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 экономики и управления АПК
Кафедра Прикладной информатики

УТВЕРЖДАЮ:
Директор института
экономики и управления АПК
_____ Хоружий Л.И.
«____» _____ 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.19 Информационная безопасность

для подготовки бакалавров

ФГОС ВО

Направление: 09.03.02 Информационные системы и технологии
Направленность: Большие данные и машинное обучение
Направленность: Компьютерные науки и интеллектуальный анализ данных

Курс 4
Семестр 7

Форма обучения очная

Год начала подготовки 2022 г.

Москва, 2022

Разработчики: Никаноров М.С. ст. преподаватель

Греченева А.В., к.т.н., доцент

«22» 08 2022 г.

Рецензент: Щедрина Е.В. к.п.н., доцент
кафедры систем автоматизированного
проектирования и инженерных расчётов

«26» 08 2022 г.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению 09.03.02 Информационные системы и технологии, профессиональных стандартов и учебного плана 2022 года начала подготовки.

Программа обсуждена на заседании кафедры прикладной информатики
протокол № 1 от «29» 08 2022 г.

И.о. зав. кафедрой Худякова Е.В. д.э.н., профессор

«29» 08 2022 г.

Согласовано:
Председатель учебно-методической
комиссии института экономики и управления АПК
Корольков А.Ф., к.э.н., доцент

N12 «29» 08 2022 г.

И.о. заведующего выпускающей кафедрой
прикладной информатики
Худякова Е.В. д.э.н., профессор

«29» 08 2022 г.

Зав. отделом комплектования ЦНБ Ефимова Я.В.

СОДЕРЖАНИЕ

Аннотация

рабочей программы учебной дисциплины Б1.О.19 «Информационная безопасность» для подготовки бакалавра по направлению 09.03.02 Информационные системы и технологии, направленность Большие данные и машинное обучение и Компьютерные науки и интеллектуальный анализ данных

Цель освоения дисциплины: является освоение студентами теоретических и практических знаний и приобретение умений и навыков в области информационной безопасности для защиты операционной системы, информационной системы, защиты файлов, с помощью таких цифровых технологий и инструментов, как IRIS и PGP.

Место дисциплины в учебном плане: дисциплина включена в обязательную часть учебного плана по направлению 09.03.02 Информационные системы и технологии.

Требования к результатам освоения дисциплины: в результате освоения дисциплины формируются следующие компетенции (индикаторы): УК-10 (УК-10.1; УК-10.2; УК-10.3), ОПК-3 (ОПК-3.1; ОПК-3.2; ОПК-3.3), ОПК-4 (ОПК-4.1; ОПК-4.2).

Краткое содержание дисциплины: Основы информационной безопасности, Цели и задачи информационной безопасности. Место информационной безопасности в национальной безопасности РФ, Построение системы защиты информации в организации, Современные методы защиты, Современные методики анализа и управления рисками информационной безопасности, Перспективные направления в области информационной безопасности, Криптографическая защита информации.

Общая трудоемкость дисциплины: 4 зач.ед. (144 часа).

Промежуточный контроль: Экзамен.

1. Цель освоения дисциплины

Целью освоения дисциплины «Информационная безопасность» является освоение студентами теоретических и практических знаний и приобретение умений и навыков в области информационной безопасности для защиты операционной системы, информационной системы, защиты файлов.

2. Место дисциплины в учебном процессе

Дисциплина «Информационная безопасность» включена в обязательную часть учебного плана. Дисциплина «Информационная безопасность» реализуется в соответствии с требованиями ФГОС ВО, ОПОП ВО, профессиональных стандартов и Учебного плана по направлению 09.03.02 Информационные системы и технологии.

Предшествующими курсами, на которых непосредственно базируется дисциплина «Информационная безопасность» являются «Инфокоммуникационные системы и сети», «Операционные системы», «Информационные технологии».

Дисциплина «Информационная безопасность» является основополагающей для изучения следующих дисциплин: «Администрирование информационных систем» и «ERP-системы в управлении бизнесом».

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, соотнесенных с планируемыми результатами освоения образовательной программы

Изучение данной учебной дисциплины направлено на формирование у обучающихся компетенций, представленных в таблице 1.

