МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ОРЛОВСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.В. ПАРАХИНА»

Утверждаю:
И.о. проректора по УМР
_____ Е.Ю. Калиничева
30 апреля 2019 г

Рабочая программа дисциплины

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В СФЕРЕ БЕЗОПАСНОСТИ

Направление подготовки **20.04.01 Техносферная безопасность**

Направленность **Безопасность в техносфере**

Квалификация **магистр**

Форма обучения **заочная**

Год начала подготовки **- 2019**

Орел , 2019г.

Составитель: к.с.-х.н., доцент В.А. Половитсков 16.04 2019 г.

Рецензент: к.т.н., доцент Е.В. Кулакова 16.04 2019 г.

Программа разработана в соответствии с ФГОС ВО по направлению подготовки 20.04.01 Техносферная безопасность, направленность Безопасность в техносфере, квалификация магистр.

Программа обсуждена на заседании кафедры БЖД на производстве

протокол № 11 от 17.04 2019 г.

Зав. кафедрой: к.с.-х.н., доцент Е.В. Яковлева 17.04 2019 г.

Программа рассмотрена и одобрена на заседании Ученого совета факультета агротехники и энергообеспечения

протокол № 12 от 25.04 2019 г.

Декан факультета агротехники и энергообеспечения

к.т.н., доцент И.В. Коношин 25.04 2019 г.

Программа принята учебно-методической комиссией по направлению подготовки 20.04.01 Техносферная безопасность

протокол № 3 от 25.04 2019 г.

Председатель учебно-методической комиссии по направлению подготовки 20.04.01 Техносферная безопасность

к.с.-х.н., доцент Т.А. Шендакова 25.04 2019 г.

Директор научной библиотеки Е.В. Ишханова 24.04 2019 г.

Оглавление

Введение	4
1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы (компетенции обучающегося, формируемые в результате освоения дисциплины)	4
2. Место дисциплины в структуре образовательной программы	4
3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу (во взаимодействии с преподавателем) обучающихся (по видам учебных занятий) и на самостоятельную работу обучающихся..	4
4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий	5
4.1 Содержание модулей и разделов дисциплины	5
4.2 Разделы дисциплин и виды занятий	6
4.3 Тематический план лекций	6
4.4 Практические занятия .	7
4.5 Самостоятельная работа обучающихся	7
5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)	8
6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)	8
7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)	8
8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)	9
9. Перечень методических указаний для обучающихся по освоению дисциплины (модуля)	9
10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости).	11
11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)	11
12. Критерии оценки знаний обучающихся	11
Приложение 1 ФОС.	15

Введение

Рабочая программа (РП) составлена для обучающихся по направлению 20.04.01. «Техносферная безопасность» с присвоением квалификации «Магистр», в соответствии с учебным планом факультета агротехники и энергообеспечения ФГБОУ ВО Орловский ГАУ.

Программа разработана в соответствии с требованиями ФГОС ВО по направлению подготовки 20.04.01 Техносферная безопасность.

РП может быть использована преподавателями при подготовке к занятиям (лекционным, практическим, семинарским, самостоятельным) по дисциплине «Информационные технологии в сфере безопасности»; обучающимися.

Информационные технологии в обеспечении безопасности жизнедеятельности занимают сегодня ключевую позицию в обеспечении техносферной безопасности в России. Перспективы развития данных технологий являются одним из важнейших научных направлений. Стремительность развития информационных технологий, поднимая на новый уровень практическое значение информации, вместе с тем все больше отдаляет нас от понимания сущности самой информации, форм и способов ее проявления, методов воздействия информации на развитие общества, государства и личности. Эти знания необходимы прежде всего для понимания общих принципов и основ информационной безопасности, формулирования всего спектра связанных с ней проблем и определения путей их решения.

«Информационные технологии в сфере безопасности» - специальная дисциплина по направлению 20.04.01 Техносферная безопасность, которую изучают на 1 курсе (1 модуль). Трудоемкость дисциплины в соответствии с ФГОС ВО и Учебным планом направления подготовки 20.04.01 Техносферная безопасность составляет 3 зачетные единицы (108 часа). В конце изучения курса обучающийся сдает экзамен.

1.**Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы (компетенции обучающегося, формируемые в результате освоения дисциплины).**

Целью изучения дисциплины является формирование навыков использования информационных технологий в практической инженерной и научно-исследовательской деятельности.

Задачи:

- сформировать умение анализировать, оптимизировать и применять современные информационные технологии при решении научных задач.

-сформировать навыки использования компьютерных и информационных технологий при решении практических задач в сфере безопасности.

Изучение дисциплины «Информационные технологии в сфере безопасности» при подготовке обучающихся по направлению 20.04.01 Техносферная безопасность, квалификация «Магистр» позволит сформировать следующую общекультурную компетенцию:

ОК-4 способность самостоятельно получать знания, используя различные источники информации.

В результате освоения дисциплины обучающиеся должны:

Знать:

Основные способы обеспечения информационной безопасности в сфере профессиональной деятельности

Уметь:

Решать задачи обеспечения информационной безопасности в сфере профессиональной деятельности

Владеть:

Базовыми приемами работы с программными средствами (офисным программным обеспечением, табличными процессорами и графическими редакторами, программами для работы в сети Интернет)**.**

2. Место дисциплины в структуре образовательной программы.

Дисциплина «Информационные технологии в сфере безопасности» относится к Блоку 1 - базовой части учебного плана по направлению 20.04.01 Техносферная безопасность, которую изучают на 1 курсе.

Трудоемкость дисциплины в соответствии с ФГОС ВО и Учебным планом направления подготовки 20.04.01 Техносферная безопасность составляет 3 зачетные единицы (108 часа). В конце изучения курса магистрант сдает экзамен.

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу (во взаимодействии с преподавателем) обучающихся (по видам учебных занятий) и на самостоятельную работу обучающихся.

Таблица 1. Общая трудоемкость дисциплины 3 зачетные единицы.

Виды учебной нагрузки	Всего часов	1 курс
Аудиторные занятия (всего) в том числе:	12	12
Лекции	4	4
из них: интерактивные формы обучения	2	2
Практические работы из них: • активные формы обучения	8 2	8 2
Самостоятельная работа, КСР	87 9	87 9
Вид промежуточной аттестации	экзамен	экзамен
Общая трудоемкость час/зач. ед	108/3	108/3

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических и видов учебных занятий.

