МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

РАБОЧАЯ ПРОГРАММА

Шифр	Наименование дисциплины (модуля)
Б1.О	**Информационная безопасность**

Код направления подготовки	44.03.05
Направление подготовки	Педагогическое образование (с двумя профилями подготовки)
Наименование (я) ОПОП (направленность / профиль)	Физическая культура. Безопасность жизнедеятельности
Уровень образования	бакалавр
Форма обучения	очная

Разработчики:

Должность	Учёная степень, звание	Подпись	ФИО
Доцент	кандидат биологических наук, доцент		Сарайкин Дмитрий Андреевич

Рабочая программа рассмотрена и одобрена (обновлена) на заседании кафедры (структурного подразделения)

Кафедра	Заведующий кафедрой	Номер протокола	Дата протокола	Подпись
Кафедра безопасности жизнедеятельности и медико-биологических дисциплин	Тюмасева Зоя Ивановна	10	13.06.2019	
Кафедра безопасности жизнедеятельности и медико-биологических дисциплин	Тюмасева Зоя Ивановна	1	17.09.2020	

ОГЛАВЛЕНИЕ

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.1 Дисциплина «Информационная безопасность» относится к модулю обязательной части Блока 1 «Дисциплины/модули» основной профессиональной образовательной программы по направлению подготовки 44.03.05 «Педагогическое образование (с двумя профилями подготовки)» (уровень образования бакалавр). Дисциплина является обязательной к изучению.

1.2 Общая трудоемкость дисциплины составляет 3 з.е., 108 час.

1.3 Изучение дисциплины «Информационная безопасность» основано на знаниях, умениях и навыках, полученных при изучении обучающимися следующих дисциплин: «Безопасность жизнедеятельности», «Здоровый и безопасный образ жизни», «Цифровые технологии в образовании».

1.4 Дисциплина «Информационная безопасность» формирует знания, умения и компетенции, необходимые для освоения следующих дисциплин: «Опасности социального характера и защита от них», «Комплексная безопасность образовательных организаций».

1.5 Цель изучения дисциплины:

формирование у обучающихся представлений об информационной безопасности в процессе изучения различных аспектов защиты информации для последующего применения в учебной и практической деятельности.

1.6 Задачи дисциплины:

1) Овладеть знаниями по основным положениям теории информации, информационной безопасности и стандартам шифрования.

2) Иметь представление об информационной безопасности, характере воздействия опасных факторов информационных угроз на человека и его среду обитания.

3) Формировать навыки работы с методиками шифрования и криптоанализа.

1.7 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы:

№ п/п	Код и наименование компетенции по ФГОС
	Код и наименование индикатора достижения компетенции
1	ОПК-1 способен осуществлять профессиональную деятельность в соответствии с нормативными правовыми актами в сфере образования и нормами профессиональной этики
	ОПК.1.1 Знать приоритетные направления развития образовательной системы РФ, законы, нормативно-правовые акты, регламентирующие образовательную деятельность в РФ, нормативные документы по вопросам обучения и воспитания.
	ОПК.1.2 Уметь анализировать основные нормативно-правовые акты в сфере образования и нормы профессиональной этики.
	ОПК.1.3 Владеть приёмами организации профессиональной деятельности на основе правовых и нравственных норм, требований профессиональной этики в условиях реальных педагогических ситуаций.
2	УК-8 способен создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций
	УК.8.1 Знает классификацию и источники чрезвычайных ситуаций природного и техногенного происхождения; причины, признаки и последствия опасностей, способы защиты от чрезвычайных ситуаций; принципы организации безопасности труда.
	УК.8.2 Умеет создавать и поддерживать безопасные условия жизнедеятельности; выявлять факторы, приводящие к возникновению опасных ситуаций; предотвращать возникновение опасных ситуаций, в том числе базируясь на основах медицинских знаний и умениях по оказанию первой доврачебной помощи.
	УК.8.3 Владеет навыками оценки факторов риска, создания комфортной и безопасной образовательной среды, формирования культуры безопасного и ответственного поведения

№ п/п	Код и наименование индикатора достижения компетенции	Образовательные результаты по дисциплине
1	ОПК.1.1 Знать приоритетные направления развития образовательной системы РФ, законы, нормативно-правовые акты, регламентирующие образовательную деятельность в РФ, нормативные документы по вопросам обучения и воспитания.	З.1 Знать нормативно-правовые акты, регламентирующие образовательную деятельность в РФ в сфере информационной безопасности

