Учебная аудитория для проведения учебных занятий** 440014, Пензенская область, г. Пенза, ул. Ботаническая, д. 30; аудитория 1228	**Специализированная мебель:** столы аудиторные со скамьей, столы аудиторные без скамьи, скамьи аудиторные, столы-президиум, стул жесткий, трибуны, доска. **Оборудование и технические средства обучения:** плакаты. **Набор демонстрационного оборудования (стационарный):** персональный компьютер, проектор, экран.	• Linux Mint (GNU GPL); • Libre Office (GNU GPL); • СПС «КонсультантПлюс» («Договор об информационной поддержке» от 03 мая 2018 года (бессрочный))*.
3	Информационная безопасность	**Учебная аудитория для проведения учебных занятий Помещение для самостоятельной работы** 440014, Пензенская область, г. Пенза, ул. Ботаническая, д. 30; аудитория 1102 *Кабинет информатики (компьютерный класс)*	**Специализированная мебель:** столы аудиторные 2-х местные, скамьи аудиторные 2-х местные, компьютерные столы, стол компьютерный двух тумбовый, стулья жесткие, стул мягкий, кресло офисное, шкаф угловой, доска маркерная, стол СИ-1 (стол рабочий для инвалидов колясочников детей и взрослых), парта для слабовидящих. **Оборудование и технические средства обучения**: персональные компьютеры; видеоувеличитель портативный HV-MVC; ресивер для беспроводной связи; клавиатура адаптированная с крупными кнопками + пластиковая накладка, разделяющая клавиши, беспроводная; джойстик компьютерный адаптированный беспроводной; выносные компьютерные кнопки: большая бес-	• MS Windows 11 (V9414975, 2021); • MS Office 2019 (V9414975, 2021); • CorelDRAW Graphics Suite 2021 Education License (Windows) (single User) Лицензия № 731078 (бессрочная) от 03 февраля 2022 года; • Yandex Browser (GNU Lesser General Public License)**; • VirtualBox (Linux openSUSE (GNU General Public License (GPL))) (GNU General Public License (GPL)); • Visual Studio 2022 Community (Free edition); • MS SQL SERVER Express (Free edition); • SciLAB (GNU General

			проводная, малая беспроводная; компьютерный комплекс для слабовидящего, включающий в себя программу экранного доступа, ноутбук с наклейками на клавиатуру шрифтом Брайля; радиокласс (радиомикрофон) «Сонет-РСМ» РМ-1-1 (заушный индуктор и индукционная петля); плакаты «Компьютер и безопасность»; плакаты. Доступ в электронную информационно-образовательную среду университета; Выход в Интернет.	Public License); • 1С:Предприятие (Договор поставки № 3 от 03.12.2021)*; • СПС «Консультант-Плюс» («Договор об информационной поддержке» от 03 мая 2018 года (бессрочный))*; • Project Expert (Договор на передачу программы для ЭВМ № 0716/2П-01 от 01.12.2005; Договор консультационного сопровождения № 0003/1КУ-01 от 15.03.2023)*.
4	Информационная безопасность	**Учебная аудитория для проведения учебных занятий** **Помещение для самостоятельной работы** 440014, Пензенская область, г. Пенза, ул. Ботаническая, д. 30; аудитория 1107 *Кабинет информатики (компьютерный класс)*	**Специализированная мебель:** столы аудиторные 2-х местные, компьютерные столы, стулья жесткие, стул мягкий, шкаф угловой, доска маркерная, стол однотумбовый. **Оборудование и технические средства обучения:** персональные компьютеры, плакаты «Компьютер и безопасность», учебно-наглядные пособия (плакаты) для кафедры «Финансы и информатизация бизнеса». Доступ в электронную информационно-образовательную среду университета; Выход в Интернет.	• MS Windows 11 (V9414975, 2021); • MS Office 2021 (V9414975, 2021); • Yandex Browser (GNU Lesser General Public License)**; • VirtualBox (Linux openSUSE (GNU General Public License (GPL))) (GNU General Public License (GPL)); • Visual Studio 2022 Community (Free edition); • MS SQL SERVER Express (Free edition); • SciLAB (GNU General Public License); • 1С:Предприятие (Договор поставки № 3 от 03.12.2021)*; • СПС «Консультант-Плюс» («Договор об информационной поддержке» от 03 мая 2018 года (бессрочный))*.
5	Информационная безопасность	**Учебная аудитория для проведения учебных занятий** **Помещение для самостоятельной работы** 440014, Пензенская область, г. Пенза, ул. Ботаническая, д. 30; аудитория 1107а *Лаборатория информационных технологий*	**Специализированная мебель:** столы аудиторные 2-х местные, скамьи аудиторные 2-х местные, компьютерные столы, стол компьютерный двух тумбовый, стулья жесткие, стул мягкий, кресло офисное, шкаф угловой, доска маркерная. **Оборудование и технические средства обучения:** персональные компьютеры, плакаты «Компьютер и безопасность», плакаты для кафедры «Финансы и информатизация бизнеса». («Договор об информационной поддержке» от 03 мая 2018 года (бессрочный)). Доступ в электронную информационно-образовательную среду университета;	• MS Windows 11 (V9414975, 2021); • MS Office 2021 (V9414975, 2021); • Yandex Browser (GNU Lesser General Public License)**; • VirtualBox (Linux openSUSE (GNU General Public License (GPL))) (GNU General Public License (GPL)); • Visual Studio 2022 Community (Free edition); • MS SQL SERVER Express (Free edition)**; • SciLAB (GNU General Public License); • 1С:Предприятие (Договор поставки № 3 от

