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
_______________ Л.И. Хоружий
«30» августа 2021 г.

РАБОЧАЯ ПРОГРАММА МОДУЛЬНОЙ ДИСЦИПЛИНЫ
Б1.В.01.03 «Безопасность и защита информационных систем»

для подготовки бакалавров

ФГОС ВО

Направление: 44.03.04 Профессиональное обучение (по отраслям)
Направленность: Информационные технологии в образовании

Курс: 4
Семестр: 7

Форма обучения: очная

Год начала подготовки: 2021

Москва, 2021

Разработчики:

Лемешко Т.Б., старший преподаватель

Худякова Е.В., д.э.н., профессор

«25» августа 2021 г.

Рецензент: Ивашова О.Н., к.с/х.н., ст. преподаватель

«25» августа 2021 г.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 44.03.04 «Профессиональное обучение» (по отраслям) и учебного плана 2021 года начала подготовки.

Программа обсуждена на заседании кафедры прикладной информатики протокол № 1 от «26» августа 2021 г.

Зав. кафедрой прикладной информатики: Худякова Е.В., д.э.н., профессор

«26» августа 2021 г.

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

(подпись)

«26» 01 2021 г.

Заведующий выпускающей кафедрой педагогики и психологии профессионального образования, д.п.н., профессор Кубрушко П.Ф.

(подпись)

«26» августа 2021 г.

Заведующий отделом комплектования ЦНБ Ефимова Я.Р.
(подпись)

СОДЕРЖАНИЕ

АННОТАЦИЯ
рабочей программы модульной учебной дисциплины
Б1.В.01.03 «Безопасность и защита информационных систем»
для подготовки бакалавра по направлению 44.03.04 «Профессиональное обучение» (по отраслям), направленности «Информационные технологии в образовании»

Цель освоения дисциплины: ознакомление с основами информационной безопасности и защиты информации, законодательной и нормативно-правовой базой информационной безопасности, методами защиты информационных систем.

Место дисциплины в учебном плане: дисциплина включена в часть, формируемую участниками образовательных отношений учебного плана по направлению подготовки 44.03.04 «Профессиональное обучение» (по отраслям).

Требования к результатам освоения дисциплины: в результате освоения дисциплины формируются следующие компетенции (индикаторы): **ПКос-2 (Пкос-2.1; Пкос-2.2; Пкос-2.3)**

Краткое содержание дисциплины:

Основы информационной безопасности и защиты информации. Законодательный и нормативно-правовой уровни обеспечения информационной безопасности. Программно-технические меры обеспечения информационной безопасности. Методы защиты информационных систем. Виды воздействий информационных угроз на информационные системы (ИС): внешние и внутренние. Методы шифрования данных. Криптография. Идентификация и аутентификация пользователей. Методы разграничения и контроля прав пользователей средствами операционных систем. Шифрование симметричным ключом, шифрование асимметричными ключами, алгоритм с использованием открытого ключа. Цифровая подпись. Биометрические методы и др.

Общая трудоемкость дисциплины: 144/4 (часы/зач. ед.), в том числе 4 часа практической подготовки.

Промежуточный контроль: экзамен в 7 семестре.

1. Цель освоения дисциплины

Целью освоения дисциплины «Безопасность и защита информационных систем» является ознакомление с основами информационной безопасности и защиты информации, законодательной и нормативно-правовой базой информационной безопасности, методами защиты информационных систем.

2. Место дисциплины в учебном процессе

Дисциплина «Безопасность и защита информационных систем» относится к части, формируемой участниками образовательных отношений учебного плана. Дисциплина «Безопасность и защита информационных систем» реализуется в соответствии с требованиями ФГОС ВО, ОПОП ВО и Учебного плана по направлению 44.03.04 «Профессиональное обучение» (по отраслям).

Предшествующими курсами, на которых непосредственно базируется дисциплина «Безопасность и защита информационных систем» является

«Информатика», «Технологии работы с информацией», «Базы данных», «ИТ-инфраструктура организации», «Компьютерные коммуникации и сети».

Дисциплина «Безопасность и защита информационных систем» является основополагающей для изучения следующих дисциплин: «Проектирование информационных систем в образовании», «Информационные системы управления образовательным процессом».

