

Документ подписан простой электронной подписью
 Информация о владельце:
 ФИО: ЧУМАЧЕНКО ТАТЬЯНА АЛЕКСАНДРОВНА
 Должность: РЕКТОР
 Дата подписания: 14.04.2022 09:39:38
 Уникальный программный ключ:
 9c9f7aaffa4840d284abe156657b8f85432bdb16




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	заочная

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	3
2. Трудоемкость дисциплины (модуля) и видов занятий по дисциплине (модулю)	5
3. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий	6
4. Учебно-методическое и информационное обеспечение дисциплины	10
5. Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)	11
6. Методические указания для обучающихся по освоению дисциплины	15
7. Перечень образовательных технологий	17
8. Описание материально-технической базы	18

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 среду его 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.	3.1 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 информационной 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	4	8	87	99
Первый период контроля				
Раздел 1. Общие проблемы безопасности. Роль и место информационной безопасности	4	4	36	44
Информационные технологии сферы образования	2		4	6
Национальные интересы и безопасность России			4	4
Защита информации	2		4	6
Организационно-правовое обеспечение информационной безопасности		4	4	8
Уровни обеспечения национальной безопасности			4	4
Основные угрозы безопасности России			4	4
Информационная война			4	4
Информационное оружие			4	4
Отечественные и зарубежные стандарты информационной безопасности			4	4
Раздел 2. Защита информации в автоматизированных системах обработки данных (АСОД). Криптографические методы защиты информации. Защита информации в персональных компьютерах		2	24	26
Элементы и объекты защиты информации в АСОД			4	4
Системный анализ угроз безопасности в компьютерных системах			4	4
Функции, задачи, методы и системы защиты информации			4	4
Криптографические методы защиты информации в автоматизированных системах			4	4
Защита персонального компьютера от несанкционированного доступа		2	4	6
Защита информации в компьютерных системах от несанкционированного доступа			4	4
Раздел 3. Компьютерные вирусы и антивирусные программы. Проблемы защиты информации в сетях ЭВМ. Технические средства и комплексное обеспечение безопасности		2	27	29
Компьютерный вирус			4	4
Методы защиты от компьютерных вирусов			4	4
Антивирусы		2	4	6
Защита информации в сетях ЭВМ			4	4
Архитектура механизмов защиты информации в сетях ЭВМ			3	3
Технические средства защиты АСОД			4	4
Средства контроля доступа			4	4
Итого по видам учебной работы	4	8	87	99
Форма промежуточной аттестации				
Экзамен				9
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	4
Формируемые компетенции, образовательные результаты: ОПК-1: 3.1 (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. Защита информации 1. Защита информации (ЗИ). 2. Основные предметные направления ЗИ. 3. Охрана персональных данных. 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	4
Формируемые компетенции, образовательные результаты: ОПК-1: 3.1 (ОПК.1.1), У.1 (ОПК.1.2), В.1 (ОПК.1.3)	
1.1. 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: 3.2 (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	2
Формируемые компетенции, образовательные результаты: УК-8: В.2 (УК.8.3), У.2 (УК.8.2), 3.2 (УК.8.1)	
3.1. Антивирусы 1. Классы антивирусных программ. 2. Примеры антивирусных программ. Учебно-методическая литература: 2, 3, 5, 6, 7	2