			Выход в Интернет.	03.12.2021)*; • СПС «Консультант-Плюс»*
6	Информационная безопасность	**Учебная аудитория для проведения учебных занятий** **Помещение для самостоятельной работы** 440014, Пензенская область, г. Пенза, ул. Ботаническая, д. 30; аудитория 1114 *Лаборатория прогнозирования и планирования*	**Специализированная мебель:** столы аудиторные 2-х местные, стулья офисные, столы компьютерные, доска маркерная, трибуна настольная, шкафы со стеклом, тумбочка, стол однотумбовый с тумбой приставкой, кресло офисное. **Оборудование и технические средства обучения:** персональные компьютеры, телевизор, плакаты для кафедры «Финансы и информатизация бизнеса». («Договор об информационной поддержке» от 03 мая 2018 года (бессрочный)). Доступ в электронную информационно-образовательную среду университета; Выход в Интернет.	• MS Windows 10 (9879093834, 2020) или MS Windows 10 (87550822, 2019); • MS Office 2019 (9879093834, 2020) или MS Office 2019 (87550822, 2019); • Yandex Browser (GNU Lesser General Public License)**; • 1С:Предприятие (Договор поставки № 3 от 03.12.2021)*; • СПС «Консультант-Плюс»*
7	Информационная безопасность	**Помещение для самостоятельной работы** 440014, Пензенская область, г. Пенза, ул. Ботаническая, д. 30; аудитория 1237 *Зал обслуживания научными ресурсами, автоматизации RFID-технологий, коворкинга* *Отдел учета и хранения фондов*	**Специализированная мебель:** столы читательские, столы компьютерные, стол однотумбовый, стулья, шкафы-витрины для выставок. **Оборудование и технические средства обучения:** персональные компьютеры. Доступ в электронную информационно-образовательную среду университета; Выход в Интернет.	• MS Windows 7 (46298560, 2009); • MS Office 2010 (61403663, 2013); • Yandex Browser (GNU Lesser General Public License)**; • СПС «Консультант-Плюс» («Договор об информационной поддержке» от 03 мая 2018 года (бессрочный))*.
8	Информационная безопасность	**Помещение для самостоятельной работы** 440014, Пензенская область, г. Пенза, ул. Ботаническая, д. 30; аудитория 5202 *Зал обеспечения цифровыми ресурсами и сервисами, коворкинга* *Помещение для научно-исследовательской работы*	**Специализированная мебель:** парты треугольные, столы компьютерные, стол сотрудника, витрина для книг, стулья. **Оборудование и технические средства обучения:** персональные компьютеры, телевизор, экранизированное устройство книговыдачи, считыватели электронных читательских билетов/банковских карт. Доступ в электронную информационно-образовательную среду университета; Выход в Интернет.	• MS Windows 10 (V9414975, 2021); • MS Office 2019 (V9414975, 2021). • Yandex Browser (GNU Lesser General Public License); • СПС «Консультант-Плюс» («Договор об информационной поддержке» от 03 мая 2018 года (бессрочный)); • НЭБ РФ.

* - лицензионное программное обеспечение отечественного производства;

** - свободно распространяемое программное обеспечение отечественного производства.

Таблица 10.1 – Материально-техническое обеспечение дисциплины (редакция от 01.09.2024)

№ п/п	Наименование дисциплины в соответствии с учебным планом	Наименование учебных аудиторий и помещений для самостоятельной работы	Перечень оборудования и технических средств обучения, наличие возможности подключения к сети «Интернет»	Перечень лицензионного и свободно распространяемого программного обеспечения, в т.ч. отечественного производства. Реквизиты подтверждающего документа
1	Информационная безопасность	**Учебная аудитория для проведения учебных занятий** 440014, Пензенская область, г. Пенза, ул. Ботаническая, д. 30; аудитория 1121	**Специализированная мебель:** столы аудиторные 4-х местные со скамьей, скамьи аудиторные 4-х местные, скамьи 2-х местные, столы аудиторные 4-х местные, стол преподавательский (3 части), трибуны напольные, доска аудиторная. **Оборудование и технические средства обучения,** плакаты. **Набор демонстрационного оборудования (стационарный):** персональный компьютер, проектор, колонки звуковые, микрофон, экран.	• MS Windows 10 (9879093834, 2020); • MS Office 2019 (9879093834, 2020).
2	Информационная безопасность	**Учебная аудитория для проведения учебных занятий Помещение для самостоятельной работы** 440014, Пензенская область, г. Пенза, ул. Ботаническая, д. 30; аудитория 1102 *Кабинет информатики (компьютерный класс)*	**Специализированная мебель:** столы аудиторные 2-х местные, скамьи аудиторные 2-х местные, компьютерные столы, стол компьютерный двух тумбовый, стулья жесткие, стул мягкий, кресло офисное, шкаф угловой, доска маркерная, стол СИ-1 (стол рабочий для инвалидов колясочников детей и взрослых), парта для слабовидящих. **Оборудование и технические средства обучения:** персональные компьютеры; видеоувеличитель портативный HV-MVC; ресивер для беспроводной связи; клавиатура адаптированная с крупными кнопками + пластиковая накладка, разделяющая клавиши, беспроводная; джойстик компьютерный адаптированный беспроводной; выносные компьютерные кнопки: большая беспроводная, малая беспроводная; компьютерный комплекс для слабовидящего, включающий в себя программу экранного доступа, ноутбук с наклейками на клавиатуру шрифтом Брайля; радиокласс (радиомикрофон) «Сонет-РСМ» РМ-1-1 (заушный индуктор и ин-	• MS Windows 11 (V9414975, 2021); • MS Office 2019 (V9414975, 2021); • CorelDRAW Graphics Suite 2021 Education License (Windows) (single User) Лицензия № 731078 (бессрочная) от 03 февраля 2022 года; • Yandex Browser** (GNU Lesser General Public License); • VirtualBox (Linux openSUSE (GNU General Public License (GPL))) (GNU General Public License (GPL); • MS SQL SERVER Express (Free edition); • SciLAB (GNU General Public License); • 1С:Предприятие* (Договор поставки № 3 от 03.12.2021); • СПС «КонсультантПлюс»* («Договор об информационной поддержке» от 03 мая 2018 года (бессрочный)); • Project Expert (Договор на передачу программы для ЭВМ № 0716/2П-01 от 01.12.2005; Договор консультационного сопровождения № 0003/1КУ-01 от 15.03.2023).

			дукционная петля); плакаты «Компьютер и безопасность»; плакаты. Доступ в электронную информационно-образовательную среду университета; Выход в Интернет.	
3	Информационная безопасность	**Учебная аудитория для проведения учебных занятий** **Помещение для самостоятельной работы** 440014, Пензенская область, г. Пенза, ул. Ботаническая, д. 30; аудитория 1114	**Специализированная мебель:** столы аудиторные 2-х местные, стулья офисные, столы компьютерные, доска маркерная, трибуна настольная, шкафы со стеклом, тумбочка, стол однотумбовый с тумбой приставкой, кресло офисное. **Оборудование и технические средства обучения:** персональные компьютеры, телевизор, плакаты. Доступ в электронную информационно-образовательную среду университета; Выход в Интернет.	• MS Windows 10 (9879093834, 2020) или MS Windows 10 (87550822, 2019); • MS Office 2019 (9879093834, 2020) или MS Office 2019 (87550822, 2019); • Yandex Browser** (GNU Lesser General Public License); • 1С:Предприятие* (Договор поставки № 3 от 03.12.2021); • СПС «КонсультантПлюс»* («Договор об информационной поддержке» от 03 мая 2018 года (бессрочный)); • VirtualBox (Linux openSUSE (GNU General Public License (GPL))) (GNU General Public License (GPL); • MS SQL SERVER Express (Free edition); • SciLAB (GNU General Public License).
4	Информационная безопасность	**Помещение для самостоятельной работы** 440014, Пензенская область, г. Пенза, ул. Ботаническая, д. 30;аудитория 1237 *Зал обслуживания научными ресурсами, автоматизации RFID-технологий, коворкинга* *Отдел учета и хранения фондов*	**Специализированная мебель:** столы читательские, столы компьютерные, стол однотумбовый, стулья, шкафы-витрины для выставок. **Оборудование и технические средства обучения:** персональные компьютеры. Доступ в электронную информационно-образовательную среду университета; Выход в Интернет.	• MS Windows 7 (46298560, 2009); • MS Office 2010 (61403663, 2013); • Yandex Browser** (GNU Lesser General Public License); • СПС «КонсультантПлюс»* («Договор об информационной поддержке» от 03 мая 2018 года (бессрочный)).
5	Информационная безопасность	**Помещение для самостоятельной работы** 440014, Пензенская область, г. Пенза, ул. Ботаническая, д. 30; аудитория 5202 *Зал обеспечения цифровыми ресурсами и сервисами, коворкинга* *Помещение для научно-исследовательской работы*	**Специализированная мебель:** парты треугольные, столы компьютерные, стол сотрудника, витрина для книг, стулья. **Оборудование и технические средства обучения:** персональные компьютеры, телевизор, экранизированное устройство книговыдачи, считыватели электронных читательских билетов/банковских карт. Доступ в электронную информационно-образовательную среду университета; Выход в Интернет.	• MS Windows 10 (V9414975, 2021); • MS Office 2019 (V9414975, 2021). • Yandex Browser** (GNU Lesser General Public License); • СПС «КонсультантПлюс»* («Договор об информационной поддержке» от 03 мая 2018 года (бессрочный)); • НЭБ РФ.

