

Составитель(и):

Титовская Н.В., канд. техн. наук, доцент
(ФИО, ученая степень, ученое звание)

«20» марта 2023г.

Программа разработана в соответствии с ФГОС СПО по специальности 09.02.07 «Информационные системы и программирование» (№1547 от 9.12.2016 г.) и примерной основной образовательной программы (№09.02.07-170511 от 11.05.2017 г.), профессионального стандарта «Специалист по информационным системам» (№896н от 18.11.2014 г.)

Программа обсуждена на заседании кафедры
«Информационные технологии и математическое обеспечение информационных систем»

протокол № 7 «20» марта 2023г.

Заведующий кафедрой ИТ и МОИС

Бронов С.А., д.т.н., доцент «20» марта 2023г.

* - В качестве рецензентов могут выступать работодатели, вузы по профилю, НИИ

Лист согласования рабочей программы

Программа принята методической комиссией института

Экономики и управления АПК _____ протокол № 7 «21» марта 2023г.

Председатель методической комиссии

Рожкова А.В., ст. преподаватель.

_____ «21» марта 2023г.

(ФИО, ученая степень, ученое звание)

Заведующий выпускающей кафедры по специальности

Бронов С.А., д.т.н., доцент

_____ «21» марта 2023г.

(ФИО, ученая степень, ученое звание)

Оглавление

АННОТАЦИЯ	5
1. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	6
2. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	6
3. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЕ ДАННЫЕ ДИСЦИПЛИНЫ	8
4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ	9
4.1. ТРУДОЁМКОСТЬ МОДУЛЕЙ И МОДУЛЬНЫХ ЕДИНИЦ ДИСЦИПЛИНЫ	9
4.2. СОДЕРЖАНИЕ МОДУЛЕЙ ДИСЦИПЛИНЫ	9
4.3. ЛЕКЦИОННЫЕ/СЕМИНАРСКИЕ ЗАНЯТИЯ	10
4.4. ЛАБОРАТОРНЫЕ/ПРАКТИЧЕСКИЕ ЗАНЯТИЯ	12
4.5. САМОСТОЯТЕЛЬНОЕ ИЗУЧЕНИЕ РАЗДЕЛОВ ДИСЦИПЛИНЫ И ВИДЫ САМОПОДГОТОВКИ К ТЕКУЩЕМУ КОНТРОЛЮ ЗНАНИЙ	13
4.5.1. <i>Перечень вопросов для самостоятельного изучения и видов самоподготовки к текущему контролю знаний</i>	13
4.5.2. <i>Курсовые проекты (работы)/ контрольные работы/ расчетно-графические работы</i>	13
5. ВЗАИМОСВЯЗЬ ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ	14
6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ	14
6.1. КАРТА ОБЕСПЕЧЕННОСТИ ЛИТЕРАТУРОЙ	14
6.2. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ» (ДАЛЕЕ – СЕТЬ «ИНТЕРНЕТ»)	14
6.3. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ	15
7. КРИТЕРИИ ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И ЗАЯВЛЕННЫХ КОМПЕТЕНЦИЙ	17
8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ	17
9. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ	18
9.1. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ДИСЦИПЛИНЕ ДЛЯ ОБУЧАЮЩИХСЯ.....	18
9.2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ДИСЦИПЛИНЕ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ	19
ПРОТОКОЛ ИЗМЕНЕНИЙ РПД	21

Аннотация

Дисциплина «Информационная безопасность» является частью общепрофессионального цикла дисциплин подготовки студентов по специальности 09.02.07 «Информационные системы и программирование». Дисциплина реализуется в институте Экономики и управления АПК кафедрой Информационных технологий и математического обеспечения информационных систем.

Дисциплина нацелена на формирование общих компетенций

- ~ ОК 01. - *Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам;*
- ~ ОК 02. - *Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;*
- ~ ОК 09. - *Пользоваться профессиональной документацией на государственном и иностранном языках;*
профессиональных компетенций
- ~ ПК 5.3. - *Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием;*
- ~ ПК 6.4. - *Оценивать качество и надежность функционирования информационной системы в соответствии с критериями технического задания;*
- ~ ПК 7.5. - *Проводить аудит систем безопасности баз данных и серверов с использованием регламентов по защите информации;*

выпускника.

Содержание дисциплины охватывает круг вопросов, связанных с принципами информационной безопасности, основным положениям теории информационной безопасности информационных систем, методам защиты информации

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, практические занятия, самостоятельная работа студентов.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса и промежуточный контроль в форме зачета с оценкой.

Общая трудоемкость освоения дисциплины составляет 60 часов. Программой дисциплины предусмотрены лекционные (26 часов), практические (30 часов) занятия и самостоятельная (4 часа) работа.

