МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Алтайский государственный педагогический университет»
(ФГБОУ ВО «АлтГПУ»)

УТВЕРЖДАЮ
проректор по образовательной деятельности

_____С.П. Волохов

Информационная безопасность

рабочая программа дисциплины (модуля)

Закреплена за кафедрой	**Информационных технологий**
Учебный план	ПИИОБП09.03.03-2023.plx 09.03.03 Прикладная информатика
Квалификация	**бакалавр**
Форма обучения	**очная**
Общая трудоемкость	**3 ЗЕТ**

Часов по учебному плану	108	Виды контроля в семестрах:
в том числе:		зачеты 4
аудиторные занятия	48	
самостоятельная работа	54	

Программу составил(и):
ктн, Доц., Скурыдина Е.М. _____

Рабочая программа дисциплины
Информационная безопасность

разработана на основании ФГОС ВО - бакалавриат по направлению подготовки 09.03.03 Прикладная информатика (приказ Минобрнауки России от 19.09.2017 г. № 922)

составлена на основании учебного плана 09.03.03 Прикладная информатика (Уровень: бакалавриат; квалификация: бакалавр), утвержденного Учёным советом ФГБОУ ВО «АлтГПУ» от 24.04.2023, протокол № 9.

Рабочая программа одобрена на заседании кафедры
Информационных технологий

Протокол № 7 от 18.02.2023 г.
Срок действия программы: 2022-2026 уч.г.
Зав. кафедрой Абрамкин Геннадий Петрович

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**4 (2.2)**		Итого	
Недель	18 2/6			
Вид занятий	УП	РП	УП	РП
Лекции	24	24	24	24
Лабораторные	24	24	24	24
Контроль самостоятельной работы	6	6	6	6
Итого ауд.	48	48	48	48
Контактная работа	54	54	54	54
Сам. работа	54	54	54	54
Итого	108	108	108	108

1.1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1.1	изучение основ информационной безопасности, научить правильно проводить анализ угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности, изучение методов и средств обеспечения информационной безопасности, изучить криптографические методы; формирование представления о видах и применимости компьютерной безопасности для решения педагогических задач, применению их в профессиональной деятельности. Другой целью является формирование системы понятий, знаний, умений и навыков в области информационной безопасности, включающего в себя методы проектирования, анализа и создания программных продуктов, основанные на использовании методологии информационной безопасности.

1.2. ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.2.1	сформировать целостное представление о принципах информационной безопасности;
1.2.2	дать представление о месте и роли информационной безопасности в решении прикладных задач с использованием компьютера;
1.2.3	сформировать знания, умения и навыки анализа и проектирования математических и информационных моделей реальных задач криптографии;
1.2.4	овладеть умениями и навыками решения типовых задач информационной безопасности;
1.2.5	овладеть умениями и навыками использования анализ угроз информационной безопасности и методов и средств обеспечения информационной безопасности для решения практических задач.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Алгоритмизация и программирование
2.1.2	Информационные системы и технологии
2.1.3	Операционные системы
2.1.4	Архитектура компьютера
2.1.5	Вычислительные системы, сети и телекоммуникации
2.1.6	Программное обеспечение ЭВМ
2.1.7	Математика
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Производственная практика: преддипломная практика

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ОПК-4.1: Знает основные стандарты оформления технической документации на раз-личных стадиях жизненного цикла информационной системы
ОПК-4.2: Умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы
ОПК-4.3: Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы
ОПК-3.1: Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
ОПК-3.2: Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно¬коммуникационных технологий и с учетом основных требований информационной безопасности
ОПК-3.3: Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно¬исследовательской работе с учетом требований информационной безопасности
ОПК-2.1: Знает современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности
ОПК-2.2: Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности

ОПК-2.3: Владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	современные информационные технологии и программные средства, в том числе отечественного производства при решении задач обеспечения информационной безопасности
3.1.2	принципы, методы и средства решения стандартных задач обеспечения информационной безопасности на основе информационной и библиографической культуры с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности
3.1.3	основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы с учетом задач обеспечения информационной безопасности
3.2	**Уметь:**
3.2.1	выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач обеспечения информационной безопасности.
3.2.2	решать стандартные задачи обеспечения информационной безопасности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
3.2.3	применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы
3.3	**Владеть:**
3.3.1	навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач обеспечения информационной безопасности
3.3.2	навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.
3.3.3	навыками составления технической документации на различных этапах жизненного цикла информационной системы

