МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ – МСХА имени К.А. ТИМИРЯЗЕВА»
(ФГБОУ ВО РГАУ - МСХА имени К.А. Тимирязева)

Институт мелиорации, водного хозяйства и строительства имени А. Н. Костякова

Кафедра систем автоматизированного проектирования и инженерных расчетов

УТВЕРЖДАЮ:
Директор института мелиорации, водного хозяйства и строительства имени А.Н. Костякова
Д. М. Бенин, к.т.н., доцент

31 10 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ Б1.О.27 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

для подготовки бакалавров

ФГОС ВО

Направление: 20.03.01 Техносферная безопасность
Направленности: Безопасность цифровых роботизированных технологических процессов и производств; Инженерное обеспечение безопасности населения, окружающей среды и объектов техносферы

Курс 2
Семестр 4

Форма обучения: очная

Год начала подготовки: 2023

Москва, 2023

Разработчик: Петухова М. В., к.п.н, доцент

«28» августа 2023г.

Щедрина Е.В., к.п.н, доцент

«28» августа 2023г.

Рецензент: Худякова Е.В., док.эк.наук, профессор

«29» августа 2023г.

Программа составлена в соответствии с требованиями ФГОС ВО, ПООП, профессионального стандарта по направлению подготовки 20.03.01 «Техносферная безопасность» и учебного плана.

Программа обсуждена на заседании кафедры «Систем автоматизированного проектирования и инженерных расчетов» протокол № 1 от «28» августа 2023г.

И.о. зав. кафедрой Палиивец М.С., канд.тех.наук, доцент

«28» августа 2023г.

Согласовано:
Председатель учебно-методической комиссии института мелиорации, водного хозяйства и строительства имени А.Н. Костякова
Гавриловская Н.В., к.т.н.

«31» 10 2023г.

Заведующий выпускающей кафедрой техносферной безопасности
Борулько В. Г., к.т.н., доцент

«31» 10 2023г.

Заведующий отделом комплектования ЦНБ Ефимова Я.В.

2

СОДЕРЖАНИЕ

Аннотация

рабочей программы учебной дисциплины
Б1.О.27 «Информационная безопасность»
для подготовки бакалавра по направлению
20.03.01 «Техносферная безопасность» направленностей
«Безопасность цифровых роботизированных технологических процессов и производств», «Инженерное обеспечение безопасности населения, окружающей среды и объектов техносферы»

Цель освоения дисциплины: формирование у обучающихся компетенций, обеспечивающих способность осуществлять безопасный поиск, анализ и синтез информации, применять системный подход для решения задач с учетом обеспечения информационной безопасности, способность выстраивать и реализовывать траекторию саморазвития с учетом требований информационной безопасности, способность учитывать современные тенденции развития техники и технологий в области информационной безопасности, информационных технологий при решении типовых задач в области профессиональной деятельности, связанной с защитой окружающей среды и обеспечением безопасности человека, способность понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

Место дисциплины в учебном плане: дисциплина включена в обязательную часть учебного плана по направлению подготовки 20.03.01 «Техносферная безопасность» направленностей «Безопасность цифровых роботизированных технологических процессов и производств», «Инженерное обеспечение безопасности населения, окружающей среды и объектов техносферы», осваивается в 4 семестре.

Требования к результатам освоения дисциплины: в результате освоения дисциплины формируются следующие компетенции: УК-1.1; УК-1.2; УК-1.3; УК-6.3; ОПК-1.1; ОПК-1.2; ОПК-1.3; ОПК-4.1; ОПК-4.2; ОПК-4.3.

Краткое содержание дисциплины:

Понятия информационной безопасности и защиты информации. Основные составляющие информационной безопасности. Категории интересов субъектов информационных отношений (доступность, целостность, конфиденциальность). Угрозы информационной безопасности. Группы мер по защите информации (организационные, программно-технические, правовые). Законодательный уровень информационной безопасности. Вопросы информационной безопасности в законодательных документах РФ. Понятие лицензии на программный продукт. Виды программ по способам распространения.

Защита информации в компьютерных сетях. Общие понятия компьютерных сетей. Структура компьютерной сети. Сетевые средства и службы. Носители для передачи данных в компьютерной сети, соединительное оборудование. Сетевые протоколы. Классификации КС. Топологии локальных КС. Глобальная сеть Интернет: основные службы. Адресация компьютеров в КС. Адрес ресурса в сети. Методы и средства обеспечения информационной безопасности в компьютерной сети организации. Основы безопасности при совместной работы над проектами в локальной сети организации. Совместная работа с документами, возможности рецензирования. Защита документов и форм в Word. Защита в Excel.

Общая трудоемкость дисциплины: 108/3 (часы/зач. ед.).

Промежуточный контроль: зачет в 4 семестре.

1. Цель освоения дисциплины

Целью освоения дисциплины «Информационная безопасность» является формирование у обучающихся компетенций, обеспечивающих способность осуществлять безопасный поиск, критический анализ и синтез информации, применять системный подход для решения задач с учетом обеспечения информационной безопасности, способность управлять своим временем, выстраивать и реализовывать траекторию саморазвития с учетом требований информационной безопасности, способность учитывать современные тенденции развития техники и технологий в области информационной безопасности, вычислительной техники, информационных технологий при решении типовых задач в области профессиональной деятельности, связанной с защитой окружающей среды и обеспечением безопасности человека, способность понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

2. Место дисциплины в учебном процессе

Дисциплина «Информационная безопасность» включена в перечень дисциплин обязательной части учебного плана и реализуется в соответствии с требованиями ФГОС ВО и учебного плана по направлению 20.03.01 «Техносферная безопасность» направленностей «Безопасность цифровых роботизированных технологических процессов и производств», «Инженерное обеспечение безопасности населения, окружающей среды и объектов техносферы». Изучение дисциплины начинается в 4 семестре.

Предшествующими курсами, на которых базируется дисциплина «Информационная безопасность» являются: «Высшая математика», «Информатика и основы САПР», «Безопасность жизнедеятельности».

Дисциплина «Информационная безопасность» является основополагающей для изучения следующих дисциплин: «Применение цифровых инструментов в решении профессиональных задач», «Обеспечение безопасности объектов АПК».

Особенностью дисциплины является использование персональных компьютеров на всех занятиях и работа в прикладном программном обеспечении и государственных базах данных.

Рабочая программа дисциплины «Информационная безопасность» для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

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

Образовательные результаты освоения дисциплины обучающимся, представлены в таблице 1.