Рабочая программа дисциплины «Безопасность и защита информационных систем» 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

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.	**ПКос-2**	Способен выполнять деятельность и (или) демонстрировать элементы осваиваемой обучающимися деятельности, предусмотренной программой учебной дисциплины (модуля), практики	**ПКос-2.1** Знает: современные информационные технологии и программные средства, методы алгоритмизации, языки и системы программирования, основные платформы, технологии и инструментальные программно-аппаратные средства для реализации информационных систем в сфере образования	Законодательный и нормативно-правовой уровни обеспечения информационной безопасности. Основные составляющие информационной безопасности. Наиболее распространенные угрозы информационной безопасности. Виды мер обеспечения информационной безопасности. Направления и методы защиты информационной системы.	-	-
			ПКос-2.2 Умеет: выбирать современные информационные технологии и программные средства, применять методы алгоритмизации, языки и системы программирования, осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем при решении профессиональных задач в сфере образования	-	Применять методы защиты информационных систем при решении профессиональных задач	-
			ПКос-2.3 Владеет: навыками применения современных информационных	-	-	Навыками применения технологий

№ п/п	Код компетенции	Содержание компетенции (или её части)	Индикаторы компетенций	В результате изучения учебной дисциплины обучающиеся должны:		
				знать	уметь	владеть
			технологий и программных средств, навыками программирования и инструментальными программно-аппаратными средствами в сфере образования			защиты данных в информационных системах

4. Структура и содержание дисциплины

4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет 4 зач. единиц (144 часа), их распределение по видам работ в 7 семестре представлено в табл. 2.

Таблица 2

Распределение трудоёмкости дисциплины по видам работ по семестрам

Вид учебной работы	Трудоёмкость	
	час. всего/*	в т.ч. по семестрам
		№ 7/*
Общая трудоёмкость дисциплины по учебному плану	**144/4**	**144/4**
1. Контактная работа:	**52,4/4**	**52,4/4**
Аудиторная работа	**52,4/4**	**52,4/4**
лекции (Л)	16	16
практические занятия (ПЗ)	34/4	34/4
Консультация перед экзаменом	2	2
контактная работа на промежуточном контроле (КРА)	0,4	0,4
2. Самостоятельная работа (СРС)	**91,6**	**91,6**
самостоятельное изучение тем, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к практическим занятиям и т.д.)	58	58
Подготовка к экзамену (контроль)	33,6	33,6
Вид промежуточного контроля:		Экзамен

* в том числе практическая подготовка

4.2 Содержание дисциплины

Таблица 3

Тематический план учебной дисциплины

Наименование тем дисциплины	Всего часов на тему/ всего/*	Аудиторная Работа			Внеаудиторная работа (СРС)
		Л	ПЗ/ всего/*	ПКР	
Тема 1. Основы информационной безопасности и защиты информации	29,6	2	4	-	23,6
Тема 2. Законодательный и нормативно-правовой уровни обеспечения информационной безопасности	30/2	4	6/2	-	20
Тема 3. Программно-технические меры обеспечения информационной безопасности	40	4	12	-	24
Тема 4. Методы защиты информационных систем	42/2	6	12/2	-	24
Консультация перед экзаменом	2	-	-	2	-
Контактная работа на промежуточном контроле (КРА)	0,4	-	-	0,4	-
ИТОГО за 7 семестр	**144/4**	**16**	**34/4**	**2,4**	**91,6**

* в том числе практическая подготовка

Тема 1. Основы информационной безопасности и защиты информации

Актуальность проблемы обеспечения безопасности в цифровом обществе. Основные понятия и определения информационной безопасности. Основные составляющие информационной безопасности. Наиболее распространенные угрозы информационной безопасности. Виды мер обеспечения информационной безопасности. Средства защиты от несанкционированного доступа: средства авторизации, мандатное управление доступом, избирательное управление доступом, управление доступом на основе ролей, журналирование (аудит).

Тема 2. Законодательный и нормативно-правовой уровни обеспечения информационной безопасности

Обзор российского законодательства в области информационной безопасности. Стандарты и спецификации в области информационной безопасности. Морально-этические нормы поведения в цифровом мире. Организационно-правовые механизмы обеспечения информационной безопасности предприятия. Доктрина информационной безопасности РФ, утвержденная Указом Президента РФ от 5.12.2016 г. Закон 149-ФЗ «Об информации…». Закон 1-ФЗ «Об электронной цифровой подписи». Закон 63-ФЗ «Об электронной подписи». Обзор зарубежного законодательства в области информационной безопасности. Сетевые сервисы безопасности по уровням модели OSI. Сетевые механизмы безопасности. Администрирование средств безопасности. Критерии оценки информационной безопасности ISO/IEC 15408. Российское и международное законодательство в области защиты прав на интеллектуальную собственность.

Административный и процедурный уровни обеспечения информационной безопасности. Анализ рисков информационной безопасности. Политика информационной безопасности. Программа работ в области обеспечения информационной безопасности. Основные классы мер процедурного уровня: управление персоналом, физическая защита, поддержание работоспособности, реагирование на нарушения режима безопасности, планирование восстановительных работ.