Используемые сокращения

ФГОС СПО - Федеральный государственный образовательный стандарт среднего профессионального образования

ОПОП - основная профессиональная образовательная программа

ТО – теоретическое обучение (лекции, семинары)

ЛПЗ – лабораторные и практические занятия

СРС – самостоятельная работа студентов

1. Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность» включена в ОПОП, в цикл общепрофессиональных дисциплин.

Реализация в дисциплине «Информационная безопасность» требований ФГОС СПО, ОПОП СПО и Учебного плана по специальности 09.02.07 «Информационные системы и программирование» должна формировать следующие компетенции:

- ~ ОК 01. - *Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам;*
- ~ ОК 02. - *Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;*
- ~ ОК 09. - *Пользоваться профессиональной документацией на государственном и иностранном языках;*
профессиональных компетенций
- ~ ПК 5.3. - *Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием;*
- ~ ПК 6.4. - *Оценивать качество и надежность функционирования информационной системы в соответствии с критериями технического задания;*
- ~ ПК 7.5. - *Проводить аудит систем безопасности баз данных и серверов с использованием регламентов по защите информации;*

Предшествующими курсами, на которых непосредственно базируется дисциплина «Информационная безопасность» являются «Информационные технологии», «Архитектура аппаратных средств», «Операционные системы и среды».

Дисциплина «Информационная безопасность» является основополагающей для изучения следующих дисциплин: «Проектирование и дизайн информационных систем», «Тестирование информационных систем», «Устройство и функционирование информационной системы».

Контроль знаний студентов проводится в форме текущей и промежуточной аттестации.

2. Цели и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Целью дисциплины «Информационная безопасность» обучить студентов принципам информационной безопасности, основным положениям теории информационной безопасности информационных систем, методам защиты информации.

Задачи изучения дисциплины: после изучения дисциплины студент должен обладать специальной подготовкой в предметной области, знать принципы организации информационной безопасности и методы защиты информации, знать международные стандарты информационного обмена.

Таблица 1

Перечень планируемых результатов обучения дисциплине

Код компетенции	Содержание компетенции	Перечень планируемых результатов обучения по дисциплине
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	Умения: распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать

		составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)
		Знания: актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;	<p>Умения: определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска. Применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение;</p> <p>Использовать информационные технологии в профессиональной деятельности.</p> <p>Знания: номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации. Современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности</p> <p>основные виды информационных технологий, используемых в профессиональной деятельности.</p>
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках;	<p>Умения: Пользоваться профессиональной документацией на государственном и иностранном языках:</p> <p>заполнять и оформлять профессиональную документацию на государственном и иностранном языках.</p> <p>понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы;</p> <p>участвовать в диалогах на знакомые общие и профессиональные темы;</p> <p>строить простые высказывания о себе и о своей профессиональной деятельности;</p> <p>кратко обосновывать и объяснить свои действия (текущие и планируемые);</p> <p>писать простые связные сообщения на знакомые или интересующие профессиональные темы</p> <p>Знания: правила построения простых и сложных предложений на профессиональные темы;</p> <p>основные общепотребительные глаголы (бытовая и профессиональная лексика);</p> <p>лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения;</p> <p>знать приемы и способы заполнения и оформления профессиональной документации на государственном и иностранном языках.</p> <p>правила чтения текстов профессиональной направленности на государственном и иностранном языках</p>
ПК 5.3	Разрабатывать подсистемы	Практический опыт: Управлять процессом разработки приложений с использованием инструментальных средств. Модифицировать

	безопасности информационной системы в соответствии с техническим заданием.	отдельные модули информационной системы. Умения: Создавать и управлять проектом по раз работке приложения и формулировать его задачи. Знания: Национальной и международной системы стандартизации и сертификации и систему обеспечения качества продукции. Методы контроля качества объектно - ориентированного программирования. Объектно-ориентированное программирование. Спецификации языка программирования, принципы создания графического пользовательского интерфейса (GUI), файлового ввода-вывода, создания сетевого сервера и сетевого клиента
ПК 6.4	Оценивать качество и надежность функционирования информационной системы в соответствии с критериями технического задания	Практический опыт: Выполнять оценку качества и надежности функционирования информационной системы на соответствие техническим требованиям. Умения: Применять документацию систем качества. Применять основные правила и документы системы сертификации РФ. Знания: Характеристики и атрибуты качества ИС. Методы обеспечения и контроля качества ИС в соответствии со стандартами. Политику безопасности в современных информационных системах.
ПК 7.5	Проводить аудит систем безопасности баз данных и серверов с использованием регламентов по защите информации	Практический опыт: Разрабатывать политику безопасности SQL сервера, базы данных и отдельных объектов базы данных. Умения: Разрабатывать политику безопасности SQL сервера, базы данных и отдельных объектов базы данных. Владеть технологиями проведения сертификации программного средства. Знания: Технология установки и настройки сервера баз данных. Требования к безопасности сервера базы данных. Государственные стандарты и требования к обслуживанию баз данных.