Таблица 1

Требования к результатам освоения учебной дисциплины

№ п/п	Код компетенции	Содержание компетенции (или её части)	Индикаторы компетенций	В результате изучения учебной дисциплины обучающиеся должны:		
				знать	уметь	владеть
1.	УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач.	УК-1.1 Знать основы поиска, критического анализа и синтеза информации, системного подхода для решения поставленных задач.	основы поиска, критического анализа и синтеза информации, системного подхода для решения поставленных задач с учетом требований информационной безопасности	осуществлять поиск, критический анализ и синтез информации, системный подход для решения поставленных задач с учетом требований информационной безопасности	методами поиска, критического анализа и синтеза информации, системного подхода для решения поставленных задач с учетом требований информационной безопасности
2.			УК-1.2 Уметь анализировать и систематизировать разнородные данные, оценивать эффективность процедур анализа проблем и принятия решений в профессиональной деятельности.	средства и методы анализа и систематизации данных из сетевых источников, оценки проблем обеспечения информационной безопасности	анализировать и систематизировать данные из сетевых источников, оценивать проблемы обеспечения информационной безопасности	методами анализа и систематизации данных из сетевых источников, оценки проблем обеспечения информационной безопасности
3.			УК-1.3 Владеть навыками научного поиска и практической работы с информационными источниками и методами принятия решений.	средства и методы научного поиска и практической работы с информационными источниками в сети с учетом обеспечения информационной безопасности	применять средства и методы научного поиска и практической работы с информационными источниками в сети с учетом обеспечения информационной безопасности	методами научного поиска и практической работы с информационными источниками в сети с учетом обеспечения информационной безопасности

4.	УК-6	Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни.	УК-6.3 Владеть навыками работы в направлении личностного, образовательного и профессионального роста.	средства и методы работы в направлении личностного, образовательного и профессионального роста в сфере информационных технологий и обеспечения информационной безопасности	применять средства и методы работы в направлении личностного, образовательного и профессионального роста в сфере информационных технологий и обеспечения информационной безопасности	методами работы с информационными технологиями и обеспечения информационной безопасности
5.	ОПК-1	Способен учитывать современные тенденции развития техники и технологий в области техносферной безопасности, измерительной и вычислительной техники, информационных технологий при решении типовых задач в области профессиональной деятельности, связанной с защитой окружающей среды и обеспечением безопасности человека.	ОПК-1.1 Знание принципов, методов и средств решения стандартных задач профессиональной деятельности на основе применения информационно-коммуникационных технологий.	принципы, методы и средств решения стандартных задач профессиональной деятельности на основе применения информационно-коммуникационных технологий	применять принципы, методы и средств решения стандартных задач профессиональной деятельности на основе применения информационно-коммуникационных технологий	методами решения стандартных задач профессиональной деятельности на основе применения информационно-коммуникационных технологий
6.			ОПК-1.2 Умение ориентироваться в основных методах обеспечения техносферной безопасности, используя основные виды измерительной и вычислительной техники при решении типовых задач профессиональной деятельности.	методы обеспечения информационной безопасности, используя вычислительную технику при решении типовых задач профессиональной деятельности	применять методы обеспечения информационной безопасности, используя вычислительную технику при решении типовых задач профессиональной деятельности	методами обеспечения информационной безопасности, используя вычислительную технику при решении типовых задач профессиональной деятельности
7.			ОПК-1.3 Владение техникой и технологиями в области тех-	технологии в области информационной безопасности с учетом со-	применять технологии в области информационной безопасности с уче-	технологиями в области информационной безопасности с учетом

			носферной безопасности с учетом современных тенденций их развития.	временных тенденций их развития	том современных тенденций их развития	современных тенденций их развития
8.	ОПК-4	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-4.1 Знать общие принципы решения научных и практических задач безопасности с применением средств вычислительной техники	общие принципы решения научных и практических задач информационной безопасности с применением средств вычислительной техники	применять общие принципы решения научных и практических задач информационной безопасности с применением средств вычислительной техники	методами решения научных и практических задач информационной безопасности с применением средств вычислительной техники
9.			ОПК-4.2 Уметь использовать существующие информационные технологии, применяемые в области обеспечения экологической, производственной и промышленной безопасности	информационные технологии, применяемые в области обеспечения информационной безопасности	применять информационные технологии в области обеспечения информационной безопасности	методами информационных технологий в области обеспечения информационной безопасности
10.			ОПК-4.3 Навыками работы с информационными технологиями для повышения эффективности управления ТБ	информационные технологии для повышения эффективности обеспечения информационной безопасности	применять информационные технологии для повышения эффективности обеспечения информационной безопасности	методами информационных технологий для повышения эффективности обеспечения информационной безопасности

4. Структура и содержание дисциплины

4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет 3 зач.ед. (108 часов), их распределение по видам работ по семестрам представлено в таблице 2.

ОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 2

Распределение трудоёмкости дисциплины по видам работ по семестрам

Вид учебной работы	Трудоёмкость	
	час. всего	В т.ч. по семестрам
		№4
Общая трудоёмкость дисциплины по учебному плану	**108**	**108**
1. Контактная работа:	**50,25**	**50,25**
Аудиторная работа	**50,25**	**50,25**
в том числе:		
лекции (Л)	16	16
практические занятия (ПЗ)	34	34
контактная работа на промежуточном контроле (КРА)	0,25	0,25
2. Самостоятельная работа (СРС)	**57,75**	**57,75**
самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к практическим занятиям)	48,75	48,75
Подготовка к зачёту	9	9
Вид промежуточного контроля:	Зачет	

4.2 Содержание дисциплины

ОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 3

Тематический план учебной дисциплины

Наименование разделов и тем дисциплин (укрупнённо)	Всего	Аудиторная работа			Внеаудиторная работа СР
		Л	ПЗ всего	ПКР всего	
Раздел 1. Информационная безопасность. Защита информации	53	8	16	-	29
Раздел 2. Защита информации в компьютерных сетях	54,75	8	18	-	28,75
Контактная работа на промежуточном контроле (КРА)	0,25	-	-	0,25	-
Всего за 4 семестр	108	16	34	0,25	57,75
Итого по дисциплине	**108**	**16**	**34**	**0,25**	**57,75**

Раздел 1. Информационная безопасность. Защита информации

Тема 1. Общие понятия информационной безопасности и защиты информации

Понятия информационной безопасности и защиты информации. Основные составляющие информационной безопасности. Категории интересов субъектов информационных отношений (доступность, целостность, конфиденциальность). Угрозы информационной безопасности. Понятие угрозы, атаки, злоумышленника, уязвимых мест в защите, окна опасности. Классификации угроз информационной безопасности. Основные угрозы информационной безопасности. Группы мер по защите информации (организационные, программно-технические, правовые).