Таблица 1

Требования к результатам освоения учебной дисциплины

№ п/п	Код компетенции	Содержание компетенции (или её части)	Индикатор достижения компетенции и его содержание	В результате изучения учебной дисциплины обучающиеся должны:		
				знать	уметь	владеть
1.	УК-10	Способен формировать нетерпимое отношение к коррупционному поведению	УК-10.1 Знать: сущность коррупционного поведения и его взаимосвязь с социальными, экономическими, политическими и иными условиями	сущность коррупционного поведения и его взаимосвязь с социальными, экономическими, политическими и иными условиями, посредством электронных ресурсов, официальных сайтов	-	-
			УК-10.2 Уметь: анализировать, толковать и правильно применять правовые нормы о противодействии коррупционному поведению	-	анализировать, толковать и правильно применять правовые нормы о противодействии коррупционному поведению, посредством электронных ресурсов, официальных сайтов	-
			УК-10.3 Иметь навыки: работы с законодательными и другими нормативными правовыми актами	-	-	работы с законодательными и другими нормативными правовыми актами, посредством электронных ресурсов, официальных сайтов
2.	ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с	ОПК-3.1 Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением ин-	принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной безопасности; применение информационно-коммуникационных тех-	-	-

		применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	формационно-коммуникационных технологий и с учетом основных требований информационной безопасности	нологий с учетом основных требований информационной безопасности, в том числе с применением современных цифровых инструментов (IRIS и PGP)		
			ОПК-3.2 Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	-	решать стандартные задачи профессиональной деятельности на основе информационной безопасности; применять информационно-коммуникационные технологии с учетом основных требований информационной безопасности, в том числе с применением современных цифровых инструментов (IRIS и PGP)	-
			ОПК-3.3 Иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	-	-	подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований профессиональных задач в информационной безопасности, посредством электронных ресурсов, официальных сайтов
3.	ОПК-4	Способен участвовать в разработке технической доку-	ОПК-4.1 Знать: основные стандарты оформления технической документации на различ-	основные стандарты оформления технической документации на различных стадиях жизненного	-	-

		ментации, связанной с профессиональной деятельностью с использованием стандартов, норм и правил;	ных стадиях жизненного цикла информационной системы	цикла информационной системы с учетом информационной безопасности, посредством электронных ресурсов, официальных сайтов		
			ОПК-4.2 Уметь: применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы	-	применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы с учетом информационной безопасности, посредством электронных ресурсов, официальных сайтов	-

4. Структура и содержание дисциплины

4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет 4 зач.ед. (144 часа), их распределение по видам работ семестрам представлено в таблице 2.

Таблица 2

Распределение трудоёмкости дисциплины по видам работ

Вид учебной работы	**Трудоёмкость (7 семестр)**
	час. всего/*
Общая трудоёмкость дисциплины по учебному плану	**144**
1. Контактная работа:	**52,4**
Аудиторная работа	
в том числе:	
лекции (Л)	16
практические занятия (ПЗ)	34
консультации перед экзаменом	2
контактная работа на промежуточном контроле (КРА)	0,4
2. Самостоятельная работа (СРС)	**91,6**
самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к практическим занятиям, устным опросам и т.д.)	67
Подготовка к экзамену (контроль)	24,6
Вид промежуточного контроля:	Экзамен

* в том числе практическая подготовка

4.2 Содержание дисциплины

Таблица 3

Тематический план учебной дисциплины

Наименование разделов и тем дисциплин (укрупнёно)	**Всего**	**Аудиторная работа**			**Внеаудиторная работа СР**
		Л	**ПЗ всего/***	**ПКР всего/***	
Раздел 1. «Основы информационной безопасности»	53,5	6	14	-	33,5
Раздел 2. «Современные методы защиты»	88,1	10	20	-	58,1
Контактная работа на промежуточном контроле (КРА)	0,4	-	-	0,4	-
Консультации перед экзаменом	2			2	
Итого по дисциплине	**144**	**16**	**34**	**2,4**	**91,6**

* в том числе практическая подготовка

Раздел 1 Основы информационной безопасности

Тема 1 Цели и задачи информационной безопасности. Место информационной безопасности в национальной безопасности РФ

Понятие информации. Фазы обращения информации в информационных системах. Место информационной безопасности в национальной безопасности РФ. Цели и задачи обеспечения информационной безопасности. Составляющие информационной безопасности. Правовые, организационные, технические, программно-аппаратные и криптографические методы обеспечения информационной безопасности. Виды и источники угроз информационной безопасности РФ. Структура государственной системы обеспечения информационной безопасности РФ.