Тема 3. Программно-технические меры обеспечения информационной безопасности

Основные понятия программно-технического уровня информационной безопасности. Особенности современных информационных систем, существенные с точки зрения безопасности. Технологии защиты данных. Идентификация и аутентификация, управление доступом. Шифрование, контроль целостности. Криптографические алгоритмы. Анализ защищенности. Обеспечение высокой доступности. Сервисы безопасности. Классификация сервисов безопасности с точки зрения места в общей архитектуре мер безопасности. Технологии защиты межсетевого обмена данными. Методы управления средствами сетевой безопасности.

Тема 4. Методы защиты информационных систем

Направления защиты информационной системы: защита объектов информационной системы; защита процессов, процедур и программ обработки информации; защита каналов связи (акустические, инфракрасные, проводные,

радиоканалы и др.), включая защиту информации в локальных сетях; подавление побочных электромагнитных излучений; управление системой защиты.

Виды воздействий информационных угроз на информационные системы (ИС): внешние и внутренние. Методы защиты ИС. Методы дублирования информации, архивирование данных, зеркальное отображение информации, RAID массивы. Методы шифрования данных. Криптография. Идентификация и аутентификация пользователей. Методы разграничения и контроля прав пользователей средствами операционных систем. Шифрование симметричным ключом, шифрование асимметричными ключами, алгоритм с использованием открытого ключа. Цифровая подпись. Биометрические методы.

4.3 Лекции/практические занятия

Таблица 4

Содержание лекций/ практических занятий и контрольные мероприятия

№ п/п	№ темы	№ и название лекций/ практических занятий	Формируемые компетенции (индикаторы)	Вид контрольного мероприятия	Кол-во часов/*
1.	Тема 1. Основы информационной безопасности и защиты информации	Лекция № 1. Основы информационной безопасности и защиты информации	ПКос-2.1; ПКос-2.2; ПКос-2.3	-	2
		Практическое занятие № 1. Использование сетевых сервисов Веб 2.0. для создания ментальной карты, веб-микса и др. по ИБ		Защита практической работы № 1.	4
2.	Тема 2. Законодательный и нормативно-правовой уровни обеспечения информационной безопасности	Лекция № 2. Законодательный и нормативно-правовой уровни обеспечения информационной безопасности	ПКос-2.1; ПКос-2.2; ПКос-2.3	-	4
		Практическое занятие № 2. Анализ стандартов. Поиск и анализ законодательных актов по ИБ в справочно-правовой системе КонсультантПлюс. Анализ рисков ИБ.		защита практической работы № 2.	6/2
3.	Тема 3. Программно-технические меры обеспечения информационной безопасности	Лекция № 3. Программно-технические меры обеспечения информационной безопасности	ПКос-2.1; ПКос-2.2; ПКос-2.3	-	4
		Практическое занятие № 3. Программно-технические меры обеспечения информационной безопасности»		защита практической работы № 3.	12

№ п/п	№ темы	№ и название лекций/ практических занятий	Формируемые компетенции (индикаторы)	Вид контрольного мероприятия	Кол-во часов/*
4.	Тема 4. Методы защиты информационных систем	Лекция № 4. Методы защиты информационных систем	ПКос-2.1; ПКос-2.2; ПКос-2.3	-	6
		Практическое занятие № 4. Методы защиты ИС		защита практической работы № 4.	6/2
		Практическое занятие № 5. Шифрование. Цифровая подпись. Биометрия. Идентификация и аутентификация		защита практической работы № 5.	6

* в том числе практическая подготовка

Таблица 5

Перечень вопросов для самостоятельного изучения дисциплины

№ п/п	№ темы	Перечень рассматриваемых вопросов для самостоятельного изучения
1.	Тема 1, 2. Основы информационной безопасности и защиты информации. Законодательный и нормативно-правовой уровни обеспечения информационной безопасности	1. Актуальность проблемы обеспечения безопасности в цифровом обществе, в условиях цифровой экономики и цифровизации сельского хозяйства. 2. Законодательные акты РФ, регулирующие правовые отношения в сфере информационной безопасности и защиты государственной тайны. 3. Морально-этические нормы поведения в цифровом мире. 4. Политика информационной безопасности. Программа работ в области обеспечения информационной безопасности. ПКос-2.1; ПКос-2.2; ПКос-2.3
2.	Тема 3. Программно-технические меры обеспечения информационной безопасности	1. Методы управления средствами сетевой безопасности. 2. Технологии обнаружения вторжений. 3. Инфраструктура защиты на прикладном уровне. 4. Технологии межсетевых экранов. 5. Обеспечение безопасности операционных систем. 6. Технологии аутентификации ПКос-2.1; ПКос-2.2; ПКос-2.3
3.	Тема 4. Методы защиты информационных систем	1. Криптография, её особенности. 2. Биометрия 3. Идентификация и аутентификация пользователей. ПКос-2.1; ПКос-2.2; ПКос-2.3