4.1 Содержание модулей и разделов дисциплины

Таблица 2 Содержание модулей и разделов дисциплины

Курс 1 (количество модулей 1)			
Модуль I. Информационная безопасность и уровни ее обеспечения. *Цель*: приобретение знаний, умений и навыков в объеме содержания модуля. В результате усвоения данного модуля формируется компетенция ОК-4.			
№ п/п	Наименование раздела дисциплины, входящего в данный модуль.	Содержание раздела	
		Контактная работа	СР
1	Раздел 1 Информационная безопасность и уровни ее обеспечения.	1.1 Проблема информационной безопасности общества. 1.2. Составляющие информационной безопасности 1.3 Система формирования режима информационной безопасности 1.4 1.4 Нормативно-правовые основы	Проблема информационной безопасности общества. Определение доступности информации. Взаимосвязь между собой составляющие информационной безопасности. Конфиденциальность информации. Стандарты информационной безопасности распределенных систем. Стандарты

		информационной безопасности в РФ	информационной безопасности в РФ. Административный уровень обеспечения информационной безопасности. Классификация угроз "информационной безопасности"
2	Раздел 2 Компьютерные вирусы и защита от них	2.1 Вирусы как угроза информационной безопасности . 2.2 Классификация компьютерных вирусов 2.3 Характеристика "вирусоподобных" программ 2.4 Антивирусные программы	Расширяющий блок. Компьютерные вирусы и информационная безопасность. Профилактика компьютерных вирусов. Правила защиты от компьютерных вирусов. Обнаружение неизвестного вируса. Обнаружение макровируса. Общий алгоритм обнаружения вируса. Обнаружение резидентного вируса. Обнаружение загрузочного вируса.
3	Раздел 3. Информационная безопасность вычислительных сетей	3.1. Особенности обеспечения информационной безопасности в компьютерных сетях. 3.2 Сетевые модели передачи данных. 3.3 Классификация удаленных угроз в вычислительных сетях	Модель взаимодействия открытых систем OSI/ISO. Сравнение сетевых моделей передачи данных TCP/IP и OSI/ISO. Адресация в глобальных сетях. Типовые удаленные атаки и их характеристика. Причины успешной реализации удаленных угроз в вычислительных сетях. Принципы защиты распределенных вычислительных сетей. Механизмы обеспечения "информационной безопасности". Криптография и шифрование. Методы разграничение доступа. Регистрация и аудит.

4.2. Разделы дисциплин и виды занятий

Таблица 3 Разделы дисциплин и виды занятий

Название модуля	Раздел дисциплины, входящего в данный модуль	Лекц.	ПЗ	ЛЗ	СРС	Всего часов
Курс 1						
Модуль I	Раздел 1 Информационная безопасность и уровни ее обеспечения.	0,5	1		12	13,5
	Раздел 2 Компьютерные вирусы и защита от них	0,5	1		12	13,5
	Раздел 3. Информационная безопасность вычислительных сетей	0,5	1		12	13,5
	Раздел 4 Механизмы обеспечения "информационной безопасности"	0,5	1		12	13,5

	Раздел 5 Информационное моделирование и формализация	0,5	1		12	13,5
	Раздел 6 Технологии и средства обработки информации	1	1		15	17
	Раздел 7 Стандарты информационной безопасности распределенных систем	0,5	2		12	14,5
КРС					9	9
Итого		4	8		96	108

4.3. Тематический план лекций

Таблица 4 Тематический план лекций

Название модуля	Раздел дисциплины, входящий в данный модуль	Тема лекции	Трудоемкость (час.)
Курс 1			
Модуль I	Раздел 1 Информационная безопасность и уровни ее обеспечения.	1 Проблема информационной безопасности общества 2 Доступность информации 3 Целостность информации 4 Конфиденциальность информации	0,5
	Раздел 2 Компьютерные вирусы и защита от них	1 Классификация компьютерных вирусов по среде обитания 2 Классификация компьютерных вирусов по особенностям алгоритма работы 3 Классификация компьютерных вирусов по деструктивные возможностям	0,5
	Раздел 3. Информационная безопасность вычислительных сетей	1.Особенности информационной безопасности в компьютерных сетях 2 Специфика средств защиты в компьютерных сетях	0,5
	Раздел 4 Механизмы обеспечения "информационной безопасности"	1 Особенности обеспечения информационной безопасности в компьютерных сетях. 2 Идентификация и аутентификация 3 Регистрация и аудит информационных систем	0,5
	Раздел 5 Информационное моделирование и формализация	1 Информационное моделирование 2 Информационная формализация 3 Информационные процессы и информационные системы	0,5

	Раздел 6 Технологии и средства обработки информации	1 Технологии и средства обработки текстовой информации 2 Технологии и средства обработки числовой информации 3 Технологии и средства обработки графической информации	1
	Раздел 7 Стандарты информационной безопасности распределенных систем	1.Сервисы безопасности в вычислительных сетях 2. Механизмы безопасности 3. Администрирование средств безопасности	0,5
Итого:			**4**

4.4. Практические занятия

Таблица 5 Тематический план

Название модуля	Раздел дисциплины, входящий в данный модуль	Тема	Трудоемкость (час.)
Курс 1			
Модуль I	Раздел 1 Информационная безопасность и уровни ее обеспечения. Раздел 2 Компьютерные вирусы и защита от них	Составляющие информационной безопасности	1
		Нормативно-правовые основы информационной безопасности в РФ	1
	Раздел 3. Информационная безопасность вычислительных сетей	Характеристика "вирусоподобных" программ	1
	Раздел 4 Механизмы обеспечения "информационной безопасности"	Классификация удаленных угроз в вычислительных сетях	1
	Раздел 5 Информационное моделирование и формализация	Сетевые модели передачи данных.	1
	Раздел 6 Технологии и средства обработки информации	1 работа антивирусных программ 2. Классификация антивирусных программ 3. Факторы, определяющие качество антивирусных программ	1
	Раздел 7 Стандарты информационной безопасности распределенных систем	Классификация межсетевых экранов Характеристика межсетевых экранов	2
Итого:			**8**

4.5.Самостоятельная работа обучающихся

Таблица 7 Тематический план самостоятельной работы

	Самостоятельное изучение теоретического материала	Выполнение домашних упражнений и заданий	Написание реферата	Подготовка к отчету по модулям	Трудоемкость (час.)
	Семестр 2				
Модуль I	Проблема информационной безопасности общества. Определение доступности информации. Взаимосвязь между собой составляющие информационной безопасности.	Изучение теоретического материала	написание реферата и подготовка презентации	Изучение теоретического материала	12
	..Конфиденциальность информации. Стандарты информационной безопасности распределенных систем. "	Изучение теоретического материала	написание реферата и подготовка презентации	Изучение теоретического материала	12
	Стандарты информационной безопасности в РФ. Административный уровень обеспечения информационной безопасности. Классификация угроз "информационной безопасности	Изучение теоретического материала	написание реферата и подготовка презентации	Изучение теоретического материала	12
	Расширяющий блок. Компьютерные вирусы и информационная безопасность. Профилактика компьютерных вирусов. Правила защиты от компьютерных вирусов	изучение теоретического материала	написание реферата и подготовка презентации	изучение теоретического материала	12
	Обнаружение неизвестного вируса. Обнаружение макровируса. Общий алгоритм обнаружения вируса. Обнаружение резидентного вируса. Обнаружение загрузочного вируса	изучение теоретического материала	написание реферата и подготовка презентации	изучение теоретического материала	12
	Модель взаимодействия открытых систем OSI/ISO. Сравнение сетевых моделей передачи данных TCP/IP и OSI/ISO. Адресация в глобальных сетях. Типовые удаленные атаки и их характеристика.	изучение теоретического материала	написание реферата и подготовка презентации	изучение теоретического материала	15
	Причины успешной реализации удаленных угроз в вычислительных сетях. Принципы защиты распределенных вычислительных сетей. Механизмы обеспечения "информационной безопасности". Криптография и	изучение теоретического материала	написание реферата и подготовка презентации	изучение теоретического материала	12

	шифрование. Методы разграничение доступа. Регистрация и аудит.				
КСР:					9
Всего часов:					96

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю).