Тема 2 Построение системы защиты информации в организации

Архитектура СЗИ организации и основные требования к средствам защиты. Функциональное построение СЗИ организации и назначение основных подразделений. Элементарные модели СЗИ организации. Семирубежная модель защиты. Последовательность и содержание основных этапов проектирования СЗИ организации. Содержание процесса эксплуатации СЗИ организации. Анализ угроз информационной безопасности. Внутренние и внешние источники угроз информационной безопасности. Схема воздействия угроз на информационную систему. Перечень основных формальных и неформальных средств защиты информации. Стратегии защиты информации на объекте информатизации. Основы защиты информации в телекоммуникационных сетях. Роль персонала в обеспечении информационной безопасности предприятия.

Раздел 2 Современные методы защиты

Тема 1 Современные методики анализа и управления рисками информационной безопасности

Управление рисками на различных стадиях жизненного цикла информационной системы. Трехмерная модель “куб безопасности”. Анализ информационных рисков, угроз и уязвимостей системы. Оценка рисков по двум факторам. Анализ информационных рисков, угроз и уязвимостей системы. Оценка рисков по трем факторам. Программное обеспечение для анализа рисков информационной безопасности.

Тема 2 Перспективные направления в области информационной безопасности

Стеганографические методы защиты информации. Обобщенная модель стегосистемы. Классификация современных стеганографических методов защиты информации. Цифровые водяные знаки. Области применения и особенности аутентификации сообщений с использованием ЦВЗ. Вредоносное программное обеспечение и методы борьбы с ним. Методологические и практические проблемы обеспечения информационной безопасности в современном обществе.

Тема 3 Криптографическая защита информации

Классические криптоалгоритмы – моно- и многоалфавитные подстановки. Классические криптоалгоритмы - перестановки. Шифрование методом гаммирования. Современные симметричные системы шифрования. Обобщенная схема симметричного шифрования. Симметричная система шифрования DES. Отечественный стандарт симметричного шифрования. Принцип открытого распространения ключей. Алгоритм Диффи-Хеллмана. Современные асимметричные системы шифрования. Обобщенная схема асимметричного шифрования. Асимметричная система шифрования RSA. Электронная цифровая подпись. Обобщенная схема постановки и проверки ЭЦП. Электронная цифровая подпись на основе алгоритма RSA. Отечественный стандарт цифровой подписи ГОСТ Р34.10-2012.

4.3 Лекции/практические занятия

Таблица 4

Содержание лекций/практических занятий и контрольные мероприятия

№ п/п	№ раздела	№ и название лекций/ практических занятий	Формируемые компетенции (индикаторы)	Вид контрольного мероприятия	Кол-во часов/из них практическая подготовка
1.	**Раздел 1. Основы информационной безопасности**				**20**
	Тема 1. Цели и задачи информационной безопасности. Место информационной безопасности в национальной безопасности РФ	Лекция № 1. Основные понятия. Актуальность. ООП. Физическая защита. Концепция построения защиты	УК-10.1, ОПК-3.1, ОПК-3.2		2
		Практическое занятие № 1. Простейший шифр (IRIS)	ОПК-3.3	устный опрос, защита практической работы	4
		Лекция № 2. Основные определения и критерии классификации угроз. Меры противодействия угрозам. Принципы построения систем защиты	УК-10.1, УК-10.2, ОПК-3.1, ОПК-3.2		2
		Практическое занятие № 2. Подстановочный шифр (IRIS)	ОПК-3.3	устный опрос, защита практической работы	4
	Тема 2. Построение системы защиты информации в организации	Лекция № 3. Процедурный и программно-технические уровни ИБ	УК-10.2, ОПК-3.1, ОПК-3.2		2
		Практическое занятие № 3. Блочный шифр (IRIS)	ОПК-3.3	устный опрос, защита практической работы	6
2.	**Раздел 2. Современные методы защиты**				**30**