2	ОПК.1.2 Уметь анализировать основные нормативно-правовые акты в сфере образования и нормы профессиональной этики.	У.1 Уметь анализировать основные нормативно-правовые акты в сфере информационной безопасности
3	ОПК.1.3 Владеть приёмами организации профессиональной деятельности на основе правовых и нравственных норм, требований профессиональной этики в условиях реальных педагогических ситуаций.	В.1 Владеть приёмами организации профессиональной деятельности на основе правовых и нравственных норм в сфере информационной безопасности
1	УК.8.1 Знает классификацию и источники чрезвычайных ситуаций природного и техногенного происхождения; причины, признаки и последствия опасностей, способы защиты от чрезвычайных ситуаций; принципы организации безопасности труда.	З.2 Знать классификацию и источники опасности при изучении информационный безопасности
2	УК.8.2 Умеет создавать и поддерживать безопасные условия жизнедеятельности; выявлять факторы, приводящие к возникновению опасных ситуаций; предотвращать возникновение опасных ситуаций, в том числе базируясь на основах медицинских знаний и умениях по оказанию первой доврачебной помощи.	У.2 Уметь выявлять факторы, приводящие к возникновению опасных ситуаций при изучении основ информационной безопасности
3	УК.8.3 Владеет навыками оценки факторов риска, создания комфортной и безопасной образовательной среды, формирования культуры безопасного и ответственного поведения	В.2 Владеть навыками оценки факторов риска и формирования ответственного поведения при изучении информационной безопасности

2. ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ (МОДУЛЯ) И ВИДОВ ЗАНЯТИЙ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Наименование раздела дисциплины (темы)	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)			Итого часов
	Л	ПЗ	СРС	
Итого по дисциплине	**18**	**14**	**40**	**72**
Первый период контроля				
Раздел 1. Общие проблемы безопасности. Роль и место информационной безопасности. Здоровье и компьютер	***8***	***8***	***20***	***36***
Информационные технологии сферы образования	2	4	4	10
Национальные интересы и безопасность России	2		4	6
Защита информации	2		4	6
Организационно-правовое обеспечение информационной безопасности		4	4	8
Здоровье и компьютер	2		4	6
Раздел 2. Защита информации в автоматизированных системах обработки данных (АСОД). Криптографические методы защиты информации. Защита информации в персональных компьютерах	***8***	***2***	***10***	***20***
Элементы и объекты защиты информации в АСОД	2		2	4
Системный анализ угроз безопасности в компьютерных системах	2		2	4
Функции, задачи, методы и системы защиты информации	2		2	4
Криптографические методы защиты информации в автоматизированных системах	2		2	4
Защита персонального компьютера от несанкционированного доступа		2	2	4
Раздел 3. Компьютерные вирусы и антивирусные программы. Проблемы защиты информации в сетях ЭВМ. Технические средства и комплексное обеспечение безопасности	***2***	***4***	***10***	***16***
Компьютерный вирус	2		4	6
Методы защиты. Антивирусы		4	2	6
Защита информации в сетях ЭВМ			2	2
Технические средства защиты АСОД			2	2
Итого по видам учебной работы	18	14	40	72
Форма промежуточной аттестации				
Экзамен				36
Итого за Первый период контроля				**108**

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ), СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

3.1 Лекции

Наименование раздела дисциплины (модуля)/ Тема и содержание	**Трудоемкость (кол-во часов)**
1. Раздел 1. Общие проблемы безопасности. Роль и место информационной безопасности. Здоровье и компьютер	***8***
Формируемые компетенции, образовательные результаты: ОПК-1: З.1 (ОПК.1.1), У.1 (ОПК.1.2), В.1 (ОПК.1.3)	
1.1. Информационные технологии сферы образования 1. Психолого-педагогические и технологические тенденции в области образования. 2. Педагогические инновации в мировой педагогике. 3. Система открытого образования, ее принципы и особенности. Учебно-методическая литература: 1, 2, 3, 4	2
1.2. Национальные интересы и безопасность России 1. Национальные интересы и информационная безопасность России. 2. Уровни обеспечения национальной безопасности. 3. Основные угрозы безопасности России. 4. Информационная война. 5. Информационное оружие. 6. Принципы, основные задачи и функции обеспечения информационной безопасности (ИБ). 7. Отечественные и зарубежные стандарты информационной безопасности. Учебно-методическая литература: 1, 2, 3, 4	2
1.3. Защита информации 1. Защита информации (ЗИ). 2. Основные предметные направления ЗИ. 3. Охрана персональных данных. Учебно-методическая литература: 1, 2, 3, 4	2
1.4. Здоровье и компьютер 1. Здоровье компьютера. 2. Здоровье пользователя. 3. Работа за компьютером. 4. Требования к установке компьютера в помещениях. 5. Техника безопасности и правила подключения внешних устройств. Учебно-методическая литература: 1, 2, 3, 4	2
2. Раздел 2. Защита информации в автоматизированных системах обработки данных (АСОД). Криптографические методы защиты информации. Защита информации в персональных компьютерах	***8***
Формируемые компетенции, образовательные результаты: УК-8: З.2 (УК.8.1), У.2 (УК.8.2), В.2 (УК.8.3)	
2.1. Элементы и объекты защиты информации в АСОД 1. Объекты защиты информации в АСОД. Надежность информации. 2. Уязвимость информации. 3. Основные элементы АСОД и типовые структурные компоненты. 4. Дестабилизирующие факторы АСОД. 5. Преднамеренные угрозы безопасности АСОД. Учебно-методическая литература: 1, 2, 3, 4	2
2.2. Системный анализ угроз безопасности в компьютерных системах 1. Структурная и функциональная организация информационных компьютерных систем (КС). 2. КС как объект защиты. 3. Содержательная сущность защиты КС. Учебно-методическая литература: 1, 2, 3, 4	2