3. Организационно-методические данные дисциплины

Общая трудоёмкость дисциплины составляет 60 часов, их распределение по видам работ и по семестрам представлено в таблице 2.

Таблица 2

Распределение трудоёмкости дисциплины по видам работ по семестрам

Вид учебной работы	Трудоёмкость		
	час.	по семестрам	
		№ 5	№ 6
Общая трудоёмкость дисциплины по учебному плану	60	26	34
Контактная работа	56	24	32
в том числе:			
Теоретическое обучение (ТО) (лекции, семинары)	26	12	14
Лабораторные и практические занятия (ЛПЗ)	30	12	18
Самостоятельная работа (СРС)	4	2	2
в том числе:			
самоподготовка к текущему контролю знаний	4	2	2
Вид контроля:			Зачет с оценкой

4. Структура и содержание дисциплины
4.1. Трудоёмкость модулей и модульных единиц дисциплины

Таблица 3

Трудоёмкость модулей и модульных единиц дисциплины

Наименование модулей и модульных единиц дисциплины	Всего часов на модуль	Контактная работа		Внеаудиторная работа (СРС)
		ТО	ЛЗ/ПЗ	
Календарный модуль 1	26	12	12	2
Модуль 1 Общие сведения об информационной безопасности	26	12	12	2
Модульная единица 1. Понятие информационной безопасности. Понятие угрозы. Международные стандарты информационного обмена.	6	4	2	
Модульная единица 2. Информационная безопасность в условиях функционирования в России глобальных сетей.	4	2	2	
Модульная единица 3. Виды противников или "нарушителей". Понятия о видах вирусов.	4	2	2	
Модульная единица 4. Виды возможных нарушений информационной системы. Виды защиты.	6	2	4	
Модульная единица 5. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности.	6	2	2	2
Календарный модуль 2	34	14	18	2
Модуль 2 Способы защиты информации	34	14	18	2
Модульная единица 6. Основные положения теории информационной безопасности. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающих их существование.	12	4	6	2
Модульная единица 7. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии.	8	4	4	
Модульная единица 8. Основные технологии построения защищенных ЭИС.	8	4	4	
Модульная единица 9. Место информационной безопасности экономических систем в национальной безопасности страны.	6	2	4	
ИТОГО	60	26	30	4

4.2. Содержание модулей дисциплины

Модуль 1 Общие сведения об информационной безопасности

Модульная единица 1 Понятие информационной безопасности. Понятие угрозы. Международные стандарты информационного обмена.

Модульная единица 2. Информационные технологии обеспечения конфиденциальности и сохранности данных в условиях функционирования в России глобальных сетей.

Организационные меры обеспечения информационной безопасности. Порядок использования конфиденциальных архивных документов. Политика ИБ. Стандарты ИБ. Модели защиты информации.

Модульная единица 3. Виды противников или "нарушителей". Понятия о видах вирусов. Программно-аппаратные способы борьбы с вирусами и другим вредоносным программным обеспечением

Модульная единица 4. Виды возможных нарушений информационной системы. Виды защиты. Общая классификация информационных угроз. Информационные угрозы безопасности РФ. Доктрина информационной безопасности РФ.

Модульная единица 5. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности. Типы преднамеренных помех и защита от них. Экономика защиты информации. Интеллектуальная собственность и ее защита

Модуль 2 Способы защиты информации

Модульная единица 6. Основные положения теории информационной безопасности. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающих их существование. Специализированное программное обеспечение. Инженерно техническое обеспечение ИБ.

Модульная единица 7. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии. Вредоносное программное обеспечение. Программно аппаратные средстваЗИ. Криптографические методы защиты информации. Типовые удаленные атаки с использованием уязвимостей сетевых протоколов. Классификация удаленных атак.

Модульная единица 8. Основные технологии построения защищенных ЭИС. Виды возможных нарушений информационной системы. Правовое регулирование защиты информации (анализ статей УК, других нормативных актов).

Модульная единица 9. Место информационной безопасности экономических систем в национальной безопасности страны.

