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 2023 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

По дисциплине Теория информации и обеспечение информационной безопасности

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 «Теория информации и обеспечение информационной безопасности» по направлению подготовки 09.04.03 Прикладная информатика (магистерская программа «Прикладная информатика в экономике»). – 10 с.

Рабочая программа учебной дисциплины «Теория информации и обеспечение информационной безопасности» 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./

© Сычева Л.Ф. 2023 год
© ФГБОУ ВО «ЛГУ им. В. Даля», 2023 год

Структура и содержание дисциплины

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

Цель освоения дисциплины - ознакомление студентов с основными понятиями теории информации, принципами получения, преобразования, передачи, хранения и представления информации, с современными методами защиты информации и обеспечения ее безопасности.

Задачи: формирование знаний, умений и навыков, позволяющих самостоятельно проводить анализ закономерностей информационных процессов и оценивать реальные и предельные возможности пропускной способности и помехоустойчивости, а также качества информационных систем; ознакомление с основными угрозами информационной безопасности, правилами их выявления, анализа и определение требований.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Теория информации и обеспечение информационной безопасности» относится к профессиональному циклу дисциплин (базовая часть).

Необходимыми условиями для освоения дисциплины являются:

знания теории информации, защиты информации; умения использовать методы разграничения доступа к информации; навыки владения методами разграничения доступа пользователей и процессов к ресурсам защищенной информационной системы.

Содержание дисциплины является логическим продолжением содержания дисциплин безопасность информационных технологий, динамическая теория информации и служит основой для научно-исследовательской работы магистра.

3. Требования к результатам освоения содержания дисциплины

Студенты, завершившие изучение дисциплины «Теория информации и обеспечение информационной безопасности», должны

Знать:

- различные подходы к определению понятия "информационная безопасность";
- отличие "компьютерной безопасности" от "информационной безопасности";
- составляющие понятия "информационная безопасность";
- определение целостности информации;
- определения конфиденциальности и доступности информации.
- задачи информационной безопасности;
- уровни формирования режима информационной безопасности;
- особенности законодательно-правового и административного уровней;
- подуровни программно-технического уровня.
- механизмы идентификации и аутентификации;

- идентификаторы, используемые при реализации механизма идентификации и аутентификации;
- методы разграничения доступа;
- защитные свойства механизма регистрации и аудита;
- методы аудита безопасности информационных систем;
- механизм межсетевого экранирования.

Уметь:

- объяснить сущность проблемы "информационной безопасности";
- распределять задачи информационной безопасности по уровням ее обеспечения;
- использовать механизмы идентификации и аутентификации для защиты информационных систем;
- использовать методы разграничения доступа;
- использовать механизмы регистрации и аудита для анализа защищенности системы;
- выбирать межсетевые экраны для защиты информационных систем;
- определять политику безопасности виртуальной частной сети.

Владеть:

- методами разграничения доступа пользователей и процессов к ресурсам защищенной информационной системы;
- принципами организации межсетевого экранирования как механизма обеспечения безопасности информационных систем;
- методами технологий виртуальных частных сетей и механизмом ее реализации.

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

а) профессиональных (ПК):

ОПК-3: способен анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями.

б) профессиональных компетенций (ПК):

ПК-5: способен использовать современные методы оценки качества, надежности и информационной безопасности информационных систем в процессе их проектирования и эксплуатации.

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:	**64**	**14**
Лекции	32	6
Семинарские занятия	-	

Практические занятия	-	
Лабораторные работы	32	8
Курсовая работа (курсовой проект)	-	
Другие формы и методы организации образовательного процесса	-	4
Самостоятельная работа студента (всего)	**80**	**126**
Форма аттестации	зачет	зачет

4.2. Содержание разделов дисциплины

Тема 1. Основы теории информации.

Понятие «информация». Качество информации. Информация в форме сообщения.

Тема 2. Понятие энтропии.

Комбинаторный подход к вычислению количества информации. Формула Хартли. Вероятностный подход к вычислению количества информации. Формула Шеннона.

Тема 3. Количество информации и его оценка.

Свойства функции энтропии. Энтропия сложных событий. Условная энтропия.

Тема 4. Информация в системах управления.

Понятие и роль информации в управлении. Классификация информации. Свойства и качественные характеристики информации. Информационный процесс. Информационная система, её формирование и развитие. Формы адекватности информации.

Тема 5. Понятие "информационная безопасность"

Проблема информационной безопасности общества. Определение понятия «информационная безопасность».

Тема 6. Составляющие информационной безопасности

Доступность информации. Целостность информации. Конфиденциальность информации.

