МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ДЕПАРТАМЕНТ НАУЧНО-ТЕХНОЛОГИЧЕСКОЙ ПОЛИТИКИ И ОБРАЗОВАНИЯ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«КРАСНОЯРСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

Институт экономики и управления АПК
Кафедра Информационные технологии и математическое обеспечение информационных систем

СОГЛАСОВАНО:
Директор ИЭиУ АПК
Шапорова З.Е.
« 28 » марта 2024 г.

УТВЕРЖДАЮ:
Ректор
Пыжикова Н.И.
« 29 » марта 2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Технологии защиты информации в компьютерных сетях

ФГОС ВО

Направление подготовки **09.04.03** «Прикладная информатика»

Направленность (профиль) «Цифровые технологии в АПК»

Курс 2

Семестр (*ы*) 3

Форма обучения очная

Квалификация выпускника магистр

ДОКУМЕНТ ПОДПИСАН
УСИЛЕННОЙ КВАЛИФИЦИРОВАННОЙ
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
ВЫДАННОЙ: ФГБОУ ВО КРАСНОЯРСКИ ГАУ
ВЛАДЕЛЕЦ: РЕКТОР ПЫЖИКОВА Н.И.
ДЕЙСТВИТЕЛЕН: 27.03.2024 – 20.06.2025

Красноярск, 2024

Составители: Титовская Наталья Викторовна, к.т.н., доцент

« 5 » 03 2024 г.

Программа разработана в соответствии с ФГОС ВО по направлению подготовки 09.04.03 Прикладная информатика профессионального стандарта № 922 от 19.09.2017 г.

Программа обсуждена на заседании кафедры Информационных технологий и и математического обеспечения информационных систем (ИТМОИС)
протокол № 7 «5» 03 2024 г.

Зав. кафедрой ИТМОИС Калитина В.В. канд.пед.наук

«5» 03 2024 г.

* - 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 «18» марта 2024 г.

Председатель методической комиссии Института экономики и управления АПК ст. преподаватель Рожкова А.В. «18» марта 2024 г.

Заведующий выпускающей кафедрой по направлению подготовки
09.04.03 – «Прикладная информатика»

Калитина В.В. канд.пед.наук

«18» 03 2024 г.

Оглавление

Аннотация

Дисциплина Технологии защиты информации в компьютерных сетях относится к части, формируемой участниками образовательных отношений Блока 1. Дисциплины (модули) учебного плана подготовки магистрантов по направлению 09.04.03 «Прикладная информатика». Дисциплина реализуется в институте Экономики и управления АПК кафедрой Информационных технологий и математического обеспечения информационных систем.

Дисциплина нацелена на формирование общепрофессиональных компетенций выпускника:

УК-2 Способен управлять проектом на всех этапах его жизненного цикла

ПК-5 Способность использовать передовые методы оценки качества, надежности и технологии защиты информации в компьютерных сетях в процессе эксплуатации прикладных ИС

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, лабораторные работы, самостоятельная работа магистранта.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса, выполнения заданий лабораторных работ и промежуточная аттестация в форме зачета с оценкой.

Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы, 144 часа, лекций 28 часов, лабораторных работ - 28 часов и 88 часов самостоятельной работы.

Используемые сокращения

ФГОС ВО – Федеральный государственный образовательный стандарт высшего образования

ООП – основная образовательная программа

Л – лекции

ЛЗ – лабораторные занятия

ПЗ- практические занятия

СРС – самостоятельная работа студентов

1. Место дисциплины в структуре образовательной программы

Дисциплина «Технологии защиты информации в компьютерных сетях» относится к части, формируемой участниками образовательных отношений Блока 1. Дисциплины (модули) учебного плана подготовки магистрантов по направлению 09.04.03 «Прикладная информатика». Дисциплина читается на 2 курсе в 3 семестре.

Предшествующими курсами, на которых непосредственно базируется дисциплина «Технологии защиты информации в компьютерных сетях» являются «Методология и технология проектирования информационных систем», «Управление ИТ-проектами» «Современные технологии разработки программного обеспечения».