4.3. Лекционные/семинарские занятия

Таблица 4

Содержание лекционного курса (семинаров)

№ модуля и модульной единицы дисциплины	№ и тема лекции (семинара)	Вид ¹ контрольного мероприятия	Кол-во часов
Календарный модуль 1		опрос	12
Модуль 1 Общие сведения об информационной безопасности		опрос	12
Модульная единица 1. Понятие информационной безопасности. Понятие угрозы. Международные стандарты информационного обмена.	Лекция № 1 Понятие информационной безопасности. Понятие угрозы. Международные стандарты информационного обмена.	опрос	4
Модульная единица 2. Информационная безопасность в условиях функционирования в России глобальных сетей.	Лекция № 2 Информационная безопасность в условиях функционирования в России глобальных сетей.	опрос	2
Модульная единица 3. Виды противников или "нарушителей". Понятия о видах вирусов.	Лекция № 3 Виды противников или "нарушителей". Понятия о видах вирусов	опрос	2

¹ Вид мероприятия: тестирование, коллоквиум, зачет, экзамен, другое

№ модуля и модульной единицы дисциплины	№ и тема лекции (семинара)	Вид ¹ контрольного мероприятия	Кол-во часов
Модульная единица 4. Виды возможных нарушений информационной системы. Виды защиты.	Лекция № 4 Виды возможных нарушений информационной системы. Виды защиты.	опрос	2
Модульная единица 5. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности.	Лекция № 5 Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности.	опрос	2
Календарный модуль 2		Зачет с оценкой	14
Модуль 2 Способы защиты информации		Зачет с оценкой	14
Модульная единица 6. Основные положения теории информационной безопасности. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающих их существование.	Лекция № 6 Основные положения теории информационной безопасности. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающих их существование	опрос	4
Модульная единица 7. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии.	Лекция № 7 Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии.	опрос	4
Модульная единица 8. Основные технологии построения защищенных ЭИС.	Лекция № 8 Основные технологии построения защищенных ЭИС.	опрос	4
Модульная единица 9. Место информационной безопасности экономических систем в национальной безопасности страны.	Лекция № 9 Место информационной безопасности экономических систем в национальной безопасности страны.	опрос	2
ИТОГО		Зачет с оценкой	26

4.4. Лабораторные/практические занятия

Таблица 5

Содержание занятий и контрольных мероприятий

№ модуля и модульной единицы дисциплины	№ и название лабораторных/практических занятий с указанием контрольных мероприятий	Вид ² контрольного мероприятия	Кол-во часов
Календарный модуль 1		опрос	12
Модуль 1 Общие сведения об информационной безопасности		опрос	12
Модульная единица 1. Понятие информационной безопасности. Понятие угрозы. Международные стандарты информационного обмена.	Занятие № 1 Понятие информационной безопасности. Понятие угрозы. Международные стандарты информационного обмена.	опрос	2
Модульная единица 2. Информационная безопасность в условиях функционирования в России глобальных сетей.	Занятие № 2 Установка и настройка системы. Установка параметров автоматического обновления системы. Установка новых устройств. Управление дисковыми ресурсами Информационная безопасность в условиях функционирования в России глобальных сетей.	опрос	2
Модульная единица 3. Виды противников или "нарушителей". Понятия о видах вирусов.	Занятие № 3 Виды противников или "нарушителей". Понятия о видах вирусов.	опрос	2
Модульная единица 4. Виды возможных нарушений информационной системы. Виды защиты.	Занятие № 4 Виды возможных нарушений информационной системы. Виды защиты.	опрос	4
Модульная единица 5. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности.	Занятие № 5 Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности	опрос	2
Календарный модуль 2		Зачет с оценкой	18
Модуль 2 Способы защиты информации		Зачет с оценкой	18
Модульная единица 6. Основные положения теории информационной безопасности. Модели безопасности и их применение. Таксономия нарушений информационной	Занятие № 6 Основные положения теории информационной безопасности. Модели безопасности и их применение. Таксономия нарушений информационной безопасности	опрос	6

² Вид мероприятия: защита, тестирование, коллоквиум, другое

№ модуля и модульной единицы дисциплины	№ и название лабораторных/практических занятий с указанием контрольных мероприятий	Вид ² контрольного мероприятия	Кол-во часов
безопасности вычислительной системы и причины, обуславливающих их существование.	вычислительной системы и причины, обуславливающих их существование		
Модульная единица 7. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии.	Занятие № 7 Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии.	опрос	4
Модульная единица 8. Основные технологии построения защищенных ЭИС.	Занятие № 8 Основные технологии построения защищенных ЭИС.	опрос	4
Модульная единица 9. Место информационной безопасности экономических систем в национальной безопасности страны.	Занятие № 9 Место информационной безопасности экономических систем в национальной безопасности страны.	опрос	4
ИТОГО		Зачет с оценкой	30

4.5. Самостоятельное изучение разделов дисциплины и виды самоподготовки к текущему контролю знаний

4.5.1. Перечень вопросов для самостоятельного изучения и видов самоподготовки к текущему контролю знаний

Таблица 6

Перечень вопросов для самостоятельного изучения и видов самоподготовки к текущему контролю знаний