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.	Основы информационной безопасности и защиты информации	Л	Интерактивная лекция
2.	Использование сетевых сервисов Веб 2.0. для создания ментальной карты, веб-микса и др. по ИБ	ПЗ	Групповое обсуждение
3.	Законодательный и нормативно-правовой уровни обеспечения информационной безопасности	Л	Интерактивная лекция
4.	Анализ стандартов. Поиск и анализ законодательных актов по ИБ в справочно-правовой системе КонсультантПлюс. Анализ рисков ИБ.	ПЗ	Групповое обсуждение
5.	Методы защиты информационных систем	Л	Интерактивная лекция
6.	Шифрование. Цифровая подпись. Биометрия. Идентификация и аутентификация	ПЗ	Групповое обсуждение

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) Примеры заданий практических работ

Практическая работа № 1. Использование сетевых сервисов Веб 2.0. для создания ментальной карты, веб-микса и др. по ИБ

Пример задания:

1. Создание ментальной карты (https:// www.mindmup.com) на тему: «Виды вредоносных программ и методы защиты от них».
2. Создание вебмикса (https:// www.symbaloo.com) для реализации проекта «Интернет: проблемы защиты интеллектуальной собственности».
3. Использование сервиса ленты времени (https:// www.sutori.com) по истории развития компьютерных вирусов.

Практическая работа № 2. Анализ стандартов. Поиск и анализ законодательных актов по ИБ в справочно-правовой системе КонсультантПлюс. Анализ рисков ИБ.

Пример задания:

Используя информационную систему Консультант Плюс, найти и отобразить с добавлением в раздел «Избранное» и экспортом в Microsoft Word:

1) основные нормативно-правовые акты, регулирующие деятельность в информационной сфере.

2) определения основных категорий информационной безопасности.

3) подборку статей по защите информации.

Практическая работа № 3. «Программно-технические меры обеспечения информационной безопасности».

Пример 1. Используя справочные средства операционной системы Windows найти и отобразить с экспортом в Microsoft Word:

1) понятия учетной записи и домена и типов доступа к операционной системе: глобальные, локальные, ограниченные и административные.

2) описание порядка создания, изменения, активации и удаления учетных записей.

3) основные категории локальных пользователей (пользователи и группы) и конкретных прав каждого вида учетных записей, включая администраторов, пользователей, опытных пользователей, операторов архива, репликаторов и гостей.

Пример 2. Используя средства Internet (kaspersky.ru и т.п.), справочные средства и антивирусное программное обеспечение:

1) найти и отобразить с экспортом в Microsoft Word понятия мошеннического программного обеспечения, хакерских атак, фишинга и спама.

2) найти и отобразить с экспортом в Microsoft Word описание порядка использования и ключевых функций Kaspersky Unlocker и Kaspersky Internet Security, дать сравнительную характеристику ключевых функций Kaspersky Rescue Disk и Kaspersky Antivirus (Kaspersky Virusscanner, Kaspersky Virus Removal Tool и т.д.).

3) открыть антивирусную программу, произвести настройку параметров ее работы, запустить проверку и сформировать отчет о результатах работы.

Пример 3.

1. Зашифровать следующие сообщения методом перестановки:
ИНФОРМАЦИОННЫЕ СИСТЕМЫ
ТЕЛЕКОММУНИКАЦИИ.
2. Зашифровать следующие сообщения методом подстановки:
КОНФИДЕНЦИАЛЬНОСТЬ
ШИФРОВАНИЕ
КРИПТОГРАФИЯ
3. Расшифровать следующее сообщение методом перестановки без ключа:
ЕЫНЬЛАНОСРЕП НАДЕЫН

Пример 4. Используя средства Internet и справочные средства программ резервного копирования найти и отобразить с экспортом в Microsoft Word:

1) понятия полного, дифференциального и инкрементного резервного копирования.

2) описание порядка создания образа и восстановления из него.

3) дать сравнительную характеристику основных функций трех программ резервного копирования по следующим критериям: условия распространения, планирование (работа по расписанию), возможности работы с разделами диска, создания загрузочного диска, шифрования, сжатия, настройки фильтров, онлайн резервного копирования.

Практическая работа № 4, 5. Методы защиты информационных систем

1. Шифрование данных
2. Создание цифровой подписи
3. Идентификация и аутентификация
4. Биометрия

2) Примерный перечень вопросов, выносимых на промежуточную аттестацию (экзамен в 7 семестре)

