МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ЛУГАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ ВЛАДИМИРА ДАЛЯ»

Факультет компьютерных систем и информационных технологий

Кафедра Информатики и Программной инженерии

УТВЕРЖДАЮ
Декан факультета Компьютерных систем
и информационных технологий
_____ Кочевский А.А.
«_19_» ____04_____ 20_23_ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

По дисциплине Безопасность информационных технологий

По направлению подготовки 09.04.03 Прикладная информатика
Магистерская программа 09.04.03.01 Прикладная информатика в экономике

Луганск 2023_

Лист согласования РПУД

Рабочая программа учебной дисциплины «Безопасность информационных технологий» по направлению подготовки 09.04.03 Прикладная информатика (магистерская программа «Прикладная информатика в экономике»). – 10 с.

Рабочая программа учебной дисциплины «Безопасность информационных технологий» составлена с учетом Федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.04.03 Прикладная информатика, утвержденного приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 года № 916 (с изменениями и дополнениями), зарегистрированным в Министерстве юстиции Российской Федерации от 10 октября 2017 года № 48495, учебного плана по направлению подготовки 09.04.03 Прикладная информатика, (магистерская программа «Прикладная информатика в экономике») и Положения о рабочей программе учебной дисциплины в ФГБОУ ВО «ЛГУ им. В. Даля».

СОСТАВИТЕЛЬ:
старший преподаватель Сычева Л.Ф.

Рабочая программа дисциплины утверждена на заседании кафедры информатики и программной инженерии
18 апреля 2023 г., протокол № 17

Заведующий кафедрой информатики и программной инженерии _____ Кочевский А.А.

Переутверждена: «___» _____20___ г., протокол № _____

Согласована:

Декан факультета
компьютерных систем и информационных технологий _____Кочевский А.А.

Переутверждена: «___» _____20____ года, протокол № _____

Рекомендована на заседании учебно-методической комиссии факультета компьютерных систем и информационных технологий

19 апреля 2023 г., протокол № 8

Председатель учебно-методической
комиссии факультета _____/Ветрова Н.Н./

Структура и содержание дисциплины

1. Цели и задачи дисциплины, ее место в учебном процессе

Цель изучения дисциплины - обучение современным информационным технологиям в области информационных систем, создания и эксплуатации систем защиты информации.

Задачи: ознакомление с основными угрозами информационной безопасности; правилами их выявления, анализа и определение требований к различным уровням обеспечения информационной безопасности; ознакомление с угрозами информационной безопасности, создаваемыми компьютерными вирусами, изучение особенности этих угроз и характерные черты компьютерных вирусов; изучение особенности обеспечения информационной безопасности в компьютерных сетях и специфику средств защиты компьютерных сетей; изучение содержания и механизмов реализации сервисов безопасности «идентификация» и «аутентификация»; характеристика сетевой технологии Internet.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Безопасность информационных технологий» относится к общенаучному циклу дисциплин (вариативная часть).

Необходимыми условиями для освоения дисциплины являются: знания информационных технологий, защиты информации.

Основывается на базе дисциплин предыдущего уровня образования и является логическим продолжением содержания дисциплин профессионального цикла. Служит основой для освоения дисциплины «Теория информации и обеспечение информационной безопасности».

3. Требования к результатам освоения содержания дисциплины

Студенты, завершившие изучение дисциплины «Безопасность информационных технологий», должны

знать:

- различные подходы к определению понятия "информационная безопасность";
- определения конфиденциальности и доступности информации.
- задачи информационной безопасности;
- уровни формирования режима информационной безопасности;
- характерные черты компьютерных вирусов и защита от них;
- механизмы идентификации и аутентификации.

уметь:

- распределять задачи информационной безопасности по уровням ее обеспечения;
- использовать механизмы идентификации и аутентификации для защиты информационных технологий;
- использовать методы разграничения доступа.

владеть:

- механизмами обеспечения информационной безопасности.