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература
	Раздел 1. Основные определения информационной безопасности. Информационная безопасность в системе национальной безопасности России.				
1.1	Информационная безопасность в системе национальной безопасности России. /Лек/	4	2	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-4.1 ОПК-4.2 ОПК-4.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
1.2	Содержание и задачи процесса управления информационной безопасностью /Лаб/	4	2	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-4.1 ОПК-4.2 ОПК-4.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6

1.3	Государственная информационная политика. /Ср/	4	4	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-4.1 ОПК-4.2 ОПК-4.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
1.4	Информационная безопасность в системе национальной безопасности Российской Федерации. /Лек/	4	4	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-4.1 ОПК-4.2 ОПК-4.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
	Раздел 2. Информационная война, методы и средства ее ведения.				
2.1	Вредоносное программное обеспечение. Примеры угроз доступности. /Ср/	4	4	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-4.1 ОПК-4.2 ОПК-4.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
2.2	Основные угрозы целостности. /Ср/	4	8		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
2.3	Основные угрозы конфиденциальности. /Лаб/	4	4	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-4.1 ОПК-4.2 ОПК-4.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
2.4	Угрозы информационной безопасности. Классификация и анализ угроз. /Лек/	4	4	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-4.1 ОПК-4.2 ОПК-4.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
	Раздел 3. Критерии защищенности компьютерных систем.				
3.1	Основные теории защиты информации. /Ср/	4	6	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-4.1 ОПК-4.2 ОПК-4.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6

3.2	Модели безопасности. /Ср/	4	6	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-4.1 ОПК-4.2 ОПК-4.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
3.3	Управление рисками. /Лаб/	4	2	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-4.1 ОПК-4.2 ОПК-4.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
3.4	Методы формирования функций защиты. /Лаб/	4	2	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-4.1 ОПК-4.2 ОПК-4.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
3.5	Стратегии защиты информации. /Лаб/	4	2	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-4.1 ОПК-4.2 ОПК-4.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
3.6	Оценка уязвимости информации. /Лек/	4	2	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-4.1 ОПК-4.2 ОПК-4.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
3.7	Система с полным перекрытием. /Лек/	4	2	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-4.1 ОПК-4.2 ОПК-4.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
	Раздел 4. Защита информации, обрабатываемой в информационных системах.				

4.1	Криптографические хеш-функции. /Ср/	4	4	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-4.1 ОПК-4.2 ОПК-4.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
4.2	Обеспечиваемая шифром степень защиты. /Ср/	4	4	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-4.1 ОПК-4.2 ОПК-4.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
4.3	Криптоанализ и атаки на криптосистемы. /Ср/	4	4	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-4.1 ОПК-4.2 ОПК-4.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
4.4	Платформы. Сеть Фейштеля. /Ср/	4	4	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-4.1 ОПК-4.2 ОПК-4.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
4.5	Дифференциальный и линейный криптоанализ. /Ср/	4	4	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-4.1 ОПК-4.2 ОПК-4.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
4.6	Используемые критерии при разработке алгоритмов. /Лаб/	4	6	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-4.1 ОПК-4.2 ОПК-4.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
4.7	Криптография. /Лек/	4	2	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-4.1 ОПК-4.2 ОПК-4.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
4.8	Криптоанализ. /Лек/	4	2		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6

	Раздел 5. Защита автоматизированных системам (АС) и средств вычислительной техники (СВТ) от внешнего электромагнитного воздействия.				
5.1	Программные средства поддержки процессов управления информационной безопасности. /Ср/	4	6	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-4.1 ОПК-4.2 ОПК-4.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
5.2	Программные средства автоматизации процедур управления информационной безопасности и анализа политики информационной безопасности. /Лаб/	4	6	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-4.1 ОПК-4.2 ОПК-4.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
5.3	Генераторы электромагнитных импульсов: эффекты, возникающие от внешнего электромагнитного воздействия на АС и СВТ. /Лек/	4	3	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-4.1 ОПК-4.2 ОПК-4.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
5.4	Методы защиты АС и СВТ от внешнего электромагнитного воздействия»: экранирование, создание преднамеренных помех, кодировка сигнала. /Лек/	4	3	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-4.1 ОПК-4.2 ОПК-4.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
5.5	Зачет /Зачёт/	4	0	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-4.1 ОПК-4.2 ОПК-4.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Перечень индикаторов достижения компетенций, форм контроля и оценочных средств