№п/п	№ модуля и модульной единицы	Перечень рассматриваемых вопросов для самостоятельного изучения и видов самоподготовки к текущему контролю знаний	Кол-во часов
1	Модульная единица 5	Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности	2
2	Модульная единица 6	Основные положения теории информационной безопасности. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающих их существование	2
	Всего		4

4.5.2. Курсовые проекты (работы)/ контрольные работы/ расчетно-графические работы

Таблица 7

№ п/п	Темы курсовых проектов (работ)/ контрольные работы/ расчетно- графические работы	Рекомендуемая литература (номер источника в соответствии с прилагаемым списком)
Учебным планом не предусмотрено		

5. Взаимосвязь видов учебных занятий

Таблица 8

Взаимосвязь компетенций с учебным материалом и контролем знаний студентов

Компетенции	Лекции	ЛЗ/ПЗ/С	СРС	Другие виды	Вид контроля
ОК 01. - Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	1 - 9	1 - 9	1,2		Зачет с оценкой
ОК 02. - Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	1 - 9	1 - 9	1,2		Зачет с оценкой
ОК 09. - Использовать информационные технологии в профессиональной деятельности	1 - 9	1 - 9	1,2		Зачет с оценкой
ПК 5.3 Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием.	1 - 9	1 - 9	1,2		Зачет с оценкой
ПК 6.4. - Оценивать качество и надежность функционирования информационной системы в соответствии с критериями технического задания	1 - 9	1 - 9	1,2		Зачет с оценкой
ПК 7.5. - Проводить аудит систем безопасности баз данных и серверов с использованием регламентов по защите информации	1 - 9	1 - 9	1,2		Зачет с оценкой

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Карта обеспеченности литературой

Карта обеспеченности литературой приведена в таблице 9.

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»)

Интернет-ресурсы

1. Национальный Открытый Университет «ИНТУИТ» <https://intuit.ru/>
 2. Портал CIT Forum <http://citforum.ru/>
 3. Информационно-аналитическая система «Статистика» <http://www.ias-stat.ru/>
- Электронные библиотечные системы*
4. Каталог библиотеки Красноярского ГАУ -- www.kgau.ru/new/biblioteka/ ;
 5. Центральная научная сельскохозяйственная библиотека - www.cnshb.ru/ ;
 6. Научная электронная библиотека "eLibrary.ru" – www.elibrary.ru ;
 7. Электронная библиотечная система «Лань» - <https://e.lanbook.com/>
 8. Электронно-библиотечная система «Юрайт» - <https://urait.ru/>
 9. Электронно-библиотечная система «AgriLib» - <http://ebs.rgazu.ru/>
 10. Электронная библиотека Сибирского Федерального университета - <https://bik.sfu-kras.ru/>
 11. Национальная электронная библиотека - <https://rusneb.ru/>

12. Электронная библиотечная система «ИРБИС64+» - http://5.159.97.194:8080/cgi-bin/irbis64r_plus/cgiirbis_64_ft.exe?C21COM=F&I21DBN=IBIS_FULLTEXT&P21DBN=IBIS&Z21ID=&S21CNR=5
13. Электронный каталог Государственной универсальной научной библиотеки Красноярского края - <https://www.kraslib.ru/>
Информационно-справочные системы
14. Справочно-правовая система КонсультантПлюс
<http://www.consultant.ru/cons/cgi/online.cgi?req=home;rnd=0.8636296761039928>
15. Информационно-правовой портал «Гарант». <http://www.garant.ru/>
Профессиональные базы данных
16. Коллективный блог по информационным технологиям, бизнесу и интернету.
<https://habr.com/ru/>
17. Форум программистов и сисадминов Киберфорум <https://www.cyberforum.ru/>
Сторонние электронно-образовательные ресурсы
18. Министерство науки и высшего образования РФ
19. Российское образование
20. Единое окно доступа к образовательным ресурсам
21. Единая коллекция цифровых образовательных ресурсов
22. Федеральный центр информационно-образовательных ресурсов
23. Современная цифровая образовательная среда в РФ <http://window.edu.ru/>
24. http://window.edu.ru/catalog/resources?p_rubr=2.2.75.6