Дисциплина « Технологии защиты информации в компьютерных сетях» является основополагающим для изучения следующих дисциплин: « Микропроцессорные системы в агропромышленном комплексе», « Технологии обработки больших данных»

Контроль знаний магистрантов 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

Цель дисциплины: обучить магистрантов принципам технологий защиты информации в компьютерных сетях, основным положениям теории технологии защиты информации в компьютерных сетях, методам защиты информации.

Задачи изучения дисциплины: после изучения дисциплины магистрант должен обладать специальной подготовкой в предметной области, знать принципы организации технологии защиты информации в компьютерных сетях, знать международные стандарты информационного обмена.

Таблица 1

Перечень планируемых результатов обучения по дисциплине

Код компетенции	Содержание компетенции	Индикаторы достижения компетенции (по реализуемой дисциплине)	Перечень планируемых результатов обучения по дисциплине
УК-2	Способен управлять проектом на всех этапах его жизненного цикла	ИУК-2.1. Разрабатывает концепцию проекта в рамках обозначенной проблемы: формулирует цель, задачи, обосновывает актуальность, значимость, ожидаемые результаты и возможные сферы их применения ИУК-2.2. Способен разрабатывать и анализировать альтернативные варианты проектов для достижения намеченных результатов; разрабатывать проекты, определять целевые этапы и основные направления работ. ИУК-2.3. Предлагает процедуры и механизмы оценки качества проекта, инфраструктурные условия для внедрения результатов про-	УК-2.1. Знать: - этапы жизненного цикла проекта; - этапы разработки и реализации проекта; - методы разработки и управления проектами; УК-2.2. Уметь: - разрабатывать проект с учетом анализа альтернативных вариантов его реализации, определять целевые этапы, основные направления работ; - объяснить цели и сформулировать задачи, связанные с подготовкой и реализацией проекта - управлять проектом на всех этапах его жизненного цикла; УК-2.3. Владеть: - методиками разработки и управления проектом; - методами оценки потребности в ресурсах и эффективности проекта.

		екта	
ПК-5	Способность использовать передовые методы оценки качества, надежности и технологии защиты информации в компьютерных сетях в процессе эксплуатации прикладных ИС	ПК -5.1 Понимает передовые методы оценки качества, надежности и информационной безопасности ИС ПК -5.2 Способен использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС ПК - 5.3 Применяет передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС	*Знает* методы оценки качества, надежности технологии защиты информации в компьютерных сетях *Умеет* использовать методы оценок качества, надежности и технологией защиты информации в компьютерных сетях в процессе эксплуатации прикладных ИС. *Владеет* навыками передовых методов оценки качеств, надежности и технологией защиты информации в компьютерных сетях в процессе эксплуатации прикладных ИС.

3. Организационно-методические данные дисциплины

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

Таблица 2

Распределение трудоемкости дисциплины по видам работ по семестрам

Вид учебной работы	Трудоемкость			
	зач. ед.	час.	по семестрам	
			№ 3	
Общая трудоемкость дисциплины по учебному плану	**4**	**144**	**144**	
Контактная работа	**1,5**	**56**	**56**	
в том числе:				
Лекции (Л) / в том числе в интерактивной форме		28/8	28/8	
Практические занятия (ПЗ) / в том числе в интерактивной форме				
Семинары (С) / в том числе в интерактивной форме				
Лабораторные работы (ЛР) / в том числе в интерактивной форме		28/8	28/8	
Самостоятельная работа (СРС)	**2,5**	**88**	**88**	
в том числе:				
курсовая работа (проект)				
самостоятельное изучение тем и разделов		43	43	
контрольные работы				
реферат				
самоподготовка к текущему контролю знаний		36	36	
подготовка к зачету		9	9	
др. виды				
Вид контроля:			Зачет с оценкой	