Тема 2. Правовые основы информационной безопасности и защиты информации

Законодательный уровень информационной безопасности. Вопросы информационной безопасности в Конституции РФ. Вопросы информационной безопасности в Уголовном кодексе РФ. Основные вопросы, связанные с информационной безопасностью, отраженные в федеральных законах («Об информации, информационных технологиях и защите информации», «Об электронной подписи», «О персональных данных» и др.). Понятие лицензии на программный продукт. Виды программ по способам распространения. Типовые условия, включаемые в коммерческую лицензию. Понятие и условия открытой лицензия GNU GPL. Понятие нелицензионного программного продукта. Угрозы при использовании нелицензионных программ.

Раздел 2. Защита информации в компьютерных сетях

Тема 3. Общие понятия компьютерных сетей

Понятие компьютерной сети (КС). Общая структура компьютерной сети. Сетевые средства и службы: понятие, примеры и назначение сетевых служб. Носители для передачи данных в компьютерной сети: кабельное соединение (виды кабелей), беспроводное соединение. Соединительное оборудование: основные устройства и их назначение. Сетевые протоколы: понятие, назначение. Модель OSI, стек протоколов TCP/IP. Классификации КС. Топологии локальных КС. Глобальная сеть Интернет: основные службы. Адресация компьютеров в КС. Адрес ресурса в сети.

Тема 4. Защита информации в компьютерной сети

Методы и средства обеспечения информационной безопасности в компьютерной сети организации. Политика информационной безопасности. Антивирусная защита, брандмауэры, электронные ключи.

Основы безопасности при совместной работы над проектами в локальной сети организации. Совместная работа с документами, возможности рецензирования. Защита документов и форм в Word: установка параметров автосохранения, установка пароля на открытие и редактирование документа, создание форм и установка ограничений на редактирование форм. Защита в Excel: установка параметров автосохранения, установка пароля на открытие книги, защита элементов листа. Создание интерактивного файла Excel с применением с защитой

блоков листа от доступа, от изменения. Доступ к открытым данным в государственных информационных системах.

4.3 Лекции/практические занятия

ОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 4

Содержание лекций, практических занятий и контрольные мероприятия

№ п/п	Название раздела, темы	№ и название лекций/ практических занятий	Формируемые компетенции	Вид контрольного мероприятия	Кол-во часов
1.	**Раздел 1. Информационная безопасность. Защита информации**				**24**
	Тема 1. Общие понятия информационной безопасности и защиты информации	Лекция №1. Общие понятия информационной безопасности и защиты информации	УК-1.1, ОПК-1.1, ОПК-4.1	-	2
		Практическое занятие №1, 2. Виды угроз информационной безопасности и определение объектов защиты информации организации или структурного подразделения	УК-1.2, УК-1.3, УК-6.3, ОПК-1.2, ОПК-1.3, ОПК-4.2, ОПК-4.3	тестирование	4
		Лекция №2. Группы мер по защите информации	УК-1.1, ОПК-1.1, ОПК-4.1	-	2
		Практическое занятие №3, 4. Классификация информации по конфиденциальности и анализ инцидентов информационной безопасности	УК-1.2, УК-1.3, УК-6.3, ОПК-1.2, ОПК-1.3, ОПК-4.2, ОПК-4.3	защита практических заданий	4
	Тема 2. Правовые основы информационной безопасности и защиты информации	Лекция №3. Нормативные документы в сфере информационной безопасности и защиты информации	УК-1.1, ОПК-1.1, ОПК-4.1	-	2
		Практическое занятие №5, 6. Анализ нормативных документов в сфере информационной безопасности и защиты информации, и ознакомление с регламентирующими документами в сфере информации, ИТ и ИС в РФ	УК-1.2, УК-1.3, УК-6.3, ОПК-1.2, ОПК-1.3, ОПК-4.2, ОПК-4.3	тестирование, защита практических заданий	4
		Лекция №4. Классификация программ по способам распространения	УК-1.1, ОПК-1.1, ОПК-4.1	-	2

№ п/п	Название раздела, темы	№ и название лекций/ практических занятий	Формируемые компетенции	Вид контрольного мероприятия	Кол-во часов
		Практическое занятие №7, 8. Сравнение законодательства в сфере ИБ в РФ и другой страны (на выбор), основы криптографии	УК-1.2, УК-1.3, УК-6.3, ОПК-1.2, ОПК-1.3, ОПК-4.2, ОПК-4.3	тестирование	4
2.	**Раздел 2. Защита информации в компьютерных сетях**				**26**
	Тема 3. Общие понятия компьютерных сетей	Лекция №5. Понятие и структура компьютерной сети	УК-1.1, ОПК-1.1, ОПК-4.1	-	2
		Лекция №6. Сетевые протоколы. Адресация в сети	УК-1.1, ОПК-1.1, ОПК-4.1	-	2
	Тема 4. Защита информации в компьютерной сети	Лекция №7, 8. Методы и средства обеспечения информационной безопасности в компьютерной сети организации	УК-1.2, УК-1.3, УК-6.3, ОПК-1.2, ОПК-1.3, ОПК-4.2, ОПК-4.3	-	4
		Практическое занятие №9, 10, 11. Сетевые протоколы, адресация устройств в сетях, схема сети	УК-1.2, УК-1.3, УК-6.3, ОПК-1.2, ОПК-1.3, ОПК-4.2, ОПК-4.3	защита практических заданий	4
		Практическое занятие №12, 13. Работа с открытыми отраслевыми данными, визуализация данных	УК-1.2, УК-1.3, УК-6.3, ОПК-1.2, ОПК-1.3, ОПК-4.2, ОПК-4.3	защита практических заданий	4
		Практическое занятие №14. Защита документов и форм в Word	УК-1.2, УК-1.3, УК-6.3, ОПК-1.2, ОПК-1.3, ОПК-4.2, ОПК-4.3	защита практических заданий	4
		Практическое занятие №15, 16. Защита данных в Excel	УК-1.2, УК-1.3, УК-6.3, ОПК-1.2, ОПК-1.3, ОПК-4.2, ОПК-4.3	защита практических заданий	4

№ п/п	Название раздела, темы	№ и название лекций/ практических занятий	Формируемые компетенции	Вид контрольного мероприятия	Кол-во часов
		Практическое занятие №17. Защита данных в Access	УК-1.2, УК-1.3, УК-6.3, ОПК-1.2, ОПК-1.3, ОПК-4.2, ОПК-4.3	защита практических заданий	2