1. Прогресс информационных технологий и необходимость обеспечения безопасности
2. Основные понятия информатизации общества и информационной безопасности
3. Структура понятия «Информационная безопасность»
4. Субъекты и объекты информационной безопасности
5. Нормативно-правовое регулирование информационной безопасности
6. Типы международных организаций в сфере информационной безопасности
7. Направления работы крупных альянсов в сфере информационной безопасности
8. Понятие и особенности экономической информации как объекта безопасности
9. Перечень сведений, относящихся к коммерческой тайне
10. Перечень сведений, которые не могут составлять коммерческую тайну
11. Объекты банковской тайны
12. Статьи Уголовного кодекса о компьютерных преступлениях
13. Доктрина информационной безопасности РФ
14. Федеральный закон от №149-ФЗ «Об информации, информационных технологиях и о защите информации»
15. Федеральный закон от №63-ФЗ «Об электронной подписи»
16. Принципиальные подходы к обеспечению информационной безопасности
17. Сравнительная характеристика фрагментного и комплексного подхода к защите информации
18. Общие принципы обеспечения информационной безопасности
19. Специфические методы обеспечения информационной безопасности
20. Принципы построения системы информационной безопасности

21. Системный подход к защите информации
22. Требования к системе мер защиты информации
23. Принципы построения и особенности практической реализации системы защиты информации экономического субъекта
24. Механизм обеспечения информационной безопасности РФ в сфере экономики
25. Цели, задачи и функции системы защиты информации
26. Защиты от несанкционированного доступа. Идентификация и аутентификация пользователя.
27. Защита интеллектуальной собственности средствами патентного и авторского права.
28. Программно-аппаратные средства обеспечения информационной безопасности в информационных сетях.
29. Симметричные шифры.
30. Ассиметричные шифры.
31. Криптографические протоколы.
32. Криптографические хеш-функции.
33. Электронная подпись.
34. Организационное обеспечение информационной безопасности.
35. Служба безопасности организации.
36. Обеспечивающие компоненты системы защиты информации
37. Методы и средства обеспечения информационной безопасности
38. Сущность криптографических методов
39. Организационно-административные мероприятия обеспечения компьютерной безопасности
40. Принципы обеспечения информационной безопасности на основе инженерно-технического обеспечения
41. Меры предупреждения и защиты от компьютерных преступлений
42. Информационные угрозы и их классификация
43. Действия и события, нарушающие информационную безопасность
44. Основные виды каналов утечки информации
45. Пути несанкционированного доступа к информации
46. Стратегия и тактика злоумышленника при несанкционированном доступе
47. Личностно - профессиональные характеристики сотрудников, способствующие реализации информационных угроз
48. Способы воздействия угроз на информационные объекты
49. Вредоносные программы, их виды
50. Признаки воздействия вирусов на компьютерную систему
51. Исторические аспекты компьютерных преступлений
52. Уголовно-правовая характеристика компьютерных преступлений,
53. Компьютерные преступления и их классификация
54. Субъекты компьютерных преступлений
55. Объективная сторона компьютерных преступлений
56. Уголовно-правовой контроль над компьютерной преступностью в РФ
57. Организация системы защиты информации экономических систем
58. Этапы построения системы защиты информации

59. Политика информационной безопасности
60. Способы практической реализации механизмов защиты информации
61. План построения системы защиты информации
62. Организация конфиденциального делопроизводства
63. Структура и функции службы информационной безопасности компании
64. Типы политики информационной безопасности
65. Оценка эффективности инвестиций в информационную безопасность
66. Обеспечение информационной безопасности автоматизированных банковских систем
67. Информационная безопасность электронной коммерции
68. Обеспечение компьютерной безопасности учетной информации
69. Информационная безопасность предпринимательской деятельности
70. Методика защиты электронной почты
71. Обеспечение информационной безопасности должностных лиц и представителей деловых кругов
72. Электронная цифровая подпись и особенности ее применения
73. Защита информации в Интернете
74. Информационная безопасность пользователей мобильных устройств
75. Методы защиты образовательных информационных систем
76. Внешние и внутренние угрозы на информационные системы
77. Идентификация и аутентификация пользователей
78. Цифровая подпись
79. Биометрические методы
80. Направления защиты информационной системы

6.2 Описание показателей и критериев контроля успеваемости, описание шкал оценивания

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

Промежуточный контроль знаний проводится в форме экзамена в 7 семестре.

Критерии оценки экзамена представлены в таблицах 7, 8.

Таблица 7

Промежуточный контроль знаний обучающихся

Шкала оценивания	Экзамен
5	Отлично
4	Хорошо
3	Удовлетворительно
2	Неудовлетворительно

Таблица 8

Критерии оценки экзамена

Оценка	Критерии оценивания
Высокий уровень «5» (отлично)	Оценку «**отлично**» заслуживает студент, освоивший знания, умения, компетенции и теоретический материал без пробелов, на высоком