ОПК-2.1.Знает современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.
ОПК-2.2.Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.
ОПК-2.3.Владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности
ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности.
ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационнокоммуникационных технологий и с учетом основных

требований информационной безопасности.
ОПК-3.3. Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научноисследовательской работе с учетом требований информационной безопасности
ОПК-4.1. Знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.
ОПК-4.2. Умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.
ОПК-4.3. Владеет навыками составления технической документации на различных этапах жизненного цикла информационной систем

5.2. Технологическая карта достижения индикаторов

Семестр 4
Лекционные занятия 20 баллов
Лабораторные занятия 40 баллов
Самостоятельная работа 20 баллов
Зачет 20 баллов

5.3. Формы контроля и оценочные средства

Тестовые задания
1. В число граней, позволяющих структурировать средства достижения информационной безопасности, входят:
a) меры обеспечения целостности;
b) административные меры;
c) меры обеспечения конфиденциальности.

2. Дублирование сообщений является угрозой:
a) доступности;
b) конфиденциальности;
c) целостности.

3. Вредоносное ПО Melissa подвергает атаке на доступность:
a) системы электронной коммерции;
b) геоинформационные системы;
c) системы электронной почты.

4. Выберите вредоносную программу, которая открыла новый этап в развитии данной области.
a) Melissa.
b) Bubble Boy.
c) ILO VE YOU.

5. Самыми опасными источниками внутренних угроз являются:
a) некомпетентные руководители;
b) обиженные сотрудники;
c) любопытные администраторы.

6. Среди нижеперечисленных выделите главную причину существования многочисленных угроз информационной безопасности.
a) просчеты при администрировании информационных систем;
b) необходимость постоянной модификации информационных систем;
c) сложность современных информационных систем.

7. Агрессивное потребление ресурсов является угрозой:
a) доступности
b) конфиденциальности
c) целостности

Тематика докладов, сообщений:
1. Разработка комплексной системы защиты информации предприятия.
2. Защита облачных сервисов в системах электронного документооборота.
3. Программный комплекс ограничения функциональности условно-бесплатного программного обеспечения, распространяемого в исходных кодах.
4. Правовые основы защиты информации в РФ.
5. Методы и средства удалённого доступа.
6. Автоматизация управления производственным предприятием и анализ его эффективности.
7. Гражданско-правовая защита информации конфиденциального характера.
8. Разработка информационной системы документооборота.
9.Актуальность проблемы информационной безопасности.
10.Понятия и определения в информационной безопасности.

11. Основные составляющие информационной безопасности
12.Анализ способов нарушений информационной безопасности.
13.Использование защищенных компьютерных систем.
14.Основные определения и критерии классификации угроз.
15.Основные закономерности возникновения и классификация угроз информационной безопасности.

Задания для лабораторных работ:
1. Используя основные положения части 4, главы 70 Гражданского кодекса РФ решить следующую ситуационную задачу: Гражданин Алексеев создал инструментальное программное средство для работы с трехмерной компьютерной графикой под названием «Alex 3D» и зарегистрировал на него свои права. 20.09.2012 этот гражданин заключил договор с компанией «MoscowTechnology» и передал свои имущественные права на распространение своего программного продукта сроком на один год. После заключения договора компания «MoscowTechnology» распространила версию программы «Alex 3D» с предварительной модификацией данного программного продукта без ведома автора. Имеет ли место в данной ситуации нарушение авторского права гражданина Алексеева? 2. Зашифровать пословицу или поговорку тремя методами: методом Цезаря, методом Гронсфельда и методом Вижинера: «Уменье работать дороже золота»

Вопросы для самоконтроля:
1. Сканеры портов. Обзор. Возможности.
2. Применение сканеров портов.
3. Криптографические протоколы. Применение, характеристики.
4. Причины существования дыр в системе безопасности.
5. Сканеры уязвимостей. Возможности, ограничения.
6. Сетевые анализаторы. Выбор расположения.
7. Практическое применение сетевых анализаторов.
8. Системы обнаружения вторжений. Выбор расположения системы обнаружения.
9. Классификация firewall’ов и определение политики firewall’а.
10. Политика безопасности современных операционных систем.
11. Электронная цифровая подпись