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	36

Формируемые компетенции, образовательные результаты: ОПК-1: 3.1 (ОПК.1.1), У.1 (ОПК.1.2), В.1 (ОПК.1.3)	
1.1. Информационные технологии сферы образования <i>Задание для самостоятельного выполнения студентом:</i> Работа с рекомендованной литературой. Подготовка к контрольной работе. Оформление схемы. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	4
1.2. Национальные интересы и безопасность России <i>Задание для самостоятельного выполнения студентом:</i> Работа с рекомендованной литературой. Подготовка к контрольной работе. Оформление схемы. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	4
1.3. Защита информации <i>Задание для самостоятельного выполнения студентом:</i> Работа с рекомендованной литературой. Подготовка к контрольной работе. Оформление схемы. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	4
1.4. Организационно-правовое обеспечение информационной безопасности <i>Задание для самостоятельного выполнения студентом:</i> Работа с рекомендованной литературой. Подготовка к контрольной работе. Оформление практической работы. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	4
1.5. Уровни обеспечения национальной безопасности <i>Задание для самостоятельного выполнения студентом:</i> Работа с рекомендованной литературой. Подготовка к контрольной работе. Оформление схемы. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	4
1.6. Основные угрозы безопасности России <i>Задание для самостоятельного выполнения студентом:</i> Работа с рекомендованной литературой. Подготовка к контрольной работе. Оформление схемы. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	4
1.7. Информационная война <i>Задание для самостоятельного выполнения студентом:</i> Работа с рекомендованной литературой. Подготовка к контрольной работе. Оформление схемы. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	4
1.8. Информационное оружие <i>Задание для самостоятельного выполнения студентом:</i> Работа с рекомендованной литературой. Подготовка к контрольной работе. Оформление схемы. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	4
1.9. Отечественные и зарубежные стандарты информационной безопасности <i>Задание для самостоятельного выполнения студентом:</i> Работа с рекомендованной литературой. Подготовка к контрольной работе. 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	24
Формируемые компетенции, образовательные результаты: УК-8: 3.2 (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. Подготовка к контрольной работе. Оформление схемы. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	4
2.2. Системный анализ угроз безопасности в компьютерных системах Задание для самостоятельного выполнения студентом: Работа с рекомендованной литературой. Подготовка к контрольной работе. Оформление схемы. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	4
2.3. Функции, задачи, методы и системы защиты информации Задание для самостоятельного выполнения студентом: Работа с рекомендованной литературой. Подготовка к контрольной работе. Оформление схемы. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	4
2.4. Криптографические методы защиты информации в автоматизированных системах Задание для самостоятельного выполнения студентом: Работа с рекомендованной литературой. Подготовка к контрольной работе. Оформление схемы. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	4
2.5. Защита персонального компьютера от несанкционированного доступа Задание для самостоятельного выполнения студентом: Работа с рекомендованной литературой. Подготовка к контрольной работе. Оформление практической работы. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	4
2.6. Защита информации в компьютерных системах от несанкционированного доступа Задание для самостоятельного выполнения студентом: Работа с рекомендованной литературой. Подготовка к контрольной работе. Оформление схемы. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	4
3. Раздел 3. Компьютерные вирусы и антивирусные программы. Проблемы защиты информации в сетях ЭВМ. Технические средства и комплексное обеспечение безопасности	27
Формируемые компетенции, образовательные результаты: УК-8: В.2 (УК.8.3), У.2 (УК.8.2), З.2 (УК.8.1)	
3.1. Компьютерный вирус Задание для самостоятельного выполнения студентом: Работа с рекомендованной литературой. Подготовка к контрольной работе. Оформление схемы. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	4
3.2. Методы защиты от компьютерных вирусов Задание для самостоятельного выполнения студентом: Работа с рекомендованной литературой. Подготовка к контрольной работе. Оформление схемы. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	4
3.3. Антивирусы Задание для самостоятельного выполнения студентом: Работа с рекомендованной литературой. Подготовка к контрольной работе. Оформление практической работы. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	4

3.4. Защита информации в сетях ЭВМ Задание для самостоятельного выполнения студентом: Работа с рекомендованной литературой. Подготовка к контрольной работе. Оформление схемы. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	4
3.5. Архитектура механизмов защиты информации в сетях ЭВМ Задание для самостоятельного выполнения студентом: Работа с рекомендованной литературой. Подготовка к контрольной работе. Оформление схемы. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	3
3.6. Технические средства защиты АСОД Задание для самостоятельного выполнения студентом: Работа с рекомендованной литературой. Подготовка к контрольной работе. Оформление схемы. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	4
3.7. Средства контроля доступа Задание для самостоятельного выполнения студентом: Работа с рекомендованной литературой. Подготовка к контрольной работе. Оформление схемы. Учебно-методическая литература: 1, 2, 3, 4, 5, 6, 7	4