Оценка	Критерии оценивания
	качественном уровне; практические навыки профессионального применения освоенных знаний сформированы. Студент самостоятельно и полностью раскрывает сущность теоретических вопросов, самостоятельно использует возможности программных средств для решения прикладных задач; самостоятельно подтверждает ответ конкретными примерами и заданиями; правильно и обстоятельно отвечает на дополнительные вопросы преподавателя. 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, в основном сформировал практические навыки. Студент допускает незначительные ошибки в заданиях и ответах; самостоятельно использует основные функции программных средств; самостоятельно подтверждает ответ конкретными примерами и заданиями. 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, некоторые практические навыки не сформированы. Студент не может самостоятельно использовать значительную часть функций программных средств, затрудняется подтвердить ответ конкретными примерами и заданиями; слабо отвечает на дополнительные вопросы. Компетенции, закреплённые за дисциплиной, сформированы на уровне – достаточный.
Минимальный уровень «2» (неудовлетворительно)	Оценку «**неудовлетворительно»** заслуживает студент, не освоивший знания, умения, компетенции и теоретический материал, практические навыки не сформированы. Студент не может использовать программные средства при решении прикладных задач; не может подтвердить ответ конкретными примерами и заданиями; не отвечает на дополнительные вопросы преподавателя. Компетенции, закреплённые за дисциплиной, не сформированы.

7. Учебно-методическое и информационное обеспечение дисциплины

7.1 Основная литература

1. Нестеров, С. А. Основы информационной безопасности: учебное пособие / С. А. Нестеров. – 5-е изд., стер. – Санкт-Петербург: Лань, 2019. – 324 с. – ISBN 978-5-8114-4067-2. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/114688

2. Петренко, В. И. Защита персональных данных в информационных системах. Практикум: учебное пособие для вузов / В. И. Петренко, И. В. Мандрица. – 3-е изд., стер. – Санкт-Петербург: Лань, 2021. –108 с. – ISBN 978-5-8114-8370-9. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/175506

3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. – Москва: Издательство Юрайт, 2022. – 312 с. – (Высшее образование). – ISBN 978-5-9916-9043-0. – Текст: электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/491249

7.2 Дополнительная литература

1. Краковский, Ю. М. Методы защиты информации: учебное пособие для вузов / Ю. М. Краковский. – 3-е изд., перераб. – Санкт-Петербург: Лань, 2021. – 236 с. – ISBN 978-5-8114-5632-1. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/156401

2. Казарин, О. В. Надежность и безопасность программного обеспечения: учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. – Москва: Издательство Юрайт, 2022. – 342 с. – (Высшее образование). – ISBN 978-5-534-05142-1. – Текст: электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/493262

3. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. – Москва: Издательство Юрайт, 2022. – 325 с. – (Высшее образование). – ISBN 978-5-534-03600-8. – Текст: электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/498844

4. Васильева, И. Н. Криптографические методы защиты информации: учебник и практикум для вузов / И. Н. Васильева. – Москва: Издательство Юрайт, 2022. – 349 с. – (Высшее образование). – ISBN 978-5-534-02883-6. – Текст: электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/489919

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

1. Бесплатное дистанционное обучение в Национальном Открытом Университете «ИНТУИТ» [Электронный ресурс]. – Режим доступа: http://www.intuit.ru (открытый доступ).
2. Образовательная платформа «Юрайт» [Электронный ресурс]. Режим доступа: https://urait.ru/news/1064 (открытый доступ).
3. Образовательная платформа размещения массовых открытых онлайн-курсов [Электронный ресурс]. Режим доступа: https://stepik.org/catalog (открытый доступ).
4. Агрегатор онлайн-курсов [Электронный ресурс]. – Режим доступа: https://online.edu.ru/public/promo (открытый доступ).
5. Курсы ведущих вузов страны [Электронный ресурс]. – Режим доступа: https://openedu.ru/ (открытый доступ).
6. Массовые открытые онлайн-курсы [Электронный ресурс]. – Режим доступа: https://ru.coursera.org/ (открытый доступ).

9. Перечень программного обеспечения

Таблица 9

Перечень программного обеспечения

Наименование темы учебной дисциплины	Наименование программы	Тип программы	Автор	Год разработки
По всем темам дисциплины	Microsoft Windows 10 и выше	Операционная система	Microsoft	2009
	Microsoft Office 2010/16/19. СУБД MS Access. SQL Server	Пакет офисных программ. Базы данных		2010
	Google Chrome	Браузер		2018
	GoogleDrive, Яндекс Диск	Облачные хранилища		2018
	Moodle	Платформа дистанционного обучения	LMS Moodle	2019

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

Для проведения лекционных и практических занятий по дисциплине «Безопасность и защита информационных систем» необходимы аудитория и компьютерный класс, подключенные к сети Интернет, оснащенные средствами мультимедиа и программными средствами: MS Windows 10; MS Office 2010/2013/2019/365 (Office Online), цифровыми технологиями и инструментами, программой демонстрации NetOp School, браузером Google Chrome.

Лекции проводятся в специализированной аудитории, оборудованной мультимедийным проектором для демонстрации компьютерных презентаций.