Обучающейся имеет не ограниченный доступ к информационно-образовательной среде университета http://80.76.178.26/subject/index/card/subject_id/1455

1. *Казарин, О. В.* Надежность и безопасность программного обеспечения : учебное пособие для бакалавриата и магистратуры / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2019. — 342 с. — (Бакалавр и магистр. Модуль). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/441287

2. *Щеглов, А. Ю.* Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — М. : Издательство Юрайт, 2018. — 309 с. — (Серия : Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. Режим доступа: https://biblio-online.ru/viewer/9CD7BE3A-F9DC-4F6D-8EC6-6A90CB9A4E0E/zaschita-informacii-osnovy-teorii#page/1

6 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Фонд оценочных средств представлен в Приложении 1 рабочей программы и включает в себя:

- перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программа;

-описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;

- типовые контрольные задания и материалы, необходимые для оценки знаний, умений, навыков и опыта деятельности, характеризующих этапы формированиякомпетенций в процессе освоения образовательной программы;

- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

а) основная литература

1. *Казарин, О. В.* Надежность и безопасность программного обеспечения : учебное пособие для бакалавриата и магистратуры / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2019. — 342 с. — (Бакалавр и магистр. Модуль). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/441287 (дата обращения 16.04.19).

2. *Внуков, А. А.* Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019. — 240 с. — (Профессиональное образование). — ISBN 978-5-534-10711-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/431332 (дата обращения 16.04.19)

б) дополнительная литература

Полякова Т.А. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2019. — 325 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/432966 (дата обращения 16.04.19)

Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — (Университеты России). — ISBN 978-5-534-00258-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/434171 (дата обращения 16.04.19).

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. ЭБС издательства «Юрайт» https://biblio-online.ru/ (http://library.orelsau.ru/els-remote-access-by-subscription.php) (дата обращения 16.04.19), неограниченный доступ;

2. ЭБС издательства «Лань» https://e.lanbook.com/ (http://library.orelsau.ru/els-remote-access-by-subscription.php) (дата обращения 16.04.19), неограниченный доступ;

3. ЭБС «IPRbooks» http://www.iprbookshop.ru/ (http://library.orelsau.ru/els-remote-access-by-subscription.php) (дата обращения 16.04.19), неограниченный доступ;

4. Национальный цифровой ресурс «Руконт» https://rucont.ru/chapter/rucont (http://library.orelsau.ru/els-remote-access-by-subscription.php) (дата обращения 16.04.19), неограниченный доступ;

5. Научная электронная библиотека eLIBRARY https://elibrary.ru/defaultx.asp (http://library.orelsau.ru/els-remote-access-by-subscription.php) (дата обращения 16.04.19), неограниченный доступ;

6. Электронный каталог (АИБС «МАРК-SQL»): http://library.orelsau.ru/marcweb/ (http://library.orelsau.ru/els-remote-access-by-subscription.php (дата обращения 16.04.19), неограниченный доступ.

9. Методические указания для обучающихся по освоению дисциплины (модуля).

Приступая к изучению дисциплины, обучающимся необходимо внимательно ознакомиться с тематическим планом занятий, списком рекомендованной научной литературы.

Преподавание дисциплины предусматривает:

- лекции
- практические занятия
- самостоятельную работу,
- консультации преподавателя.

Лекции по дисциплине читаются как в традиционной форме, так и с использованием активных форм обучения.

Главной задачей каждой лекции является раскрытие сущности темы и анализ ее главных положений. Рекомендуется на первой лекции довести до внимания обучающихся структуру курса и его разделы, а также рекомендуемую литературу. В дальнейшем указывать начало каждого раздела, суть и его задачи, а, закончив изложение, подводить итог по этому разделу, чтобы связать его со следующим.

Содержание лекций определяется рабочей программой курса. Каждая лекция должна охватывать определенную тему курса и представлять собой логически вполне законченную работу.

Для максимального усвоения дисциплины рекомендуется изложение лекционного материала с элементами обсуждения. Лекционный материал может сопровождаться конкретными примерами.

Целями проведения практических занятий являются:

- установление связей теории с практикой в форме экспериментального подтверждения положений теории;
- развитие логического мышления;
- умение выбирать оптимальный метод решения;
- приобретение навыков анализа полученных результатов;
- контроль самостоятельной работы обучающихся по освоению курса.

Каждое практическое занятие целесообразно начинать с повторения теоретического материала (устный опрос).

На практических занятиях могут проводиться предусмотренные рабочей программой деловые игры, контрольные работы, выполнение кейс-заданий и практикующих упражнений, тестирование и др.

Самостоятельная работа обучающихся предусматривает:

- Самостоятельное изучение теоретического материала.

Теоретический материал по тем темам, которые вынесены на самостоятельное изучение, обучающийся прорабатывает в соответствии с вопросами для подготовки к экзамену или зачету. При возникновении затруднений в ходе самостоятельного изучения тем, обучающийся может обратиться за консультацией к преподавателю.

- Подготовка к практическим занятиям.

В ходе подготовки к практическим занятиям обучающимся следует внимательно ознакомиться с планом, вопросами, вынесенными на обсуждение, изучить соответствующий лекционный материал, предлагаемую учебно-методическую и научную литературу. Нельзя ограничиваться только имеющейся учебной литературой (учебниками и учебными пособиями). Обращение к монографиям, статьям из специальных журналов, хрестоматийным выдержкам, а также к материалам средств массовой информации позволит в значительной мере углубить проблему, что разнообразит процесс ее обсуждения.

С другой стороны, обучающимся следует помнить, что они должны не просто воспроизводить сумму полученных знаний по заданной теме, но и творчески переосмыслить существующее в современной науке подходы к пониманию тех или иных проблем, явлений, событий продемонстрировать и убедительно аргументировать собственную позицию.

В целом же активное заинтересованное участие обучающихся в семинарской работе способствует более глубокому изучению дисциплины, повышению уровня культуры будущих специалистов и формированию основ профессионального мышления. В ходе занятий отрабатываются умения применять полученные теоретические знания в различных экономических ситуациях.

- Выполнение домашних заданий.

Для закрепления теоретического материала и получения практических навыков обучающиеся выполняют домашние задания. Выполнение домашних заданий призвано обратить внимание обучающихся на наиболее сложные, ключевые и дискуссионные аспекты изучаемой темы, помочь систематизировать и лучше усвоить пройденный материал.

Контроль самостоятельной работы обучающихся по выполнению домашних заданий осуществляется преподавателем с помощью выборочной и фронтальной проверок письменных и устных индивидуальных заданий на практических занятиях.

Пакет заданий для самостоятельной работы рекомендуется выдавать в начале семестра, определив предельные сроки их выполнения и сдачи. Результаты самостоятельной работы контролируются преподавателем и учитываются при аттестации обучающегося (при сдаче зачета, экзамена).

Задания для самостоятельной работы составляются, как правило, по темам и вопросам, по которым не предусмотрены аудиторные занятия, либо требуется дополнительно проработать и проанализировать рассматриваемый преподавателем материал в объеме запланированных часов.