Вопросы к зачету:
1. Информационная безопасность.
2. Основные определения.
3. Содержание и задачи процесса управления информационной безопасностью информационная безопасность в системе национальной безопасности Российской Федерации.
4. Государственная информационная политика.
5. Угрозы информационной безопасности.
6. Классификация и анализ угроз.
7. Вредоносное программное обеспечение.
8. Примеры угроз доступности.
9. Основные угрозы целостности.
10. Основные угрозы конфиденциальности.
11. Оценка уязвимости информации.
12. Система с полным перекрытием.
13. Управление рисками.
14. Основные теории защиты информации.
15. Модели безопасности.
16. Методы формирования функций защиты.
17. Стратегии защиты информации.
18. Методы и системы защиты информации.
19. Криптография.
20. Криптоанализ. Криптографические хеш-функции.
21. Обеспечиваемая шифром степень защиты.
22. Криптоанализ и атаки на криптосистемы.
23. Платформы. Сеть Фейштеля.
24. Дифференциальный и линейный криптоанализ.
25. Используемые критерии при разработке алгоритмов.
26. Криптографические стандарты DES и ГОСТ 28147–89.
27. Алгоритм DES. Шифрование. Дешифрование. Проблемы DES.
28. Контроль целостности. 29. Генераторы электромагнитных импульсов: эффекты, возникающие от внешнего электромагнитного воздействия на АС и СВТ.
30. Методы защиты АС и СВТ от внешнего электромагнитного воздействия»: экранирование, создание преднамеренных помех, кодировка сигнала.
31. Программные средства автоматизации процедур управления информационной безопасности и анализа политики информационной безопасности.
32. Программные средства поддержки процессов управления информационной безопасности.
33. Пути и каналы утечки информации и их обобщенная модель.

34. Классификация каналов утечки информации.
35. Угрозы доступности.
36. Угрозы целостности.
37. Угрозы конфиденциальности.
38. Методы сбора сведений для вторжения в сеть.
39. Обобщенная модель нарушителя безопасности информации.
40. Распределенные атаки на отказ от обслуживания.
41. Вирусы и механизмы их работы.
42. Классификации вирусов. Среда обитания. Способ заражения среды обитания. Деструктивная возможность. Особенности алгоритма вируса.
43. Методы обнаружения и удаления вирусов.
44. Антивирусная стратегия. Антивирусная защита.
45. Основные функции современных антивирусов.
46. Типовая структура корпоративной сети.
47. Способы НСД к каналам передачи данных.
48. Основные пути обеспечения безопасности информации.

5.4. Оценка результатов обучения в соответствии с индикаторами достижения компетенций

Неудовл.: не достигнут

Удовл. Пороговый уровень: Знает современные информационные технологии и программные средства, в том числе отечественного производства при решении задач обеспечения информационной безопасности; принципы, методы и средства решения стандартных задач обеспечения информационной безопасности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий. Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач обеспечения информационной безопасности. Владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач обеспечения информационной безопасности.

Хорошо. Базовый уровень: Знает современные информационные технологии и программные средства, в том числе отечественного производства при решении задач обеспечения информационной безопасности; принципы, методы и средства решения стандартных задач обеспечения информационной безопасности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы с учетом задач обеспечения информационной безопасности. Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач обеспечения информационной безопасности; решать стандартные задачи обеспечения информационной безопасности на основе информационной и библиографической культуры с применением информационнокоммуникационных технологии. Владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач обеспечения информационной безопасности; навыками составления технической документации на различных этапах жизненного цикла информационной системы.

Отлично. Высокий уровень: Знает современные информационные технологии и программные средства, в том числе отечественного производства при решении задач обеспечения информационной безопасности; принципы, методы и средства решения стандартных задач обеспечения информационной безопасности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы с учетом задач обеспечения информационной безопасности. Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач обеспечения информационной безопасности; решать стандартные задачи обеспечения информационной безопасности на основе информационной и библиографической культуры с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности; применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.
Владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач обеспечения информационной безопасности; навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности; навыками составления технической документации на различных этапах жизненного цикла информационной системы.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Издание	Экз.