Таблица 5

Перечень вопросов для самостоятельного изучения дисциплины

№ п/п	Название раздела, темы	Перечень рассматриваемых вопросов для самостоятельного изучения
Раздел 1. Информационная безопасность. Защита информации		
1.	Тема 1. Общие понятия информационной безопасности и защиты информации	Изучение Доктрины информационной безопасности РФ, типовые причины угроз информационной безопасности, (УК-1.1, ОПК-1.1, ОПК-4.1)
2.	Тема 2. Правовые основы информационной безопасности и защиты информации	Вопросы, связанные с информационной безопасностью, отраженные в федеральных законах («Об информации, информационных технологиях и защите информации», «Об электронной подписи», «О персональных данных»). Угрозы при использовании нелицензионных программ (УК-1.1, ОПК-1.1, ОПК-4.1)
Раздел 2. Защита информации в компьютерных сетях		
3.	Тема 3. Общие понятия компьютерных сетей	Соединительное оборудование в сети: основные устройства и их назначение (УК-1.1, ОПК-1.1, ОПК-4.1)
4.	Тема 4. Защита информации в компьютерной сети	Антивирусная защита, брандмауэры, электронные ключи (УК-1.2, УК-1.3, УК-6.3, ОПК-1.2, ОПК-1.3, ОПК-4.2, ОПК-4.3)

5. Образовательные технологии

Таблица 6

Применение активных и интерактивных образовательных технологий

№ п/п	Тема и форма занятия		Наименование используемых активных и интерактивных образовательных технологий (форм обучения)
1.	Лекция №2. Правовые основы информационной безопасности и защиты информации	Л	Лекция-дискуссия
3.	Практическое занятие №5. Защита данных в Excel	ПЗ	Тренинг

6. Текущий контроль успеваемости и промежуточная аттестация по итогам освоения дисциплины

6.1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности

1) Примерные тестовые задания

1. Защищенность каких объектов входит в понятие информационной безопасности?
   а) законодательных органов
   б) пользователей информации
   в) поддерживающей инфраструктуры
   г) владельцев поддерживающей инфраструктуры
   д) владельцев информации
   е) информации
2. Защищенность от каких воздействий предусматривает информационная безопасность?
   а) случайных и преднамеренных только искусственного характера
   б) случайных и преднамеренных естественного и искусственного характера
   в) только преднамеренных естественного и искусственного характера
3. Возможность за приемлемое время получить информационную услугу называется …
   а) оперативностью информации
   б) конфиденциальностью информации
   в) доступностью информации
   г) целостностью информации
4. Напишите пропущенное слово в приведенной фразе: «_____ - это потенциальная возможность нарушить информационную безопасность»
5. К какому типу угроз доступности относится нарушение работы систем связи, электропитания, водо- и теплоснабжения?
   а) программные атаки
   б) вредоносное программное обеспечение
   в) отказы пользователей
   г) внутренние отказы
   д) отказы поддерживающей инфраструктуры
6. К какому типу угроз информационной безопасности относится ввод неверных данных в систему?
   а) угрозы доступности
   б) угрозы целостности
   в) угрозы конфиденциальности
7. Выберите основные угрозы конфиденциальности:
   а) кражи оборудования
   б) размещение данных в слабозащищенной среде
   в) отказы пользователей
   г) отказы поддерживающей инфраструктуры

д) перехват
е) злоупотребление полномочиями

8. К программно-техническим средствам защиты информации относятся:
а) идентификация и аутентификация пользователей
б) разграничение доступа пользователей к ресурсам
в) шифрование информации
г) защита территории и помещений от проникновения нарушителей и наблюдений
д) защита аппаратных средств и носителей информации от хищения
е) организация доступа в помещения сотрудников
ж) противопожарная защита помещений

9. Выберите преступления в компьютерной сфере, за которые определена ответственность в Уголовном кодексе РФ:
а) неправомерный доступ к компьютерной информации
б) неправомерные действия против владельцев поддерживающей инфраструктуры информационной системы
в) превышение полномочий при работе с электронными документами
г) создание, использование и распространение вредоносных программ для ЭВМ
д) нарушение правил эксплуатации ЭВМ, повлекшие за собой уничтожение охраняемой информации

10. Федеральный закон «Об информации, информационных технологиях и о защите информации» регулирует отношения, возникающие при…
а) обеспечении защиты информации
б) документировании информации
в) использовании электронно-цифровой подписи в электронных документах
г) осуществлении права на поиск, получение, передачу, производство и распространение информации
д) производстве компьютерной техники
е) применении информационных технологий

11. Открытая лицензия (GNU GPL) на программное обеспечение гарантирует пользователям свободу…
а) использовать и изменять это программное обеспечение
б) продавать это программное обеспечение
в) лицензировать это программное обеспечение

2) Примеры заданий на практических работах

Практическое занятие №3, 4. Анализ инцидентов информационной безопасности

Задание: Проанализировать инциденты информационной безопасности (описание инцидентов дается для различных вариантов) и ответить на вопросы:

a) В чем проявилась угроза?
b) Кто выступил источником угрозы?

c) Определить тип угрозы (случайная или преднамеренная, естественного или искусственного характера).
d) Классифицировать угрозу по аспектам ИБ (доступность, целостность, конфиденциальность).
e) Высказать предложения по нейтрализации или минимизации ущерба от подобной угрозы в будущем.

Описание инцидентов:

1. Желая поздравить с Новым годом коллег, сотрудник К. составляет базу рассылки из 1500 адресов, после чего создает письмо с роликом размером в 1,5 Мбайт и запускает рассылку. Подобные операции производят также его коллеги, рассылая поздравительные письма с вложенными картинками, роликами и звуковыми файлами. В результате создается ситуация DoS на почтовом сервере и блокируется прием-отправка деловой корреспонденции.
2. Сотрудник крупной полиграфической компании украл диск с приватными сведениями почти девяти миллионов граждан.
3. Бывший системный администратор одного из крупных банков перевел через банк, в котором раньше работал, со счета региональной таможни на счет несуществующей фирмы-банкрота большую сумму денег.
4. Ученик одиннадцатого класса ради развлечения взломал ряд ПК пользователей, а также информационные системы нескольких предприятий. Школьник уничтожил архивы сетевых дисков подразделений, образ операционной системы компьютера сисадмина, базы данных специализированных программ. На восстановление информации у работников предприятия ушли недели, убытки от шалости школьника оцениваются сотнями миллионов рублей.
5. Сотрудник С., работавший системным администратором, имел доступ к редактированию данных в интернет-магазине, электронным базам данных предприятия. За нарушение трудового контракта был уволен. В качестве мести он взломал систему защиты и удалил около 140 тысяч файлов, что привело к потере части прибыли коммерческого предприятия и большим временным затратам на восстановление информации.