2.3. Функции, задачи, методы и системы защиты информации 1. Функции и задачи защиты информации. 2. Механизмы защиты, их управление. 3. Методы и системы защиты информации. 4. Подтверждение подлинности пользователя и разграничение их доступа к компьютерным ресурсам. 5. Общие сведения о контроле информационной целостности. Учебно-методическая литература: 1, 2, 3, 4	2
2.4. Криптографические методы защиты информации в автоматизированных системах 1. Криптология и основные этапы ее развития. 2. Методы криптографического преобразования данных. 3. Шифрование заменой (подстановка). 4. Шифрование методом перестановки. 5. Шифрование методом программирования. 6. Системы с открытым ключом. 7. Электронная цифровая подпись. 8. Технические и программные средства защиты криптографии. Учебно-методическая литература: 1, 2, 3, 4	2
3. Раздел 3. Компьютерные вирусы и антивирусные программы. Проблемы защиты информации в сетях ЭВМ. Технические средства и комплексное обеспечение безопасности	***2***
Формируемые компетенции, образовательные результаты: УК-8: З.2 (УК.8.1), У.2 (УК.8.2), В.2 (УК.8.3)	
3.1. Компьютерный вирус 1. Классификация вирусов. 2. Алгоритмы действия вирусов. 3. Структура вирусов. Учебно-методическая литература: 1, 2, 3, 4	2

3.2 Практические

Наименование раздела дисциплины (модуля)/ Тема и содержание	**Трудоемкость (кол-во часов)**
1. Раздел 1. Общие проблемы безопасности. Роль и место информационной безопасности. Здоровье и компьютер	***8***
Формируемые компетенции, образовательные результаты: ОПК-1: З.1 (ОПК.1.1), У.1 (ОПК.1.2), В.1 (ОПК.1.3)	
1.1. Информационные технологии сферы образования 1. Понятие и содержание технологии обучения. Понятие информационной технологии. 2. Информационные и коммуникационные технологии в построении открытой системы образования. 3. Этапы описания автоматического действия: постановка задачи, моделирование, алгоритмизация, программирование. 4. Кризис автоматизации. Развитие технологий программирования. Создатели универсального автомата. Преодоление кризиса автоматизации всех сфер человеческой деятельности. Учебно-методическая литература: 2, 3, 5, 6, 7	4
1.2. Организационно-правовое обеспечение информационной безопасности 1. Правовые основы защиты информации. 2. Ответственность за нарушение законодательства в информационной сфере. 3. Статьи Кодекса РФ, Уголовного кодекса РФ. Учебно-методическая литература: 2, 3, 5, 6, 7	4
2. Раздел 2. Защита информации в автоматизированных системах обработки данных (АСОД). Криптографические методы защиты информации. Защита информации в персональных компьютерах	***2***
Формируемые компетенции, образовательные результаты: УК-8: З.2 (УК.8.1), У.2 (УК.8.2), В.2 (УК.8.3)	
2.1. Защита персонального компьютера от несанкционированного доступа 1. Защита персонального компьютера от несанкционированного доступа. 2. Угрозы информации. 3. Вредоносные закладки в ПК и борьба с ними. Учебно-методическая литература: 2, 3, 5, 6, 7	2

3. Раздел 3. Компьютерные вирусы и антивирусные программы. Проблемы защиты информации в сетях ЭВМ. Технические средства и комплексное обеспечение безопасности	***4***
Формируемые компетенции, образовательные результаты: УК-8: З.2 (УК.8.1), У.2 (УК.8.2), В.2 (УК.8.3)	
3.1. Методы защиты. Антивирусы 1. Классы антивирусных программ. 2. Примеры антивирусных программ. Учебно-методическая литература: 2, 3, 5, 6, 7	4