	Авторы, составители	Издание	Экз.
Л1.1	Алтайский государственный педагогический университет ; сост.: Е. Р. Кирколуп, Ю. Г. Скурыдин, Е. М. Скурыдина	Информационная безопасность [Электронный ресурс]: учебное пособие — Барнаул : АлтГПУ, 2017 — URL: http://library.altspu.ru/dc/pdf/skuridina.pdf	9999
Л1.2	В. Ф. Шаньгин	Информационная безопасность и защита информации: [учебное пособие] — Саратов : Профобразование, 2019 — URL: http://www.iprbookshop.ru/87995.html	9999
Л1.3	Ю. А. Брюхомицкий	Безопасность информационных технологий: в 2 частях. Часть 1: учебное пособие — Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2020 — URL: http://www.iprbookshop.ru/107943.html	9999
Л1.4	С. М. Авдошин, А. А. Савельева, В. А. Сердюк	Технологии и продукты Microsoft в обеспечении информационной безопасности: учебное пособие — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ) : Ай Пи Ар Медиа, 2021 — URL: https://www.iprbookshop.ru/102070.html	9999

6.1.2. Дополнительная литература

	Авторы, составители	Издание	Экз.
Л2.1	В. Ф. Шаньгин	Защита компьютерной информации. Эффективные методы и средства: [учебное пособие] — Саратов : Профобразование, 2019 — URL: http://www.iprbookshop.ru/87992.html	9999
Л2.2	В. А. Галатенко	Основы информационной безопасности: учебное пособие — Москва : ИНТУИТ : Ай Пи Ар Медиа, 2020 — URL: http://www.iprbookshop.ru/97562.html	9999
Л2.3	А. Е. Фаронов	Основы информационной безопасности при работе на компьютере: учебное пособие — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ) ; Саратов : Ай Пи Ар Медиа, 2020 — URL: http://www.iprbookshop.ru/89453.html	9999
Л2.4	А. В. Морозов, Л. В. Филатова, Т. А. Полякова	Информационное право и информационная безопасность: учебник для магистров и аспирантов — Саратов : Ай Пи Эр Медиа ; Москва : Всероссийский государственный университет юстиции (РПА Минюста России), 2016 — URL: http://www.iprbookshop.ru/66771.html	9999
Л2.5	А. В. Морозов, Л. В. Филатова, Т. А. Полякова	Информационное право и информационная безопасность. Часть 1: учебник для магистров и аспирантов — Саратов : Ай Пи Эр Медиа ; Москва : Всероссийский государственный университет юстиции (РПА Минюста России), 2016 — URL: http://www.iprbookshop.ru/72395.html	9999
Л2.6	Д. А. Скрипник	Обеспечение безопасности персональных данных: учебное пособие — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ) ; Саратов : Ай Пи Ар Медиа, 2020 — URL: http://www.iprbookshop.ru/89449.html	9999

6.3.1 Перечень программного обеспечения

6.3.1.1	Пакет LibreOffice
6.3.1.2	Интернет браузер
6.3.1.3	Медиа проигрыватель
6.3.1.4	Программа 7zip

6.3.2 Перечень информационных справочных систем

6.3.2.1	Президентская библиотека имени Б. Н. Ельцина
6.3.2.2	Сетевая электронная библиотека педагогических вузов // Электронно-библиотечная система Лань / Издательство Лань
6.3.2.3	Национальная электронная библиотека : федеральная государственная информационная система / Министерство культуры Российской Федерации, Российская государственная библиотека
6.3.2.4	Межрегиональная аналитическая роспись статей : поиск статей в российской периодике (МАРС) / АРБИКОН
6.3.2.5	МЭБ. Межвузовская электронная библиотека / Новосибирский государственный педагогический университет
6.3.2.6	Электронная библиотека НПБ / Алтайский государственный педагогический университет, Научно-педагогическая библиотека
6.3.2.7	eLIBRARY.RU : научная электронная библиотека
6.3.2.8	Цифровой образовательный ресурс IPR Smart / Ай Пи Ар Медиа
6.3.2.9	Гарант: информационное-правовое обеспечение

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1	1. Оборудованные учебные аудитории, в том числе с использованием видеопроектора и подключением к сети «Интернет» и доступом в электронную информационнообразовательную среду Университета.
7.2	2. Аудитории для самостоятельной работы с подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду Университета.
7.3	3. Компьютерный класс с подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду Университета.
7.4	4. Аудио, -видеоаппаратура.

