

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Финк Анастасия Федоровна
Должность: Проректор по учебной работе
Дата подписания: 30.06.2026 13:57:27
Уникальный программный ключ:
2431bd5130e74d20a9fc74baab365dd497e3afa3

ЧОУ ВО «Тольяттинская академия управления»

Кафедра

прикладной информатики и высшей математики



Б1.В.08

РАБОЧАЯ ПРОГРАММА

Учебная дисциплина	<i>Информационная безопасность</i>
По направлению подготовки	<i>09.03.03 «Прикладная информатика»</i>
Профиль (программа бакалавриата)	<i>«Дизайн и разработка цифровых программных продуктов»</i>
Форма обучения	<i>Очно-заочная</i>

Программа дисциплины рассмотрена (актуализирована) и утверждена на заседании кафедры прикладной информатики и высшей математики

Протокол заседания № 10 от «25» мая 2026 г.

Заведующий кафедрой Стрекалова Наталья Борисовна

1. ОБЩАЯ ИНФОРМАЦИЯ

Рабочая программа дисциплины «Информационная безопасность» составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 09.03.03 «Прикладная информатика», утвержденного приказом Министерства образования и науки Российской Федерации 19.09.2017 №922 (с изменениями и дополнениями от 26.11.2020, 08.02.2021, 19.07.2022, 27.02.2023), и учебного плана направления подготовки 09.03.03 «Прикладная информатика», профиль «Дизайн и разработка цифровых программных продуктов» (программа бакалавриата).

Трудоемкость дисциплины: 4 ЗЕТ / 144 академических часа, в том числе 44 часа контактной работы и 100 часов самостоятельной работы обучающихся.

Распределение часов дисциплины по семестрам и видам занятий (по учебному плану)

Вид учебной работы		Количество часов									
		Всего по учебному плану	Семестры								
			1	2	3	4	5	6	7	8	9
Контактная работа (всего):		44						44			
в том числе:											
Лекции		8						8			
Практические занятия		28						28			
Контроль самостоятельной работы (КСР)		8						8			
Самостоятельная работа (всего):		100						100			
в том числе: курсовая работа		36						36			
Виды промежуточной аттестации (зачет, защита курсовой работы)		зачет						зачет, защита курсовой работы			
ОБЩАЯ трудоемкость дисциплины:	Часы:	144						144			
	Зач. ед.:	4						4			

2. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цель дисциплины – формирование у обучающихся знаний в области теоретических основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных средств в информационных и вычислительных системах. Воспитательной целью дисциплины выступает развитие у обучающихся навыков критического мышления, позволяющего понимать проблемы информационного общества, осознавать риски в своей профессиональной деятельности и ее социальную значимость, стремиться находить способы разрешения возникающих проблем;

формирование навыков самостоятельной деятельности, как в образовательной, так и профессиональной сфере.

Задачи дисциплины:

- развить навыки по описанию информационной безопасности и реализации бизнес-процессов заказчика;
- сформировать у обучающихся компетенции в области безопасности современных цифровых программных продуктов в сфере управления деятельностью предприятия;
- развить навыки применения системного подхода к безопасности, информатизации и автоматизации решения прикладных задач;
- дать представление об инструментах интеллектуального анализа данных;
- развить навыки формирования обобщенных требований к информационной системе предприятия, её структуре и основным данным.

3. МЕСТО ДИСЦИПЛИНЫ В УЧЕБНОМ ПЛАНЕ

Учебная дисциплина «Информационная безопасность» относится к дисциплинам части Блока 1. Дисциплины (модули), формируемой участниками образовательных отношений. Изучение данной дисциплины базируется на материале, изученном в дисциплине «Общие информационные технологии», «Цифровое обеспечение профессиональной деятельности», «Программно-аппаратное обеспечение цифровых устройств». Знания, умения и навыки, приобретенные в результате изучения дисциплины, будут востребованы при освоении дисциплин «Правовые основы сферы информационных технологий», «Программная инженерия» и написании выпускной квалификационной работы.

4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ ОБУЧАЮЩИХСЯ

Результаты освоения образовательной программы (компетенции обучающихся) устанавливаются в соответствии с федеральным государственным образовательным стандартом по направлению подготовки и профессиональными стандартами, соответствующими профессиональной деятельности выпускников, а также на основе анализа требований работодателей, предъявляемых к выпускникам. Планируемые результаты освоения дисциплины (знания, умения, навыки) соотносятся с установленными в образовательной программе индикаторами достижения компетенций, что обеспечивает формирование у обучающихся запланированных результатов освоения образовательной программы.