4. Структура и содержание дисциплины

4.1. Трудоёмкость модулей и модульных единиц дисциплины

Таблица 3

Трудоемкость модулей и модульных единиц дисциплины

Наименование модулей и модульных единиц дисциплины	Всего часов на модуль	Контактная работа		Внеаудиторная работа (СРС)
		Л	ЛПЗ	
Календарный модуль 1. Информационные технологии обеспечения конфиденциальности и сохранности данных	**72**	**14**	**14**	**44**
Модульная единица 1. Понятие информационной безопасности. Понятие угрозы. Международные стандарты информационного обмена.	12	2	2	4
Модульная единица 2. Информационная безопасность в условиях функционирования в России глобальных сетей.	14	2	2	8
Модульная единица 3. Виды противников или "нарушителей". Понятия о видах вирусов.	14	2	4	10
Модульная единица 4. Виды возможных нарушений информационной системы. Виды защиты.	16	4	4	10
Модульная единица 5. Основные нормативные руководящие документы , касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности.	16	4	4	12
Календарный модуль 2. Технологии построения защищенных компьютерных систем. Методы криптографии	**72**	**14**	**14**	**44**
Модульная единица 6. Основные положения теории информационной безопасности. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающих их существование.	16	2	2	8
Модульная единица 7. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии.	18	4	4	12
Модульная единица 8. Основные технологии построения защищенных ЭИС.	18	4	4	12
Модульная единица 9. Место информационной безопасности экономических систем в национальной безопасности страны.	20	4	4	12
ИТОГО	**144**	**28**	**28**	**88**

4.2. Содержание модулей дисциплины

Календарный модуль 1. Информационные технологии обеспечения конфиденциальности и сохранности данных

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

Календарный модуль 2. Технологии построения защищенных ЭИС.

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 средства ЗИ. 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/лабораторные/практические/семинарские занятия

Таблица 4

Содержание лекционного курса

№ п/п	№ модуля и модульной единицы дисциплины	№ и тема лекции	Вид[1] контрольного мероприятия	Кол-во часов
1	**Календарный модуль 1. Информационные технологии обеспечения конфиденциальности и сохранности данных**			
1	**Модульная единица 1**. Понятие информационной безопасности. Понятие угрозы. Международные стандарты информационного обмена.	Лекция №1 Понятие информационной безопасности. Понятие угрозы. Международные стандарты информационного обмена	опрос, тестирование	2
2	**Модульная единица 2**. Информационная безопасность в условиях функционирования в России глобальных сетей.	Лекция №2 Информационные технологии обеспечения конфиденциальности и сохранности данных в условиях функционирования в России глобальных сетей. Организационные меры обеспечения информационной безопасности. Поря-	опрос, тестирование	2

[1]**Вид мероприятия:** тестирование, коллоквиум, зачет, экзамен, другое4

№ п/п	№ модуля и модульной единицы дисциплины	№ и тема лекции	Вид[1] контрольного мероприятия	Кол-во часов
		док использования конфиденциальных архивных документов. Политика ИБ. Стандарты ИБ. Модели защиты информации		
3	**Модульная единица 3**. Виды противников или "нарушителей". Понятия о видах вирусов.	Лекция №3 Виды противников или "нарушителей". Понятия о видах вирусов. Программно-аппаратные способы борьбы с вирусами и другим вредоносным программным обеспечением	опрос, тестирование	2
4	**Модульная единица 4.** Виды возможных нарушений информационной системы. Виды защиты.	Лекция №4,5 Виды возможных нарушений информационной системы. Виды защиты. Общая классификация информационных угроз. Информационные угрозы безопасности РФ. Доктрина информационной безопасности РФ	опрос, тестирование	4
5	**Модульная единица 5.** Основные нормативные руководящие документы , касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности.	Лекция №6,7 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.	опрос, тестирование	4
	Календарный модуль 2. Технологии построения защищенных компьютерных систем. Методы криптографии			
6	**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 №8 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.	опрос, тестирование	2
7	**Модульная единица 7**. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Мето-	Лекция №9 Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии. Вредоносное программное обеспече-	опрос, тестирование	4