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 (МАБИБ), 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
	Конспект по теме	Контрольная работа по разделу/теме	Схема/граф-схема	Зачет/Экзамен
ОПК-1				
3.1 (ОПК.1.1)		+		+
У.1 (ОПК.1.2)	+			+
В.1 (ОПК.1.3)			+	+
УК-8				
3.2 (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":

1. Конспект по теме

Практическое занятие 1

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 документов в сфере информационной безопасности

Количество баллов: 20

2. Контрольная работа по разделу/теме

Тематика контрольной работы:

1. Информационные технологии сферы образования.
2. Психолого-педагогические и технологические тенденции в области образования.
3. Система открытого образования, ее принципы и особенности.
4. Национальные интересы и информационная безопасность России.
5. Уровни обеспечения национальной безопасности.
6. Основные угрозы информационной безопасности России.
7. Информационная война.
8. Информационное оружие.
9. Принципы, основные задачи и функции обеспечения информационной безопасности.
10. Охрана персональных данных.

Количество баллов: 10

3. 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. Конспект по теме

Практическое занятие 2

Защита персонального компьютера от несанкционированного доступа

План:

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.

Практическая часть

Сделайте краткий конспект

Количество баллов: 10

2. Контрольная работа по разделу/теме

Тематика контрольной работы:

1. Криптографические методы защиты информации в автоматизированных системах.
2. Использование классических криптоалгоритмов подстановки и перестановки для защиты текстовой информации.
3. Исследование различных методов защиты текстовой информации и их стойкости на основе подбора ключей.
4. Генерация простых чисел, используемых в асимметричных системах шифрования.
5. Электронная цифровая подпись.
6. Шифрование методом скользящей перестановки
7. Защита персонального компьютера от несанкционированного доступа.
8. Угрозы информации.
9. Вредоносные закладки в ПК и борьба с ними.
10. Защита информации в компьютерных системах от несанкционированного доступа.

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. Конспект по теме

Практическое занятие 3

Антивирусы

План:

1. Классы антивирусных программ.
2. Примеры антивирусных программ.
3. Алгоритм работы антивирусной программы.
4. Распространенных антивирусных программ.

Практическая часть

1. Распишите признаки появления вируса.
2. Сделайте каталог антивирусных программ с их аннотацией.
3. Распишите алгоритм работы антивирусной программы.

Количество баллов: 10

2. Контрольная работа по разделу/теме

Тематика контрольной работы:

1. Цели, функции и задачи защиты информации в сетях ЭВМ.
2. Понятие сервисов безопасности.
3. Архитектура механизмов защиты информации в сетях ЭВМ.
4. Услуги механизмов защиты в сетях.
5. Технические средства защиты АСОД.
6. Средства контроля доступа.
7. Признаки появления вируса.
8. Примеры антивирусных программ.
9. Международные стандарты защита информации в сетях ЭВМ.
10. Комплекс физической защиты АСОД.

Количество баллов: 10

3. Схема/граф-схема

Индивидуальная или групповая работа:

Составить схему «Средства защиты персональных данных»

Составить схему «История криптографии».

Составить схему «Виды криптографической защиты».

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 «ЮУрГТТУ».

Первый период контроля

1. Экзамен

Вопросы к экзамену:

1. Информация как средство отражения окружающего мира и как средство его познания. Количественные оценки и показатели качества информации.
2. Эволюция информационных процессов в обществе. Информатизация и компьютеризация. Информационные ресурсы, продукты и услуги. Объективная необходимость и общественная потребность защиты информации.
3. Информационная безопасность личности, общества и государства. Массовая и конфиденциальная информация. Виды тайн.
4. 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.
5. Компьютерная система (КС) как объект защиты информации. Угрозы информационной безопасности в КС. Классификация угроз.
6. Общая характеристика случайных угроз информационной безопасности в КС.
7. Общая характеристика преднамеренных угроз информационной безопасности в КС.
8. Эволюция концепции информационной безопасности в КС. Основные принципы обеспечения информационной безопасности в КС. Политика безопасности.
9. Реализация угроз информационной безопасности в КС путем несанкционированного доступа (НСД). Классификация каналов НСД. Собираательный образ потенциального нарушителя.
10. Обобщенные модели системы защиты информации в КС. Одноуровневые, многоуровневые и многозвенные модели. Общая характеристика средств и методов защиты информации в КС.
11. Общая характеристика организационных мероприятий, обеспечивающих информационную безопасность КС. Основные задачи службы безопасности.
12. Необходимость правового регулирования в области защиты информации. Информация как объект права собственности. Правоотношения собственника, владельца и пользователя информационных ресурсов.
13. Отечественное законодательство в области информации и защиты информации.
14. Ответственность за правонарушения при работе с компьютерными системами.
15. Эксплуатационная надежность КС как источник возникновения случайных угроз информационной безопасности. Пути ее повышения. Резервирование технических средств. Программно-аппаратный контроль и тестирование.
16. Оптимизация взаимодействия пользователя с КС как средство предотвращения ошибочных операций случайного характера.
17. Помехоустойчивое кодирование. Избыточные коды для обнаружения и исправления случайных ошибок в работе КС.

18. Дублирование информации как средство парирования угроз безопасности в КС. Многоуровневое дублирование.
19. Минимизация ущерба, наносимого КС авариями и стихийными бедствиями.
20. Система охраны объектов КС.
21. Общая характеристика технических каналов утечки информации в КС.
22. Методы и средства защиты информации в КС от утечки по каналам побочных электромагнитных излучений и наводок.
23. Средства противодействия подслушивания и дистанционному наблюдению.
24. Базовые принципы, лежащие в основе моделей политики безопасности в КС. Матричная (дискреционная) модель и мандатная (полномочная) модель управления доступом к ресурсам КС.
25. Идентификация и аутентификация субъектов доступа к ресурсам КС. Парольные методы и оценка их эффективности. Биометрические методы.
26. Средства и методы разграничения доступа к ресурсам КС.
27. Защита программных средств КС от несанкционированного копирования и исследования.
28. Защита от несанкционированного изменения структуры КС в процессе эксплуатации.
29. Контроль целостности программ и данных в процессе эксплуатации КС.
30. Общие понятия, история развития и классификация криптографических средств.
31. Общая характеристика различных методов шифрования. Криптостойкость.
32. Общая характеристика и классификация компьютерных вирусов.
33. Механизм заражения файловыми и загрузочными вирусами. Особенности макровирусов.
34. Средства, используемые для обнаружения компьютерных вирусов.
35. Профилактика заражения компьютерными вирусами.
36. Антивирусные средства для лечения и удаления компьютерных вирусов. Программы-полифаги. Эвристические анализаторы.
37. Чем вызвана необходимость разработки стандартов по защите информации? Охарактеризуйте отечественные нормативы и зарубежные стандарты в этой области.
38. Содержательный смысл понятия комплексной системы защиты информации (КСЗИ) в компьютерных системах. Основные принципы и положения, реализующие системный подход к построению КСЗИ.
39. Функции и задачи защиты, механизмы защиты, уровень защищенности, управление защитой и другие базовые понятия, используемые при формировании КСЗИ.
40. Общетеоретическая постановка задачи оптимизации КСЗИ на основе выбранного критерия эффективности защиты.

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

Отметка	Критерии оценивания
"Отлично"	<ul style="list-style-type: none"> - 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"	<ul style="list-style-type: none"> - 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")	<ul style="list-style-type: none"> - 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")	<ul style="list-style-type: none"> - 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 удастся 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. 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.

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. Контрольная работа по разделу/теме

Контрольная работа выполняется с целью проверки знаний и умений, полученных студентом в ходе лекционных и практических занятий и самостоятельного изучения дисциплины. Написание контрольной работы призвано установить степень усвоения студентами учебного материала раздела/темы и формирования соответствующих компетенций.

Подготовку к контрольной работе следует начинать с повторения соответствующего раздела учебника, учебных пособий по данному разделу/теме и конспектов лекций.

Контрольная работа выполняется студентом в срок, установленный преподавателем в письменном (печатном или рукописном) виде.

При оформлении контрольной работы следует придерживаться рекомендаций, представленных в документе «Регламент оформления письменных работ».

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