6.3. Программное обеспечение

1. Операционная система Windows (академическая лицензия № 44937729 от 15.12.2008).
2. Офисный пакет приложений Microsoft Office (академическая лицензия № 44937729 от 15.12.2008).
3. Программа для создания и просмотра электронных публикаций в формате PDF ‒ Acrobat Professional (образовательная лицензия № CE0806966 от 27.06.2008).
4. Kaspersky Endpoint Security для бизнеса Стандартный Russian Edition. 1000-1499 Node 2 year Educational License (1B08-230201-012433-600-1212 с 01.02.2023 до 09.02.2024).
5. Moodle 3.5.6a (система дистанционного образования) - Открытые технологии договор 969.2 от 17.04.2020.
6. Библиотечная система «Ирбис 64», контракт 37–5–20 от 27.10.2020
7. Python - среда программирования, свободно распространяемое ПО
8. Visual Studio Community – бесплатная среда разработки программного обеспечения на C++
9. PGP Freeware, бесплатно распространяемое ПО
10. Ad Muncher, бесплатно распространяемое ПО
11. Malwarebytes AdwCleaner, бесплатно распространяемое ПО
12. Ad-Aware, бесплатно распространяемое ПО
13. SUPERAntiSpyware, бесплатно распространяемое ПО
14. Ghostery, бесплатно распространяемое ПО
15. Spyware Terminator, бесплатно распространяемое ПО
16. Spyware Process Detector, бесплатно распространяемое ПО

КАРТА ОБЕСПЕЧЕННОСТИ ЛИТЕРАТУРОЙ

Кафедра Информационных технологий и математического обеспечения информационных систем

Специальность 09.02.07 «Информационные системы и программирование»

Дисциплина **Информационная безопасность**

Вид занятий	Наименование	Авторы	Издательство	Год издания	Вид издания		Место хранения		Необходимое количество экз.	Количество экз. в вузе
					Печ.	Электр.	Библ.	Каф.		
1	2	3	4	6	7	8	9	10	11	12
Основная										
Лекции, практические занятия	Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособие для среднего профессионального образования	О. В. Казарин, И. Б. Шубинский	Москва : Издательство Юрайт	2021		Электр.				URL: https://urait.ru/bcode/475889
Лекции, практические занятия	Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования	А. А. Внуков	Москва : Издательство Юрайт	2021		Электр.				URL: https://urait.ru/bcode/475890
Дополнительная										
Лекции, практические занятия	Организационное и правовое обеспечение информационной безопасности: учебник и практикум для среднего профессионального образования	Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов	Москва : Издательство Юрайт	2021		Электр.				URL: https://urait.ru/bcode/470351

Директор Научной библиотеки _____

7. Критерии оценки знаний, умений, навыков и заявленных компетенций

Текущая аттестация обучающихся производится в форме опроса.

Промежуточный контроль по дисциплине – зачет с оценкой - проходит в форме контрольного итогового тестирования по всем темам курса.

Рейтинг – план дисциплины «Информационная безопасность»

	Модули	Часы	Баллы
1	Модуль № 1	26	30
	Модуль № 2	34	30
	Зачет с оценкой		40
	Итого	60	100

Распределение баллов по модулям

№	Модули	Баллы по видам работ		Итого
		Опрос	Итоговое тестирование (зачет с оценкой)	
1	Модуль № 1	30		30
	Модуль № 2	30		30
	Зачет с оценкой		40	40
	Итого	60	40	100

Задания по всем видам текущей работы и промежуточной аттестации, а также подробные критерии оценивания приведены в ФОС по дисциплине «Информационная безопасность».

Текущие задолженности учащийся отрабатывает, готовя ответы на вопросы по темам задолженности в письменном виде.

Баллы, полученные на итоговом тестировании, суммируются с баллами, полученными в течение семестра на текущей аттестации, и выводится итоговая оценка по следующим критериям:

60 – 73 – минимальное количество баллов – оценка «удовлетворительно».

74 – 86 – среднее количество баллов – оценка «хорошо».

87 – 100 – максимальное количество баллов – оценка «отлично».

8. Материально-техническое обеспечение дисциплины

Для реализации программы учебной дисциплины предусмотрены следующие специальные помещения:

Лаборатория «Программного обеспечения и сопровождения компьютерных систем», оснащенная оборудованием и техническими средствами обучения: рабочее место преподавателя; посадочные места обучающихся (по количеству обучающихся); учебные наглядные пособия (таблицы, плакаты); тематические папки дидактических материалов; комплект учебно-методической документации; комплект учебников (учебных пособий) по количеству обучающихся, компьютеры с лицензионным программным обеспечением; мультимедиа проектор.