Практическое занятие №5, 6. Правовые основы информационной безопасности и защиты информации

Поиск документов можно выполнять в бесплатных онлайн версиях правовых информационно-поисковых системах, например: КонсультантПлюс: http://www.consultant.ru/online/, Гарант: http://base.garant.ru/

Задание 1. Найти определения терминов, принятых в Федеральном законе №149-ФЗ «Об информации, информационных технологиях и о защите информации»:

- информационно-телекоммуникационная сеть
- обладатель информации
- доступ к информации
- конфиденциальность информации

- электронное сообщение
- электронный документ
- сайт в сети "Интернет"
- страница сайта в сети "Интернет"
- доменное имя
- сетевой адрес
- владелец сайта в сети "Интернет"
- провайдер хостинга
- единая система идентификации и аутентификации.

*Задание 2***.** Выполнить обзор статей Конституции РФ об информационных правах граждан (в таблицу поместить только ту часть статьи, которая связана с информационными правами граждан).

Номер статьи	Содержание статьи, связанное с информационными правами граждан
23	
24	
29	

Задание 3. Найти определения терминов, принятых в Федеральном законе №63-ФЗ «Об электронной подписи».

- электронная подпись
- сертификат ключа проверки электронной подписи
- ключ электронной подписи
- ключ проверки электронной подписи
- удостоверяющий центр
- средства электронной подписи
- корпоративная информационная система
- информационная система общего пользования

Практическое занятие №9-11. Сетевые протоколы, адресация устройств в сетях, схема сети
Задание

1. Изучите представленный теоретический материал.
2. Расставьте по уровням модели OSI следующее:
    - повторитель (repeater);
    - концентратор (hub);
    - мост (bridge);
    - коммутатор (switch);
    - маршрутизатор (router);
    - шлюз (gateway);
    - разъем RJ-45;
    - MAC-адрес;
    - IP-адрес;
    - документ RFC792;
    - стандарт IEEE 802.3;

- единицу данных "кадр" (frame);
- единицу данных "пакет" (packet);
- единицу данных "сообщение" (message);
- протокол SSL;
- протокол SPX;
- протокол HTTP;
- протокЬл ARP;
- протокол OSPF;
- протокол PPP;
- стек протоколов NetBIOS/SMB.

Задание

1. Воспользовавшись служебной программой командной строки ipconfig, определить аппаратный, символьный и составной числовой адрес рабочего компьютера. Сделать вывод о том, сколько сетевых адаптеров установлено в ЭВМ, а также выяснить, какой адрес имеет сервер DNS для данной машины и используется ли для получения IP-адреса DHCP-сервер.
2. При помощи программы ping проверить наличие связи с DNS- и DHCP-серверами при их наличии в сети.
3. С помощью команды net view определите символьные имена узлов локальной сети, а также имя сервера.
4. Определить к какому типу (A – E) относится сеть в учебном классе.
5. Начертить схему локальной сети с указанием для каждого узла и сервера символьного имени, адреса IP, MAC-адреса.

Задание

Предположив, что ваш компьютер имеет адрес 192.168.4.85 с маской подсети 255.255.255.240, вычислить, какое максимальное количество компьютеров может быть в той же подсети, а также определить, какое максимальное количество подсетей может быть организовано внутри сети 192.168.4.0 и какая при этом должна быть маска.

Задание 5

1. Выведите таблицу маршрутизации с помощью сетевой утилиты ***route***.

Таблица 1

Таблица маршрутизации. Активные маршруты				
Сетевой адрес	**Маска подсети**	**Адрес шлюза**	**Интерфейс**	**Метрика**

2. Выведите таблицу ARP-кэша с помощью утилиты arp.

Таблица 2

Таблица ARP-кэша		
IP-адрес	**MAC-адрес**	**Тип**

3. Даны имена web-серверов:

Таблица 3

Южная Америка	www.uba.ar	www.castelobranko.br	www.univalle.edu.co	www.ucv.ve
Австралия и Океания	www.usyd.edu.au	www.usp.ac.fj	www.adelaide.edu.au	www.vu.edu.au
Африка	www.uz.ac.zw	www.unisa.ac.za	www.bau.edu.lb	www.aast.edu
Азия	www.mu.ac.in	www.ntu.edu.tw	www.sharjah.ac.ae	www.kimep.kz
Европа	www.us.es	www.sorbonne.fr	www.ox.ac.uk	www.unizh.ch
Северная Америка	www.stanford.edu	www.ufl.edu	www.nmt.edu	www.yale.edu
Россия	www.kubstu.ru	www.kbsu.ru	www.spbu.ru	www.festu.ru

4. Получение информации о сервере:

1. Выберите по 5 серверов. Следующие действия нужно выполнять для каждого выбранного сервера, результаты оформлять в виде таблицы.
2. Определите IP-адрес и каноническое имя (***nslookup***).
3. Определите среднее время прохождения пакетов до сервера (***ping***).

5. Анализ маршрута:

1. Выберите два любых нероссийских сервера. Следующие действия нужно выполнять для каждого выбранного сервера, результаты оформлять в виде таблицы.
2. Определите маршрут до него (***tracert***).
3. Перечислите сети (домены второго уровня), через которые проходит маршрут.
4. Попытайтесь найти информацию о каждом маршрутизаторе (владелец, местонахождение)***http://networking.ringofsaturn.com/Tools/whois.php***.
5. Найдите большие временные скачки в маршруте и объясните, с чем они связаны.

Практическое занятие №12, 13. Работа с открытыми отраслевыми данными, визуализация данных

Задание
1. На сайте Росстата (www.gks.ru) найти отраслевые данные по выпуску продукции/услуг в рамках субъекта Российской Федерации или отрасли, по инновациям в отрасли.
2. На сайте Электронной научной библиотеки (www.elibrary.ru) найти научные статьи по тематике направления подготовки.
3. На сайте Федерального института промышленной собственности (https://www.fips.ru/) найти патенты на изобретения и полезные модели по направлению подготовки.
Задание

Создайте диаграммы для визуализации динамики показателей анализа статистических данных. Разработайте презентацию в MS Power Point.

Практическое занятие №14. Защита документов и форм в Word
Задание

1. Создайте анкету участника проекта примерно такого вида:

Анкета участника проекта
Дата заполнения анкеты: 01.03.2021
Фамилия: Имя: Отчество:
Образование: высшее Специальность:
Место работы или учёбы: Должность:
Дата рождения:
Пол: мужской В браке: ☐ Несовершеннолетние дети: ☐
E-mail:
ИНН:

ПРИМЕЧАНИЕ: можно сделать не эту анкету, а любую форму по вашим профессиональным интересам, главное требование – наличие полей, в которых можно применить все следующие настройки.