№ п/п	№ модуля и модульной единицы дисциплины	№ и тема лекции	Вид[1] контрольного мероприятия	Кол-во часов
	ды криптографии.	ние. Программно аппаратные средства ЗИ. Лекция 10 Криптографические методы защиты информации. Типовые удаленные атаки с использованием уязвимостей сетевых протоколов. Классификация удаленных атак		
8	**Модульная единица 8.** Основные технологии построения защищенных ЭИС.	Лекция №11,12 Основные технологии построения защищенных ЭИС. Виды возможных нарушений информационной системы. Правовое регулирование защиты информации (анализ статей УК, других нормативных актов)	опрос, тестирование	4
9	**Модульная единица 9**. Место информационной безопасности экономических систем в национальной безопасности страны.	Лекция №13,14 Место информационной безопасности экономических систем в национальной безопасности страны	опрос, тестирование	4
	Итого		Зачет, Зачет с оценкой	28
Интерактивные формы обучения: диалоговое обсуждение отдельных вопросов, совместное (групповое) решение типовых задач				8

4.4. Лабораторные/практические/семинарские занятия

Таблица 5

Содержание занятий и контрольных мероприятий

№ п/п	№ модуля и модульной единицы дисциплины	№ и название лабораторных/ практических занятий с указанием контрольных мероприятий	Вид[2] контрольного мероприятия	Кол-во часов
	Календарный модуль 1. Информационные технологии обеспечения конфиденциальности и сохранности данных			
1	**Модульная единица 1**. Понятие информационной безопасности. Понятие угрозы. Международные стандарты информационного обмена.	Работа №1 Понятие информационной безопасности. Понятие угрозы. Международные стандарты информационного обмена.	Лабораторная работа	2
2	**Модульная единица 2**. Информационная безопасность в условиях функционирования в России глобальных сетей.	Работа №2 Информационная безопасность в условиях функционирования в России глобальных сетей	Лабораторная работа	2
3	**Модульная единица 3**. Виды противников или "нарушителей".	Работа №3,4 Виды противников или "нару-	Лабораторная	4

[2]**Вид мероприятия:** тестирование, коллоквиум, зачет, экзамен, другое

№ п/п	№ модуля и модульной единицы дисциплины	№ и название лабораторных/ практических занятий с указанием контрольных мероприятий	Вид[2] контрольного мероприятия	Кол-во часов
	Понятия о видах вирусов.	шителей". Понятия о видах вирусов.	работа	
4	**Модульная единица 4.** Виды возможных нарушений информационной системы. Виды защиты.	Работа №5,6 Виды возможных нарушений информационной системы. Виды защиты.	Лабораторная работа	4
5	**Модульная единица 5.** Основные нормативные руководящие документы , касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности.	Работа №7,8 Основные нормативные руководящие документы , касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности.	Лабораторная работа	4
	Календарный модуль 2. Технологии построения защищенных компьютерных систем. Методы криптографии			
6	**Модульная единица 6.** Основные положения теории информационной безопасности. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины,обуславливающих их существование.	Работа №9 Основные положения теории информационной безопасности. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины,обуславливающих их существование	Лабораторная работа	2
7	**Модульная единица 7**. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии.	Работа №10,11 Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии.	Лабораторная работа	4
8	**Модульная единица 8.** Основные технологии построения защищенных ЭИС.	Работа №12,13 Основные технологии построения защищенных ЭИС	Лабораторная работа	4
9	**Модульная единица 9**. Место информационной безопасности экономических систем в национальной безопасности страны.	Работа №14 Место информационной безопасности экономических систем в национальной безопасности страны.	Лабораторная работа	4
	Итого		Зачет, Зачет с оценкой	**28**
Интерактивные формы обучения: диалоговое обсуждение отдельных вопросов, совместное (групповое) решение типовых задач				**8**