* - лицензионное программное обеспечение отечественного производства;
** - свободно распространяемое программное обеспечение отечественного производства.

11 Методические рекомендации по изучению дисциплины

При подборе литературы по изучению данной дисциплины следует обращаться к предметно-тематическим каталогам и библиографическим справочникам библиотеки, а также использовать систему Internet.

Изучение литературы по выбранной теме нужно начинать с общих работ. При изучении литературы желательно соблюдать следующие рекомендации:

- начинать следует с литературы, раскрывающей теоретические аспекты изучаемого вопроса - монографий и журнальных статей, после этого использовать инструктивные материалы;

- детальное изучение студентом литературных источников заключается в их конспектировании и систематизации (выписки, цитаты, краткое изложение содержания литературного источника или характеристика фактического материала); систематизацию получаемой информации следует проводить по основным разделам выпускной квалификационной работы, предусмотренным планом;

- изучая литературные источники, следите за оформлением выписок, чтобы в дальнейшем было легко ими пользоваться;

- старайтесь ориентироваться на последние данные по соответствующей проблеме, опираться на авторитетные источники, точно указывать, откуда взяты материалы; при отборе фактов из литературы подходить к ним критически.

Особой формой фактического материала являются цитаты, которые используются для того, чтобы без искажений передать мысль автора первоисточника. Число используемых цитат должно быть оптимальным, т.е. определяться потребностями разработки темы.

При изучении сложных тем курса целесообразно использовать правило дидактики, предусматривающее переход от известного к неизвестному, от простого – к сложному, а также максимальное привлечение наглядности. Особого внимания заслуживает словарная работа по изучению новых терминов. Теоретический материал целесообразно подкреплять конкретными примерами, и прежде всего – из сферы деятельности, близкой студентам.

Учитывая проблемы ряда студентов с чтением, необходимо добиваться соблюдения ими орфоэпических норм. Обеспечение принципа наглядности достигается привлечением разнообразных схем, диаграмм, таблиц. Учитывая степень сложности схем и диаграмм, целесообразно наиболее сложные изображать на доске до начала занятия. Это позволит экономить время занятия, сосредоточив усилия на уяснение нового материала.

Готовясь к экзамену, полезно повторять материал по вопросам. Прочитав вопрос, сначала вспомните и обязательно кратко запишите все, что вы знаете по этому вопросу, и лишь затем проверьте себя по учебнику. Особое внимание обратите на подзаголовки, главы или параграфы учебника, на правила и выделенный текст. Проверьте правильность дат, основных фактов. Только после этого внимательно, медленно прочтите учебник, выделяя главные мысли, - опорные пункты ответа.

Готовясь к экзамену, нужно составить четкий план подготовки. Достижение цели и чувство выполненного долга - мощный стимул.

Обязательно следует чередовать работу и отдых, например, 40 минут занятий, затем 10 минут – перерыв. В конце каждого дня подготовки следует проверить, как вы усвоили материал: вновь кратко запишите планы всех вопросов, которые были проработаны в этот день.

Одной из форм подготовки является тестирование знаний студентов. Последовательное изучение тестового материала даст возможность снизить затраты времени на овладение курсом бухгалтерского учета.

Использование тестов особенно эффективно при внедрении новых форм обучения.

Задачи в области образовательного тестирования можно разделить на три основные части: теоретическую, прикладную и нормативную (законодательную). Задачи теоретической части являются наиболее важными. Структура теоретической части состоит из четырех блоков:

1) основные представления образовательного тестирования,
2) основы обеспечения единства процедур тестирования,
3) основы разработки и применения образовательных тестов,
4) основы обеспечения точности оценивания знаний.

Содержание названных блоков следующее:

1. *Основные представления образовательного тестирования.* В образовательном тестировании необходимо сформулировать основные понятия, термины, разработать научные положения о мерах образовательной информации и методологию исследований. В основе тестирования лежат представление об объекте исследования. Недостаточная обоснованность основных представлений приводит к многократному решению аналогичных задач заново.

2. *Основы обеспечения единства процедур тестирования*. Это блок определяет практическую ценность новой технологии оценивания знаний. Он включает в себя теоретическое обоснование характеристик образовательной информации.

3. *Основы разработки и применения образовательных тестов*. Этот блок обобщает опыт разработки и практического применения различных форм заданий теста, а также методов распознания знаний по этом тестам. Актуальность этого блока объясняется тем, что все большее значение приобретают универсальные формы заданий тестов и оценка знаний в лингвистической и количественной форме.

4. *Основы обеспечения точности оценивания знаний методом тестирования*. Этот блок связан с теорией погрешностей системы предметного тестирования. Актуален вопрос о предельно достижимой погрешности оценивания знаний методом тестирования.

Рекомендации по работе с литературой

Основным источником получения знаний для студента вуза по-прежнему остается книга.

Современная научная вузовская библиотека является довольно сложным научно-информационным комплексом, включающим книжные фонды, ресурсы

Интернет; электронные каталоги и электронные ресурсы; разветвленную систему традиционных каталогов и картотек, справочно-информационный фонд; информационные, периодические и библиографические издания. Чтобы пользоваться всеми этими богатствами, нужно обладать культурой чтения. При чтении студентами учебной и научной литературы отмечаются три ступени усвоения материала.

На **первой** ступени студент понимает суть прочитанного, но не может изложить его ни в устной, ни в письменной форме.

На **средней** ступени проявляется работа памяти: студент пересказывает материал, нередко словами оригинала.

Высшая ступень усвоения материала характеризуется тем, что студент может анализировать материал, использовать методы сопоставления и оценки его с позиций полученных ранее знаний.