Шифр и название компетенции	Индикаторы компетенции	Планируемые результаты обучения по дисциплине
УК-8 Способен создавать и	УК-8.3. - Обеспечивает	Знать: - нормативно-правовые основы

поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	персональную информационную безопасность в цифровой среде, в том числе средствами криптографии	информационной безопасности в Российской Федерации; - международные и отечественные стандарты, регламентирующие профессиональную деятельность в области информационной безопасности; Уметь: - разрабатывать политику информационной безопасности программных продуктов и организаций с опорой на нормативно-правовые документы Владеть: - навыками документирования инцидентов и процессов информационной безопасности.
ПК-1. Способен выявлять информационные потребности пользователей и составлять техническое задание на разработку цифрового программного продукта	ПК-1.1. - Проводит обследование организаций, выявляет информационные потребности заказчика, используя цифровые инструменты и облачные решения для сбора и анализа данных	Знать: - требования безопасности к информационным системам; - программно-аппаратное, организационное, инженерно-техническое обеспечение защиты информации Уметь: - проводить анализ предметной области и выявлять информационные угрозы в организации; - разрабатывать концептуальное решение по обеспечению защиты информации в разрабатываемых системах Владеть: - навыками анализа информационных рисков; - навыками оформления документов на разработку информационной системы в части информационной безопасности в соответствии с требованиями
ПК-5 Способен обеспечивать качество работы цифрового программного продукта	ПК-5.4. - Обеспечивает безопасность работы цифрового программного продукта	Знать: - способы и методы обеспечения информационной безопасности в компьютерных сетях, удаленные угрозы и атаки, основы криптографической защиты информации, способы управления инцидентами информационной безопасности; - нормативно-правовые основы информационной безопасности в Российской Федерации, международные и отечественные стандарты, регламентирующие

		профессиональную деятельность в области информационной безопасности; - возможные риски, возникающие при работе с информационными системами в организации; Уметь: - применять цифровые и отраслевые технологии для проведения анализа рисков работы информационных систем; Владеть: - навыками анализа рисков работы цифровых программных продуктов; - навыками использования инструментальных средств защиты информации в ходе профессиональной деятельности; - навыками управления инцидентами информационной безопасности
--	--	--

5. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ

Семестр изучения: 6

Раздел, модуль	Подраздел, тема	Виды учебной работы					Промежуточна я аттестация в часах	Форма текущего контроля	Формир уемые компете нции
		Контактная работа (в часах)			Самостоятельная работа				
		Лекц ии	Практиче ские занятия	КСР (пропо рцион ально темам)	в часах	формы организации самостоятельной работы			
	Тема 1. Основы защиты информации в web-приложениях	1		-	6	Повторение лекционного материала, подготовка к практическим занятиям	-	Устный опрос	ПК-1.1 ПК-5.4
	Тема 2. Нормативное регулирование информационной безопасности	1	2	-	10	Повторение лекционного материала, подготовка к практическим занятиям	-	Устный опрос	УК-8.3
	Тема 3. Виды информационных угроз	1	2	-	10	Повторение лекционного материала, подготовка к практическим занятиям	-	Устный опрос	ПК-1.1 ПК-5.4
	Тема 4. Информационная безопасность в компьютерных сетях	1	2	-	10	Повторение лекционного материала, подготовка к практическим занятиям. Выполнение курсовой работы.	-	Устный опрос	ПК-1.1 ПК-5.4
	Тема 5. Программно-аппаратное обеспечение	1	2	-	10	Повторение лекционного материала, подготовка к практическим занятиям	-	Проверка выполненных работ	УК-8.3 ПК-1.1 ПК-5.4

	информационной безопасности					Выполнение курсовой работы.			
	Тема 6. Криптографическая защита информации	1	4		10	Повторение лекционного материала, подготовка к практическим занятиям Выполнение курсовой работы.		Устный опрос	УК-8.3 ПК-5.4
	Тема 7. Организационное обеспечение защиты информации	1	4		10	Повторение лекционного материала, подготовка к практическим занятиям Выполнение курсовой работы.		Устный опрос	УК-8.3 ПК-1.1
	Тема 8. Инженерно-техническое обеспечение защиты информации	1	4		10	Повторение лекционного материала, подготовка к практическим занятиям Выполнение курсовой работы.		Проверка выполненных работ	УК-8.3 ПК-1.1 ПК-5.4
	Тема 9. Системы управления информационной безопасностью	-	4	-	10	Повторение лекционного материала, подготовка к практическим занятиям Выполнение курсовой работы.	-	Устный опрос	УК-8.3 ПК-1.1 ПК-5.4
	Тема 10. Организационное управление инцидентами информационной безопасностью	-	4	-	10	Подготовка к практическим занятиям Выполнение курсовой работы.	-	Проверка выполненных работ	УК-8.3 ПК-1.1 ПК-5.4
Зачет, защита курсовой работы		-	-	-	4	Подготовка к промежуточной аттестации		-	-
Всего		8	28	8	100	-			