№ п/п	№ раздела	№ и название лекций/ практических занятий	Формируемые компетенции (индикаторы)	Вид контрольного мероприятия	Кол-во часов/из них практическая подготовка
	Тема 1. Современные методики анализа и управления рисками информационной безопасности	Лекция № 4. Типы вред. ПО. История вирусов. Признаки присут. вирусов	ОПК-4.1, ОПК-4.2		2
		Лекция № 5. Атаки. Защита от вред. ПО	УК-10.3, ОПК-4.1, ОПК-4.2		2
		Практическое занятие № 4. Потоковый шифр (IRIS)	ОПК-3.3	устный опрос, защита практической работы	6
	Тема 2. Перспективные направления в области информационной безопасности	Лекция № 6. Брандмауэр	ОПК-4.1, ОПК-4.2		2
		Практическое занятие № 5. Изучение тестов на простоту и ознакомление с алгоритмами генерации ключей для асимметричной криптосхемы типа rsa (PGP)	ОПК-3.3	устный опрос, защита практической работы	4
		Лекция № 7. Режим секретности	УК-10.3, ОПК-4.1, ОПК-4.2		2
		Практическое занятие № 6. Изучение асимметричной криптосхемы с открытым распределением ключей и алгоритма электронной подписи (PGP)	ОПК-3.3	устный опрос, защита практической работы	4
	Тема 3. Криптографическая защита информации	Лекция № 8. Криптоалгоритмы	ОПК-4.1, ОПК-4.2		2
		Практическое занятие № 7. Реализация шифрующей системы (PGP)	ОПК-3.3	устный опрос, защита практической работы	6

Таблица 5

Перечень вопросов для самостоятельного изучения дисциплины

№ п/п	№ раздела и темы	Перечень рассматриваемых вопросов для самостоятельного изучения
Раздел 1. Основы информационной безопасности		
1.	Тема 1. Цели и задачи информационной безопасности. Место информационной безопас-	1. Понятия: информация, информатизация, информационные технологии, информационные ресурсы. УК-10.1, УК-10.2, ОПК-3.1, ОПК-3.2. 2. Место информационной безопасности в национальной

№ п/п	№ раздела и темы	Перечень рассматриваемых вопросов для самостоятельного изучения
	ности в национальной безопасности РФ	безопасности РФ. УК-10.1, УК-10.2, ОПК-3.1, ОПК-3.2. 3. Правовые, организационные, технические, программно-аппаратные и криптографические методы обеспечения информационной безопасности. УК-10.3, ОПК-3.1, ОПК-3.2. 4. Виды и источники угроз информационной безопасности РФ. ОПК-3.1, ОПК-3.2. 5. Структура государственной системы обеспечения информационной безопасности РФ. ОПК-3.1, ОПК-3.2. 6. Правовое регулирование информационной сферы в РФ. УК-10.1, УК-10.2, УК-10.3, ОПК-3.1, ОПК-3.2. 7. Основные нормативно-методические материалы. УК-10.3, ОПК-3.1, ОПК-3.2.
2.	Тема 2. Построение системы защиты информации в организации	1. Функциональное построение СЗИ организации и назначение основных подразделений. ОПК-3.1, ОПК-3.2. 2. Элементарные модели СЗИ организации. Семирубежная модель защиты. ОПК-3.1, ОПК-3.2. 3. Последовательность и содержание основных этапов проектирования СЗИ организации. ОПК-3.1, ОПК-3.2. 4. Содержание процесса эксплуатации СЗИ организации. ОПК-3.1, ОПК-3.2.
Раздел 2. Современные методы защиты		
1.	Тема 1. Современные методики анализа и управления рисками информационной безопасности	1. Анализ информационных рисков, угроз и уязвимостей системы. ОПК-4, ПК-7. 2. Оценка рисков по двум факторам. УК-10.3, ОПК-4. 3. Оценка рисков по трем факторам. УК-10.3, ОПК-4.
2.	Тема 2. Перспективные направления в области информационной безопасности	1. Вредоносный программный код документов офисных приложений и его возможности. ОПК-4.1, ОПК-4.2. 2. Классификация и основные особенности различных видов вредоносных программ. ОПК-4.1, ОПК-4.2. 3. Возможности и особенности сетевых вредоносных программ. ОПК-4.1, ОПК-4.2. 4. Виды несанкционированного копирования компьютерной информации. ОПК-4.1, ОПК-4.2. 5. Виды нарушений работоспособности удаленного компьютера со стороны вредоносных программ. ОПК-4.1, ОПК-4.2. 6. Современное антивирусное программное обеспечение. ОПК-4.1, ОПК-4.2.
3.	Тема 3. Криптографическая защита информации	1. Электронная цифровая подпись. Обобщенная схема постановки и проверки ЭЦП. ОПК-4.1, ОПК-4.2. 2. Отечественный стандарт цифровой подписи ГОСТ Р34.10-2012. ОПК-4.1, ОПК-4.2. 3. Защищенный электронный документооборот. ОПК-4.1, ОПК-4.2. 4. Особенности защиты мультимедийного контента в телекоммуникационных сетях. ОПК-4.1, ОПК-4.2.