3.3 СРС

Наименование раздела дисциплины (модуля)/ Тема для самостоятельного изучения	**Трудоемкость (кол-во часов)**
1. Раздел 1. Общие проблемы безопасности. Роль и место информационной безопасности. Здоровье и компьютер	***20***
Формируемые компетенции, образовательные результаты: ОПК-1: З.1 (ОПК.1.1), У.1 (ОПК.1.2), В.1 (ОПК.1.3)	
1.1. Информационные технологии сферы образования ***Задание для самостоятельного выполнения студентом:*** Работа с рекомендованной литературой. Подготовка доклада/сообщения. Оформление схемы. Поиск информации для подготовки презентации. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	4
1.2. Национальные интересы и безопасность России ***Задание для самостоятельного выполнения студентом:*** Работа с рекомендованной литературой. Поиск информации для подготовки презентации. Оформление схемы. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	4
1.3. Защита информации ***Задание для самостоятельного выполнения студентом:*** Работа с рекомендованной литературой. Поиск информации для подготовки презентации. Оформление схемы. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	4
1.4. Организационно-правовое обеспечение информационной безопасности ***Задание для самостоятельного выполнения студентом:*** Работа с рекомендованной литературой. Поиск информации для подготовки презентации. Оформление схемы. Подготовка аннотированного каталога нормативно-правовой документации. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	4
1.5. Здоровье и компьютер ***Задание для самостоятельного выполнения студентом:*** Работа с рекомендованной литературой. Поиск информации для подготовки презентации. Оформление схемы. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	4
2. Раздел 2. Защита информации в автоматизированных системах обработки данных (АСОД). Криптографические методы защиты информации. Защита информации в персональных компьютерах	***10***
Формируемые компетенции, образовательные результаты: УК-8: З.2 (УК.8.1), У.2 (УК.8.2), В.2 (УК.8.3)	
2.1. Элементы и объекты защиты информации в АСОД ***Задание для самостоятельного выполнения студентом:*** Работа с рекомендованной литературой. Поиск информации для подготовки презентации. Оформление схемы. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	2

2.2. Системный анализ угроз безопасности в компьютерных системах ***Задание для самостоятельного выполнения студентом:*** Работа с рекомендованной литературой. Поиск информации для подготовки презентации. Оформление схемы. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	2
2.3. Функции, задачи, методы и системы защиты информации ***Задание для самостоятельного выполнения студентом:*** Работа с рекомендованной литературой. Поиск информации для подготовки презентации. Оформление схемы. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	2
2.4. Криптографические методы защиты информации в автоматизированных системах ***Задание для самостоятельного выполнения студентом:*** Работа с рекомендованной литературой. Поиск информации для подготовки презентации. Оформление схемы. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	2
2.5. Защита персонального компьютера от несанкционированного доступа ***Задание для самостоятельного выполнения студентом:*** Работа с рекомендованной литературой. Подготовка доклада/сообщения. Оформление схемы. Поиск информации для подготовки презентации. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	2
3. Раздел 3. Компьютерные вирусы и антивирусные программы. Проблемы защиты информации в сетях ЭВМ. Технические средства и комплексное обеспечение безопасности	***10***
Формируемые компетенции, образовательные результаты: УК-8: З.2 (УК.8.1), У.2 (УК.8.2), В.2 (УК.8.3)	
3.1. Компьютерный вирус ***Задание для самостоятельного выполнения студентом:*** Работа с рекомендованной литературой. Оформление схемы. Поиск информации для подготовки презентации. Учебно-методическая литература: 1, 2, 3, 4, 6, 7	4
3.2. Методы защиты. Антивирусы ***Задание для самостоятельного выполнения студентом:*** Работа с рекомендованной литературой. Подготовка доклада/сообщения. Оформление схемы. Поиск информации для подготовки презентации. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	2
3.3. Защита информации в сетях ЭВМ ***Задание для самостоятельного выполнения студентом:*** Работа с рекомендованной литературой. Оформление схемы. Поиск информации для подготовки презентации. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	2
3.4. Технические средства защиты АСОД ***Задание для самостоятельного выполнения студентом:*** Работа с рекомендованной литературой. Оформление схемы. Поиск информации для подготовки презентации. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	2

4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-методическая литература

№ п/п	Библиографическое описание (автор, заглавие, вид издания, место, издательство, год издания, количество страниц)	Ссылка на источник в ЭБС
	Основная литература	
1	Артемов А.В. Информационная безопасность [Электронный ресурс] : курс лекций / А.В. Артемов. – Электрон. текстовые данные. – Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. – 256 с.	http://www.iprbookshop.ru/33430.html. — ЭБС «IPRbooks»
2	Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. – Электрон. текстовые данные. – М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – 266 с.	http://www.iprbookshop.ru/52209.html. — ЭБС «IPRbooks»
3	Основы информационной безопасности [Электронный ресурс] : учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В.Ю. Рогозин [и др.]. – Электрон. текстовые данные. – М. : ЮНИТИ-ДАНА, 2017. – 287 с.	http://www.iprbookshop.ru/72444.html. — ЭБС «IPRbooks»
4	Солопова В.А. Информационные технологии в управлении безопасностью жизнедеятельности [Электронный ресурс]: конспект лекций/ Солопова В.А.– Электрон. текстовые данные.– Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2015.– 117 с.	http://www.iprbookshop.ru/61890.html. – ЭБС «IPRbooks»
	Дополнительная литература	
5	Кубанков А.Н. Система обеспечения информационной безопасности Российской Федерации: организационно-правовой аспект [Электронный ресурс] : учебное пособие / А.Н. Кубанков, Н.Н. Куняев. – Электрон. текстовые данные. – М. : Всероссийский государственный университет юстиции (РПА Минюста России), 2014. – 78 с.	http://www.iprbookshop.ru/47262.html. — ЭБС «IPRbooks»
6	Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт [Электронный ресурс] : монография / Л.Л. Ефимова, С.А. Кочерга. – Электрон. текстовые данные. – М. : ЮНИТИ-ДАНА, 2015. – 239 с.	http://www.iprbookshop.ru/52672.html. — ЭБС «IPRbooks»
7	Дождиков В.Г. Краткий энциклопедический словарь по информационной безопасности [Электронный ресурс] / В.Г. Дождиков, М.И. Салтан. – Электрон. текстовые данные. – М. : Энергия, 2010. – 239 с.	http://www.iprbookshop.ru/5729.html. — ЭБС «IPRbooks»