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

Самостоятельная работа магистрантов (СРС) организуется с целью развития навыков работы с учебной и научной литературой, выработки способности вести научно-исследовательскую работу, а также для систематического изучения дисциплины. При изучении дисциплины «Информационная безопасность» используются следующие формы организации самостоятельной работы магистрантов:

- организация и использование электронного курса дисциплины размещенного на платформе LMS Moodle для СРС.
- работа над теоретическим материалом, прочитанным на лекциях;
- самостоятельное изучение отдельных разделов дисциплины;
- подготовка к практическим и лабораторным занятиям;
- самотестирование по контрольным вопросам (тестам);
- самостоятельная работа с обучающими программами в компьютерных классах и в домашних условиях.

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	Кол-во часов
	Самостоятельное изучение вопросов разделов, тем:		**79**
1.	**Календарный модуль 1.**		**40**
	Модульная единица 1.	Международные стандарты информационного обмена Работа в среде LMS Moodle	8
	Модульная единица 2.	Информационная безопасность в условиях функционирования в России глобальных сетей. Работа в среде LMS Moodle	8
	Модульная единица 3	Типовые удаленные атаки и их характеристика. Анализ способов нарушений ИБ. Меры защиты информации при возникновении угроз/ Работа в среде LMS Moodle	8
	Модульная единица 4.	Виды возможных нарушений информационной системы. Виды защиты..Работа в среде LMS Moodle	8
	Модульная единица 5.	Назначение и задачи в сфере обеспечения информационной безопасности. Работа в среде LMS Moodle	8
	Календарный модуль 2		**39**
	Модульная единица 6	Модели безопасности и их применение Алгоритмы симметричного шифрования. Работа в среде LMS Moodle	9
	Модульная единица 7	Стандарт криптографической защиты 21 века(AES). Структура шифра Работа в среде LMS Moodle	10
	Модульная единица 8	Основные технологии построения защищенных ЭИС. Работа в среде LMS Moodle	10
	Модульная единица 9	Место информационной безопасности экономических систем в национальной безопасности страны. Работа в среде LMS Moodle	10
4.	Самоподготовка к зачету с оценкой		**9**
	Итого		**88**

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

Курсовые работы не предусмотрены учебным планом.

5. Взаимосвязь видов учебных занятий

Взаимосвязь учебного материала лекций, лабораторных работ с тестовыми вопросами и формируемыми компетенциями представлены в таблице 8.

Таблица 8

Взаимосвязь компетенций с учебным материалом и контролем знаний магистрантов

Компетенции	Лекции	ЛЗ	СРС	Другие виды	Вид контроля
УК-2	1-14	1-14	1-44		Зачет с оценкой
ПК-5	1-14	1-14	1-44		Зачет с оценкой

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Карта обеспеченности литературой

Таблица 9

КАРТА ОБЕСПЕЧЕННОСТИ ЛИТЕРАТУРОЙ

Кафедра Информационные технологии и математическое обеспечение информационных систем
Направление подготовки (специальность) 09.04.03 «Прикладная информатика»
Дисциплина Технологии защиты информации в компьютерных сетях

Вид занятий	Наименование	Авторы	Издательство	Год издания	Вид издания		Место хранения		Необходи-мое количество экз.	Количество экз. в вузе
					Печ.	Электр.	Библ.	Каф.		
1	2	3	4	6	7	8	9	10	11	12
Основная										
Лекции, лаборат. работы.	Защита информации: основы теории: учебник для вузов/ А.Ю.Щеглов, К.А.Щеглов.— Москва : Издательство Юрайт, 2021. —309с. https://urait.ru/bcode/469866	А.Ю.Щеглов, К.А.Щеглов	М. : Издательство Юрайт	2021		Электр.	Библ.		7	