Консультации преподавателя для обучающихся проводятся в соответствии с утвержденным на кафедре графиком. Консультации могут быть индивидуальными или групповыми, проводиться в соответствующих аудиториях или в информационно-образовательной среде вуза.

Текущий контроль знаний по основным терминам и понятиям изучаемой дисциплины осуществляется на учебных занятиях в виде устного опроса и тестирования. При подготовке к контактной работе, обучающимся необходимо повторить изученный материал.

Обучающийся получает допуск к сдаче зачета при успешном выполнении вех видов учебных занятий.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости).

Образовательный портал Орловского ГАУ на платформе eLearning Server 4G, разработчик Hypermethod

Программное обеспечение:

Microsoft Windows XP Professional, число лицензий: н/д, номер лицензии: 61760053, срок действия: бессрочно;

Microsoft Office 2013 Russian Academic версия 2013, Sku: O21-10232, число лицензий: 42, авторизационный номер лицензиата: 91766136ZZE1504, номер лицензии: 61760053, дата выдачи настоящей лицензии: 05.04.2013, срок действия: бессрочно;

Kaspersky Endpoint Security для бизнеса — Стандартный Russian Edition, Sku: Tr000266331/Tr023274, число лицензий: 600, авторизационный номер лицензиата: KL4863RATFQ номер лицензии: 17EO-180723-132302-727-122, дата выдачи настоящей лицензии: с 23.07.2018 до 31.08.2019

Современные профессиональные базы данных и информационные справочные системы:

1. Электронно-библиотечная система Издательства Лань - e.lanbook.com (неограниченный доступ);
2. Информационно-справочная система «Техэксперт» - https://cntd.ru (неограниченный доступ);
3. Информационный портал «Охрана труда в России» - Электронно-библиотечная система - https://ohranatruda.ru (открытый доступ);
4. ПримТруд.ру – Новости и информация по Охране труда в России - https://primtrud.ru/ (открытый доступ);

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

Для проведения занятий используются специальные помещения, представляющие собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

Наименование специальных помещений и помещений для самостоятельной работы	**Оснащенность специальных помещений и помещений для самостоятельной работы**
Учебная аудитория № 7 (учебно-производственная база) – аудитория для проведения занятий лекционного типа	Специализированная мебель; мультимедийное оборудование стационарного или переносного типа; учебно-наглядные пособия, обеспечивающие тематические иллюстрации в соответствии с рабочей программой; компьютерная техника с подключением к сети «Интернет» и электронной информационно-образовательной среде вуза; копирующая доска UB-5315, цифровой проектор RowerLight, экран на треноге DRAPER DIPLOMAT, плакат на баннерной ткани
Учебная аудитория № 2-213Б (учебный корпус 2) (компьютерный класс)	Специализированная (учебная) мебель, мультимедийное оборудование, учебно-наглядные пособия, обеспечивающие тематические иллюстрации; компьютерная техника.
Учебная аудитория № 2-306 (учебный корпус 2) (компьютерный класс) – аудитория для самостоятельной работы	Специализированная (учебная) мебель, мультимедийное оборудование, интерактивная доска, рабочие компьютерные станции.

12. Критерии оценки знаний обучающихся

По результатам аудиторной и самостоятельной работы, отчётов по темам модуля обучающийся набирает определённое количество баллов. Распределение баллов в семестре приведено в схеме 1 «Распределение баллов в семестре».

Критерии начисления основных баллов по результатам текущего контроля знаний

Критерии оценки отчета по модулю

Модуль	**Кол-во баллов**	**Кол-во баллов, необходимых для сдачи модуля**
1	0…40	8…40
Всего	0…40	8…40

Критерии начисления дополнительных баллов

Критерии оценки письменной самостоятельной работы обучающихся обобщающего творческого характера

Критерий	Кол-во баллов
Понимание содержания самостоятельной работы, через четкую формулировку целей и ее задач	0…2
Наличие плана выполнения самостоятельной работы	0…2
Наличие теоретических знаний при выполнении самостоятельной работы	0…5
Наличие практических умений при выполнении самостоятельной работы	0…5
Наличие и формулировка выводов	0…2
Грамматика и стилистика письменного отчета по самостоятельной работе	0…2
Оформление отчета	0…2
Всего	0…20

Активное участие в занятиях, проводимых в интерактивной форме, оценивается 0…5 баллов.

Критерии начисления поощрительных баллов

По результатам научно-исследовательской и творческой работы обучающийся максимально может набрать 15 баллов, которые начисляются следующим образом:

- участие в олимпиаде – 3 балла;
- участие в конкурсе – 3 балла;
- выступление на конференции, круглом столе и т.п. – 3 балла;
- публикация статьи – 3 балла;
- выполнение индивидуальных творческих заданий – 3 балла.

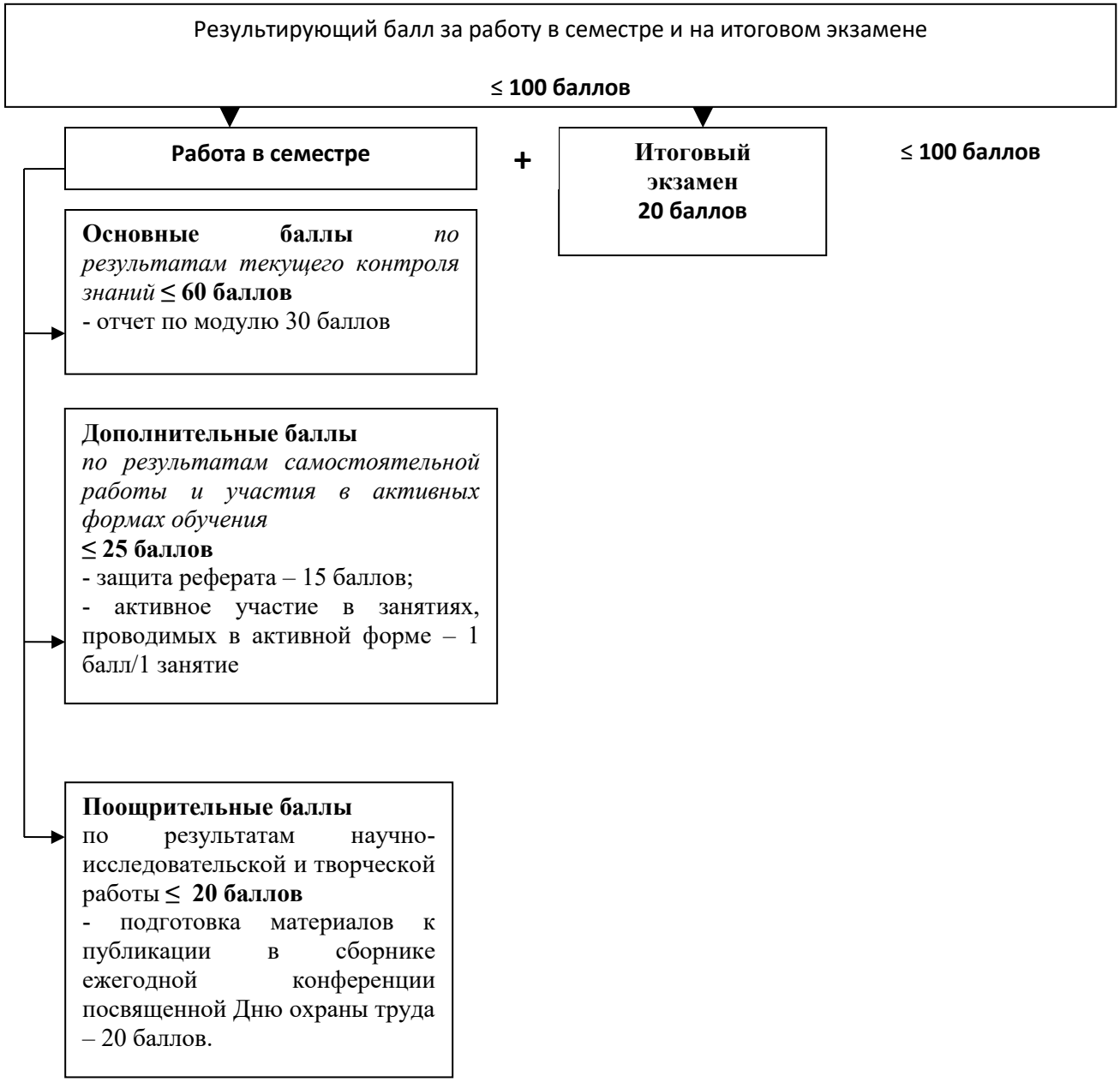
После проведения контрольных мероприятий по дисциплинарному модулю, преподавателем выставляется рейтинговая оценка, представляющая собой сумму рейтинговых баллов, полученных обучающимся на текущем контроле.