Для проведения практических занятий по дисциплине «Безопасность и защита информационных систем» необходим компьютерный класс с установленными на ПК 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
Аудитории для проведения занятий лекционного типа (№ 129, уч. корпус № 12; 101, 102)	Проекционная техника, компьютеры, столы и стулья
Аудитория для проведения практических занятий, групповых и индивидуальных	Персональные компьютеры в количестве 25 штук, столы и стулья

Наименование специальных помещений и помещений для самостоятельной работы (№ учебного корпуса, № аудитории)	Оснащенность специальных помещений и помещений для самостоятельной работы
1	2
консультаций, текущего контроля и промежуточной аттестации (№ 101, 102, 129, уч. корпус №12)	
Центральная научная библиотека имени Н.И. Железнова	Читальные залы библиотеки
Общежитие	Комната для самоподготовки

11. Методические рекомендации студентам по освоению дисциплины

Изучение учебной дисциплины «Безопасность и защита информационных систем» включает освоение материалов лекций, приобретение практических навыков работы с программными средствами, самостоятельную работу.

На лекциях при помощи мультимедиа проектора и презентаций раскрываются основные теоретические вопросы дисциплины, делаются акценты на наиболее сложные положения изучаемого материала.

Лекционный материал следует просматривать и изучать по конспекту/электронной презентации и в LMS Moodle самостоятельно после аудиторных занятий. Для более углубленного изучения материала необходимо использовать рекомендованную литературу и Интернет-ресурсы.

Практические занятия проводятся в компьютерных классах с применением раздаточных материалов. На занятиях необходимо иметь электронный носитель информации – флэш-карту для сохранения результатов своей работы и копирования методических материалов и домашних заданий. Учебные материалы можно сохранять в облачных сервисах: Google Диск, Яндекс.Диск, Облако Mail.Ru, Dropbox.

Посещение лекций и практических занятий – обязательно.

Самостоятельная работа студентов заключается в подготовке вопросов по дисциплине (таблица 5).

Консультирование по выполнению заданий проводится в компьютерных классах во время консультаций по графику (см. на стендах кафедры), а также через электронную информационно-образовательную среду Университета: электронный обмен сообщениями на портале Университета, электронную корпоративную почту, мессенджеры, LMS Moodle.

Необходимо соблюдать сроки выполнения всех заданий.

Полученные оценки за выполненные задания являются основой для промежуточной аттестации.

Виды и формы отработки пропущенных занятий

Студент, обязан отработать:

– пропущенные лекции в форме конспекта лекции, ответов на вопросы теста на платформе Moodle, устного опроса;

– пропущенные практические занятия – в форме выполнения заданий, посещения дополнительных занятий, освоения материалов в Moodle.

12. Методические рекомендации преподавателям по организации обучения по дисциплине

Учебный процесс по курсу «Безопасность и защита информационных систем» включает следующие организационные формы: лекции, практические занятия и консультации, а также систему контроля знаний, самостоятельную работу студентов.

Методика чтения лекций зависит от цели и задач изучения предмета/раздела, а также уровня общей подготовки обучающихся, форма ее проведения – от характера темы и содержания материала. Высокая эффективность деятельности преподавателя во время чтения лекции достигается за счет глубокого освоения предметной области, педагогического мастерства, высокой речевой культуры и ораторского искусства, когда учитывается психология аудитории, закономерности восприятия, внимания, мышления, эмоциональные процессы учащихся, обратная связь и принципы дидактики.

При подготовке материала лекции преподавателю необходимо:

– учитывать требования государственного образовательного стандарта, учебного плана и рабочей программы;

– применять принципы дидактики (наглядность, от теории к практике, доступность, структуризация и систематизация и т.д.);

– уметь создавать интерактивные презентации;

– уметь использовать технические (проектор) и программные средства (например, программу подготовки презентаций MS PowerPoint, программу управления компьютерным классом NetOp School), LMS Moodle для размещения учебных курсов с определением цифровых следов, фиксации учебных действий и др.

Для проведения практических занятий преподавателю следует разрабатывать задания различной степени сложности, инструкции (методические указания) по выполнению каждого задания, раздаточный материал в электронном виде.

По курсу «Безопасность и защита информационных систем» должны быть организованы:

– «очные» консультации в компьютерном классе, проводимые преподавателем согласно графику (размещается на стендах кафедры);

– коммуникация и групповая работа в электронной информационно-образовательной среде Университета через личный кабинет (портал) и LMS Moodle, мессенджеры, корпоративную электронную почту, социальные сети.

Преподаватель должен использовать различные методы обучения:

– объяснительно-иллюстративный (лекция, объяснение, работа с учебником, демонстрация презентаций);

– репродуктивный (воспроизведение действий по применению знаний на практике, деятельность по алгоритму, программирование);

– частично-поисковый (поиск решения познавательных задач под руководством преподавателя);

– исследовательский метод, в котором после анализа материала, постановки проблем и задач и краткого устного или письменного инструктажа обучаемые самостоятельно изучают литературу, источники, ведут наблюдения и измерения и выполняют другие действия поискового характера.