Лекции, лаборат. работы..	Надежность и безопасность программного обеспечения: учебное пособие для вузов / О.В.Казарин, И.Б.Шубинский.— Москва: Издательство Юрайт, 2021.— https://urait.ru/bcode/473348	О.В.Казарин, И.Б.Шубинский	М. : Издательство Юрайт:	2021		Электр.	Библ.		7	
Лекции, лаборат. работы.	Информатика в 2 ч. Часть 1: учебник для вузов/ О.П.Новожилов.— 3-е изд., перераб. и доп.— Москва: Издательство Юрайт, 2021.— 320с.—https://urait.ru/bcode/474159	О.П.Новожилов	М. : Издательство Юрайт:	2021		Электр.	Библ.		7	
Дополнительная										
Лекции, лаборат. работы.	Информатика в 2 ч. Часть 2: учебник для вузов/ О.П.Новожилов.— 3-е изд., перераб. и доп.— Москва: Издательство Юрайт, 2021.— 302с.—https://urait.ru/bcode/474160	О.П.Новожилов	М. : Издательство Юрайт:	2021		Электр.	Библ.		7	

Директор Научной библиотеки _____

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

Интернет-ресурсы

1. Информационная безопасность. Электронный обучающий ресурс https://e.kgau.ru/course/view.php?id=1051 (Moodle)
2. Национальный Открытый Университет «ИНТУИТ» https://intuit.ru/
3. Портал CIT Forum http://citforum.ru/
4. Форум программистов и сисадминов Киберфорум https://www.cyberforum.ru/
5. Информационно-аналитическая система «Статистика» http://www.ias-stat.ru/

Электронные библиотечные системы

1. Каталог библиотеки Красноярского ГАУ -- www.kgau.ru/new/biblioteka/ ;
2. Центральная научная сельскохозяйственная библиотека - www.cnshb.ru/ ;
3. Научная электронная библиотека "eLibrary.ru" – www.elibrary.ru ;
4. Электронная библиотечная система «Лань» - https://e.lanbook.com/
5. Электронно-библиотечная система «Юрайт» - https://urait.ru/
6. Электронно-библиотечная система «AgriLib» - http://ebs.rgazu.ru/
7. Электронная библиотека Сибирского Федерального университета - https://bik.sfu-kras.ru/
8. Национальная электронная библиотека - https://rusneb.ru/
9. 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
10. Электронный каталог Государственной универсальной научной бибилиотеки Краснояр-ского края - https://www.kraslib.ru/

Информационно-справочные системы

1. Справочно-правовая система КонсультантПлюс http://www.consultant.ru/cons/cgi/online.cgi?req=home;rnd=0.8636296761039928
2. Информационно-правовой портал «Гарант». http://www.garant.ru/

Профессиональные базы данных

1. Коллективный блог по информационным технологиям, бизнесу и интернету. https://habr.com/ru/
2. Конференция форумов по технологии баз данных. https://www.sql.ru/

6.3. Программное обеспечение

Лицензионное ПО Красноярского ГАУ

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 (лицензия 17E0-171204-043145-330-825 с 12.04.2017 до 12.12.2019).
5. Kaspersky Endpoint Security для бизнеса Стандартный Russian Edition. 1000-1499 Node 2 year Educational License (лицензия 1800-191210-144044-563-2513 с 10.12.2019 до 17.12.2021).
6. Moodle 3.5.6a (система дистанционного образования) – бесплатно распространяемое ПО.

Свободно-распространяемое ПО

1. Wireshark,
2. Oracle VM Virtual Box,
3. Lazarus (Свободно распространяемое ПО (GPL));

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

7.1 Календарный модуль 1-2

Текущая аттестация обучающихся производится в дискретные временные интервалы преподавателем, ведущим лекционные и практические занятия по дисциплине, в следующих формах:

- тестирование;

- опрос
- выполнение лабораторных работ
- отдельно оцениваются личностные качества магистранта (аккуратность, исполнительность, инициативность) – работа у доски, своевременная сдача тестов.