	144		
--	-----	--	--

6. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Введение в информационную безопасность, уровни ее обеспечения

Проблемы информационных войн и информационной безопасности общества. Понятие «информационная безопасность». Составляющие информационной безопасности (доступность, целостность, конфиденциальность информации). Уровни формирования режима информационной безопасности. Стратегии построения системы защиты информации. Административный уровень обеспечения информационной безопасности.

Тема 2. Стандарты информационной безопасности

Нормативно-правовые основы информационной безопасности в РФ. Стандарты информационной безопасности. Требования безопасности к информационным системам. Документы по оценке защищенности автоматизированных систем в РФ. Федеральная служба по техническому и экспортному контролю. Стандарты информационной безопасности распределенных систем.

Тема 3. Информационные угрозы

Классы угроз информационной безопасности. Каналы несанкционированного доступа к информации. Технические каналы утечки информации. Наиболее распространенные угрозы нарушения доступности информации. Основные угрозы нарушения целостности и конфиденциальности информации.

Тема 4. Информационная безопасность в компьютерных сетях

Особенности обеспечения информационной безопасности в компьютерных сетях. Сетевые модели передачи данных. Модель взаимодействия открытых систем. Классификация удаленных угроз в вычислительных сетях. Типовые удаленные атаки и их характеристика.

Тема 5. Программно-аппаратное обеспечение информационной безопасности

Вредоносные программы и антивирусные программы. Идентификация и аутентификация. Методы разграничения доступа. Регистрация и аудит событий информационных систем. Межсетевое экранирование. Технология виртуальных частных сетей.

Тема 6. Криптографическая защита информации

Современные технологии криптографии. Симметричные системы шифрования. Ассиметричные системы шифрования. Электронно-цифровая подпись. Управление криптографическими ключами.

Тема 7. Организационное обеспечение защиты информации

Задача организационного обеспечения защиты информации. Анализ и оценка угроз информационной безопасности объекта. Оценка ущерба вследствие противоправного раскрытия информации. Служба безопасности объекта. Организация и обеспечение режима секретности. Защита информации при авариях и иных экстремальных ситуациях. Обеспечение защиты информации при осуществлении международного научно-

технического и экономического сотрудничества.

Тема 8. Инженерно-техническое обеспечение защиты информации

Общие вопросы организации противодействия технической разведке. Классификация каналов утечки информации. Способы добывания информации. Классификация методов и средств инженерно-технической защиты информации и объектов информатизации. Методы защиты информации специальными средствами.

Тема 9. Системы управления информационной безопасностью

Архитектура систем управления информационной безопасностью. Принципы управления. ГОСТ Р ИСО/МЭК 27001-2006. Сертификация систем управления информационной безопасностью.

Тема 10. Организационное управление инцидентами информационной безопасностью

Методика управления инцидентами. Структура и задачи группы реагирования на инциденты, ее состав и процесс создания. Оценка эффективности реагирования на инциденты. Методы обнаружения инцидентов. Анализ аномалий информационной безопасности.

7. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩИХСЯ

В рамках данной учебной дисциплины обучающиеся выполняют самостоятельную внеаудиторную работу в виде: изучения теоретического материала по темам 1, 3, 6, 7, 9; изучения документов по теме 9; подготовки к практическим занятиям по темам 2, 4, 5, 8, 10; выполнения курсовой работы по выбранной теме, подготовки к ее защите и сдачи зачета.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

При изучении данной дисциплины используются следующие образовательные технологии:

Тема занятия	Вид образовательной технологии	Форма проведения занятия
Тема 1. Введение в информационную безопасность, уровни ее обеспечения	Традиционная технология	Лекция
Тема 2. Стандарты информационной безопасности	Традиционная технология	Лекция
		Практическое занятие
Тема 3. Информационные угрозы	Традиционная технология	Лекция
		Практическое занятие
Тема 4. Информационная безопасность в компьютерных сетях	Традиционная технология	Лекция
		Практическое занятие
Тема 5. Программно-аппаратное обеспечение информационной безопасности	Традиционная технология	Лекция
		Практическое занятие

Тема 6. Криптографическая защита информации	Традиционная технология	Лекция
		Практическое занятие
Тема 7. Организационное обеспечение защиты информации	Традиционная технология	Лекция
		Практическое занятие
Тема 8. Инженерно-техническое обеспечение защиты информации	Традиционная технология	Лекция
		Практическое занятие
Тема 9. Системы управления информационной безопасностью	Традиционная технология	Лекция
		Практическое занятие
Тема 10. Организационное управление инцидентами информационной безопасностью	Традиционная технология	Лекция
		Практическое занятие

9. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ДИСЦИПЛИНЕ

9.1. Формы контроля по дисциплине

Текущий контроль. В процессе изучения учебной дисциплины обучающиеся участвуют в устных теоретических опросах, выполняют практические задания. Результаты выполнения в устных опросах и выполнения практических заданий являются основанием для выставления оценок текущего контроля по данной учебной дисциплине. Выполнение всех практических заданий является обязательным для всех обучающихся. Обучающиеся, не выполнившие в полном объеме все задания, не допускаются к сдаче зачета по данной учебной дисциплине.

Промежуточная аттестация. Для контроля усвоения обучающимися данной дисциплины учебным планом предусмотрен зачет, который проводится в форме устного ответа на вопрос и выполнения практического задания, и защита курсовой работы, выполняемой в течение семестра.

9.2. Оценочные материалы (оценочные средства) для текущего контроля успеваемости и промежуточной аттестации по дисциплине

Текущий контроль.

Список вопросов для устного опроса

по теме «Введение в информационную безопасность, уровни ее обеспечения»

1. Теория защиты информации. Основные направления.
2. Обеспечение информационной безопасности и направления защиты.
3. Комплексность (целевая, инструментальная, структурная, функциональная, временная).
4. Требования к системе защиты информации.
5. Угрозы информации.

6. Виды угроз. Основные нарушения.
7. Характер происхождения угроз.
8. Источники угроз. Предпосылки появления угроз.
9. Система защиты информации.
10. Классы каналов несанкционированного получения информации.
11. Причины нарушения целостности информации.
12. Методы и модели оценки уязвимости информации.
13. Общая модель воздействия на информацию.

по теме «Стандарты информационной безопасности»

1. Общая модель процесса нарушения физической целостности информации.
2. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных.
3. Методологические подходы к оценке уязвимости информации.
4. Модель защиты системы с полным перекрытием.
5. Рекомендации по использованию моделей оценки уязвимости информации.
6. Допущения в моделях оценки уязвимости информации.
7. Методы определения требований к защите информации.
8. Факторы, обуславливающие конкретные требования к защите, обусловленные спецификой автоматизированной обработки информации.
9. Классификация требований к средствам защиты информации.
10. Требования к защите, определяемые структурой автоматизированной системы обработки данных.
11. Требования к защите, обуславливаемые видом защищаемой информации.
12. Требования, обуславливаемые взаимодействием пользователя с комплексом средств автоматизации.
13. Стандарт США «Критерии оценки гарантировано защищенных вычислительных систем в интересах министерства обороны США». Основные положения.
14. Руководящем документе Гостехкомиссии России «Классификация автоматизированных систем и требований по защите информации», выпущенном в 1992 году. Часть 1.
15. Классы защищенности средств вычислительной техники от несанкционированного доступа.

по теме «Информационные угрозы»

1. Дайте определение понятий «угроза», «уязвимость» и «атака».
2. Какие классификационные схемы угроз ИБ вам известны?
3. Перечислите источники угроз ИБ.

4. Назовите каналы проникновения в автоматизированную систему и утечки информации.
5. Какие факторы лежат в основе формирования модели нарушителя?
6. Каковы цели разработки моделей угроз и нарушителей?
7. В чем разница между нарушителем и злоумышленником?
8. Функции и задачи защиты информации. Основные положения механизмов непосредственной защиты и механизмы управления механизмами непосредственной защиты.
9. Методы формирования функций защиты.
10. События, возникающие при формировании функций защиты.