Настройте поля следующим образом:

- Для поля Дата заполнения анкеты выберите тип Текущая дата, чтобы в поле автоматически подставлялась дата заполнения формы.
- Для полей Образование и Пол создайте поля со списком.
- Для текстового поля Дата рождения выберите тип Дата и формат dd.mm.yyyy.
- Для полей В браке и Несовершеннолетние дети сделайте флажки.
- Для поля ИНН задайте тип Число и укажите максимальный размер поля (12 цифр), в качестве формата выберите 0 – это обозначение положительного целого числа.
- Остальные поля формы – текстовые поля, настройки их сделайте на ваше усмотрение.

2. Установите защиту формы. Сохраните как шаблон под именем Анкета участника.dotx.

Практическое занятие №15, 16. Защита данных в Excel
Задание

1. Войдите в систему с учетной записи Admin.
2. Создайте папку с доступом для всех пользователей в локальной сети:
3. Создайте в своей папке новый файл Excel – опросник по материалу прошедших лекций (имя файла Опрос). Он должен включать 5 вопросов. Лист Excel надо защитить от изменений, но оставить незащищенными ячейки для ввода фамилии и имени отвечающего, а также ответов на вопросы. На отдельном листе сделать проверку и выставление оценки.
4. Заполнить опросник вашего соседа, сидящего через два компьютера справа.

Практическое занятие №17. Защита данных в Access

1. Создайте структуру базы данных «Учебный процесс».

2. Зашифруйте созданную базу данных.
3. Выполните статистическую обработку данных из таблиц Ученики и Ведомость.

3) Примерный перечень вопросов, выносимых на зачет

1. Понятия информационной безопасности (ИБ) и защиты информации.
2. Основные составляющие ИБ.
3. Категории интересов субъектов информационных отношений (доступность, целостность, конфиденциальность).
4. Угрозы ИБ. Понятие угрозы, атаки, злоумышленника, уязвимых мест в защите, окна опасности.
5. Классификации угроз ИБ.
6. Основные угрозы ИБ.
7. Подходы и общие принципы обеспечения ИБ.
8. Методы и средства защиты информации.
9. Вопросы информационной безопасности в Конституции РФ.
10. Вопросы информационной безопасности в Уголовном кодексе РФ.
11. Основные вопросы, связанные с информационной безопасностью, отраженные в федеральном законе «Об информации, информационных технологиях и защите информации».
12. Основные вопросы, связанные с информационной безопасностью, отраженные в федеральном законе «Об электронной подписи».
13. Основные вопросы, связанные с информационной безопасностью, отраженные в федеральном законе «О персональных данных».
14. Понятие лицензии на программный продукт. Виды программ по способам распространения.
15. Типовые условия, включаемые в коммерческую лицензию.
16. Понятие и условия открытой лицензия GNU GPL.
17. Понятие нелицензионного программного продукта. Угрозы при использовании нелицензионных программ.
18. Понятие компьютерной сети (КС). Общая структура компьютерной сети.
19. Сетевые средства и службы: понятие, примеры и назначение сетевых служб.
20. Носители для передачи данных в компьютерной сети: кабельное соединение (виды кабелей), беспроводное соединение.
21. Соединительное оборудование: основные устройства и их назначение.
22. Сетевые протоколы: понятие, назначение.
23. Модель OSI, стек протоколов TCP/IP.
24. Классификации КС.
25. Топологии локальных КС.
26. Глобальная сеть Интернет: основные службы.
27. Адресация компьютеров в КС.
28. Адрес ресурса в сети.
29. Методы и средства обеспечения информационной безопасности в компьютерной сети организации.
30. Политика информационной безопасности.
31. Антивирусная защита, брандмауэры, электронные ключи.

32.Защита документов и форм в Word: установка параметров автосохранения, установка пароля на открытие и редактирование документа.
33.Создание форм в Word и установка ограничений на редактирование форм.
34.Защита в Excel: установка параметров автосохранения, установка пароля на открытие книги.
35.Защита элементов листа в Excel.
36.Шифрование данных в Access.

6.2. Описание показателей и критериев контроля успеваемости, описание шкал оценивания

Для оценки знаний, умений, навыков и формирования компетенции по дисциплине на промежуточном контроле в форме зачета применяется итоговое электронное тестирование.

Количество тестовых вопросов в выдаче итогового теста составляет 46, время тестирования 1,5 часа. Оценивание результатов усвоения, предлагается осуществлять в соответствии со шкалами, представленными в таблицах 9-10.

Таблица 9

Шкала оценивания	**Зачет**
70-100	Зачтено
0-69	Не зачтено

Таблица 10

Оценка	**Критерии оценивания**
Пороговый уровень «зачет» (удовлетворительно)	Оценку «зачет» заслуживает студент, полностью или частично с пробелами освоивший знания, умения, компетенции и теоретический материал, многие учебные задания либо не выполнил, либо они оценены числом баллов близким к минимальному, некоторые практические навыки не сформированы. **Компетенции,** закрепленные за дисциплиной, **сформированы на уровне- достаточный или** выше.
Минимальный уровень «незачет» (неудовлетворительно)	оценку «незачет» заслуживает студент, не освоивший знания, умения, компетенции и теоретический материал, учебные задания не выполнил, практические навыки не сформированы. **Компетенции**, закрепленные за дисциплиной, **не сформированы.**

На этапе текущего контроля успеваемости применяется традиционная система контроля и оценки успеваемости студентов (решение типовых и индивидуальных задач). Критерии оценивания представлены в таблице 11.

Критерии оценивания результатов обучения

Таблица 11

Оценка	**Критерии оценивания**
Высокий уровень «5» (отлично)	оценку **«отлично»** заслуживает студент, освоивший знания, умения, компетенции и теоретический материал без пробелов; выполнивший все задания, предусмотренные учебным планом на высоком качественном уровне; практические навыки профессионального применения освоенных знаний сформированы. **Компетенции**, закреплённые за дисциплиной, **сформированы на уровне – высокий**.