Таблица 11

Материально-техническое обеспечение дисциплины

Виды занятий	Аудиторный фонд
Лекции	Занятия лекционного типа проводятся в кабинете Э 3-09 (660130, Красноярский край, г. Красноярск, ул. Елены Стасовой 44 «И»), компьютерный класс Э 2-09 – для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации: рабочие места

	<p>преподавателя и студентов, укомплектованные специализированной мебелью, и техническими средствами обучения, служащими для представления учебной информации большой аудитории.</p> <p>Рабочие места преподавателя и студентов, укомплектованные специализированной мебелью, и техническими средствами обучения, служащими для представления учебной информации большой аудитории. Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, аудиторная доска, информационные и методические материалы, общая локальная компьютерная сеть, Internet, 1 компьютер, комплект мультимедийного оборудования: Проектор NEC V281WG DLP/ 1280x800/ 3000ANSI/ 2800:1/ 2.5кг/ 3D/HDTV, кронштейн Kromax</p>
Практические занятия	<p>Практические занятия проводятся в лаборатории «Программного обеспечения и сопровождения компьютерных систем» - Э 3-06 (660130, Красноярский край, г. Красноярск, ул. Елены Стасовой 44 «И»), имеющей достаточное количество посадочных мест для размещения студентов и оснащенной наборами демонстрационного оборудования и учебно-наглядными пособиями; имеется выход в общую локальную компьютерную сеть Internet, компьютер на базе процессора Celeron в комплектации с монитором Samsung и др. внешними периферийными устройствами, 15 компьютеров на базе процессора Core 2 Duo в комплектации с монитором Samsung и др. внешними периферийными устройствами, комплект мультимедийного оборудования: ноутбук Acer Aspire 5, переносной экран на треноге Medium Professional, переносной проектор Epson EB-X8 2500 со встроенными динамиками.</p>
Самостоятельная работа	<p>Помещение для самостоятельной работы 3-13 - (660130, Красноярский край, г. Красноярск, ул. Елены Стасовой 44 «И») - рабочие места студентов, укомплектованные специализированной мебелью, общая локальная компьютерная сеть Internet, 10 компьютеров на базе процессора Intel Celeron в комплектации с мониторами Samsung, LG, Aser, Viewsonic и др. внешними периферийными устройствами.</p> <p>Помещение для самостоятельной работы 1-06 (ул. Е.Стасовой, 44 «Г») - Информационно-ресурсный центр Научной библиотеки - рабочие места студентов, укомплектованные специализированной мебелью, компьютеры на базе процессора Intel Core i3 в комплектации с монитором Samsung и др. внешними периферийными устройствами, с подключением к сети интернет, мультимедийный комплект: проектор Panasonic, экран, принтер (МФУ) LaserJet M1212, столы, стулья, учебно-методическое аудио и видеоматериалы, учебно-методическая литература</p> <p>Помещение для самостоятельной работы 2-06 - (660130, Красноярский край, г. Красноярск, ул. Елены Стасовой, 44 «Г») - на 51 посадочное место: рабочие места студентов, укомплектованные специализированной мебелью, Гигабитный интернет, Wi-fi, 2 компьютера на базе процессора Intel Core i3 в комплектации с монитором Samsung и др. внешними периферийными устройствами (инв.№ 1101040757-1101040759, 1101040761, 1101040762, 1101040767, 1101040768, 1101040775), мультимедийный проектор Acer X 1260P, экран, телевизор Samsung</p>

9. Методические рекомендации для обучающихся по освоению дисциплины

9.1. Методические указания по дисциплине для обучающихся

Успешное изучение курса требует от студентов посещения лекций, активной работы на практических занятиях, выполнения всех учебных заданий преподавателя, ознакомления с базовыми учебниками, основной и дополнительной литературой. Запись лекции – одна из форм активной самостоятельной работы студентов, требующая навыков и умения кратко, схематично, последовательно и логично фиксировать основные положения, выводы,

обобщения, формулировки. Для конспектирования лекций рекомендуется создать собственную удобную систему сокращений, аббревиатур и символов.

Лекции нацелены на освещение наиболее трудных вопросов, а также призваны способствовать формированию навыков работы с литературой.

При изучении дисциплины для улучшения качества учебного процесса преподаватели используют демонстрацию основных принципов работы на компьютере с использованием мультимедийных средств и презентаций, сопровождая информационный материал комментариями, что позволяет внести позитивное разнообразие в учебный процесс и способствует повышению знаний студентов.

Основной формой проведения практических занятий является выполнение конкретных заданий в виде лабораторных работ на компьютерах.

Лабораторно-практическое занятие - это форма организации учебного процесса, предполагающая выполнение студентами по заданию и под руководством преподавателя одной или работ. И если на лекции основное внимание студентов сосредотачивается на разъяснении теории конкретной учебной дисциплины, то практические занятия служат для обучения методам ее применения. Главной целью практических занятий является усвоение метода использования теории, приобретение профессиональных умений, а также практических умений, необходимых для изучения последующих дисциплин.

Кроме того, для закрепления навыков работы с компьютерами, студенты занимаются самостоятельно с имеющимися программами и изучают теоретические вопросы.