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

5.1. Описание показателей и критериев оценивания компетенций

Код компетенции по ФГОС					
Код образовательного результата дисциплины	Текущий контроль				Промежуточная аттестация
	Доклад/сообщение	Конспект по теме	Мультимедийная презентация	Схема/граф-схема	Зачет/Экзамен
ОПК-1					
З.1 (ОПК.1.1)	+				+
У.1 (ОПК.1.2)			+		+
В.1 (ОПК.1.3)		+		+	+
УК-8					
З.2 (УК.8.1)	+				+
У.2 (УК.8.2)			+		+
В.2 (УК.8.3)				+	+

5.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

5.2.1. Текущий контроль.

Типовые задания к разделу "Раздел 1. Общие проблемы безопасности. Роль и место информационной безопасности. Здоровье и компьютер":

1. Доклад/сообщение

Практическое занятие 1
Информационные технологии сферы образования
Вопросы для доклада/сообщения:
1. Понятие и содержание технологии обучения.
2. Понятие информационной технологии.
3. Информационные и коммуникационные технологии в построении открытой системы образования.
4. Этапы описания автоматического действия: постановка задачи, моделирование, алгоритмизация, программирование.
5. Кризис автоматизации.
6. Развитие технологий программирования.
7. Создатели универсального автомата.
8. Преодоление кризиса автоматизации всех сфер человеческой деятельности.

Количество баллов: 10

2. Конспект по теме

Практическое занятие 2
Организационно-правовое обеспечение информационной безопасности
План практического занятия:
1. Правовые основы защиты информации.
2. Ответственность за нарушение законодательства в информационной сфере.
3. Статьи Кодекса РФ, Уголовного кодекса РФ.
Практическая часть:
Составьте аннотированный каталог нормативно-правовой документации отразив следующие пункты: 1-ый столбик – порядковый номер; 2-ой столбик – название нормативно-правового документа; 3-ий столбик – краткая аннотация нормативно-правового документа; 4-ый столбик – ответственность за нарушение законодательства в информационной сфере.

Количество баллов: 10

3. Мультимедийная презентация

Создать мультимедийную презентацию на одну из ниже представленных тем:

1. Основные задачи в сфере обеспечения ИБ.
2. Уровни доступа к информации с точки зрения законодательства.
3. Гражданский кодекса РФ в сфере ИБ.
4. Зарубежные стандарты ИБ.
5. Функции государственной системы по обеспечению ИБ.
6. Коммерческая тайна.
7. Банковская тайна.
8. Профессиональная тайна.
9. Служебная тайна.
10. Охрана интеллектуальной собственности.

Количество баллов: 10

4. Схема/граф-схема

Индивидуальная или групповая работа:
Составить схему «Этапы развития информационных технологий в сфере образования».
Составить схему «Информационных угроз интересам национальной безопасности России».
Составить схему «Защита персональных данных».
Составить памятку техники безопасности при работе с компьютером.

Количество баллов: 10

Типовые задания к разделу "Раздел 2. Защита информации в автоматизированных системах обработки данных (АСОД). Криптографические методы защиты информации. Защита информации в персональных компьютерах":

1. Доклад/сообщение

Практическое занятие 3
Защита персонального компьютера от несанкционированного доступа
Вопросы для доклада/сообщения:
1. Защита персонального компьютера от несанкционированного доступа.
2. Угрозы информации.
3. Вредоносные закладки в ПК и борьба с ними.
4. Настройка параметров безопасности в ОС Windows.
5. Изучение программных продуктов защиты информации.
6. Программа поиска и удаления вредоносных закладок.
7. Программное обеспечение для защиты информации в ПК.

Количество баллов: 10

2. Мультимедийная презентация

Создать мультимедийную презентацию на одну из ниже представленных тем:

1. Причины нарушения целостности информации.
2. Каналы несанкционированного получения информации в АСОД.
3. Контроль правильности функционирования системы защиты.
4. Проблема управления ключами.
5. Характеристики криптографических средств защиты.
6. Криптографические стандарты.
7. Средства вторжения в частную жизнь.
8. Троянские и другие вредоносные программы.
9. Регистрация действий пользователя.