Средний уровень «4» (хорошо)	оценку **«хорошо»** заслуживает студент, практически полностью освоивший знания, умения, компетенции и теоретический материал, учебные задания не оценены максимальным числом баллов, в основном сформировал практические навыки. **Компетенции**, закреплённые за дисциплиной, **сформированы на уровне – хороший (средний)**.
Пороговый уровень «3» (удовлетворительно)	оценку **«удовлетворительно»** заслуживает студент, частично с пробелами освоивший знания, умения, компетенции и теоретический материал, многие учебные задания либо не выполнил, либо они оценены числом баллов близким к минимальному, некоторые практические навыки не сформированы. **Компетенции**, закреплённые за дисциплиной, **сформированы на уровне – достаточный**.
Минимальный уровень «2» (неудовлетворительно)	оценку «неудовлетворительно» заслуживает студент, не освоивший знания, умения, компетенции и теоретический материал, учебные задания не выполнил, практические навыки не сформированы. **Компетенции**, закреплённые за дисциплиной, **не сформированы**.

7. Учебно-методическое и информационное обеспечение дисциплины

7.1 Основная литература

1. Быстренина И.Е. Новые информационные технологии: учебное пособие / И. Е. Быстренина; Российский государственный аграрный университет - МСХА им. К. А. Тимирязева — Москва: Росинформагротех, 2017 — 76 с. — Режим доступа : http://elib.timacad.ru/dl/local/t765.pdf.
2. Лемешко Т. Б. Современные информационные технологии: учебное пособие / Т. Б. Лемешко, В. Н. Шурыгин; Российский государственный аграрный университет - МСХА имени К. А. Тимирязева — Москва: Росинформагротех, 2017 — 136 с. <URL:http://elib.timacad.ru/dl/local/t495.pdf>.

7.2 Дополнительная литература

1. Биткова Л. А. Информационное право: методические указания / Л. А. Биткова; Российский государственный аграрный университет - МСХА имени К. А. Тимирязева — Москва: Реарт, 2017 — 68 с.: <URL:http://elib.timacad.ru/dl/local/d9372.pdf>.
2. Карпузова, В. И.. Проектирование информационных систем: учебное пособие / В. И. Карпузова, Н. В. Карпузова, К. В. Чернышева; Российский государственный аграрный университет - МСХА имени К. А. Тимирязева — Москва: РГАУ-МСХА им. К. А. Тимирязева, 2019 — 147 с. <URL:http://elib.timacad.ru/dl/local/umo390.pdf>
3. Соколов А.Л. Информатика: учебно-методическое пособие / А. Л. Соколов; Российский государственный аграрный университет - МСХА имени К.А. Тимирязева — Москва: Росинформагротех, 2017 — 101 с. Режим доступа : http://elib.timacad.ru/dl/full/umo141.pdf.

7.3 Нормативные правовые акты

1. Доктрина информационной безопасности Российской Федерации.

2. Федеральный закон N 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральном законе №63-ФЗ «Об электронной подписи».
4. Конституция РФ.
5. Уголовный кодекс РФ.
6. Стратегия развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года.

7.4 Методические указания, рекомендации и другие материалы к занятиям

1. Вычислительная техника и сети в отрасли: практикум. Е.В. Щедрина. М. : ООО УМЦ «Триада», 2018. 25 с.
2. Вычислительная техника и сети в отрасли: Методические рекомендации для выполнения контрольной работы. Е.В. Щедрина. М. : ООО УМЦ «Триада», 2018. 40 с.

При проведении занятий по дисциплине необходимо ориентироваться на современные образовательные технологии, например, путем использования программы NetOp School, позволяющей осуществлять тиражирование заданий в электронном виде и осуществлять контроль за их исполнением.

Большое значение имеют вопросы, связанные с закреплением и расширением навыков использования современных информационных технологий при обработке информации, в том числе интернет-технологии.

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

1. http://www.consultant.ru Справочная правовая система «Консультант-Плюс».

2. http://www.garant.ru/ Справочная правовая система «Гарант»

3. http://www.gpntb.ru – государственная публичная научно-техническая библиотека

4. http://www.rsl.ru – Российская государственная библиотека

5. http://www.tehlit.ru – библиотека нормативно-технической литературы

9. Перечень программного обеспечения и информационных справочных систем

Таблица 9

Перечень программного обеспечения

№ п/п	Наименование раздела учебной дисциплины (модуля)	Наименование программы	Тип программы	Автор	Год разработки
1	Раздел 1. Информационная безопасность. Защита информации	NetOp School MS Power Point, браузер MS Intenet Explorer, ОС Windows, MS Word	контролирующая, обучающая	Разработчик фирма Microsoft	2007 и выше

2	Раздел 2. Защита информации в компьютерных сетях	ОС Windows, MS Word, MS Excel	обучающая	Разработчик фирма Microsoft	2007 и выше

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

Лекции проводятся в специализированной аудитории, оборудованной мультимедийным проектором для демонстрации компьютерных презентаций. Для проведения практических занятий по дисциплине «Информационная безопасность» необходим компьютерный класс с предустановленным на ПЭВМ программным обеспечением, указанным в п. 9.

Таблица 10

Сведения об обеспеченности специализированными аудиториями, кабинетами, лабораториями

Наименование специальных помещений и помещений для самостоятельной работы (№ учебного корпуса, № аудитории)	**Оснащенность специальных помещений и помещений для самостоятельной работы**
1	2
Компьютерные классы в учебном корпусе №29: № аудитории ИЦ	Персональный компьютер 32 шт. (Инв.№ 210134000001134; 210134000001192; 210134000001193; 210134000001194; 210134000001195; 210134000001196; 210134000001197; 410134000000590; 210134000001181; 210134000001182; 210134000001183; 210134000001184; 210134000001185; 210134000001186: 210134000001187; 210134000001188; 210134000001189; 210134000001190; 210134000001191; 210134000001168; 210134000001169; 210134000001170; 210134000001171; 210134000001172; 210134000001173; 210134000001174; 210134000001175; 210134000001176; 210134000001177; 210134000001178; 210134000001179; 210134000001180) CNetSwitchCNSN-1600 2 шт. (Инв. № 410134000000196; 410134000000196) Магнитная доска 1 шт. (Инв. № 210136000000112); Магнитная доска 1 шт. (Инв. № 210136000000113); Персональный компьютер 12 шт. (Инв. № 210134000001109; 210134000001110; 210134000001111; 210134000001112; 210134000001113; 210134000001114; 210134000001115; 210134000001116; 210134000001117; 210134000001118; 210134000001119; 210134000001120)
Центральная научная библиотека имени Н.И. Железнова, Читальные залы библиотеки	

Общежития, комнаты для самоподготовки	

11. Методические рекомендации обучающимся по освоению дисциплины

Освоение теоретических основ курса «Информационная безопасность» предусматривает прослушивание и проработку материалов лекций, работу с рекомендованными литературными источниками и интернет-ресурсами. Лекции читаются в аудиториях, оснащенных мультимедийной техникой, на основе подготовленных лектором презентаций с применением активных и интерактивных образовательных технологий.