Работа студента с литературой сопряжена с активной психической деятельностью. Она зависит, в частности, от установки. Установка - это своеобразное состояние готовности личности к деятельности, возникающее на основе единства потребности мотивов и ситуации, соответствующей потребности. Фиксированная установка способствует повышению эффективности чтения, активизации мышления, памяти, более точному восприятию. Установка на выделение в тексте фактов и мыслей, на прочное запоминание, на глубокое понимание, на критический анализ текста помогает студенту выполнить поставленную задачу. Установка на «легкое» чтение отрицательно влияет на усвоение материала. Установка на зазубривание мешает осмыслению прочитанного. Намерение возможно более подробно записать текст затрудняет выделение в нем главного.

Чтение может быть сплошным и выборочным. При сплошном выделяют 4 основных временных режима или уровня:

- 1 -й уровень - тщательное чтение, критическое или аналитическое, с пристальным вниманием к деталям, размышлением над информацией, оценкой содержания материала, напряжением мысли (чтение учебников, монографий);
- 2-й уровень - обычное чтение, в высоком темпе без особых усилий для понимания (чтение газет, журналов, художественной литературы);
- 3-й уровень - чтение в высоком темпе, требующее сосредоточенности и умственного напряжения;
- 4-й уровень - выборочное чтение с целью поиска специфической информации в тексте или получения общего впечатления от содержания материала. В этих случаях опытный читатель повышает свой КПД чтения, пропуская ту информацию, которая не соответствует поставленной цели.

Чтение новой книги надо начинать с изучения оглавления, затем прочитать библиографические данные на титульном и на обороте титула - название работы, фамилия автора, место и год издания, аннотация. После этого полезно бегло просмотреть книгу, чтобы получить общее представление о ее содержании.

Детальное изучение нужного раздела книги лучше начинать не сразу после ее беглого чтения, а через некоторый промежуток времени, когда в результате подсознательной работы головного мозга произойдет частичное усвоение полученной информации. В таком случае изучение материала будет легче, чем при

первом чтении.

«Вход» в чтение не бывает мгновенным. Вначале лишние помехи в той или иной степени отвлекают внимание. Через 10-30 минут сосредоточенность достигает максимума. Читатель врабатывается в процесс восприятия настолько, что создает вокруг себя как бы «барьер внимания», через который не может пробиться шумовой фон. Средняя скорость чтения для студента составляет 120-180 слов в минуту, норма - 100 - 150 литературных источников в год. Степень усвоения содержания текста при такой скорости чтения колеблется от 20 до 60%. Соответствующие занятия и тренировки позволяют студентам увеличить скорость чтения при одновременном росте усвояемости текста с 60 до 74 %.

Чтобы чтение было рациональным, важно освободиться от вредных привычек. Одна из них - вождение карандашом, линейкой или пальцем по строчкам во время чтения. Чтобы избавиться от этой привычки, надо держать книгу двумя руками или держать левой рукой, а правой вести запись конспекта. Увеличение расстояния от текста до глаз при неправильной рабочей позе или нерациональное расположение книги - также вредная привычка при чтении. Чтобы избежать регрессий, т.е. движений глаз вверх по странице для возвращения к уже прочитанному, на что растрачивается 1/6 времени чтения, нужно закрывать чистым листом бумаги прочитанные строки.

Для повышения эффективности чтения надо выработать привычку читать не отдельные слова, а целые смысловые блоки. Это так называемое крупноблочное чтение, когда читаются не слова, а мысли. Оно трудное, но наиболее эффективное. Полезно научиться увеличить поле восприятия информации и двигательную способность глаз. Для этого с целью тренировки следует глаза при чтении перемещать по вертикали сверху вниз.

Можно провести по центру читаемого места вертикальную линию и первое время ориентироваться на нее. Если для упражнения применен узкий столбец газетного листа, его можно согнуть по вертикали.

В ряде случаев возникает необходимость выборочного чтения, например, при подготовке к семинару, зачету. Для этого могут использоваться два вида чтения со сверхскоростями - скимирование или сканирование текста.

Скимирование - быстрый просмотр текста для осознания его основного смысла. Возможно применение трех разновидностей:

а) предварительный просмотр, за которым следует повторный более тщательный просмотр для отыскания необходимого материала;

б) сквозной просмотр - для понимания основных идей и фактов;

в) пересмотр - для изучения ранее прочитанного текста, например, конспектов лекций перед экзаменами.

Сканирование - выборочное чтение с целью ответа на конкретные вопросы, поиска цитаты, ссылки, формулировки, определения.

Схема сканирования такова - в большом массиве слов идет поиск нужного отрывка текста со скоростью от 1000 - 1300 до 10000 - 25000 слов в минуту. Взгляд глаз при сканировании следует зигзагообразно или по вертикали в центре листа.

Целесообразно комбинированное применение скимирования и сканирования текста. Рациональное чтение - один из резервов повышения эффективности умственной деятельности:

- редактирование, сокращение незначительных разделов текста;
- уплотнение материала, вплоть до замены одной фразой целого абзаца;
- составление смысловых блок-схем: (блочный прием).

Метод цепи:

- связывание новых сведений с уже имеющимися по смыслу (прием «крючка»);
- составление матриц, сводных таблиц.

Метод художественного оформления:

- изображение материалов на рисунках;
- распределение ролей, образные представления;
- эмпатия, мысленное перевоплощение;
- поиск в материале приятной информации («улыбка»).

Перечисленные методы развития, стимулирования и тренировки памяти служат резервом повышения интенсивности и эффективности умственного труда студентов.

При подборе литературы следует обращаться к предметно-тематическим каталогам и библиографическим справочникам как библиотеки, а также использовать систему Internet.

Изучение литературы по выбранной теме нужно начинать с общих работ, чтобы получить представление об основных вопросах, к которым примыкает избранная тема, а затем уже вести поиск нового материала. При изучении литературы желательно соблюдать следующие рекомендации:

- начинать следует с литературы, раскрывающей теоретические аспекты изучаемого вопроса - монографий и журнальных статей, после этого использовать инструктивные материалы (инструктивные материалы используются только последних изданий);
- детальное изучение студентом литературных источников заключается в их конспектировании и систематизации, характер конспектов определяется возможностью использования данного материала в работе - выписки, цитаты, краткое изложение содержания литературного источника или характеристика фактического материала; систематизацию получаемой информации следует проводить по основным разделам выпускной квалификационной работы, предусмотренным планом;
- при изучении литературы не стремитесь освоить всю информацию, в ней заключённую, а отбирайте только ту, которая имеет непосредственное отношение к теме работы; критерием оценки прочитанного является возможность его практического использования;
- изучая литературные источники, тщательно следите за оформлением выписок, чтобы в дальнейшем было легко ими пользоваться;
- не расстраивайтесь, если часть полученных данных окажется бесполезной, очень редко они используются полностью;

- старайтесь ориентироваться на последние данные, по соответствующей проблеме, опираться на самые авторитетные источники, точно указывать, откуда взяты материалы; при отборе фактов из литературных источников нужно подходить к ним критически.