5. Образовательные технологии

Таблица 6

Применение активных и интерактивных образовательных технологий

№ п/п	Тема и форма занятия		Наименование используемых активных и интерактивных образовательных технологий
1.	Практическое занятие № 1. Простейший шифр	ПЗ	Разбор конкретных ситуаций
2.	Практическое занятие № 2. Подстановочный шифр	ПЗ	Разбор конкретных ситуаций
3.	Практическое занятие № 3. Блочный шифр	ПЗ	Разбор конкретных ситуаций
4.	Практическое занятие № 4. Потоковый шифр	ПЗ	Разбор конкретных ситуаций

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) Вопросы для устного опроса:

1. Цели обеспечения информационной безопасности.
2. Задачи обеспечения информационной безопасности.
3. Архитектура СЗИ организации.
4. Архитектура СЗИ и основные требования к средствам защиты.
5. Методы защиты информации при передаче в телекоммуникационных сетях.
6. Вредоносное программное обеспечение и методы борьбы с ним.
7. Каково основное отличие асимметричной криптосхемы от криптосхемы с секретным ключом.
8. Почему в схеме шифрования с открытым распределением ключа для целей аутентификации применяется секретное преобразование.
9. Какими свойствами должна обладать хэш-функция.
10. Как средствами криптографии осуществлять контроль над достоверностью передачи информации.

2) Примеры заданий для практических работ

Подробный перечень заданий для практических занятий представлен в оценочных материалах дисциплины.

3) Перечень вопросов, выносимых на экзамен:

1. Понятие информационной безопасности. Компьютерная безопасность. Защита информации. Угрозы информационной безопасности.

2. Основные составляющие информационной безопасности. Доступность. Целостность. Конфиденциальность. Важность и сложность проблемы информационной безопасности.
3. О необходимости объектно-ориентированного подхода к информационной безопасности. Основные понятия объектно-ориентированного подхода
4. Основные понятия объектно-ориентированного подхода. Применение объектно-ориентированного подхода к рассмотрению защищаемых систем. Недостатки традиционного подхода к информационной безопасности с объектной точки зрения
5. Основные определения и критерии классификации угроз.
6. Наиболее распространенные угрозы доступности
7. Некоторые примеры угроз доступности
8. Вредоносное программное обеспечение.
9. Основные угрозы целостности. Основные угрозы конфиденциальности.
10. Что такое законодательный уровень информационной безопасности. Конституция РФ. Гражданский кодекс РФ. Уголовный кодекс РФ.
11. Законодательный уровень информационной безопасности. Закон «Об информации, информационных технологиях и о защите информации». Закон «О лицензировании отдельных видов деятельности». Текущее состояние российского законодательства в области информационной безопасности.
12. Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт. Основные понятия.
13. Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт. Механизмы безопасности. Классы безопасности. Сетевые механизмы безопасности.
14. Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт. Администрирование средств безопасности.
15. Административный уровень ИБ. Основные понятия.
16. Административный уровень ИБ. Политика безопасности.
17. Административный уровень ИБ. Программа безопасности
18. Административный уровень ИБ. Синхронизация программы безопасности с жизненным циклом систем
19. Управление рисками. Основные понятия.
20. Управление рисками. Подготовительные этапы управления рисками.
21. Управление рисками. Основные этапы управления рисками.
22. Процедурный уровень ИБ. Основные классы мер процедурного уровня. Управление персоналом.
23. Процедурный уровень ИБ. Физическая защита.
24. Процедурный уровень ИБ. Поддержание работоспособности.
25. Признаки присутствия на компьютере вредоносных программ. Скрытые проявления.
26. Признаки присутствия на компьютере вредоносных программ. Косвенные проявления.
27. Признаки присутствия на компьютере вредоносных программ. Явные проявления.