Тема 7. Система формирования режима информационной безопасности

Задачи информационной безопасности общества. Уровни формирования режима информационной безопасности.

Тема 8. Механизмы обеспечения "информационной безопасности"

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

Тема 9. Методы разграничение доступа

Методы разграничения доступа. Мандатное и дискретное управление доступом.

Тема 10. Регистрация и аудит

Определение и содержание регистрации и аудита информационных систем. Этапы регистрации и методы аудита событий информационной системы.

Тема 11. Межсетевое экранирование

Классификация межсетевых экранов. Характеристика межсетевых экранов.

Тема 12. Технология виртуальных частных сетей (vpn)

Сущность и содержание технологии виртуальных частных сетей. Понятие "туннеля" при передаче данных в сетях.

4.3. Лекции

№ п/п	Название темы	Объем часов	
		Очная форма	Заочная форма
1	Основы теории информации.	2	1
2	Понятие энтропии.	2	
3	Количество информации и его оценка.	2	
4	Информация в системах управления.	2	1
5	Понятие "информационная безопасность"	2	
6	Составляющие информационной безопасности	2	
7	Система формирования режима информационной безопасности	2	2
8	Механизмы обеспечения "информационной безопасности"	2	
9	Методы разграничение доступа	4	
10	Регистрация и аудит	4	2
11	Межсетевое экранирование	4	
12	Технология виртуальных частных сетей (vpn)	4	
Итого:		**32**	**6**

4.4. Практические (семинарские) занятия

Не предусмотрены.

4.5. Лабораторные работы

№ п/п	Название темы	Объем часов	
		Очная форма	Заочная форма
1	Виды информации и основные методы ее защиты.	2	2
2	Виды угроз информационной безопасности.		
3	Источники угроз информационной безопасности.	2	
4	Анализ информационной инфраструктуры государства.		
5	Исследование атаки переполнения буфера как примера нарушения конфиденциальности, целостности и доступности информации.	2	
6	Причины, виды, каналы утечки и искажения информации.		2
7	Технические средства и методы защиты информации.	2	
8	Программно-аппаратные средства обеспечения информационной безопасности.		
9	Тестовые испытания программных средств защиты.	2	2
10	Защита от утечек по каналу ПЭМИН, по акустическому и вибро акустическому каналам.		
11	Анализ сетевой топологии и установленных сервисов	2	
12	Сетевое сканирование		
13	Анализ трафика и сбор критичной информации	2	2

	программами пассивного анализа		
14	Обнаружение уязвимостей по сигнатурам	2	
15	Оценка уязвимости коммутируемого доступа	4	
16	Анализ угроз и рисков комплексной защиты информации на объекте с использованием системы «Гриф»	4	
17	Анализ и управление политикой информационной безопасности на объекте с использованием системы «Кондор»	4	
18	Аудит комплексной защиты информации предприятия	4	
Итого:		**32**	**8**

4.6. Самостоятельная работа студентов

№ п/п	Название темы	Вид СРС	Объем часов	
			Очная форма	**Заочная форма**
1	Технические средства и методы защиты информации.	Изучение тем, вынесенных на самостоятельную проработку	20	26
2	Лабораторные работы 1-18	Изучение инструкций к программным системам и подготовке к выполнению лабораторных работ	60	100
Итого:			**80**	**126**

4.7. Курсовые работы/проекты

Не предусмотрены.

5. Образовательные технологии

Преподавание дисциплины ведется с применением следующих видов образовательных технологий*:*

Информационные технологии: использование электронных образовательных ресурсов (электронный конспект лекций, электронные методические указания к выполнению лабораторных работ, размещенные 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 (опрос).

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 зачета (включает в себя ответ на теоретические вопросы и защиту лабораторных работ).

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

Характеристика знания предмета и ответов	Зачеты
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.	зачтено
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.	
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.	
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.	не зачтено

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

а) основная литература:

1. Электронное издание на основе: Теория информации и защита телекоммуникаций: монография / В.В. Котенко, К.Е. Румянцев. - Ростов н/Д: Изд-во ЮФУ, 2009. - 369 с.: ил. 49. - ISBN 978-5-9275-0670-5.

2. Электронное издание на основе: Теория информации : учебное пособие / В. В. Котенко, К. Е. Румянцев ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. - 239 с. - ISBN 978-5-9275-2370-2.

3. 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.

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

б) дополнительная литература:

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

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

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

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

5. Ярочкин, В.И. Информационная безопасность: Учебник для вузов / В.И. Ярочкин. - М.: Академический проспект, 2008. - 544 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 «Теория информации и обеспечение информационной безопасности» 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/