Рейтинг – план дисциплины «Технологии защиты информации в компьютерных сетях»

	Модули	Часы	Баллы
1	Календарный модуль № 1	67	40
2	Календарный модуль № 2	68	40
	Зачёт с оценкой	9	20
	Итого	**144**	**100**

Распределение баллов по модулям

№	Модули	Баллы по видам работ				Итого
		Опрос	Тестирование	Выполнение лабораторных работ	Итоговое тестирование (Зачёт)	
1	Календарный модуль № 1	5	15	20		40
2	Календарный модуль № 2	5	15	20		40
	Зачёт с оценкой	-	-	-	20	20
	Итого	**10**	**30**	**40**	**20**	**100**

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

Промежуточный контроль *зачет с оценкой* по результатам 3 семестра по дисциплине проходит в форме контрольного итогового тестирования.

Для допуска к промежуточному контролю магистрант должен набрать необходимое количество баллов по итогам текущей аттестации – **40-60** баллов.

Итоговое тестирование включает в себя тестирующие материалы по всему курсу «Компьютерные сети» и проводится в ЭИОС «Moodle».

Оценивание итогового тестирования осуществляется по следующим критериям:

Обучающийся, давший правильные ответы 87-100% тестирующих материалов (1-5 ошибок), получает максимальное количество баллов – 20.

Обучающийся, давший правильные ответы в пределах 73-86% тестирующих материалов (6-10 ошибок), получает 15 баллов.

Обучающийся, давший правильные ответы в пределах 60-72% (11-15 ошибок) тестирующих материалов, получает 10 баллов.

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

60 – 72 – минимальное количество баллов – оценка «удовлетворительно».

73 – 86 – среднее количество баллов – оценка «хорошо».

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

Обучающийся, не сдавший зачёт (экзамен), приходит на пересдачу в сроки в соответствии с графиком ликвидации академических задолженностей: http://www.kgau.ru/new/news/news/2017/grafik_lz.pdf

8. Материально-техническое обеспечение дисциплины

Виды занятий	Аудиторный фонд
Лекции	Занятия лекционного типа проводятся в аудиториях оснащенных комплектом мультимедийного оборудования (стационарного/переносного) с выходом в локальную сеть и Интернет; используются наборы демонстрационного оборудования и учебно-наглядных пособий, комплект мультимедийного оборудования: ноутбук Acer Aspire 5, переносной экран на треноге Medium Professional, переносной проектор Epson
Лабораторные/практические работы	Лабораторные работы проводятся в компьютерном классе, имеющем достаточное количество посадочных мест для размещения магистрантов и оснащенным наборами демонстрационного оборудования и учебно-наглядными пособиями; имеется выход в общую локальную компьютерная сеть и Internet, 15/13 компьютеров на базе процессора Intel Core 2 Duo/i3 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.
Самостоятельная работа	Помещение для самостоятельной работы 3-13 (660130, Красноярский край, г. Красноярск, ул. Елены Стасовой 44 «И») - рабочие места магистрантов, укомплектованные специализированной мебелью, общая локальная компьютерная сеть Internet, 11 компьютеров на базе процессора Intel Celeron в комплектации с мониторами Samsung, LG, Aser, Viewsonic и др. внешними периферийными устройствами. Помещение для самостоятельной работы 1-06 (660130, Красноярский край, г. Красноярск, ул. Елены Стасовой, 44 «Г») - Информационно-ресурсный центр Научной библиотеки - 16 посадочных мест: рабочие места магистрантов, укомплектованные специализированной мебелью, Гигабитный интернет, 8 компьютеров 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 Panasonic, экран, МФУ Laser Jet M1212. Помещение для самостоятельной работы 2-06 (660130, Красноярский край, г. Красноярск, ул. Елены Стасовой, 44 «Г») - на 51 посадочное место: рабочие места магистрантов, 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

9. Методические рекомендации для обучающихся по освоению дисциплины

9.1. Методические указания по дисциплине для обучающихся

Курс «Технологии защиты информации в компьютерных сетях» базируется и требует предварительного знания таких дисциплин как « Методология и технология проектирования информационных систем», «Управление ИТ-проектами», «Современные технологии разработки программного обеспечения».