Перечисленные результаты образования являются основой для формирования следующих компетенций*:*

профессиональных компетенций (ПК):

ПК-3: способность проектировать информационные процессы и системы с использованием инновационных инструментальных средств.

4. Структура и содержание дисциплины

4.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем часов (зач. ед.)**	
	Очная форма	**Заочная форма**
Общая учебная нагрузка (всего)	**144 (4зач. ед)**	**144 (4зач. ед)**
Обязательная аудиторная учебная нагрузка (всего) в том числе:	**56**	**12**
Лекции	28	6
Семинарские занятия	-	
Практические занятия	-	
Лабораторные работы	28	6
Курсовая работа (курсовой проект)	-	
Другие формы и методы организации образовательного процесса (*индивидуальное задание)*	36	9
Самостоятельная работа студента (всего)	**52**	**123**
Форма аттестации	экзамен	экзамен

4.2. Содержание разделов дисциплины

Тема 1. Информационная безопасность и уровни ее обеспечения

Понятие "информационная безопасность" Составляющие информационной безопасности. Система формирования режима информационной безопасности. Уровни формирования режима информационной безопасности. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации.

Тема 2 Стандарты информационной безопасности: "Общие критерии"

Требования безопасности к информационным системам Принцип иерархии: класс – семейство – компонент – элемент. Функциональные требования. Требования доверия.

Тема 3. Стандарты информационной безопасности распределенных систем

Сервисы безопасности в вычислительных сетях. Механизмы безопасности. Администрирование средств безопасности

Тема 4. Классификация угроз "информационной безопасности"

Классы угроз информационной безопасности. Каналы несанкционированного доступа к информации.

Тема 5. Компьютерные вирусы и защита от них

Вирусы как угроза информационной безопасности. Характерные черты компьютерных вирусов

Тема 6.Классификация компьютерных вирусов

Классификация компьютерных вирусов по среде обитания. Классификация компьютерных вирусов по особенностям алгоритма работы. Классификация компьютерных вирусов по деструктивные возможностям

Тема 7. Характеристика "вирусоподобных" программ

Виды "вирусоподобных" программ. Характеристика "вирусоподобных" программ. Утилиты скрытого администрирования. "Intended"-вирусы

Тема 8 Антивирусные программы

Особенности работы антивирусных программ Классификация антивирусных программ. Факторы, определяющие качество антивирусных программ. Профилактика компьютерных вирусов

Тема 9. Механизмы обеспечения "информационной безопасности"

Идентификация и аутентификация. Определение понятий "идентификация" и "аутентификация". Механизм идентификация и аутентификация пользователей

Тема 10. Криптография и шифрование

Структура криптосистемы. Классификация систем шифрования данных. Симметричные и асимметричные методы шифрования. Механизм электронной цифровой подписи

4.3. Лекции

№ п/п	Название темы	Объем часов	
		Очная форма	Заочная форма
1	Тема 1. Информационная безопасность и уровни ее обеспечения	2	2
2	Тема 2 Стандарты информационной безопасности: "Общие критерии"	2	
3	Тема 3. Стандарты информационной безопасности распределенных систем	2	
4	Тема 4. Классификация угроз "информационной безопасности"	2	2
5	Тема 5. Компьютерные вирусы и защита от них	2	
6	Тема 6.Классификация компьютерных вирусов	2	
7	Тема 7. Характеристика "вирусоподобных" программ	4	1
8	Тема 8 Антивирусные программы	4	
9	Тема 9. Механизмы обеспечения "информационной безопасности"	4	
10	Тема 10. Криптография и шифрование	4	1
Итого:		**28**	**6**

4.4. Практические (семинарские) занятия

Не предусмотрены.