Особой формой фактического материала являются цитаты, которые используются для того, чтобы без искажений передать мысль автора первоисточника, для идентификации взглядов при сопоставлении различных точек зрения и т. д.; отталкиваясь от их содержания, можно создать систему убедительных доказательств, необходимых для объективной характеристики изучаемого вопроса; цитаты могут использоваться и для подтверждения отдельных положений работы; во всех случаях число используемых цитат должно быть оптимальным, т.е. определяться потребностями разработки темы, цитатами не следует злоупотреблять, их обилие может восприниматься как выражение слабости собственной позиции автора.

Для максимального усвоения дисциплины рекомендуется изложение лекционного материала с элементами обсуждения, а также проведение письменного опроса студентов по материалам лекций и практических работ. Подборка вопросов для тестирования осуществляется на основе изученного теоретического материала. Такой подход позволяет повысить мотивацию студентов при конспектировании лекционного материала.

Основными формами проведения занятий с целью осмысления дисциплины являются аудиторные занятия: лекции, практические, семинарские занятия. Для организации эффективного процесса усвоения материала студентами возможно использование различных форм: лекций, докладов студентов, дискуссий, современных мультимедийных технологий и др.

Внеаудиторные занятия осуществляются путем организации и руководством самостоятельной работы студентов с литературой.

Приступая к преподаванию той или иной части данного учебного курса, преподаватель, прежде всего, подбирает необходимые учебные материалы. Для этого в программу включен перечень основной, дополнительной и справочной литературы по разделам курса, что позволит преподавателям ориентироваться в большом разнообразии имеющейся учебно-методической и научной литературы, дополняя и обновляя используемые учебные материалы.

Рекомендуемые виды лекций: традиционная, лекция-беседа, проблемная лекция, лекция с элементами дискуссии.

Рекомендуемые виды практических занятий: вопросно-ответный семинар, развернутая беседа, семинар с использованием докладов и рефератов, семинар – дискуссия, семинар – контрольная, семинар – коллоквиум, выполнение задания с элементами фронтального опроса, тестовые задания по теме, практические занятия с элементами дискуссии.

Рекомендуемые методы обучения: дискуссия, имитационные упражнения, решение разноуровневых задач.

Рекомендуемые виды практических занятий: конспектирование, реферирование, анализ ситуаций, формулирование вопросов к обсуждению, проблемных вопросов.

Рекомендуемые методы текущего контроля знаний обучающихся: беседа, фронтальный опрос (устный, письменный), тематическое экспресс-тестирование, контрольная работа, итоговое тестирование, зачет с оценкой.

Методические указания для преподавателей
по подготовке и проведению лекционных занятий.

Лекционные занятия являются основным звеном информационного и организационного обеспечения изучения дисциплины. Целью является формирование основных ориентиров по изучению проблем, составляющих предмет «Информационная безопасность».

Содержание материала должно соответствовать следующим требованиям:
- логичность и доступность изложения материала;
- изложение материала от простого к сложному, от известного к неизвестному;
- активизация внимания и деятельности слушателей на основе диалога, выделения проблемных вопросов;
- обоснование смысловой части лекции подлинными фактами, событиями, достоверными статистическими материалами;
- тесная связь материала с будущей практической деятельностью.

Лекционные занятия проводятся в группе. В процессе проведения лекций особое внимание уделяется установлению обратной связи с аудиторией: студентам предлагается отвечать на вопросы преподавателя и задавать уточняющие вопросы.

Выбор конкретных методик проведения лекций зависит от индивидуальных особенностей и предпочтений преподавателя, а также от особенностей аудитории. При изложении лекционного материала следует строго соответствовать программе курса, в соответствующих вопросах к излагаемой теме лекции. Целесообразно предоставить студентам возможность предварительно ознакомиться с планом лекции, ее тезисами. Преподаватель, читающий лекционные курсы в вузе, должен знать существующие в педагогической науке и используемые на практике приемы изложения лекционного материала, их дидактические и воспитательные возможности, а также их роль в структуре учебного процесса. Курс дисциплины «Информационная безопасность организации» включает следующие разделы:

Раздел 1. Правовые и организационные аспекты защиты информации

Раздел 2. Угрозы информационной безопасности и методы их реализации

Раздел 3. Защита от разрушающих программных воздействий

Методические рекомендации по подготовке к экзамену.

Готовясь к экзамену, студенту полезно повторять материал по вопросам. Прочитав вопрос, студент должен сначала вспомнить и обязательно кратко записать все, что он знает по этому вопросу, и лишь затем проверить себя по учебни-

ку. Особое внимание нужно обратить на подзаголовки, главы или параграфы учебника, на правила и выделенный текст. Важно проверить правильность формул расчета показателей, алгоритма способов детерминированного факторного анализа. При этом по данным годовых отчетов следует уточнить источники информации для расчета основных экономических показателей деятельности хозяйствующего субъекта.

Студенту, готовящемуся получить на экзамене хорошую отметку, нужно составить четкий план подготовки. Достижение цели и чувство выполненного долга - мощный стимул.

Обязательно следует чередовать работу и отдых, например, 40 минут занятий, затем 10 минут – перерыв. В конце каждого дня подготовки следует проверить, как вы усвоили материал: вновь кратко запишите планы всех вопросов, которые были проработаны в этот день.

Одной из эффективных форм текущего контроля знаний студентов форм является тестирование знаний студентов. Последовательное изучение тестового материала даст возможность снизить затраты времени на овладение курсом «Информационная безопасность организации».

12 СЛОВАРЬ ТЕРМИНОВ

Алгоритмы шифрования с открытым ключом — алгоритмы шифрования, в которых используются два ключа: один (закрытый) предназначен для шифрования сообщения, а второй (закрытый) — для расшифровывания.

Апеллируемость — возможность доказать, что автором является именно данный человек и никто другой.

Атака — попытка реализации угрозы.

Аутентификация **пользователей — процесс, с помощью которого одна сторона (проверяющий**) убеждается в идентичности другой стороны.

Аутентичность — возможность достоверно установить автора сообщения.

Бэкдор (backdoor) — программа, позволяющая злоумышленнику получать удаленный доступ к системе и возможность удаленного управления ею.

Блочные шифры — алгоритмы шифрования, в которых единицей шифрования является блок (последовательность бит фиксированной длины), преобразовываемые в блок зашифрованного текста такой же длины.

Виртуальная частная сеть (VPN) — логическая сеть, создаваемая поверх другой сети, чаще всего Интернет. За счет криптографической защиты передаваемых данных обеспечивает закрытые от посторонних каналы обмена информацией.

Вирус (компьютерный) — программа, способная к саморазмножению, т.е. способная, создавать свои копии (возможно, модифицированные) и распространять их некоторым образом с компьютера на компьютер.

Генератор псевдослучайных чисел (ГПСЧ) — алгоритм, генерирующий последовательность чисел, элементы которой почти независимы друг от друга и подчиняются заданному распределению (обычно равномерному).

Диспетчер доступа — абстрактная машина, которая выступает посредником при всех обращениях субъектов к объектам и на основании пра-

вил разграничения доступа разрешает, либо не разрешает субъекту доступ к объекту.

Диффузия — свойство алгоритма шифрования: каждый бит открытого текста должен влиять на каждый бит зашифрованного текста.