Дисциплина « Технологии защиты информации в компьютерных сетях» является основополагающим для изучения следующих дисциплин: « Микропроцессорные системы в агропромышленном комплексе», «Технологии обработки больших данных».

В процессе изучения дисциплины магистранты развивают, расширяют и углубляют знания в области компьютерной защиты информации.

Успешное изучение курса требует от магистрантов 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 магистрантов, 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 магистрантов.

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 магистрантами по заданию и под руководством преподавателя одной или нескольких работ. И если на лекции основное внимание магистрантов 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, магистранты занимаются самостоятельно с имеющимися программами и изучают теоретические вопросы.

Полученные навыки и знания помогут магистрантам 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, магистранту предлагаются некоторые схемы и методики, которые помогут развить самостоятельные навыки в изучении нового материала. Это позволяет магистранту повысить профессиональный кругозор, а преподавателю моделировать реальные ситуации, которые могут возникнуть при переходе магистранта от учёбы к практической деятельности.

Обязательными видами промежуточной аттестации, без наличия которых магистранты не допускаются до зачета и зачета с оценкой, является выполнение всех лабораторно-практических заданий.

Магистрант может быть освобожден преподавателем от промежуточной и окончательной аттестации при активной работе во время практических занятий, при участии в магистерских 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.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине.

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

Категории магистрантов	Формы
С нарушение слуха	• в печатной форме; • в форме электронного документа;
С нарушением зрения	в печатной форме увеличенных шрифтом; в форме электронного документа; в форме аудиофайла;
С нарушением опорно-двигательного аппарата	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 РПД

Дата	Раздел	**Изменения**	Комментарии

Программу разработали:

Титовская Наталья Викторовна, к.т.н., доцент _____

(подпись)

РЕЦЕНЗИЯ

на рабочую программу по дисциплине «Технологии защиты информации в компьютерных сетях» для подготовки магистров по направлению 09.04.03«Прикладная информатика» направленность «Прикладная информатика в агропромышленном комплексе»

Дисциплина «Технологии защиты информации в компьютерных сетях» является частью учебного плана подготовки по программе магистратуры направления 09.04.03 «Прикладная информатика» направленность «Прикладная информатика в агропромышленном комплексе». Дисциплина реализуется в институте Экономики и управления АПК.

В рабочей программе дисциплины четко сформулированы конечные результаты обучения в органичной увязке с осваиваемыми знаниями, умениями и приобретаемыми компетенциями с учетом направленности (профиля) подготовки.

Структура и содержание рабочей программы включает: аннотацию; цели и задачи освоения дисциплины; место дисциплины в структуре ОПОП; планируемые результаты освоения дисциплины; структуру и содержание дисциплины с распределением разделов по семестрам, указанием трудоемкости, видов текущего контроля успеваемости и промежуточной аттестации; самостоятельную работу обучающихся; учебно-методическое и информационное обеспечение дисциплины; критерии оценки знаний, умений, навыков и заявленных компетенций; материально-техническое обеспечение дисциплины; методические рекомендации для обучающихся по освоению дисциплины; методические указания по дисциплине для инвалидов и лиц с ограниченными возможностями здоровья.

Программой дисциплины предусмотрены текущий контроль успеваемости и промежуточная аттестация полученных знаний.

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

Содержательная часть модульных единиц каждого модуля сформирована конкретно и четко, подробно указаны темы занятий и виды контрольных мероприятий. Предложенное программное обеспечение включает актуальные и востребованные современные программы по тематике дисциплины.

На основании вышеизложенного, считаю возможным рекомендовать рабочую программу по дисциплине «**Технологии защиты информации в компьютерных сетях**» к использованию в учебном процессе по направлению подготовки 09.04.03«Прикладная информатика» направленность «Прикладная информатика в агропромышленном комплексе».

Рецензент:
зав. кафедрой Информатики Института
космических и информационных технологий
ФГАОУ ВО Сибирский федеральный университет,
канд. техн. наук, доцент
:

Александр
Сергеевич
Кузнецов

Учебно-организационный отдел Институт космических и информационных технологий