Количество баллов: 10

3. Схема/граф-схема

Индивидуальная или групповая работа:
Составить схему «Угрозы объектов и элементов в АСОД».
Составить схему «Виды угрозы информации».
Составить схему «Вредоносные закладки в ПК».
Составить схему «Средства защиты персональных данных».
Составить схему «История криптографии».
Составить схему «Виды криптографической защиты».

Количество баллов: 10

Типовые задания к разделу "Раздел 3. Компьютерные вирусы и антивирусные программы. Проблемы защиты информации в сетях ЭВМ. Технические средства и комплексное обеспечение безопасности":

1. Доклад/сообщение

Практическое занятие 4
Методы защиты. Антивирусы
Вопросы для доклада/сообщения:
1. Классы антивирусных программ.
2. Примеры антивирусных программ.
3. Алгоритм работы антивирусной программы.
4. Распространенных антивирусных программ.

Количество баллов: 10

2. Мультимедийная презентация

Создать мультимедийную презентацию на одну из ниже представленных тем:
1. Признаки появления вируса.
2. Антивирусная программа Dr.Web.
3. Антивирус Касперского.
4. Антивирус Panda.
5. Антивирус 360 Total Security.
6. Антивирус-ревизор.
7. Symantec AntiVirus.
8. Международные стандарты защита информации в сетях ЭВМ.
9. Примеры системы защиты локальной вычислительной сети.
10. Межсетевые экраны – брандмауэры.
11. Примеры систем активного аудита.
12. Комплекс физической защиты АСОД.

Количество баллов: 10

3. Схема/граф-схема

Индивидуальная или групповая работа:
Составить схему «Способы заражения ПК вирусами»

Количество баллов: 10

5.2.2. Промежуточная аттестация

Промежуточная аттестация проводится в соответствии с Положением о текущем контроле и промежуточной аттестации в ФГБОУ ВО «ЮУрГГПУ».

Первый период контроля

1. Экзамен

Вопросы к экзамену:

1. Эволюция информационных процессов в обществе. Информатизация и компьютеризация. Информационные ресурсы, продукты и услуги. Объективная необходимость и общественная потребность защиты информации.

2. Информационная безопасность личности, общества и государства. Массовая и конфиденциальная информация. Виды тайн.

3. Информационная безопасность как составляющая национальной безопасности. Задачи государства в этой области. Информационное оружие, информационные войны и терроризм. Государственные органы РФ, реализующие функции обеспечения информационной безопасности.

4. Компьютерная система (КС) как объект защиты информации. Угрозы информационной безопасности в КС. Классификация угроз.

5. Общая характеристика случайных угроз информационной безопасности в КС.

6. Общая характеристика преднамеренных угроз информационной безопасности в КС.

7. Эволюция концепции информационной безопасности в КС. Основные принципы обеспечения информационной безопасности в КС. Политика безопасности.

8. Реализация угроз информационной безопасности в КС путем несанкционированного доступа (НСД). Классификация каналов НСД. Собирательный образ потенциального нарушителя.

9. Обобщенные модели системы защиты информации в КС. Одноуровневые, многоуровневые и многозвенные модели. Общая характеристика средств и методов защиты информации в КС.

10. Общая характеристика организационных мероприятий, обеспечивающих информационную безопасность КС. Основные задачи службы безопасности.

11. Необходимость правового регулирования в области защиты информации. Информация как объект права собственности. Правоотношения собственника, владельца и пользователя информационных ресурсов.

12. Отечественное законодательство в области информации и защиты информации.

13. Ответственность за правонарушения при работе с компьютерными системами.

14. Эксплуатационная надежность КС как источник возникновения случайных угроз информационной безопасности. Пути ее повышения. Резервирование технических средств. Программно-аппаратный контроль и тестирование.

15. Оптимизация взаимодействия пользователя с КС как средство предотвращения ошибочных операций случайного характера.

16. Помехоустойчивое кодирование. Избыточные коды для обнаружения и исправления случайных ошибок в работе КС.

17. Дублирование информации как средство парирования угроз безопасности в КС. Многоуровневое дублирование.

18. Минимизация ущерба, наносимого КС авариями и стихийными бедствиями.

19. Система охраны объектов КС.

20. Общая характеристика технических каналов утечки информации в КС.

21. Методы и средства защиты информации в КС от утечки по каналам побочных электромагнитных излучений и наводок.

22. Средства противодействия подслушивания и дистанционному наблюдению.

23. Базовые принципы, лежащие в основе моделей политики безопасности в КС. Матричная (дискреционная) модель и мандатная (полномочная) модель управления доступом к ресурсам КС.

24. Идентификация и аутентификация субъектов доступа к ресурсам КС. Парольные методы и оценка их эффективности. Биометрические методы.

25. Средства и методы разграничения доступа к ресурсам КС.

26. Защита программных средств КС от несанкционированного копирования и исследования.

27. Защита от несанкционированного изменения структуры КС в процессе эксплуатации.

28. Контроль целостности программ и данных в процессе эксплуатации КС.

29. Общие понятия, история развития и классификация криптографических средств.