Доступ к информации — ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации

Доступность — свойство информации; наличие своевременного беспрепятственного доступа к информации для субъектов, обладающих соответствующими полномочиями.

Естественные угрозы — угрозы, вызванные воздействиями на АИС и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека.

Загрузочные вирусы — вирусы, распространяющиеся через сменные носители данных и активирующиеся при загрузке с этих носителей.

Зашифрованный текст — текст сообщения после применения к нему процедуры шифрования. Информация, содержащаяся в сообщении, не может быть воспринята без проведения обратного преобразования — расшифровывания.

Защита информации – комплекс мероприятий, направленных на обеспечение информационной безопасности.

Злоумышленник — нарушитель, намеренно идущий на нарушение из корыстных побуждений.

Информационная безопасность — состояние защищенности информации и информационной среды от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, (в том числе владельцам и пользователям информации).

Информационная безопасность Российской Федерации (согласно доктрине информационной безопасности РФ) — состояние защищенности ее национальных интересов в информационной сфере, определяющихся со-

вокупностью сбалансированных интересов личности, общества и государства.

Искусственные угрозы — угрозы, вызванные деятельностью человека.

Конфиденциальность — свойство информации; означает, что с ней может ознакомиться только строго ограниченный круг лиц, определенный ее владельцем.

Конфузия — свойство алгоритма шифрования: отсутствие статистической взаимосвязи между ключом и зашифрованным текстом.

Криптографическая система — система обеспечения информационной безопасности сети или АИС, использующая криптографические средства.

Криптографические алгоритмы — алгоритмы, предназначенные для противодействия определенным угрозам информационной безопасности со стороны возможного нарушителя или нежелательных воздействий естественного характера. К ним относятся алгоритмы шифрования/дешифрования, хэширования, формирования и проверки электронной цифровой подписи, распределения ключей и др.

Криптографические средства — методы и средства обеспечения информационной безопасности, использующие криптографические преобразования информации. В узком смысле под криптографическими средствами могут пониматься отдельные устройства, документы и программы, использующиеся для выполнения функций криптосистемы.

Криптографический протокол — протокол, использующийся при выполнения действий по обмену информацией для предотвращения определенных угроз информационной безопасности (в ситуации, когда цели участников могут быть нарушены злоумышленником).

Криптографическое преобразование информации — преобразование информации с использованием одного из криптографических алгоритмов.

Криптография — область науки, техники и практической деятельности, связанная с разработкой, применением и анализом криптографических систем защиты информации.

Макровирусы — разновидность файловых вирусов, заражают файлы документов, позволяющие хранить внутри себя команды на макроязыке.

Матрица доступа — таблица, в которой строки соответствуют субъектам, столбцы — объектам доступа, а на пересечении строки и столбца содержатся правила (разрешения) доступа субъекта к объекту.

Межсетевой экран (брандмауэр, файрвол) — комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях модели OSI в соответствии с заданными правилами.

Модель безопасности — описание требований безопасности к автоматизированной информационной системе. Обычно заключается в определении потоков информации, разрешенных в системе, и правил управления доступом к информации.

Нарушение — реализация угрозы.

Нарушитель — лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

Неформальная модель нарушителя — описание вероятного нарушителя, включающее его потенциальные возможности и знания, время и место действия, необходимые усилия и средства для осуществления атаки и т.п.

Объект доступа — единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа

Односторонность хэш-функции. Свойство хэш-функции: для любого хэша h должно быть практически невозможно вычислить или подобрать сообщение с таким хэшем.

Открытый текст — исходный текст сообщения до применения к нему процедуры шифрования. Доступен для вприятия и обработки.

Перестановочные алгоритмы шифрования — класс симметричных алгоритмов шифрования, в которых шифрование осуществляется путем изменения порядка следования символов или бит открытого текста.

Подстановочные алгоритмы шифрования — класс симметричных алгоритмов шифрования, в которых шифрование осуществляется путем замены каждого символа (бита) или последовательности символов (битов) открытого текста другим символом (битом) или последовательностью символов (битов).

Полиморфные вирусы — вирусы, модифицирующие свой код в зараженных программах таким образом, что два экземпляра одного и того же вируса могут не совладать ни в одном бите.

Политика безопасности — совокупность руководящих принципов, правил, процедур и практических приёмов в области безопасности, которыми руководствуется организация в своей деятельности.

Потоковые шифры — алгоритмы шифрования, в которых символы (байты или биты) открытого текста шифруются последовательно.

Правила разграничения доступа — совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Протокол — последовательность шагов, которые предпринимают две или большее количество сторон для совместного решения некоторой задачи.

Протокол обмена ключами — это такой протокол, с помощью которого знание некоторого секретного ключа разделяется между двумя или более сторонами, причем противник, имеющий возможность перехватывать пересылаемые сообщения, не способен этот ключ получить.

Резидентные вирусы — вирусы, постоянно функционирующие в оперативной памяти ЭВМ (обычно автоматически запускаются в момент старта системы).

Сетевые черви — вирусы, распространяющие свои копии по сети.

Симметричные алгоритмы шифрования — алгоритмы шифрования, в которых один и тот же ключ K используется для того, чтобы зашифровать сообщение и для его последующей расшифровки.

Система обнаружения вторжений (Intrusion Detection System — IDS) — программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими (в основном через Интернет).

Система разграничения доступа (СРД) — это совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах.

Скремблеры — программные или аппаратные реализации алгоритма, позволяющего шифровать побитно непрерывные потоки информации.

Стелс-вирус — вирус, полностью или частично скрывающий свое присутствие путем перехвата обращений к операционной системе, осуществляющих чтение, запись, чтение дополнительной информации о зараженных объектах (загрузочных секторах, элементах файловой системы, памяти и т.д.)

Стойкость к коллизиям первого рода. Свойство хэш-функции: для любого сообщения должно быть практически невозможно вычислить или подобрать другое сообщение с точно таким же хэшем.

Стойкость к коллизиям второго рода. Свойство хэш-функции: должно быть практически невозможно вычислить или подобрать любую пару различных сообщений с одинаковым хэшем.

Субъект доступа — лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Троянский конь — вредоносная программа, маскирующаяся под программу, выполняющую полезные функции.

Туннель — канал между двумя узлами, защищенный за счет шифрования проходящего по нему трафика.

Угроза – потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.

Угроза информационной безопасности — потенциально возможное событие, действие, процесс или явление, которое посредством воздействия на информацию или компоненты АИС может прямо или косвенно привести к нанесению ущерба интересам субъектов информационных отношений.

Файловые вирусы — вирусы, внедряющиеся ("заражающие") исполняемые файлы путем записывания в них своего тела (команд).

Фишинг — процедура «выуживания» паролей случайных пользователей Интернета. Обычно заключается в создании «подставных» сайтов, которые обманом вынуждают пользователя ввести свой пароль.

Хэш — результат применения к сообщению хэш-функции.

Хэш-функция — функция, преобразующая сообщение произвольной длины в значение H(M) фиксированной длины, называемое хэшем сообщения. Обладает свойствами односторонности, стойкости к коллизиям первого и второго рода.