по теме «Информационная безопасность в компьютерных сетях»

1. В чем заключается основная причина предоставления служб пользователям?
2. Почему системы, к которым осуществляется доступ из внешней среды, не могут пользоваться полным доверием?
3. Почему протокол ICMP является важным компонентом сети?
4. Скольким внутренним системам разрешается использовать NTP в интернете?
5. Можно ли рассматривать использование SSH как реализацию VPN?
6. Почему пользовательские VPN требуют строгой аутентификации?
7. Может ли шифрование полностью защитить данные, передаваемые через VPN.
8. С чем необходимо комбинировать политику, чтобы обеспечить безопасность VPN?
9. Является ли один из типов межсетевых экранов более безопасным, нежели другой?
10. Что межсетевой экран прикладного уровня по умолчанию делает с внутренними адресами?
11. В чем сходство межсетевого экрана с фильтрацией пакетов и маршрутизатора?

по теме «Программно-аппаратное обеспечение информационной безопасности»

1. Понятие угрозы безопасности компьютерной системы. Методы «взлома» компьютерных систем.
2. Защита компьютерной системы от «взлома». Программные закладки.
3. Методы уничтожения информации, хранимой на энергонезависимых носителях. Уровни степеней надежности.
4. Защита программного обеспечения. Превентивные меры защиты.
5. Защита программного обеспечения. Средства собственной защиты.
6. Защита программного обеспечения. Средства защиты в составе вычислительной системы.
7. Защита программного обеспечения. Средства защиты с запросом информации.
8. Защита программного обеспечения. Средства активной защиты.

9. Защита программного обеспечения. Средства пассивной защиты.
10. Технология защиты информации на основе: электронных ключей, смарт-карт, персональных идентификаторов.
11. Принципы и методы создания защищенной операционной системы.
12. Цели и средства защиты информации. Типичный набор функциональных подсистем.
13. Основные принципы организации защиты информации от НСД и обеспечения ее конфиденциальности.

по теме «Криптографическая защита информации»

1. Что является предметом науки Криптография
2. Первая практическая реализация криптографии с открытым ключом
3. Использование в криптографии модели открытого текста, учитывающие зависимость букв текста от предыдущих букв.
4. В чем состоит принципиальное отличие нового стандарта ГОСТ Р 34.10 – 2001 на алгоритм формирования и проверки ЭЦП от старого ГОСТ Р 34.10 – 1994.
5. Основной принцип Кергоффса.
6. Что понимается под криптографическим протоколом
7. В чем состоит криптографическая задача обеспечения целостности.
8. Методы с целью обеспечения аутентификации

по теме «Организационное обеспечение защиты информации»

1. Модель защиты системы с полным перекрытием.
2. Рекомендации по использованию моделей оценки уязвимости информации.
3. Допущения в моделях оценки уязвимости информации.
4. Методы определения требований к защите информации.
5. Факторы, обуславливающие конкретные требования к защите, обусловленные спецификой автоматизированной обработки информации.
6. Классификация требований к средствам защиты информации.
7. Требования к защите, определяемые структурой автоматизированной системы обработки данных.
8. Требования к защите, обуславливаемые видом защищаемой информации.
9. Требования, обуславливаемые взаимодействием пользователя с комплексом средств автоматизации.

по теме «Инженерно-техническое обеспечение защиты информации»

1. Стратегии защиты информации.
2. Способы и средства защиты информации.
3. Способы «абсолютной системы защиты».
4. Архитектура систем защиты информации. Требования.

5. Общеметодологических принципов архитектуры системы защиты информации.
6. Построение средств защиты информации.
7. Ядро системы защиты.
8. Семирубежная модель защиты.

по теме «Системы управления информационной безопасностью»

1. Анализ рисков
2. Политика информационной безопасности
3. Концепция информационной безопасности
4. Доступ в информационные системы. Политика доступа. Физический доступ.
5. Построение сети. Удаленный доступ.
6. Инциденты. Активы, что требуется защитить.
7. Меры безопасности в контексте ISO 27001
8. Эффективность применяемых методов обеспечения безопасности
9. Административный уровень защиты информации. Задачи различных уровней управления в решении задачи обеспечения информационной безопасности.
10. Процедурный уровень обеспечения безопасности. Авторизация пользователей в информационной системе.

по теме «Организационное управление инцидентами информационной безопасностью»

1. Понятие инцидента информационной безопасности
2. Место управления инцидентами в общей системе информационной безопасности
3. Особенности управления событиями безопасности
4. Процедура управления информационной безопасностью
5. Устранение причин и последствий события, его расследование
6. Превентивные меры, изменения стандартов и ликвидация последствий

Промежуточная аттестация.