30. Общая характеристика различных методов шифрования. Криптостойкость.

31. Общая характеристика и классификация компьютерных вирусов.

32. Механизм заражения файловыми и загрузочными вирусами. Особенности макровирусов.

33. Средства, используемые для обнаружения компьютерных вирусов.

34. Профилактика заражения компьютерными вирусами.

35. Антивирусные средства для лечения и удаления компьютерных вирусов. Программы-полифаги. Эвристические анализаторы.

36. Чем вызвана необходимость разработки стандартов по защите информации? Охарактеризуйте отечественные нормативы и зарубежные стандарты в этой области.

37. Содержательный смысл понятия комплексной системы защиты информации (КСЗИ) в компьютерных системах. Основные принципы и положения, реализующие системный подход к построению КСЗИ.

38. Функции и задачи защиты, механизмы защиты, уровень защищенности, управление защитой и другие базовые понятия, используемые при формировании КСЗИ.

39. Общетеоретическая постановка задачи оптимизации КСЗИ на основе выбранного критерия эффективности защиты.

40. Информация как средство отражения окружающего мира и как средство его познания. Количественные оценки и показатели качества информации.

5.3. Примерные критерии оценивания ответа студентов на экзамене (зачете):

Отметка	Критерии оценивания
"Отлично"	- дается комплексная оценка предложенной ситуации - демонстрируются глубокие знания теоретического материала и умение их применять - последовательное, правильное выполнение всех заданий - умение обоснованно излагать свои мысли, делать необходимые выводы
"Хорошо"	- дается комплексная оценка предложенной ситуации - демонстрируются глубокие знания теоретического материала и умение их применять - последовательное, правильное выполнение всех заданий - возможны единичные ошибки, исправляемые самим студентом после замечания преподавателя - умение обоснованно излагать свои мысли, делать необходимые выводы
"Удовлетворительно" ("зачтено")	- затруднения с комплексной оценкой предложенной ситуации - неполное теоретическое обоснование, требующее наводящих вопросов преподавателя - выполнение заданий при подсказке преподавателя - затруднения в формулировке выводов

"Неудовлетворительно" ("не зачтено")	- неправильная оценка предложенной ситуации - отсутствие теоретического обоснования выполнения заданий

6. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

1. Лекции

Лекция - одна из основных форм организации учебного процесса, представляющая собой устное, монологическое, систематическое, последовательное изложение преподавателем учебного материала с демонстрацией слайдов и фильмов. Работа обучающихся на лекции включает в себя: составление или слежение за планом чтения лекции, написание конспекта лекции, дополнение конспекта рекомендованной литературой.

Требования к конспекту лекций: краткость, схематичность, последовательная фиксация основных положений, выводов, формулировок, обобщений. В конспекте нужно помечать важные мысли, выделять ключевые слова, термины. Последующая работа над материалом лекции предусматривает проверку терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. В конспекте нужно обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.

2. Практические

Практические (семинарские занятия) представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы.

Основной формой проведения практических занятий и семинаров является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение задач и разбор примеров и ситуаций в аудиторных условиях.

При подготовке к практическому занятию необходимо, ознакомиться с его планом; изучить соответствующие конспекты лекций, главы учебников и методических пособий, разобрать примеры, ознакомиться с дополнительной литературой (справочниками, энциклопедиями, словарями). К наиболее важным и сложным вопросам темы рекомендуется составлять конспекты ответов. Следует готовить все вопросы соответствующего занятия: необходимо уметь давать определения основным понятиям, знать основные положения теории, правила и формулы, предложенные для запоминания к каждой теме.

В ходе практического занятия надо давать конкретные, четкие ответы по существу вопросов, доводить каждую задачу до окончательного решения, демонстрировать понимание проведенных расчетов (анализов, ситуаций), в случае затруднений обращаться к преподавателю.

3. Экзамен

Экзамен преследует цель оценить работу обучающегося за определенный курс: полученные теоретические знания, их прочность, развитие логического и творческого мышления, приобретение навыков самостоятельной работы, умения анализировать и синтезировать полученные знания и применять их для решения практических задач.

Экзамен проводится в устной или письменной форме по билетам, утвержденным заведующим кафедрой. Экзаменационный билет включает в себя два вопроса и задачи. Формулировка вопросов совпадает с формулировкой перечня вопросов, доведенного до сведения обучающихся не позднее чем за один месяц до экзаменационной сессии.

В процессе подготовки к экзамену организована предэкзаменационная консультация для всех учебных групп.

При любой форме проведения экзаменов по билетам экзаменатору предоставляется право задавать студентам дополнительные вопросы, задачи и примеры по программе данной дисциплины. Дополнительные вопросы, также как и основные вопросы билета, требуют развернутого ответа.

Результат экзамена выражается оценкой «отлично», «хорошо», «удовлетворительно».

4. Доклад/сообщение

Доклад − развернутое устное (возможен письменный вариант) сообщение по определенной теме, сделанное публично, в котором обобщается информация из одного или нескольких источников, представляется и обосновывается отношение к описываемой теме.