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

Основными видами учебной деятельности студентов являются лекции, лабораторные и самостоятельные занятия. На лекциях раскрываются основные положения и понятия курса, отмечаются современные подходы к решаемым проблемам. На лабораторных и самостоятельных занятиях студенты овладевают общепедагогическими и другими методическими умениями, связанными с решением учебно-профессиональных задач. Для достижения сформулированных целей и задач дисциплины отбор содержания осуществляется в соответствии с определенными принципами. Отбор содержания дисциплины, во-первых, определяется ролью и местом курса в программе подготовки бакалавра. Изучение дисциплины опирается на знания и опыт, приобретенные студентами в процессе обучения в школе и при изучении профильных дисциплин. В связи с этим она должна быть направлена на систематизацию знаний и опыта студента о структуре задач, стратегиях поиска решения задач, этапах работы с предметными задачами, основных методах решения профессиональных задач и критериях выбора метода. Основными критериями освоения дисциплины являются: усвоение студентом основных дидактических единиц дисциплины, полнота и осознанность знаний, степень владения различными видами умений – аналитическими, проектировочными, коммуникативными и др., способность использовать освоенные способы деятельности в решении профессиональных задач. Для контроля знаний и полученных студентами умений наряду с традиционными формами контроля используется тестирование (печатная и электронная версии).
Дисциплина может рассматриваться как теоретическая и практикоориентированная одновременно. Организация самостоятельной работы студентов Одним из важнейших видов учебной деятельности студентов является самостоятельная работа. Этот вид работы наряду с подготовкой к лабораторным занятиям предполагает выполнение и анализ заданий и упражнений, проектирование способов деятельности. Самостоятельная работа организуется на основе системы заданий для ее организации. В качестве основного средства организации самостоятельной работы студентов выступают как системы задач по темам, так и проработка отдельных теоретических вопросов. Необходимыми средствами являются система общих методических указаний для студентов, а также частные методические рекомендации для студентов по выполнению каждого вида самостоятельной работы в рамках каждой темы.

Методические рекомендации для обучающихся (с ОВЗ)
Под специальными условиями для получения образования обучающимися с ограниченными возможностями здоровья понимаются условия обучения, воспитания и развития, включающие в себя использование специальных образовательных программ и методов обучения и воспитания, специальных учебников, учебных пособий и дидактических материалов, специальных технических средств обучения коллективного и индивидуального пользования. Построение образовательного процесса ориентировано на учет индивидуальных возрастных, психофизических особенностей обучающихся, в частности предполагается возможность разработки индивидуальных учебных планов. Реализация индивидуальных учебных планов сопровождается поддержкой тьютора (родителя, взявшего на себя тьюторские функции в процессе обучения, волонтера). Обучающиеся с ОВЗ, как и все остальные студенты, могут обучаться по индивидуальному учебному плану в установленные сроки с учетом индивидуальных особенностей и специальных образовательных потребностей конкретного обучающегося. При составлении индивидуального графика обучения для лиц с ОВЗ возможны различные варианты проведения занятий: проведение индивидуальных или групповых занятий с целью устранения сложностей в усвоении лекционного материала, подготовке к семинарским занятиям, выполнению заданий по самостоятельной работе. Для лиц с ОВЗ, по их просьбе, могут быть адаптированы как сами задания, так и формы их выполнения. Выполнение под руководством преподавателя индивидуального проектного задания, позволяющего сочетать теоретические знания и практические навыки; применение мультимедийных технологий в процессе ознакомительных лекций и семинарских занятий, что позволяет экономить время, затрачиваемое на изложение необходимого материала и увеличить его объем.
Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации преподаватели, в соответствии с потребностями студента, отмеченными в анкете, и рекомендациями специалистов дефектологического профиля, разрабатывает фонды оценочных средств, адаптированные для лиц с ограниченными возможностями здоровья и позволяющие оценить достижение ими запланированных в основной образовательной программе результатов обучения и уровень сформированности всех компетенций, заявленных в образовательной программе. Форма проведения текущей аттестации для студентов с ОВЗ устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). Лицам с ОВЗ может быть предоставлено дополнительное время для подготовки к ответу на экзамене, выполнения задания для самостоятельной работы. При необходимости студент с ограниченными возможностями здоровья подает письменное заявление о создании для него специальных условий в Учебно-методическое управление Университета с приложением копий документов, подтверждающих статус инвалида или лица с ОВЗ.