4.5. Лабораторные работы

№ п/п	Название темы	Объем часов	
		Очная форма	Заочная форма
1	Лабораторная работа №1 «Система защиты «SecretNet 5.0»»	2	2
2	Лабораторная работа №2 «Обеспечение разграничения доступа к защищаемой информации средствами«SecretNet 5.0»»	2	
3	Лабораторная работа №3 «Построение системы защиты на базе СЗИ «SecretNet 5.0»»	2	
4	Лабораторная работа №4 «Знакомство с программно-аппаратным комплексом средств защиты информации от несанкционированного доступа «АККОРД-NT/2000»»	2	2
5	Лабораторная работа №5 «Построение системы защиты на основе комплекса «АККОРД-NT/2000»»	4	
6	Лабораторная работа №6 «Аудит безопасности в СЗИ «АККОРД-NT/2000»»	4	
7	Лабораторная работа №7 «Система защиты DallasLock 7.5. Состав и функциональные возможности»	4	1
8	Лабораторная работа №8 «Механизмы управления доступом и защиты объектов в системе DallasLock 7.5»	4	1
9	Лабораторная работа №9 «Аудит безопасности средствами СЗИ DallasLock 7.5»	4	
Итого:		**28**	**6**

4.6. Самостоятельная работа студентов

№ п/п	Название темы	Вид СРС	Объем часов	
			Очная форма	Заочная форма
1	Антивирусные программы и работа с ними.	Изучение тем, вынесенных на самостоятельную проработку	10	25
2	Лабораторные работы 1-9	Изучение инструкций к программным системам и подготовке к выполнению лабораторных работ	32	80
3	Подготовка реферата по заданной теме, оформление отчета и презентации.	Выполнение индивидуального задания.	10	18
Итого:			**52**	**123**

4.7. Курсовые работы/проекты

Не предусмотрены.

5. Образовательные технологии

Преподавание дисциплины ведется с применением следующих видов образовательных технологий*:* использование электронных образовательных ресурсов (электронный конспект, размещенный во внутренней сети) при подготовке к лекциям и лабораторным занятиям.

Работа в команде: совместная работа студентов в группе при выполнении лабораторных работ.

6. Формы контроля освоения дисциплины

Текущая аттестация студентов производится в дискретные временные интервалы лектором и преподавателем, ведущими лабораторные работы и практические занятия по дисциплине в следующих формах*:*

- контрольные работы;
- лабораторные работы;
- защита лабораторных работ (отчет).

Фонды оценочных средств, включающие типовые задания, контрольные работы, тесты и методы контроля, позволяющие оценить результаты обучающихся по данной дисциплине, помещаются в приложении к рабочей программе в соответствии с «Положением о фонде оценочных средств».

Форма аттестации по результатам освоения дисциплины проходит в форме устного экзамена (включает в себя ответ на теоретические вопросы и решения задач с использованием компьютера).

В экзаменационную ведомость и зачетную книжку выставляются оценки по шкале, приведенной в таблице.

Шкала оценивания	Характеристика знания предмета и ответов
отлично (5)	Студент глубоко и в полномобъѐме владеет программным материалом. Грамотно, исчерпывающе и логично его излагает в устной или письменной форме. При этом знает рекомендованную литературу, проявляет творческий подход в ответах на вопросы и правильно обосновывает принятые решения, хорошо владеет умениями и навыками при выполнении практических задач.
хорошо (4)	Студент знает программный материал, грамотно и по сути излагает его в устной или письменной форме, допуская незначительные неточности в утверждениях, трактовках, определениях и категориях или незначительное количество ошибок. При этом владеет необходимыми умениями и навыками при выполнении практических задач.
удовлетворительно (3)	Студент знает только основной программный материал, допускает неточности, недостаточно чѐткие формулировки, непоследовательность в ответах, излагаемых в устной или письменной форме. При этом недостаточно владеет умениями и навыками при выполнении практических задач. Допускает до 30% ошибок в излагаемых ответах.
неудовлетворительно (2)	Студент не знает значительной части программного материала. При этом допускает принципиальные ошибки в доказательствах, в трактовке понятий и категорий, проявляет низкую культуру знаний, не владеет основными умениями и навыками при

	выполнении практических задач. Студент отказывается от ответов на дополнительные вопросы.