Основные этапы подготовки доклада:

1. четко сформулировать тему;
2. изучить и подобрать литературу, рекомендуемую по теме, выделив три источника библиографической информации:
   − первичные (статьи, диссертации, монографии и т. д.);
   − вторичные (библиография, реферативные журналы, сигнальная информация, планы, граф-схемы, предметные указатели и т. д.);
   − третичные (обзоры, компилятивные работы, справочные книги и т. д.);
3. написать план, который полностью согласуется с выбранной темой и логично раскрывает ее;
4. написать доклад, соблюдая следующие требования:
   − структура доклада должна включать краткое введение, обосновывающее актуальность проблемы; основной текст; заключение с краткими выводами по исследуемой проблеме; список использованной литературы;
   − в содержании доклада общие положения надо подкрепить и пояснить конкретными примерами; не пересказывать отдельные главы учебника или учебного пособия, а изложить собственные соображения по существу рассматриваемых вопросов, внести свои предложения;
5. оформить работу в соответствии с требованиями.

5. Конспект по теме

Конспект – это систематизированное, логичное изложение материала источника.
Различаются четыре типа конспектов.
План-конспект – это развернутый детализированный план, в котором достаточно подробные записи приводятся по тем пунктам плана, которые нуждаются в пояснении.
Текстуальный конспект – это воспроизведение наиболее важных положений и фактов источника.
Свободный конспект – это четко и кратко сформулированные (изложенные) основные положения в результате глубокого осмысливания материала. В нем могут присутствовать выписки, цитаты, тезисы; часть материала может быть представлена планом.
Тематический конспект – составляется на основе изучения ряда источников и дает более или менее исчерпывающий ответ по какой-то теме (вопросу).
В процессе изучения материала источника, составления конспекта нужно обязательно применять различные выделения, подзаголовки, создавая блочную структуру конспекта. Это делает конспект легко воспринимаемым, удобным для работы.
Этапы выполнения конспекта:
1. определить цель составления конспекта;
2. записать название текста или его части;
3. записать выходные данные текста (автор, место и год издания);
4. выделить при первичном чтении основные смысловые части текста;
5. выделить основные положения текста;
6. выделить понятия, термины, которые требуют разъяснений;
7. последовательно и кратко изложить своими словами существенные положения изучаемого материала;
8. включить в запись выводы по основным положениям, конкретным фактам и примерам (без подробного описания);
9. использовать приемы наглядного отражения содержания (абзацы «ступеньками», различные способы подчеркивания, шрифт разного начертания, ручки разного цвета);
10. соблюдать правила цитирования (цитата должна быть заключена в кавычки, дана ссылка на ее источник, указана страница).

6. Схема/граф-схема

Схема — графическое представление определения, анализа или метода решения задачи, в котором используются символы для отображения данных.
Граф-схема — графическое изображение логических связей между основными субъектами текста (отношений между условно выделенными константами).
Для выполнения задания на составление схемы/граф-схемы необходимо:
1. Выделить основные понятия, изученные в данном разделе (по данной теме).
2. Определить, как понятия связаны между собой.
3. Показать, как связаны между собой отдельные блоки понятий.
4. Привести примеры взаимосвязей понятий в соответствии с созданной граф-схемой.

7. Мультимедийная презентация

Мультимедийная презентация – способ представления информации на заданную тему с помощью компьютерных программ, сочетающий в себе динамику, звук и изображение.
Для создания компьютерных презентаций используются специальные программы: PowerPoint, Adobe Flash CS5, Adobe Flash Builder, видеофайл.
Презентация – это набор последовательно сменяющих друг друга страниц – слайдов, на каждом из которых можно разместить любые текст, рисунки, схемы, видео - аудио фрагменты, анимацию, 3D – графику, фотографию, используя при этом различные элементы оформления.
Мультимедийная форма презентации позволяет представить материал как систему опорных образов, наполненных исчерпывающей структурированной информацией в алгоритмическом порядке.
Этапы подготовки мультимедийной презентации:
1. Структуризация материала по теме;
2. Составление сценария реализации;
3. Разработка дизайна презентации;
4. Подготовка медиа фрагментов (тексты, иллюстрации, видео, запись аудиофрагментов);
5. Подготовка музыкального сопровождения (при необходимости);
6. Тест-проверка готовой презентации.

7. ПЕРЕЧЕНЬ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

1. Развивающее обучение
2. Проблемное обучение
3. Проектные технологии
4. Цифровые технологии обучения

8. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ

1. компьютерный класс – аудитория для самостоятельной работы
2. учебная аудитория для лекционных занятий
3. учебная аудитория для семинарских, практических занятий
4. Лицензионное программное обеспечение:
   - Операционная система Windows 10
   - Microsoft Office Professional Plus
   - Антивирусное программное обеспечение Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition
   - Справочная правовая система Консультант плюс
   - 7-zip
   - Adobe Acrobat Reader DC