Целостность — свойство информации; заключается в сохранности информации в неискаженном виде (отсутствие неправомочных и непредусмотренных владельцем информации искажений).

Шифрование — процесс преобразования исходного сообщения открытого текста в зашифрованный текст таким образом, что простое обратное преобразование возможно только при наличии некоторой дополнительной информацией — ключа.

Экранирование — средство разграничения доступа клиентов из одного множества информационных систем к серверам из другого множества информационных систем.

Электронная цифровая подпись (ЭЦП) — реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Приложение

МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Пензенский государственный аграрный
университет»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки
09.03.03 ПРИКЛАДНАЯ ИНФОРМАТИКА

Направленность (профиль) программы
Прикладная информатика в экономике

Квалификация
«Бакалавр»

Форма обучения – очная

Пенза – 2023

1 Перечень компетенций с указанием этапов их формирования и индикаторов достижения

Таблица 1.1 – Перечень компетенций с указанием этапов их формирования и индикаторов достижения по дисциплине «Информационная безопасность»

№ пп	Код и наименование компетенции	Код индикатора достижения компетенции	Наименование индикатора достижения компетенции	Код планируемого результата обучения	Планируемые результаты обучения
1	ОПК-3 – Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	ИД-2$_{ОПК-3}$	Решает стандартные задачи профессиональной деятельности с соблюдением требований информационной безопасности	З1 (ИД-2$_{ОПК-3}$)	Знать: способы решения стандартных задач для обеспечения информационной безопасности
				У1 (ИД-2 $_{ОПК-3}$)	Уметь: формировать массив необходимой информации для оценки и интерпретации информации, в том числе с позиции обеспечения информационной безопасности организаций
				В1 (ИД-2 $_{ОПК-3}$)	Владеть: навыками решения профессиональных задач с позиции защиты информации от несанкционированного доступа
2	ОПК-4 – Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью.	ИД-1$_{ОПК-4}$	Участвует в разработке стандартов, норм и правил на различных стадиях проектирования и поддержки жизненного цикла информационной системы	З1 (ИД-1$_{ОПК-4}$)	Знать: стандарты, нормы и правила на различных этапах проектирования жизненного цикла в контексте защиты информационной системы
				У1 (ИД-1 $_{ОПК-4}$)	Уметь: выбирать инструментальные средства при проектировании жизненного цикла информационной системы в контексте реализации политики информационной безопасности

				В1 (ИД-1 ОПК-4)	Владеть: навыками разработки стандартов, норм и правил на различных стадиях проектирования жизненного цикла информационной системы и экономико-правового обеспечения информационной безопасности

2 Оценочные материалы по дисциплине «Информационная безопасность»

2.1 Оценочные материалы тестового типа

Таблица 2.1 - Задания тестового типа

№ п/п	Текст задания	Варианты ответов	Правильный ответ	Код компетенции	Семестр
1. Задание закрытого типа на установление соответствия					
Инструкция (сценарий выполнения): 1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидаются пары элементов. 2. Внимательно прочитать оба списка: список 1 — вопросы, утверждения, факты, понятия и т.д.; список 2 — утверждения, свойства объектов и т.д. 3. Сопоставить элементы списка 1 с элементами списка 2, сформировать пары элементов. 4. Записать попарно буквы и цифры (в зависимости от задания) вариантов ответа (например, А1 или Б4)					
1.	Установите соответствие в определениях: А. Несанкционированный доступ к информации – это; Б. Действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных; В. Действия с персональными данными (согласно закону), включая сбор, систематизацию, накопление, хранение, использование, распространение – это; Г. Документированная информация, доступ к которой ограничивает в соответствии с законодательством РФ.	1. Обработка персональных данных 2. Доступ к информации, не связанный с выполнением функциональных обязанностей и не оформленный документально 3. Деперсонификация 4. Конфиденциальная информация	А2Б3В1Г4	ОПК-3	6

2.	Установите соответствие в понятиях: А. Хищение информации – это Б. К какому виду угроз относится плагиат и присвоение чужой информации В. Документированная информация, доступ к которой ограничивает в соответствии с законодательством РФ	1. Конфиденциальная информация 2. Несанкционированное копирование информации 3. Нарушение права собственности	А2Б3В1	ОПК-3	6
3.	Установите соответствие в понятиях системы управления риском информационной безопасностью: А. Какие затраты связаны с формированием и поддержанием звена управления системой защиты информации Б. При страховании информационных рисков страховым случаем не является В. При защите автоматизированной системы от несанкционированного доступа оптимальное управление информационными потоками относится к	1. Хищение компьютерной техники 2. Подсистеме управления доступом 3. Организационные затраты	А3Б1В2	ОПК-4	6
4.	Установите соответствие в элементах концепции рисков информационной безопасности: А. Управление рисками в сфере информационной безопасности реализуется на уровне Б. Какое число вариантов реализации стратегии управления рисками выделяется в системе управления рисками В. К способам противодействия выявленным рискам (угрозам) в системе управления рисками не относится Г. Кто является основным ответственным за принятие решения по определению уровня классификации информации	1. Административном 2. Полное игнорирование всех рисков и угроз 3. Четыре 4. Владелец	А1Б3В2Г4	ОПК-4	6
2. Задание закрытого типа на установление последовательности					

Инструкция (сценарий выполнения):
1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов.
2. Внимательно прочитать предложенные варианты ответа.
3. Построить верную последовательность из предложенных элементов.
4. Записать буквы/цифры (в зависимости от задания) вариантов ответа в нужной последовательности без пробелов и знаков препинания (например, БВА или 135)

1.	Установите последовательно основных компонентов информационных технологий:	1. Сбор и хранение первичных данных 2. Передача информационного продукта пользователю 3. Формирование информационного продукта	132	ОПК-4	6
2.	Установите последовательность этапов разработки и внедрения систем защиты информации	1. Внедрение 2. Аттестация 3. Требования и критерии систем защиты информации. 4. Разработка	3412	ОПК-4	6
3.	Установите последовательность разработки политики информационной безопасности	1. Обучение персонала и постоянное обновление политики. 2. Анализ существующих угроз и уязвимостей, 3. Определение целей и принципов безопасности, 4. Разработку конкретных правил и процедур,	2341	ОПК-3	6
4.	Установите последовательность этапов обеспечения информационной безопасности :	1. Разработка политики безопасности; 2. Реализация политики; 3. Оценка стоимости; 4. Аудит.	3124	ОПК-3	6

3. Задание открытого типа с развернутым ответом/ задача

Инструкция (сценарий выполнения):
1. Внимательно прочитать текст задания и понять суть вопроса.
2. Продумать логику и полноту ответа.
3. Записать ответ, используя четкие компактные формулировки.
4. В случае расчетной задачи записать решение и ответ

1.	Что относится к правовым методам, обеспечивающим информационную безопасность?		Разработка и конкретизация правовых нормативных актов обеспечения безопасности	ОПК-3	6