7. Учебно-методическое и программно-информационное обеспечение дисциплины:

а) основная литература:

1. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2018. - 400 с.

2. Электронное издание на основе: Информационная безопасность и защита информации. - М.: ДМК Пресс, 2014. - 702 с.: ил. - ISBN 978-5-94074-768-0.

3. Глинская, Е.В. Информационная безопасность конструкций ЭВМ и систем: Учебное пособие / Е.В. Глинская, Н.В. Чичварин. - М.: Инфра-М, 2018. - 64 с.

б) дополнительная литература:

1. Бабаш, А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2019. - 432 с.

2. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2013. - 474 с.

3. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2010. - 324 с.

4. Гришина, Н.В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - М.: Форум, 2018. - 118 с.

5. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2018. - 88 с.

6. Семененко, В.А. Информационная безопасность / В.А. Семененко. - М.: МГИУ, 2011. - 277 с.

7. Электронное издание на основе: Основы информационных и телекоммуникационных технологий. Основы информационной безопасности: Учеб. пособие. -М.: Финансы и статистика, 2005. - 176 с.: ил. - ISBN 5-279-03007-4.

8. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. - М.: ДМК, 2014. - 702 с.

в) Интернет–ресурсы:

1. Министерство образования и науки Российской Федерации – http://минобрнауки.рф/
2. Федеральная служба по надзору в сфере образования и науки – http://obrnadzor.gov.ru/
3. Министерство образования и науки Луганской Народной Республики – https://minobr.su
4. Народный совет Луганской Народной Республики – https://nslnr.su
5. Портал Федеральных государственных образовательных стандартов высшего образования – http://fgosvo.ru
6. Федеральный портал «Российское образование» – http://www.edu.ru/

7. Информационная система «Единое окно доступа к образовательным ресурсам» – http://window.edu.ru/

8. Федеральный центр информационно-образовательных ресурсов – http://fcior.edu.ru/

Электронные библиотечные системы и ресурсы

9. Электронно-библиотечная система «Консультант студента» – http://www.studentlibrary.ru/cgi-bin/mb4x

10. Электронно-библиотечная система «StudMed.ru» – https://www.studmed.ru

Информационный ресурс библиотеки образовательной организации

11. Научная библиотека имени А. Н. Коняева – http://biblio.dahluniver.ru/

8. Материально-техническое обеспечение дисциплины

Освоение дисциплины «Безопасность информационных технологий» предполагает использование академических аудиторий, соответствующих действующим санитарным и противопожарным правилам и нормам.

Лабораторные работы: компьютерный класс, презентационная техника (проектор, экран, компьютер/ноутбук), пакеты ПО общего назначения.

Рабочее место преподавателя, оснащенное компьютером с доступом в Интернет, рабочие места студентов, оснащенные компьютерами с доступом в Интернет, предназначенные для работы в электронной образовательной среде.

Программное обеспечение:

Функциональное назначение	**Бесплатное программное обеспечение**	**Ссылки**
Офисный пакет	Libre Office 6.3.1	https://www.libreoffice.org/ https://ru.wikipedia.org/wiki/LibreOffice
Операционная система	UBUNTU 19.04	https://ubuntu.com/ https://ru.wikipedia.org/wiki/Ubuntu
Браузер	FirefoxMozilla	http://www.mozilla.org/ru/firefox/fx
Браузер	Opera	http://www.opera.com
Почтовый клиент	MozillaThunderbird	http://www.mozilla.org/ru/thunderbird
Файл-менеджер	FarManager	http://www.farmanager.com/download.php
Архиватор	7Zip	http://www.7-zip.org/
Графический редактор	GIMP (GNU Image Manipulation Program)	http://www.gimp.org/ http://gimp.ru/viewpage.php?page_id=8 http://ru.wikipedia.org/wiki/GIMP
Редактор PDF	PDFCreator	http://www.pdfforge.org/pdfcreator

Аудиоплейер	VLC	http://www.videolan.org/vlc/