Полученные навыки и знания помогут студентам в условиях развития информационных технологий быстро и профессионально ориентироваться в новых подходах, которые возникают в связи с увеличением возможностей вычислительной техники. Возрастающие возможности вычислительной техники порождают новые концепции и подходы в системе учёта, хранения, обработки, преобразования информации, её безопасности. В свою очередь новые концепции и подходы стимулируют создание новых информационных систем, которые должны быстро внедряться в практическую и хозяйственную деятельность государственных и частных структур. Поэтому курс построен так, что помимо конкретных базовых знаний, студенту предлагаются некоторые схемы и методики, которые помогут развить самостоятельные навыки в изучении нового материала. Это позволяет студенту повысить профессиональный кругозор, а преподавателю моделировать реальные ситуации, которые могут возникнуть при переходе студента от учёбы к практической деятельности.

В соответствии с учебными планами, формами контроля знаний студентов по дисциплине «Информационная безопасность» являются выполнение лабораторных работ, экзамен.

Обязательными видами промежуточной аттестации, без наличия которых студенты не допускаются до экзамена, является выполнение всех лабораторно-практических заданий.

Студент может быть освобожден преподавателем от промежуточной аттестации при активной работе во время лекций, лабораторных и практических занятий, при участии в студенческих научных конференциях по тематике предмета.

9.2. Методические указания по дисциплине для инвалидов и лиц с ограниченными возможностями здоровья

В целях освоения учебной программы дисциплины инвалидами и лицами с ограниченными возможностями здоровья обеспечивается:

1. Для инвалидов и лиц с ограниченными возможностями здоровья по зрению:
 - 1.1. размещение в доступных для обучающихся местах и в адаптированной форме справочной информации о расписании учебных занятий;
 - 1.2. присутствие ассистента, оказывающего обучающемуся необходимую помощь;
 - 1.3. выпуск альтернативных форматов методических материалов (крупный шрифт или аудиофайлы);

2. Для инвалидов и лиц с ограниченными возможностями здоровья послуху:
- 2.1. надлежащими звуковыми средствами воспроизведение информации;
3. Для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата:

3.1. возможность беспрепятственного доступа обучающихся в учебные помещения, туалетные комнаты и другие помещения института, а также пребывание в указанных помещениях.

Образование обучающихся с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах или в отдельных организациях.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в одной из форм, адаптированных к ограничениям их здоровья и восприятия информации.

Категории студентов	Формы
С нарушение слуха	<ul style="list-style-type: none"> ● в печатной форме; ● в форме электронного документа;
С нарушением зрения	<ul style="list-style-type: none"> ● в печатной форме увеличенных шрифтом; ● в форме электронного документа; ● в форме аудиофайла;
С нарушением опорно-двигательного аппарата	<ul style="list-style-type: none"> ● в печатной форме; ● в форме электронного документа; ● в форме аудиофайла.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная работа. Под индивидуальной работой подразумевается две формы взаимодействия с преподавателем: индивидуальная учебная работа (консультации), т.е. дополнительное разъяснение учебного материала и углубленное изучение материала с теми обучающимися, которые в этом заинтересованы, и индивидуальная воспитательная работа. Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или обучающимся с ограниченными возможностями здоровья.

ПРОТОКОЛ ИЗМЕНЕНИЙ РЦД

Дата	Раздел	Изменения	Комментарии

Программу разработал:

Титовская Н.В., канд. техн. наук, доцент

(подпись)

РЕЦЕНЗИЯ

на рабочую программу учебной дисциплины «Информационная безопасность»
для подготовки специалистов среднего звена по программе ФГОС СПО, специальность
09.02.07 «Информационные системы и программирование»
ФГБОУ ВО Красноярский государственный аграрный университет

Представленная на рецензию программа оформлена с соблюдением всех требований, предъявляемых к оформлению рабочих программ по стандартам ФГОС СПО.

Учебная дисциплина «Информационная безопасность» в учебном плане включена в вариативную часть общепрофессионального цикла дисциплин подготовки студентов по специальности 09.02.07 «Информационные системы и программирование».

Предложенная программа проведения практических и теоретических занятий позволяет достичь заявленной цели - сформировать необходимые компетенции у студентов, позволяет студентам получить необходимые знания в области информационной безопасности, а также подготовить их к изучению дисциплин, опирающихся на дисциплину «Информационная безопасность».

Предложенный в программе набор контрольных процедур позволяет установить степень освоения студентом материала дисциплины и качество сформированных навыков.

Считаю, что представленная на рецензию рабочая программа полностью удовлетворяет требованиям ФГОС СПО и может быть использована для подготовки специалистов среднего звена по специальности 09.02.07 «Информационные системы и программирование»

Рецензент:

доцент кафедры Вычислительной техники
ФГАОУ ВО Сибирский федеральный университет,
Институт космических и информационных
технологий, канд. техн. наук



Постников
Александр
Иванович