28. Методы защиты от вредоносных программ. Организационные методы. Правила работы за компьютером. Политика безопасности.
29. Методы защиты от вредоносных программ. Технические методы. Исправления. Брандмауэры. Антиспам.
30. Виды сетевых атак и основные уязвимости. Краткий обзор различных видов сетевых атак. Спам.
31. Виды сетевых атак и основные уязвимости. Краткий обзор различных видов сетевых атак. Основные уязвимости.
32. Межсетевые экраны. Типы.
33. Категории атак. Атаки доступа.
34. Категории атак. Атаки модификации.
35. Категории атак. Атаки на отказ в обслуживании.
36. Категории атак. Атаки на отказ от обязательств.
37. Безопасность web-содержимого. Публикация информации на сайтах.
38. Безопасность web-содержимого. Технологии активного содержимого на стороне клиента.
39. Безопасность web-содержимого. Технологии активного содержимого на стороне сервера.

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

Для оценки знаний, умений, навыков и формирования компетенций по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов.

В основу балльно-рейтинговой системы (БРС) положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего и промежуточного контроля знаний обучающихся.

Таблица 7

Система рейтинговой оценки успеваемости

Баллы	Балльная оценка текущей успеваемости			
За устный опрос	2	3	4	5
За практическую работу	2	3	4	5
За экзамен	2	3	4	5
Оценка	Неудовлетворительно	Удовлетворительно	Хорошо	Отлично

Таблица 8

Итоговая сумма баллов

Виды контроля	Количество видов контроля	Количество баллов за единицу	Количество баллов
Устный опрос	10	5	50
Защита практической работы	7	5	35

Экзамен	1	5	5
Всего	-	-	90

Таблица 9

Балльно-рейтинговая система контроля успеваемости

Шкала оценивания	**Экзамен**
81-90	Отлично
66-80	Хорошо
51-65	Удовлетворительно
0-50	Неудовлетворительно

7. Учебно-методическое и информационное обеспечение дисциплины

7.1 Основная литература

1. Нестеров, С. А. Основы информационной безопасности: учебник для вузов / С. А. Нестеров. — Санкт-Петербург: Лань, 2022. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165837 . — Режим доступа: для авториз. пользователей.
2. Моргунов, А. В. Информационная безопасность: учебно-методическое пособие / А. В. Моргунов. — Новосибирск: НГТУ, 2019. — 83 с. — ISBN 978-5-7782-3918-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/152227 . — Режим доступа: для авториз. пользователей.
3. Информационная безопасность [Электронный ресурс] : учебное пособие / сост. Е.Р. Кирколуп, Ю.Г. Скурыдин, Е.М. Скурыдина. — Электрон. дан. — Барнаул : АлтГПУ, 2017. — 316 с. — Режим доступа: https://e.lanbook.com/book/112164. (открытый доступ)

7.2 Дополнительная литература

1. Информационная безопасность: учебное пособие. — Пермь: ПГГПУ, 2018. — 87 с. — ISBN 978-5-85219-007-9. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/129509. — Режим доступа: для авториз. пользователей.
2. Гилязова, Р. Н. Информационная безопасность. Лабораторный практикум: учебное пособие для спо / Р. Н. Гилязова. — 2-е изд., стер. — Санкт-Петербург: Лань, 2022. — 44 с. — ISBN 978-5-8114-8249-8. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/173796 . — Режим доступа: для авториз. пользователей.

7.3 Нормативные правовые акты

1. Конституция Российской Федерации. http://dehack.ru/intro/ (открытый доступ)
2. Уголовный кодекс Российской федерации. http://dehack.ru/intro/ (открытый доступ)
3. Федеральный закон №149-ФЗ «Об информации, информационных технологиях и о защите информации». http://dehack.ru/intro/ (открытый доступ)
4. Федеральный закон РФ 27.07.2006 г. N 152-ФЗ «О персональных данных». http://dehack.ru/intro/ (открытый доступ)
5. Федеральный закон от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи». http://dehack.ru/intro/ (открытый доступ)
6. Руководящие документы ФСТЭК РФ: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty# (открытый доступ)
7. Доктрина информационной безопасности Российской Федерации http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=28679
8. BS ISO/IES 27005:20008 Ru. Информационные технологии - Методы обеспечения безо-пасности - Управление рисками информационной безопасности. http://gtrust.ru/show_good.php?idtov=1137 (открытый доступ)

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	Основы информационной безопасности	MS Office	обучающая	Microsoft	2007 или выше
		IRIS		MAGO	3 и выше
2	Современные методы защиты	MS Office	обучающая	Microsoft	2007 или выше
		PGP		MAGO	3 и выше