– активные методы: групповое обсуждение, интерактивная лекция и др.

Программу разработали:

Лемешко Т.Б., ст. преподаватель _____

Худякова Е.В., д.э.н., профессор _____

РЕЦЕНЗИЯ

на рабочую программу модульной дисциплины
Б1.В.01.03 «Безопасность и защита информационных систем»
ОПОП ВО по направлению 44.03.04 «Профессиональное обучение» (по отраслям),
направленность «Информационные технологии в образовании»
(квалификация выпускника – бакалавр)

Ивашовой Ольгой Николаевной, старшим преподавателем кафедры систем автоматизированного проектирования и инженерных расчетов ФГБОУ ВО РГАУ-МСХА имени К.А. Тимирязева, кандидатом сельскохозяйственных наук (далее по тексту рецензент) проведено рецензирование рабочей программы дисциплины «Безопасность и защита информационных систем» ОПОП ВО по направлению 44.03.04 «Профессиональное обучение» (по отраслям), направленность «Информационные технологии в образовании» (бакалавриат), разработанной в ФГБОУ ВО «Российский государственный аграрный университет – МСХА имени К.А. Тимирязева» на кафедре прикладной информатики (разработчики: Лемешко Т.Б., ст. преподаватель; Худякова Е.В., д.э.н., профессор,).

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

1. Предъявленная рабочая программа дисциплины «Безопасность и защита информационных систем» (далее по тексту Программа) *соответствует* требованиям ФГОС ВО по направлению 44.03.04 «Профессиональное обучение» (по отраслям). 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 части, формируемой участниками образовательных отношений учебного цикла – Б1.В.

3. Представленные в Программе ***цели*** дисциплины *соответствуют* требованиям ФГОС ВО направления 44.03.04 «Профессиональное обучение» (по отраслям).

4. В соответствии с Программой за дисциплиной «Безопасность и защита информационных систем» закреплена профессиональная ***компетенция (индикаторы) ПКос-2 (ПКос-2.1; ПКос-2.2; ПКос-2.3).*** Дисциплина «Безопасность и защита информационных систем» и представленная Программа *способна реализовать* ее 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 «Безопасность и защита информационных систем» составляет 4 зачётные единицы (144 часа, в том числе 4 часа практической подготовки).

6. Информация о взаимосвязи изучаемых дисциплин и вопросам исключения дублирования в содержании дисциплин *соответствует* действительности. Дисциплина «Безопасность и защита информационных систем» взаимосвязана с другими дисциплинами ОПОП ВО и Учебного плана по направлению 44.03.04 «Профессиональное обучение» (по отраслям).

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

8. Программа дисциплины «Безопасность и защита информационных систем» 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 44.03.04 «Профессиональное обучение» (по отраслям).

10. Представленные и описанные в Программе формы *текущей* оценки знаний (защита практических работ, групповое обсуждение) *соответствуют* специфике дисциплины и требованиям к выпускникам. Форма промежуточного контроля знаний студентов, предусмотренная Программой, осуществляется в форме экзамена в 7 семестре, что *соответствует* статусу дисциплины, как дисциплины, включенной в часть, формируемую участниками образовательных отношений учебного цикла – Б1.В. ФГОС ВО направления 44.03.04 «Профессиональное обучение» (по отраслям).

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

12. Учебно-методическое обеспечение дисциплины представлено: основной литературой – 3 источника, дополнительной литературой – 4 наименования, Интернет-ресурсы – 6 источников и *соответствует* требованиям ФГОС ВО направления 44.03.04 «Профессиональное обучение» (по отраслям).

13. Материально-техническое обеспечение дисциплины соответствует специфике дисциплины «Безопасность и защита информационных систем» 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 «Безопасность и защита информационных систем».

ОБЩИЕ ВЫВОДЫ

На основании проведенного рецензирования можно сделать заключение, что характер, структура и содержание рабочей программы дисциплины «Безопасность и защита информационных систем» ОПОП ВО по направлению 44.03.04 «Профессиональное обучение» (по отраслям), направленность «Информационные технологии в образовании» (квалификация выпускника – бакалавр), разработанная Лемешко Т.Б., ст. преподавателем и Худяковой Е.В., д.э.н., профессором кафедры прикладной информатики, соответствует требованиям ФГОС ВО, современным требованиям экономики, рынка труда и позволит при её реализации успешно обеспечить формирование заявленных компетенций.

Рецензент: Ивашова О.Н., старший преподаватель кафедры систем автоматизированного проектирования и инженерных расчетов ФГБОУ ВО РГАУ-МСХА имени К.А. Тимирязева, кандидат сельскохозяйственных наук

(подпись)

«26» августа 2021 г.