Для получения зачета без сдачи промежуточной аттестации, обучающемуся необходимо набрать не менее 55 баллов.

Таблица 10 – Таблица пересчета в традиционные оценки

Рейтинговая оценка	0..54	55...69	70…84	85...100
Академическая оценка	Неудовл.	Удовл.	Хорошо	Отлично

Схема 1 РАСПРЕДЕЛЕНИЕ БАЛЛОВ В СЕМЕСТРЕ



ПРИЛОЖЕНИЕ 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине

Информационные технологии в сфере безопасности

Направление подготовки **20.04.01 Техносферная безопасность**
Направленность **Безопасность в техносфер**е
Квалификация **магистр**

Орел – 2018

***1*. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы**

Код контролируемой компетенции (или ее части) и ее формулировка	***Контролируемые разделы (темы) дисциплины (практики) (результаты по разделам)***	***Уровни освоения компетенции***	***Наименование оценочного средства***	
			Текущий контроль	***Промежуточная аттестация***
способность самостоятельно получать знания, используя различные источники информации (**ОК-4**)	Раздел 1 Информационная безопасность и уровни ее обеспечения. Раздел 2 Компьютерные вирусы и защита от них Раздел 3. Информационная безопасность вычислительных сетей Раздел 4 Механизмы обеспечения "информационной безопасности" Раздел 5 Информационное моделирование и формализация Раздел 6 Технологии и средства обработки информации Раздел 7 Стандарты информационной безопасности распределенных систем	Пороговый	Вопросы для самопроверки, тест	Вопросы к экзамену, итоговые тесты
		Повышенный	Тест, кейс-задачи	
		Высокий	Задания для самостоятельной работы обучающихся, решение ситуационных и практических задач, написание реферата	
		Повышенный	Тест, кейс-задачи	
		Высокий	Задания для самостоятельной работы обучающихся, решение ситуационных и практических задач, написание реферата	

2.Описание показателей и критериев оценивания уровня, приобретенных компетенций на различных этапах их формирования

Код контролируемой компетенции (или ее части)	***Критерии в соответствии с уровнем освоения основной профессиональной образовательной программы***			***Технологии формирования***
	пороговый (базовый) (удовлетворительно) 55-69 баллов	***повышенный (хорошо) 70-84 баллов***	***высокий (отлично) 85-100 баллов***	
способность самостоятельно получать знания, используя	***Знает*** Анализирует, оптимизирует и применяет современные	***Знает*** Основные принципы творческой деятельности.	***Знает*** Основные сведения о дискретных структурах,	Лекции и практические занятия с использованием активных и

различные источники информации (ОК-4)	информационные технологии при решении научных задач	Определяет специфику научных исследований в практике профессиональной работы. Классифицирует информационные ресурсы предметной области. Знает основы методологии научных исследований и осуществляет их применение в основных информационных ресурсах по профилю направления.	используемых в персональных компьютерах; архитектуру компьютерной техники, состав и назначение основных элементов персонального компьютера; структуры локальных и глобальных компьютерных сетей; файловую структуру операционных систем;	интерактивных приёмов обучения. Самостоятельная работа.
	Умеет работать в качестве пользователя персонального компьютера, использовать внешние носители информации для обмена данными между машинами; использовать основные приемы управления файлами;	***Умеет*** самостоятельно получать знания, используя различные источники информации, - использовать принципы организации научно-исследовательской деятельности, методы и технологии теоретических и экспериментальных исследований в профессиональной деятельности.	***Умеет*** Обосновывать актуальность выбранного научного направления. Адекватно подбирает средства и методы для решения поставленных задач. Эффективно использует выбранные методики проведения научных исследований в сфере информационны х технологий .	Лекции и практические занятия с использованием активных и интерактивных приёмов обучения. Самостоятельная работа.
	Владеет Организует и проводит исследовательскую работу в соответствии с методологией научной и практической профессиональной деятельности	***Владеет*** Обрабатывает различными способами полученные эмпирические данных и интерпретирует их.	***Владеет*** Владеет методами анализа и самоанализа, а так же понятийно-категориальным аппаратом научной и практической профессиональн ой деятельности,	Лекции и практические занятия с использованием активных и интерактивных приёмов обучения. Самостоятельная работа.

			способствующими развитию личности научного работника..	

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения основной профессиональной образовательной программы

Оценочные средства для проведения промежуточной аттестации

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

Вопросы для экзамена по дисциплине
Информационные технологии в сфере безопасности

Вопросы для формирования компетенции ОК-4

1. Проблема информационной безопасности общества
2. Составляющие информационной безопасности
3. Система формирования режима информационной безопасности
4. Нормативно-правовые основы информационной безопасности в РФ
5. Вирусы как угроза информационной безопасности
6. Классификация компьютерных вирусов

a. Характеристика "вирусоподобных" программ

7. Антивирусные программы
8. Профилактика компьютерных вирусов
9. Особенности обеспечения информационной безопасности в компьютерных сетях

a. Сетевые модели передачи данных

10. Модель взаимодействия открытых систем OSI/ISO
11. Адресация в глобальных сетях
12. Классификация удаленных угроз в вычислительных сетях
13. Идентификация и аутентификация
14. Криптография и шифрование
15. Методы разграничение доступа
16. Регистрация и аудит
17. Межсетевое экранирование
18. Информационные технологии. Структура информационного процесса. Сбор, обработка, хранение и передача информации.
19. Понятие информационной технологии. Свойства, предмет, цель и средства информационных технологий.
20. Уровни представления информационных технологий. Концептуальное представление, описание информационных потоков, описание методов получения, обработки и хранения информации, описание инструментальных средств.
21. Информационная система. Понятия, свойства и виды информационных систем. Делимость и целостность информационных систем.
22. Классификация информационных систем по степени автоматизации. Ручные, автоматизированные и автоматические информационные системы. Примеры.
23. Классификация информационных систем по сфере применения. Научные системы, системы автоматизированного проектирования, системы организационного управления, системы автоматизированного управления технологическими процессами и др. Примеры.
24. Структура и состав информационной системы. Функциональные компоненты

25. Системы обработки данных. Виды обеспечения. Информационное, программное, техническое, правовое и лингвистическое обеспечение системы обработки данных.