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

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
Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций (1 корпус, 110 аудитория)	проектор, экран настенный, компьютер
Учебные аудитории для проведения практических занятий, групповых и индивидуальных консультаций, курсового проектирования, текущего контроля и промежуточной аттестации (1 корпус, 207, 214 аудитория)	Сервер + терминалы: 207 ауд. - 21 шт. 214 ауд. - 20 шт.
ЦНБ им. Н.И. Железнова	Читальный зал (25 компьютеров)
Общежитие	Комната для самоподготовки

11. Методические рекомендации студентам по освоению дисциплины

Основными видами обучения студентов по дисциплине являются лекции, практические занятия в компьютерном классе и самостоятельная работа студентов.

Самостоятельная работа студентов по дисциплине «Информационная безопасность» направлена на углубление и закрепление знаний, полученных на лекциях и практических занятиях, на развитие практических умений и включает такие виды работ, как:

- работа с лекционным материалом;
- работа с рекомендованной литературой при подготовке к практическим занятиям;
- подготовка к экзамену.

При изучении дисциплины "Информационная безопасность" используется рейтинговая система оценивания знаний студентов, которая позволяет реализовать непрерывную и комплексную систему оценивания учебных достижений студентов. Непрерывность означает, что текущие оценки не усредняются (как в традиционной технологии), а непрерывно складываются на протяжении семестра при изучении дисциплины. Комплексность означает учет всех форм учебной и самостоятельной работы студента в течение семестра.

Принципы рейтинга: непрерывный контроль (на каждом из аудиторных занятий) и получение более высокой оценки за работу, выполненную в срок. При проведении практических занятий предусмотрено широкое использование активных и интерактивных форм (разбор конкретных ситуаций, устный опрос,

защита практических работ).

Бально–рейтинговая система повышает мотивацию студентов.

Промежуточным контролем по дисциплине является экзамен.

В результате изучения дисциплины формируются знания и умения в области информационной безопасности, студенты получают опыт по информационной безопасности. Каждому студенту во время практических занятий предоставляется полная возможность быть индивидуальным пользователем компьютера, самостоятельно отрабатывать учебные вопросы и выполнять индивидуальные учебные задания преподавателя.

Основная рекомендация сводится к обеспечению равномерной активной работы студентов над дисциплиной в течение всего семестра: студенты должны прорабатывать курс прослушанных лекций, готовиться к выполнению и защите практических работ, а также выполнять задания, вынесенные на самостоятельную работу. Рекомендуется перед каждой лекцией просматривать содержание предстоящей лекции по учебнику и конспекту с тем, чтобы лучше воспринять материал лекции. Важно помнить, что ни одна дисциплина не может быть изучена в необходимом объеме только по конспектам. Для хорошего усвоения курса нужна систематическая работа с учебной и научной литературой, а конспект может лишь облегчить понимание и усвоение материала.

В подготовке к занятиям по дисциплине студенты должны активно использовать дополнительную литературу, поскольку именно с ее помощью можно получить наиболее полное и верное представление о происходящих в стране и в мире процессах.

Виды и формы отработки пропущенных занятий

Студент, пропустивший занятия обязан его отработать:

- лекцию отрабатывают путем устного ответа по пропущенной теме;
- практическое занятие путем выполнения практической работы, которая выполнялась на данном практическом занятии.

12. Методические рекомендации преподавателям по организации обучения по дисциплине

В процессе обучения по дисциплине «Информационная безопасность» используются лекционно-практические занятия, разбор конкретных ситуаций, организуется работа с методическими и справочными материалами, целесообразно применение современных технических средств обучения и информационных технологий. Освоение учебной дисциплины предполагает осмысление её разделов и тем на практических занятиях, в процессе которых студент должен закрепить и углубить теоретические знания.

Дисциплина «Информационная безопасность» имеет прикладной характер, её теоретические положения и практические навыки могут быть использованы в будущей практической деятельности.

Промежуточный контроль – экзамен.

Рекомендуется определять сроки проведения контрольных мероприятий, максимальная оценка за каждое из них и правила перевода общего количества

баллов, полученных при изучении дисциплины, в итоговый результат (экзамен).

Выполнение практических заданий является обязательным для всех обучающихся. Студенты, не выполнившие в полном объеме работы, предусмотренные учебным планом, не допускаются к сдаче экзамена.