Перечень примерных тем для курсовой работы

Наименование объекта защиты информации:

1. Одиночно стоящий компьютер в бухгалтерии.
2. Сервер.
3. Почтовый сервер.
4. Веб-сервер.
5. Компьютерная сеть Академии.
6. Одно ранговая локальная сеть без выхода в Интернет.
7. Одно ранговая локальная сеть с выходом в Интернет.
8. Сеть с выделенным сервером без выхода в Интернет.
9. Сеть с выделенным сервером с выхода в Интернет.

10. Телефонная база данных (содержащая и информацию ограниченного пользования) в твердой копии и на электронных носителях.
11. Телефонная сеть.
12. Средства телекоммуникации (радиотелефоны, мобильные телефоны).
13. Банковские операции (внесение денег на счет и снятие).
14. Операции с банковскими пластиковыми карточками.
15. Компьютер, хранящий конфиденциальную информацию о сотрудниках предприятия.
16. Компьютер, хранящий конфиденциальную информацию о разработках предприятия.
17. Материалы для служебного пользования на твердых носителях в производстве.

Список вопросов для подготовки к зачету

1. Проблемы информационных войн и информационной безопасности общества.
2. Понятие информационной безопасности и ее составляющие.
3. Уровни информационной безопасности.
4. Стратегии обеспечения защиты информации.
5. Нормативно-правовые основы информационной безопасности в РФ. Стандарты информационной безопасности.
6. Требования безопасности к информационным системам. Документы по оценке защищенности автоматизированных систем в РФ.
7. Стандарты информационной безопасности распределенных систем.
8. Классы угроз информационной безопасности.
9. Каналы несанкционированного доступа и утечки информации.
10. Наиболее распространенные угрозы нарушения доступности информации, нарушения целостности и конфиденциальности информации.
11. Особенности обеспечения информационной безопасности в компьютерных сетях. Сетевые модели передачи данных. Модель взаимодействия открытых систем.
12. Классификация удаленных угроз в вычислительных сетях. Типовые удаленные атаки и их характеристика.
13. Вредоносные программы и антивирусные программы.
14. Идентификация и аутентификация. Методы разграничения доступа.
15. Регистрация и аудит событий информационных систем.
16. Межсетевое экранирование.
17. Технология виртуальных частных сетей.
18. Симметричные системы шифрования. Ассиметричные системы шифрования.
19. Электронно-цифровая подпись.
20. Управление криптографическими ключами.
21. Задача организационного обеспечения защиты информации.

22. Анализ и оценка угроз информационной безопасности объекта. Оценка ущерба вследствие противоправного раскрытия информации.
23. Служба безопасности объекта. Организация и обеспечение режима секретности.
24. Защита информации при авариях и иных экстремальных ситуациях.
25. Обеспечение защиты информации при осуществлении международного сотрудничества.
26. Классификация методов и средств инженерно-технической защиты информации и объектов информатизации.
27. Методы защиты информации специальными средствами.
28. Архитектура систем управления информационной безопасностью.
29. Принципы управления информационной безопасностью.
30. Стандарты в области менеджмента информационной безопасности. Сертификация систем управления информационной безопасностью.
31. Методы обнаружения инцидентов.
32. Управление инцидентами информационной безопасности.
33. Оценка эффективности реагирования на инциденты.

Порядок проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине для инвалидов и лиц с ОВЗ предусмотрен Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся.

10. РЕСУРСНАЯ СОСТАВЛЯЮЩАЯ

Для проведения занятий лекционного типа по данной дисциплине используются аудитории с медиа-оборудованием (проектор, экран, ноутбук) и учебной мебелью.

Для проведения занятий семинарского типа (практических занятий) по данной дисциплине используются компьютерные классы, оснащенные компьютерами с доступом в Интернет и необходимым программным обеспечением.

Для самостоятельной работы обучающихся используется помещение для самостоятельной работы обучающихся, оснащенное компьютерами с необходимым программным обеспечением и доступом в Интернет и электронную информационно-образовательную среду вуза.

Для проведения контроля самостоятельной работы по данной дисциплине используются компьютерные классы, оснащенные компьютерами с доступом в Интернет и необходимым программным обеспечением.

Для проведения текущего контроля успеваемости и промежуточной аттестации по данной дисциплине используются компьютерные классы, оснащенные компьютерами с доступом в Интернет и необходимым программным обеспечением.