26. Организационные компоненты информационных систем. Проблемы и задачи, решаемые организационными компонентами. Примеры.

27. Методы исследования данных, использующиеся при сборе информации.

28. Информационная технология обработки данных. Цель. Задачи обработки данных. Характеристика и назначение. Основные компоненты. Отличительные черты. Сфера применения. Примеры.

29. Информационная технология управления. Характеристика и назначение. Цель. Задачи обработки данных. Основные компоненты. Отличительные черты. Сфера применения. Примеры.

31. Информационная технология автоматизации офисной деятельности. Характеристика и назначение. Цель. Задачи. Основные компоненты. Отличительные черты. Сфера применения. Примеры.

32. Информационная технология поддержки принятия решений. Характеристика и назначение. Цель. Задачи. Особенности. Основные компоненты. Отличительные черты. Сфера применения. Примеры.

33. Информационная технология экспертных систем. Характеристика и назначение. Цель. Задачи. Особенности. Основные компоненты. Отличительные черты. Основные режимы работы. Сфера применения. Примеры.

34. Классификация программного обеспечения. Базовое, системное, служебное и прикладное программное обеспечение. Примеры.

35. Базовое программное обеспечение компьютерных систем.

36. Системное программное обеспечение, его компоненты. Операционные системы,драйверы: их назначение. Краткий обзор операционных систем. Эволюция операционной системы Windows.

a. Служебное программное обеспечение. Утилиты. Их назначение. Архиваторы. Антивирусное программное обеспечение: состав и назначение компонентов

36. Прикладное программное обеспечение. Классификация. Офисные программные продукты, системы автоматизированного проектирования, обработки информации и управления,

информационно-обучающие системы, редакционно-издательские, мульти и гипермедиа системы,

информационно-правовые и справочные системы, вспомогательное и др. программное обеспечение.

37. Программно-аппаратные средства подготовки научных документов. Классы вычислительных машин. Поколения ЭВМ. Современные компьютерные платформы. Персональные компьютеры.

38. Устройство IBM-совместимого персонального компьютера. Классификация IBM PC по маркам процессоров, основные технические характеристики IBM PC.

39. Мониторы и видеоадаптеры, их технические характеристики. Режимы работы и разрешающая способность монитора

40. Современные устройства ввода информации, их назначение, классификация. Устройства ввода графической информации. Сканеры, фото и видеокамеры: их классификация, принцип действия, технические характеристики.

41. Современные устройства вывода информации, их назначение и классификация. Принтеры: их классификация, принцип действия, технические характеристики

42. Классификация и обзор прикладного программного обеспечения.

43. Интегрированное офисное программное обеспечение, краткий обзор существующих интегрированных пакетов (MS Office, Corel WordPerfect Office, OpenOffice.Org, Sun Star Office и др.). Пакет MS Office: его состав и назначение инструментов.

44. Текстовые редакторы и процессоры. Форматы текстовых документов. Понятие редактирования и форматирования текста. Понятия абзаца, стиля, шаблона документа. Текстовый процессор MS Word: назначение, характеристики, средства автоматизации применяемые для создания документов.

45. Электронные таблицы. Назначение и основные понятия. Типы данных. Адресация: абсолютный и относительный адрес. Табличный процессор MS Excel: назначение и характеристики. Выполнение сложных математических расчетов в MS Excel. Встроенные средства автоматизации.

Условные вычисления. Работа в MS Excel как с базой данных. Автоматический и расширенный фильтр. Выбор значений из таблиц с помощью функций ВПР, ГПР. Подведение промежуточных итогов.

46. Системы управления базами данных. Классификация БД. Модели представления данных. Виды связей. Реляционные базы данных. Система управления базами данных MS Access. Назначение и область применения. Основные элементы MS Access. Таблицы. Запросы. Формы. Отчеты. Главная и подчиненные кнопочные формы и их назначение. Конструкторы и мастера в MS Access. Их назначение, область применения и целесообразность использования.

47. Системы автоматизированного перевода текста. Система профессионального машинного перевода PROMT XT. Основные элементы программы. Термины и определения, используемые в программе. Понятие шаблона тематики, алгоритмов перевода, базы ассоциированной памяти. Типы электронных словарей. Последовательность действий для качественного перевода текста. Механизмы повышения качества перевода.

48. Система автоматизированного построения схем MS Visio. Назначение. Основные возможности. Преимущества перед другими системами. Недостатки. Основные

49. элементы MS Visio. Категории, шаблоны (stencil), чертежи (drawing), инструменты (tools), заготовки (shape) и их наборы. Мастера. Создание отчетов в MS Visio, способы эффективного использования этой возможности.

50. Технологии обработки графической информации. Понятие о компьютерной графике. Представление и обработка графической информации. Растровая и векторная графика. Способы хранения графической информации и форматы графических файлов. Графический редактор: назначение и основные возможности. Графические примитивы и объекты, операции над ними.

51. Программные прикладные интегрированные пакеты и системы. Назначение и возможности.

a. Классы решаемых задач. Графическая интерпретация результатов решения профессиональных задач

52. Обзор Case-средств и области их применения. Классификация. Методологии моделирования, используемые в Case-средствах. Возможности Case-средств, перспективы развития и применения Case-технологий.

53. Универсальный язык моделирования UML. Основные элементы. Диаграммы UML

и их назначение.

54. Основы сетевых технологий. Топология компьютерных сетей. Классификация сетей передачи данных: локальные, территориальные и глобальные компьютерные сети: технические характеристики, основные отличительные черты и возможности. Современные технологии доступа (подключения) к компьютерным сетям.

55. Сеть Интернет. Сервисы Интернет. Протоколы Интернет. Двух- и трехзвенные клиент-серверные архитектуры. Программное обеспечение для создания распределенных Интернет-приложений. HTTP-сервер Apache, интерпретатор серверных сценариев PHP, СУБД MySQL – роль и назначение, преимущества и недостатки программного обеспечения с открытым исходным кодом, для реализации Интернет-приложений

56. Понятие "информационная безопасность". Составляющие информационной безопасности.

57. Понятие web-сайта. Этапы создания сайта, методы создания интернетстраницы.