Программу разработал:

Никаноров М.С. _____

Греченева А.В. _____

РЕЦЕНЗИЯ

на рабочую программу дисциплины Б1.О.19 «Информационная безопасность» ОПОП ВО по направлению 09.03.02 «Информационные системы и технологии», направленность «Большие данные и машинное обучение» и «Компьютерные науки и интеллектуальный анализ данных» (квалификация выпускника – бакалавр)

Щедриной Еленой Владимировной, доцентом кафедры Систем автоматизированного проектирования и инженерных расчётов ФГБОУ ВО «Российский государственный аграрный университет - МСХА имени К.А. Тимирязева», кандидатом педагогических наук (далее по тексту рецензент), проведено рецензирование рабочей программы дисциплины «Информационная безопасность» ОПОП ВО по направлению 09.03.02 «Информационные системы и технологии»**,** направленность **«Большие данные и машинное обучение»** и **«Компьютерные науки и интеллектуальный анализ данных»** (бакалавриат) разработанной в ФГБОУ ВО «Российский государственный аграрный университет – МСХА имени К.А. Тимирязева», на кафедре Прикладной информатики – Никаноров М.С., старший преподаватель и Греченева А.В., к.т.н. доцент.

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 09.03.02 «Информационные системы и технологии». 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.О.

3. Представленные в Программе **цели** дисциплины соответствуют требованиям ФГОС ВО направления 09.03.02 «Информационные системы и технологии».

4. В соответствии с Программой за дисциплиной «Информационная безопасность» закреплено три компетенции (восемь индикаторов): УК-10 (УК-10.1; УК-10.2; УК-10.3), ОПК-3 (ОПК-3.1; ОПК-3.2; ОПК-3.3), ОПК-4 (ОПК-4.1; ОПК-4.2). Дисциплина «Информационная безопасность» и представленная Программа *способна реализовать* их в объявленных требованиях.

5. ***Результаты обучения***, представленные в Программе в категориях знать, уметь, владеть *соответствуют* специфике и содержанию дисциплины и *демонстрируют возможность* получения заявленных результатов.

6. Общая трудоёмкость дисциплины «Информационная безопасность» составляет 4 зачётных единицы (144 часа).

7. 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 09.03.02 «Информационные системы и технологии» и возможность дублирования в содержании отсутствует.

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

9. Программа дисциплины «Информационная безопасность» предполагает занятия в интерактивной форме.

10. Виды, содержание и трудоёмкость самостоятельной работы студентов, представленные в Программе, соответствуют требованиям к подготовке выпускников, содержащимся во ФГОС ВО направления 09.03.02 «Информационные системы и технологии»**.**

11. Представленные и описанные в Программе формы *текущей* оценки знаний (опрос, как в форме обсуждения отдельных вопросов и выступлений, а также контроль выполнения

и проверка отчетности по практическим работам), соответствуют специфике дисциплины и требованиям к выпускникам.

Форма промежуточного контроля знаний студентов, предусмотренная Программой, осуществляется в форме экзамена, что соответствует статусу дисциплины, как обязательной части учебного цикла – Б1.О ФГОС ВО направления 09.03.02 «Информационные системы и технологии».

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

13. Учебно-методическое обеспечение дисциплины представлено: основной литературой – 2 источника (базовый учебник), дополнительной литературой – 2 наименование, периодическими изданиями – 2 источника со ссылкой на электронные ресурсы и соответствует требованиям ФГОС ВО направления 09.03.02 «Информационные системы и технологии».

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

15. 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 проведенного рецензирования можно сделать заключение, что характер, структура и содержание рабочей программы дисциплины «Информационная безопасность» ОПОП ВО по направлению 09.03.02 «Информационные системы и технологии», направленности «Большие данные и машинное обучение» и «Компьютерные науки и интеллектуальный анализ данных» (квалификация выпускника – бакалавр), разработанная Никаноровым М.С., старшим преподавателем и Греченевой А.В., к.т.н., доцентом соответствует требованиям ФГОС ВО современным требованиям экономики, рынка труда и позволит при её реализации успешно обеспечить формирование заявленных компетенций.

Рецензент: Щедрина Е.В., доцент кафедры Систем автоматизированного проектирования и инженерных расчётов ФГБОУ ВО «Российский государственный аграрный университет - МСХА имени К.А. Тимирязева», кандидат педагогических наук

_____

«_____» _____ 2022 г.