Перечень лицензионного программного обеспечения

№ п/п	Наименование	Тип ресурса
1	Microsoft Office	Сублицензионный договор АО «СофтЛайн Трейд» № /131 от 10.07.2020. Период действия договора и лицензий бессрочный. Лицензионное соглашение Microsoft - Open Value Subscription для решений Education Solutions №V8265046
2	Microsoft Windows	
3	КонсультантПлюс - справочно-правовая система «Комментарии законодательства» сетевая (смарт-комплект Оптимальный - отечественного производства)	Лицензионный договор ООО «Консультант Плюс Тольятти» договор № 251 от 01.01.2024 (лицензия бессрочная, договор ежегодно продлеваемый)
4	Антивирус Касперского 10 для Windows Workstations (Kaspersky Endpoint Security для бизнеса – стандартный Russian Edition, отечественного производства)	Сублицензионный договор АО «СофтЛайн Трейд» №Tr000947217 от 04.12.2025 срок действия 10.02.2026 - 11.02.2028. Тип лицензии - проприетарная (17E0-251210-090335-980-xxxx)

Перечень свободно распространяемого программного обеспечения

1. Браузеры Yandex, Google Chrome.
2. КонсультантПлюс – интернет-версия постоянно доступной справочно-правовой системы отечественного производства.

В соответствии с Положением о создании специальных условий для инвалидов и лиц с ОВЗ информационно-технологическая база образовательного процесса предусматривает использование материально-технических средств с учетом различных нозологий инвалидов и лиц с ОВЗ.

11. ЛИТЕРАТУРА

11.1. Основная литература

№ п/п	Библиографическое описание	Тип издания	Количество в библиотеке
1.	Баранова, Е. К. Информационная безопасность и защита информации : учеб. пособие / Е. К. Баранова, А. В. Бабаш. - 5-е изд., перераб. и доп. - Москва : Инфра-М, 2026. - 383 с. - ISBN 978-5-16-114639-2 (online). - ЭБС Знаниум. - URL: https://znanium.ru/catalog/document?id=477891	учебное пособие	ЭБС
2.	Защита информации : учеб. пособие / А. П. Жук [и др.]. - 3-е изд. - Москва : Инфра-М, 2024. - 399 с. - ISBN 978-5-16-106478-8 (online). - ЭБС Знаниум. - URL: https://znanium.ru/catalog/document?id=443251	учебное пособие	ЭБС

11.2. Дополнительная литература

1. Информационный мир XXI века. Криптография - основа информационной безопасности / под ред. Э. А. Болелова. - 4-е изд. - Москва : Дашков и К, 2022. - 125 с. - ISBN 978-5-394-04804-3. - ЭБС Знаниум. - URL: <https://znanium.ru/catalog/document?id=431477>
2. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И. С. Клименко. - 5-е изд., перераб. и доп. - Москва : Инфра-М, 2026. - 179 с. - ISBN 978-5-16-108124-2 (online). - ЭБС Знаниум. - URL: <https://znanium.ru/catalog/document?id=476654>
3. Информационная безопасность объектов : метод. указания к выполнению курсовой работы / сост. Э. Р. Жолондиевский. - Тольятти : ТАУ, 2026. - Формат PDF. - 600 КБ, 28 с. - ISBN нет. - Электронная библиотека ТАУ. - URL: <http://83.234.207.58/MarcWeb2/MObjects.asp>

Периодические издания:

1. Открытые системы. СУБД : журнал. – УБД ИВИС. – URL: <https://eivis.ru/browse/publication/64072>
2. Программные продукты и системы: международный научно-практический журнал. – ЭБС Знаниум. - URL : <https://znanium.ru/catalog/magazines/issues?ref=f9bfbd0e-239e-11e4-99c7-90b11c31de4c>

11.3. Современные профессиональные базы данных, информационные справочные системы, электронные библиотечные системы:

1. Znanium: электронно-библиотечная система. – URL: <http://znanium.ru>.
2. eLIBRARY.RU: научная электронная библиотека. – URL: <https://elibrary.ru/>.
3. Цифровая библиотека IPRsmart. – URL: <https://www.iprbookshop.ru/>.
4. Консультант плюс: справочно-правовая система. – URL: T:\consultantplus\cons.exe.
5. УБД ИВИС. – URL : <https://eivis.ru/basic/details>.
6. Электронная библиотека ТАУ. – URL: <http://83.234.207.58/MarcWeb2/Default.asp>.

12. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Дисциплина «Информационная безопасность» предполагает посещение обучающимися лекций, выполнение практических заданий, большой объем самостоятельной работы. По дисциплине помимо традиционной лекции, на которой преподаватель освещает ключевые вопросы темы, также проводятся: лекция информационного характера, предполагающая объяснения преподавателя с иллюстративным изложением материала. На лекциях преподаватель может проводить устный опрос в целях выяснения степени усвоения предыдущего материала, а также предполагается выступление обучающихся с докладами по отдельным теоретическим вопросам. Данные формы работы являются элементами текущего контроля и оцениваются преподавателем. Все это предполагает подготовку и самостоятельное изучение обучающимися теоретического материала по заявленной преподавателем теме.

Выполненные практические работы проверяются преподавателем непосредственно в аудитории либо одним из следующих способов: сохранение в электронной информационно-образовательной среде, отправка преподавателю на почтовый ящик. При отправке преподавателю выполненной работы по почте обучающемуся следует обеспечить личную идентификацию. Как правило, в теме или тексте письма указывается курс, ФИО обучающегося, дисциплина, тема, по которой выполнена работы. Некоторые практические задания не могут быть сделаны только в рамках выделенного объема контактной работы (в аудитории) и «доделываются» в часы самостоятельной работы. Сдача таких работ на проверку осуществляется теми же самыми способами, что и по окончании практических занятий. Результаты проверки выполненных работ доводятся до сведения обучающегося во время аудиторных занятий и/или в часы КСР.

В ходе освоения дисциплины обучающиеся применяют изученные материалы для моделирования информационной безопасности конкретного объекта. Тема курсовой работы выбирается обучающимся из списка предложенных преподавателем, либо обучающийся предлагает свою тему. Курсовая работа состоит из теоретического

исследования в форме эссе на определенную тему и решение задачи, подтверждающей полученные компетенции обучающимся по изучаемой дисциплине. Содержание курсовой работы должно свидетельствовать о достаточно высокой теоретической подготовке обучающегося и о наличии у автора необходимых знаний по теме работы. Работа должна иметь правильно составленную библиографию, логичную структуру, обеспечивающую раскрытие темы. Курсовая работа должна быть написана грамотно, хорошим литературным и профессиональным языком, иметь правильно оформленный инструментальный аппарат. В теоретической части курсовой работы следует описать современное состояние проблемы информационной безопасности в целом, результаты анализа состояния объекта защиты, потенциальные угрозы. Содержание этой части должно показать степень ознакомления обучающегося с поставленной проблемой и современным научно-теоретическим уровнем исследований в данной области, а также умение работать с фактическим материалом, сжато и аргументированно формулировать задачи и результаты исследований и давать обоснованные рекомендации по решению выявленных проблем. В практической части должны быть приведены конкретные мероприятия по информационной защите объекта. Объем курсовой работы составляет 30 – 35 страниц.

Для выполнения курсовой работы и самостоятельной работы по данной дисциплине в домашних условиях (за пределами Академии) обучающемуся необходим персональный компьютер (планшет) и пакет прикладных программ Microsoft Office (не ниже 10 версии). Консультации по выполнению практических работ и курсовой работы, обсуждение допущенных ошибок осуществляется во время КСР на кафедре прикладной информатики или в аудитории по расписанию. Консультации могут осуществляться также посредством асинхронного (почта, ЭИОС) и синхронного (zoom, сети) коммуникационного взаимодействия по предварительной договоренности с преподавателем.

По окончании дисциплины обучающийся должен защитить курсовую работу: представить оформленную пояснительную записку и ответить на вопросы преподавателя по существу разработки. Для сдачи зачета обучающемуся необходимо подготовить ответы на теоретические вопросы к зачету и повторить решение основных практических задач.

ЛИСТ СОГЛАСОВАНИЯ

Составил:

Н.А. Иванова, ст.преп.



(подпись)

Заведующий кафедрой

Н.Б. Стрекалова, д.п.н., доцент



(подпись)

Заведующий выпускающей кафедрой

Н.Б. Стрекалова, д.п.н., доцент



(подпись)

Директор БИК

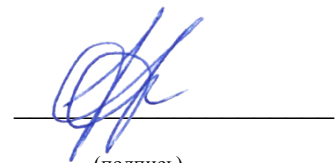
О.В. Балакина



(подпись)

Начальник ООУП

С.В. Фирсова



(подпись)