2.	Основные источники угроз информационной безопасности?		Перехват данных, хищение данных, изменение архитектуры системы	ОПК-4	6
3.	Наиболее важным при реализации защитных мер политики безопасности является..?		Аудит, анализ уязвимостей, риск-ситуаций	ОПК-3	6
4.	Наиболее распространенные угрозы информационной безопасности корпоративной системы		Ошибки эксплуатации и неумышленного изменения режима работы системы	ОПК-4	6

4. Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное

Инструкция (сценарий выполнения):

1. Внимательно прочитать текст задания и понять суть вопроса.
2. Продумать логику и полноту ответа.
3. Записать ответ в виде термина, словосочетания ….., дополнить предложенное

1.	Принципом политики информационной безопасности является _____ доступа (обязанностей, привилегий) клиентам сети (системы).		разделение доступа	ОПК-3	6
2.	Цели информационной безопасности – своевременное обнаружение, предупреждение _____ доступа, воздействия в сети.		несанкционированного	ОПК-3	6
3.	Наиболее распространены угрозы информационной безопасности корпоративной системы: _____эксплуатации и неумышленного изменения режима работы системы.		ошибки	ОПК-4	6
4.	Утечкой информации в системе называется ситуация, характеризуемая _____ данных в системе.		потерей	ОПК-4	6

5. Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных с последующим объяснением своего выбора

Инструкция (сценарий выполнения):

1. Внимательно прочитать текст задания и понять суть вопроса.
2. Продумать логику и полноту ответа.
3. Записать номер правильного ответа или номера правильных ответов без пробелов и запятых (в зависимости от задания) и дать обоснование, используя четкие компактные формулировки.

1.	Сущность принципа информационной безопасности?	1. Недопущение рисков безопасности сети; 2. Недопущение рисков безопасности системы; 3. Неоправданных ограничениях при работе в сети (системе); 4. Презумпции секретности	3 Обоснование: Сущность принципа информационной безопасности состоит в недопущения неоправданных ограничений при работе в сети (системе)	ОПК-3	6

2.	Виды информационной безопасности?	1. Персональная, корпоративная, государственная 2. Клиентская, серверная, сетевая 3. Локальная, глобальная, 4. Смешанная	1 Обоснование: К видам информационной безопасности относятся персональная, корпоративная, государственная	ОПК-3	6
3.	Что относится к правовым методам, обеспечивающим информационную безопасность?	1. Разработка аппаратных средств обеспечения правовых данных; 2. Разработка и установка во всех компьютерных правовых сетях журналов учета действий; 3. Разработка и конкретизация правовых нормативных актов обеспечения безопасности.	3 Обоснование: К правовым методам информационной безопасности относятся разработка и конкретизация правовых нормативных актов обеспечения безопасности	ОПК-4	6
4.	Электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом?	1. Неквалифицированная электронная подпись; 2. Простая электронная подпись; 3. Квалифицированная электронная подпись.	2 Обоснование: Простая электронная подпись – это электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.	ОПК-4	6

2.2 Оценочные материалы для текущего контроля

Текущий контроль успеваемости является обязательной частью внутренней системы оценки качества освоения обучающимися образовательной программы. Текущий контроль успеваемости проводится в рамках изучения дисциплины в течение семестра. Виды оценочных материалов, формы контроля, темы и график определяется педагогическим работником.

2.3 Типовые вопросы для промежуточной аттестации

Вопросы для промежуточного контроля знаний (экзамен) по оценке освоения компетенций ОПК-3 (6 семестр)

1. Программа информационной безопасности России и пути ее реализации.
2. Концепция информационной безопасности в системе экономико-правовое обеспечение экономической безопасности
3. Обзор состояния систем защиты информации в России и в ведущих зарубежных странах. Международные стандарты информационного обмена.
4. Основные принципы защиты информации в компьютерных системах.
5. Основные понятия и определения защиты информации.
6. Экономико-правовое обеспечение информационной безопасности.
7. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
8. Компьютерные преступления.
9. Организационное обеспечение информационной безопасности.
10. Виды возможных нарушений информационной системы.
11. Понятие угрозы. Анализ угроз безопасности информации.
12. Причины, виды, каналы утечки и искажения информации.
13. Основные методы реализации угроз информационной безопасности: методы нарушения секретности, целостности и доступности информации.
14. Информационная безопасность в условиях функционирования в России глобальных сетей.
15. Общая проблема информационной безопасности информационных систем.

Вопросы для промежуточного контроля знаний (экзамен) по оценке освоения компетенций ОПК-4 (6 семестр)

1. Защита информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение).
2. Основные технологии построения защищенных экономических информационных систем (ЭИС).
3. Защита информации от несанкционированного доступа.
4. Математические и методические средства защиты.
5. Компьютерные средства реализации защиты в информационных системах. Политика безопасности.
6. Критерии и классы защищенности средств вычислительной техники и автоматизированных систем.
7. Использование защищенных компьютерных систем. Стандарты по оценке защищенных систем.
8. Понятие разрушающего программного воздействия.
9. Методы перехвата и навязывания информации.
10. Компьютерные вирусы. Понятия о видах вирусов.
11. Современные антивирусные программы.

12. Общие подходы к построению парольных систем.
13. Выбор паролей. Хранение паролей. Передача пароля по сети.
14. Особенности криптографического и стеганографического преобразования информации. Стойкость алгоритмов шифрования. Типы алгоритмов шифрования.
15. Особенности применения криптографических методов.
16. Особенности реализации систем с симметричными и несимметричными ключами.
17. Электронная подпись.
18. Защита офисных документов и экономико-правовая безопасность.
19. Способы распространения программного обеспечения.
20. Техническая защита от несанкционированного копирования. Базовые методы нейтрализации систем защиты от несанкционированного копирования.
21. Идентификация параметров персонального компьютера.
22. Идентификация жестких дисков. Идентификация гибких дисков.
23. Оценка уникальности конфигурации компьютера.
24. Подходы к построению защищенной операционной системы. Административные меры защиты.
25. Стандарты защищенности операционных систем.
26. Виды уязвимости и атак на ОС. Классификация угроз безопасности операционной системы. Типичные атаки на операционную систему.
27. Классификация способов несанкционированного доступа и жизненный цикл атак.
28. Нападения на политику безопасности и процедуры административного управления.
29. Нападения на постоянные и сменные компоненты системы защиты.
30. Нападения на протоколы информационного взаимодействия.
31. Нападения на функциональные элементы компьютерных сетей.
32. Способы противодействия несанкционированному сетевому и межсетевому доступу.
33. Аутентификация пользователя локальной сети.
34. Разграничение доступа к локальной сети.
35. Противодействие несанкционированному межсетевому доступу. Использование межсетевых экранов (Firewall). Критерии их оценки.
36. Защита виртуальных потоков на различных сетевых уровнях.
37. Защита удаленного доступа к локальной сети.
38. Безопасная доставка E-mail сообщений. Использование ключей и цифровых подписей.
39. Сертификация серверов Интернет. Безопасность работы в Интернет с использованием браузера.