Критерии оценки (в баллах):

- 5 баллов выставляется студенту, если ответ соответствует теме, вопрос полностью раскрыт;

- 4 балла выставляется студенту, если в ответах имеются незначительные ошибки;

- 3балл выставляется студенту, если содержание ответа не соответствует заданному вопросу, даются ссылки на не действующие нормативно-правовые акты, студент путается в ответах, понятиях;

- 2 баллов выставляется студенту, если ответ отсутствует

Вопросы для самостоятельного изучения

Информационные технологии в сфере безопасности

1. Программный пакет OPEN OFFICE.
2. Программный пакет Photoshop и его возможности.
3. Обзор и возможности графических программ.
4. Возможности программы Statistica.
5. Обмен информацией в сети, интернет.
6. Возможности программы Grapher для построения диаграмм.
7. Базы данных на примере Acsess.
8. Программный пакет Adobe Acrobat.
9. Полнотекстовые базы данных по областям знаний и условия доступа к ним.
10. Обзор математических программный пакетов.
11. Графический редактор Corel Photo Paint, MSVisio.
12. Обзор интерфейса (меню, панели инструментов, диалоговые окна). Основные команды.
13. Графический редактор Micrografx Picture Publisher. Обзор интерфейса (меню, панели инструментов, диалоговые окна). Основные команды.
14. Обзор полнотекстовых и библиографических баз данных. Примеры использования при поиске информации в области природоохранной деятельности и защиты в чрезвычайных ситуациях
15. Обзор полнотекстовых и библиографических баз данных. Примеры использования при поиске информации в области природоохранной деятельности
16. Понятие о базах данных. Классификация БД. Модели данных.
17. Системы управления базами данных. База данных Access.
18. Основные объекты БД. Языки запросов QBE и SQL. Экспертные системы. Применение БД в области техносферной безопасности.
19. Классификация ГИС. Сферы применения ГИС.
20. Возможности ГИС. Компоненты ГИС. Работа ГИС.
21. Примеры использования ГИС в экологическом мониторинге, предупреждении чрезвычайных ситуаций и других областях.
22. Программные средства для построения зависимостей различного типа: гистограммы, 3DXYY (трехмерные графики), 3DXYZ (трехмерные графики), Contourmaps (двухмерное представление трехмерных зависимостей), Surfacemaps (трехмерное изображение XYZ данных) и др. в программах Excel, Grapher, Statistica. Построение зависимостей с аппроксимацией. Обзор интерфейса (меню, панели инструментов, диалоговые окна). Основные команды. Основные приемы управления данными в этих приложениях.
23. Современные статистические и математические комплексы: Mathematica, MathLAB, Maple, MathCAD, Statistica, SPSS, SAS, StatGraphics, Origin. Классы статистических задач, решаемые комплексами. Сравнительная характеристика.
24. Основные модули Statistica for Windows как интегрированного пакета по обработке данных: Basic Statistics, Nonparametrics/Distrib., ANOVA/MANOVA, Multiple Regression, Nonlinear Estimation, Factor Analysis, Quality Control Charts, Experimental Design и др. Обзор интерфейса (меню, панели инструментов, диалоговые окна). Графические методы представления данных. Краткий обзор типов графиков.
25. Модуль Factor Analysis. Общее назначение
26. Факторный анализ как метод редукции данных. Факторный анализ как метод классификации

Критерии оценки (в баллах):

- 5 баллов выставляется студенту, если ответ соответствует теме, вопрос полностью раскрыт;
- 4 балла выставляется студенту, если в ответах имеются незначительные ошибки;
- 3балл выставляется студенту, если содержание ответа не соответствует заданному вопросу, даются ссылки на не действующие нормативно-правовые акты, студент путается в ответах, понятиях;
- 2 баллов выставляется студенту, если ответ отсутствует

Перечень дискуссионных тем для круглого стола (дискуссии, полемики, диспута, дебатов)

по дисциплине *Информационные технологии в сфере безопасности*

1.Применение геоинформационных технологий в области защиты от чрезвычайных ситуаций

2. Применение геоинформационных технологий в области природоохранной деятельности

3. Автоматизированное место специалиста в области аттестации рабочих мест

4. Автоматизированное место специалиста в области охраны труда

5. Применение текстовых технологий в управлении техносферной безопасностью

6. Полнотекстовые базы данных и технологии поиска документов в области техносферной безопасности

7. Применение информационных технологий при оценке воздействия на окружающую среду (Эколог)

8. Применение информационных технологий при оценке воздействия на окружающую среду (Эра)

9. Базы данных и технологии их использования в сфере техносферной безопасности

10. Экспертные системы и технологии их использования в сфере техносферной безопасности

11. Техника безопасной работы в интернет (защита компьютера от взлома, вирусов при работе с сервисами Интернет).

12. Правовые информационные системы. Основные возможности правовых информационных систем в области техносферной безопасности.

13. Использование Интернет технологии в сфере техносферной безопасности

14. Информационные технологии в управлении рисками

15. Информационные технологии в управлении охраной окружающей среды

16. Применение информационных технологий при моделировании процессов в чрезвычайных ситуациях (Phoenics)

17. Применение информационных технологий при моделировании процессов в чрезвычайных ситуациях (Matlab)

18. Применение информационных технологий при моделировании химических аварий

19. Применение нормативно-правовой базы и программного обеспечения для моделирования сценария развития ЧС на потенциально опасных объектах

20. Автоматизированное место специалиста в области охраны окружающей среды

21. Применение информационных технологий при моделировании радиационных аварий

Параметры проведения круглого стола

Критерии оценки:	**Условия оценки участия в круглом столе**
5 баллов	Подготовил полный и развернутый доклад; Активно обсуждал проблему и обосновывал свою позицию; Использовал терминологию, концепции, теории при решении проблем безопасности; Проявил высокий уровень способности объективно оценивать проблемы общества в области безопасности, учитывать их в сфере профессиональной деятельности;
4 балла	Подготовил доклад; Принимал участие в обсуждении проблемы; Использовал отчасти терминологию, концепции, теории при решении проблем БЖД; Проявил способность объективно оценивать проблемы общества в области безопасности, учитывать их в сфере проф.деятельности;
3 балла	Не подготовил доклад; Принимал участие в обсуждении проблемы;

Комплект тестов (тестовых заданий)

по дисциплине

Информационные технологии в сфере безопасности

1. **Под информационной безопасностью понимается…**
А) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.
Б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия
В) нет правильного ответа

2. **Защита информации – это..**
А) комплекс мероприятий, направленных на обеспечение информационной безопасности.
Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей
В) небольшая программа для выполнения определенной задачи

3. **От чего зависит информационная безопасность?**
А) от компьютеров
Б) от поддерживающей инфраструктуры
В) от информации

4. **Основные составляющие информационной безопасности:**
А) целостность
Б) достоверность
В) конфиденциальность

5. **Доступность – это**…
А) возможность за приемлемое время получить требуемую информационную услугу.
Б) логическая независимость
В) нет правильного ответа

6. **Целостность – это..**
А) целостность информации
Б) непротиворечивость информации
В) защищенность от разрушения

7. **Конфиденциальность – это..**
А) защита от несанкционированного доступа к информации
Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
В) описание процедур

8. **Для чего создаются информационные системы?**
А) получения определенных информационных услуг
Б) обработки информации
В) все ответы правильные

9**. Целостность можно подразделить:**
А) статическую
Б) динамичную
В) структурную

10 Где применяются средства контроля динамической целостности?
А) анализе потока финансовых сообщений
Б) обработке данных

В) при выявлении кражи, дублирования отдельных сообщений

11 Какие трудности возникают в информационных системах при конфиденциальности?
А) сведения о технических каналах утечки информации являются закрытыми
Б) на пути пользовательской криптографии стоят многочисленные технические проблемы
В) все ответы правильные

12 Угроза – это…
А) потенциальная возможность определенным образом нарушить информационную безопасность
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

13 Атака – это…
А) попытка реализации угрозы
Б) потенциальная возможность определенным образом нарушить информационную безопасность
В) программы, предназначенные для поиска необходимых программ.