Практические навыки по курсу «Информационная безопасность» приобретаются путем выполнения основных работ и дополнительных индивидуальных заданий. Практические занятия проводятся в компьютерных классах, оснащенных соответствующими техническими и программными средствами.

Для самостоятельной работы студентов в компьютерных классах предусмотрены часы, которые устанавливаются сотрудниками кафедры.

Виды и формы отработки пропущенных занятий

Студент, отсутствующий на лекционном занятии, обязан написать и защитить реферат по пропущенной теме. При пропуске практического занятия студент обязан получить у преподавателя индивидуальный вариант, выполнить и защитить его.

Прием и защита индивидуальных заданий и рефератов проводятся в часы в дни и часы, устанавливаемые преподавателем.

12. Методические рекомендации преподавателям по организации обучения по дисциплине

Реализация компетентного подхода должна предусматривать широкое использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Программу разработал:

Петухова М. В., к.п.н, доцент

Щедрина Е.В., к.п.н, доцент

РЕЦЕНЗИЯ
на рабочую программу дисциплины «Информационная безопасность»
ОПОП ВО по направлению 20.03.01 «Техносферная безопасность» направленности
«Безопасность цифровых роботизированных технологических процессов
и производств», «Инженерное обеспечение безопасности населения, окружающей среды и объектов техносферы»
(квалификация выпускника – бакалавр)

Худяковой Еленой Викторовной, профессором кафедры «Прикладная информатика» ФГБОУ ВО РГАУ – МСХА им. К.А. Тимирязева, доктором экономических наук (далее по тексту рецензент), проведена рецензия рабочей программы дисциплины «Информационная безопасность» ОПОП ВО по направлению 20.03.01 «Техносферная безопасность» направленностей «Безопасность цифровых роботизированных технологических процессов и производств», «Инженерное обеспечение безопасности населения, окружающей среды и объектов техносферы» (бакалавриат), разработанной в ФГБОУ ВО «Российский государственный аграрный университет – МСХА имени К.А. Тимирязева» на кафедре систем автоматизированного проектирования и инженерных расчетов (разработчик – доцент Петухова М.В., Щедрина Е.В.).

Рассмотрев представленные на рецензию материалы, рецензент пришел к следующим выводам:

1. Предъявленная рабочая программа дисциплины «Информационная безопасность» (далее по тексту Программа) *соответствует* требованиям ФГОС ВО по направлению 20.03.01 «Техносферная безопасность». Программа *содержит* все основные разделы, *соответствует* требованиям к нормативно-методическим документам.

2. Представленная в Программе ***актуальность*** учебной дисциплины в рамках реализации ОПОП ВО *не подлежит сомнению* – дисциплина относится к обязательной части учебного цикла – Б1.

3. Представленные в Программе ***цели*** дисциплины *соответствуют* требованиям ФГОС ВО направления 20.03.01 «Техносферная безопасность».

4. В соответствии с Программой за дисциплиной «Информационная безопасность» закреплено четыре ***компетенции***. Дисциплина «Информационная безопасность» и представленная Программа *способна реализовать* их в объявленных требованиях. Результаты обучения, представленные в Программе в категориях знать, уметь, владеть *соответствуют* специфике и содержанию дисциплины и *демонстрируют возможность* получения заявленных результатов.

5. Общая трудоёмкость дисциплины «Информационная безопасность» составляет 3 зачётные единицы (108 часов).

6. Информация о взаимосвязи изучаемых дисциплин и вопросам исключения дублирования в содержании дисциплин *соответствует* действительности. Дисциплина «Информационная безопасность» взаимосвязана с другими дисциплинами ОПОП ВО и Учебного плана по направлению 20.03.01 «Техносферная безопасность» и возможность дублирования в содержании отсутствует.

7. Представленная Программа предполагает использование современных образовательных технологий, используемые при реализации различных видов учебной работы. Формы образовательных технологий *соответствуют* специфике дисциплины.

8. Программа дисциплины «Информационная безопасность» предполагает проведение занятий в интерактивной форме.

9. Виды, содержание и трудоёмкость самостоятельной работы студентов, представленные в Программе, *соответствуют* требованиям к подготовке выпускников, содержащимся во ФГОС ВО направления 20.03.01 «Техносферная безопасность».

10. Представленные и описанные в Программе формы *текущей* оценки знаний (тестирование, защита практических заданий), *соответствуют* специфике дисциплины и требованиям к выпускникам.

Форма промежуточного контроля знаний студентов, предусмотренная Программой, осуществляется в форме зачета, что *соответствует* статусу дисциплины, как дисциплины обязательной части учебного цикла – Б1 ФГОС ВО направления 20.03.01 «Техносферная безопасность».

11. Формы оценки знаний, представленные в Программе, *соответствуют* специфике дисциплины и требованиям к выпускникам.

12. Учебно-методическое обеспечение дисциплины представлено: основной литературой – 2 источника, дополнительной литературой – 3 наименования, Интернет-ресурсы – 5 источников и соответствует требованиям ФГОС ВО направления 20.03.01 «Техносферная безопасность».

13. Материально-техническое обеспечение дисциплины соответствует специфике дисциплины «Информационная безопасность» и обеспечивает использование современных образовательных, в том числе интерактивных методов обучения.

14. Методические рекомендации студентам и методические рекомендации преподавателям по организации обучения по дисциплине дают представление о специфике обучения по дисциплине «Информационная безопасность».

ОБЩИЕ ВЫВОДЫ

На основании проведенной рецензии можно сделать заключение, что характер, структура и содержание рабочей программы дисциплины «Информационная безопасность» ОПОП ВО по направлению 20.03.01 «Техносферная безопасность» направленностей «Безопасность цифровых роботизированных технологических процессов и производств», «Инженерное обеспечение безопасности населения, окружающей среды и объектов техносферы» (квалификация выпускника – бакалавр), разработанная Петуховой М.В., доцентом кафедры систем автоматизированного проектирования и инженерных расчетов, к.п.н. и Щедриной Е.В., доцентом кафедры систем автоматизированного проектирования и инженерных расчетов, к.п.н., доцентом соответствует требованиям ФГОС ВО, современным требованиям экономики, рынка труда и позволит при её реализации успешно обеспечить формирование заявленных компетенций.

Рецензент: Худякова Елена Викторовна, профессор кафедры «Прикладная информатика» ФГБОУ ВО РГАУ – МСХА им. К.А. Тимирязева, доктор экономических наук

_____ «29» августа 2023 г.