14 Источник угрозы – это..
А) потенциальный злоумышленник
Б) злоумышленник
В) нет правильного ответа

15 Окно опасности – это…
А) промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется.
Б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области
В) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере

16. Какие события должны произойти за время существования окна опасности?
А) должно стать известно о средствах использования пробелов в защите.
Б) должны быть выпущены соответствующие заплаты.
В) заплаты должны быть установлены в защищаемой И.С.

17. Угрозы можно классифицировать по нескольким критериям:
А) по спектру И.Б.
Б) по способу осуществления
В) по компонентам И.С.

18. По каким компонентам классифицируется угрозы доступности:
А) отказ пользователей
Б) отказ поддерживающей инфраструктуры
В) ошибка в программе

19. Основными источниками внутренних отказов являются:
А) отступление от установленных правил эксплуатации
Б) разрушение данных
В) все ответы правильные

20 Основными источниками внутренних отказов являются:
А) ошибки при конфигурировании системы
Б) отказы программного или аппаратного обеспечения
В) выход системы из штатного режима эксплуатации

21. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

А) невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности
Б) обрабатывать большой объем программной информации
В) нет правильного ответа

22. Какие существуют грани вредоносного П.О.?
А) вредоносная функция
Б) внешнее представление
В) способ распространения

23. По механизму распространения П.О. различают:
А) вирусы
Б) черви
В) все ответы правильные

24. Вирус – это…
А) код обладающий способностью к распространению путем внедрения в другие программы
Б) способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов
В) небольшая программа для выполнения определенной задачи

25. Черви – это…
А) код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения
Б) код обладающий способностью к распространению путем внедрения в другие программы
В) программа действий над объектом или его свойствами

Вариант 2

1. Конфиденциальную информацию можно разделить:
А) предметную
Б) служебную
В) глобальную

2. Природа происхождения угроз:
А) случайные
Б) преднамеренные
В) природные

3. Предпосылки появления угроз:
А) объективные
Б) субъективные
В) преднамеренные

4. К какому виду угроз относится присвоение чужого права?
А) нарушение права собственности
Б) нарушение содержания
В) внешняя среда

5. Отказ, ошибки, сбой – это:
А) случайные угрозы
Б) преднамеренные угрозы
В) природные угрозы

6. Отказ - это…
А) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

Б) некоторая последовательность действий, необходимых для выполнения конкретного задания
В) структура, определяющая последовательность выполнения и взаимосвязи процессов

7. Ошибка – это…
А) неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния
Б) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
В) негативное воздействие на программу

8. Сбой – это…
А) такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
Б) неправильное выполнение элементом одной или нескольких функций происходящее в следствие специфического состояния
В) объект-метод

9. Побочное влияние – это…
А) нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
Б) негативное воздействие на систему в целом или отдельные элементы
В) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

10. СЗИ (система защиты информации) делится:
А) ресурсы автоматизированных систем
Б) организационно-правовое обеспечение
В) человеческий компонент

11. Что относится к человеческому компоненту СЗИ?
А) системные порты
Б) администрация
В) программное обеспечение

12. Что относится к ресурсам А.С. СЗИ?
А) лингвистическое обеспечение
Б) техническое обеспечение
В) все ответы правильные

13. По уровню обеспеченной защиты все системы делят:
А) сильной защиты
Б) особой защиты
В) слабой защиты

14. По активности реагирования СЗИ системы делят:
А) пассивные
Б) активные
В) полупассивные

15. Правовое обеспечение безопасности информации – это…
А) совокупность законодательных актов, нормативно-правовых документов, руководств, требований, которые обязательны в системе защиты информации
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) нет правильного ответа

16. Правовое обеспечение безопасности информации делится:
А) международно-правовые нормы

Б) национально-правовые нормы
В) все ответы правильные

17. Информацию с ограниченным доступом делят:
А) государственную тайну
Б) конфиденциальную информацию
В) достоверную информацию

18. Что относится к государственной тайне?
А) сведения, защищаемые государством в области военной, экономической … деятельности
Б) документированная информация
В) нет правильного ответа

19. Вредоносная программа - это…
А) программа, специально разработанная для нарушения нормального функционирования систем
Б) упорядочение абстракций, расположение их по уровням
В) процесс разделения элементов абстракции, которые образуют ее структуру и поведение

20. Основополагающие документы для обеспечения безопасности внутри организации:
А) трудовой договор сотрудников
Б) должностные обязанности руководителей
В) коллективный договор

21. К организационно - административному обеспечению информации относится:
А) взаимоотношения исполнителей
Б) подбор персонала
В) регламентация производственной деятельности

22. Что относится к организационным мероприятиям:
А) хранение документов
Б) проведение тестирования средств защиты информации
В) пропускной режим

23. Какие средства используется на инженерных и технических мероприятиях в защите информации:
А) аппаратные
Б) криптографические
В) физические

24. Программные средства – это…
А) специальные программы и системы защиты информации в информационных системах различного назначения
Б) структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла
В) модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними

25. Криптографические средства – это…
А) средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования
Б) специальные программы и системы защиты информации в информационных системах различного назначения
В) механизм, позволяющий получить новый класс на основе существующего

Ключи к тестовым заданиям

Вариант 1

1	2	3	4	5	6	7	8	9	10
А	**А**	**АБ**	**АБВ**	**А**	**АБВ**	**А**	**А**	**Б**	**АВ**
11	12	13	14	15	16	17	18	19	20
В	**А**	**А**	**А**	**А**	**АБВ**	**АБВ**	**АБ**	**В**	**АБВ**
21	22	23	24	25					
А	**АБВ**	**В**	**А**	**А**					

Вариант 2

1	2	3	4	5	6	7	8	9	10
АБ	**АБ**	**АБ**	**А**	**А**	**А**	**А**	**А**	**Б**	**АБВ**
11	12	13	14	15	16	17	18	19	20
АБ	**В**	**АБВ**	**АБ**	**А**	**В**	**АБ**	**А**	**А**	**АБВ**
21	22	23	24	25					
АБВ	**АВ**	**АБВ**	**А**	**А**					

Критерии оценки (в баллах):

(за правильный ответ дается 1 балл)
«не зачет» – 20% и менее;
«зачет» – 21-25%

Лист регистрации изменений

Номер изменения	Текст изменения	Приказ, протокол заседания Ученого совета Университета	
		№	Дата
1.	Внесены изменения и дополнения в структурные компоненты рабочей программы дисциплины в соответствии с ежегодным обновлением литературы, современных профессиональных баз данных, информационных справочных систем, ЭБС.	1	24.09.2020
2.	Внесены изменения и дополнения в структурные компоненты рабочей программы дисциплины в соответствии с ежегодным обновлением литературы, современных профессиональных баз данных, информационных справочных систем, ЭБС.	6	25.02.2021