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 компьютерных систем и сетей

УТВЕРЖДАЮ
Декан факультета компьютерных систем
и информационных технологий
_____ Кочевский А.А.
«19» апреля 2023 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

По дисциплине «Защита информации»

По направлению подготовки 01.03.02 Прикладная математика и информатика

Профиль подготовки «Математическое и программное обеспечение вычислительных машин и компьютерных сетей»

Луганск 2023

Лист согласования РПУД

Рабочая программа учебной дисциплины (модуля) «Защита информации». – 11 с.

Рабочая программа учебной дисциплины (модуля) «Защита информации» разработана с учетом Федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 01.03.02 Прикладная математика и информатика, утвержденного приказом Министерства образования и науки Российской Федерации от 10.01.2018 г. № 9.

СОСТАВИТЕЛИ:
ст. преп. кафедры компьютерных систем и сетей Зверева О.С.

Рабочая программа учебной дисциплины утверждена на заседании кафедры компьютерных систем и сетей
«18» апреля 2023 года, протокол № 9
Заведующий кафедрой компьютерных систем и сетей _____ С.В. Попов
Переутверждена: «___» _____20__ года, протокол № _____

Согласована (для обеспечивающей кафедры):

Декан факультета компьютерных систем
и информационных технологий _____ А.А. Кочевский

Рекомендована на заседании учебно-методической комиссии факультета компьютерных систем и информационных технологий
«19» апреля 2023 года, протокол № 8

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

Структура и содержание дисциплины

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

Целями дисциплины является формирование целостного представления о современных организационных, технических, алгоритмических и других методах и средствах защиты компьютерной информации, используемых в современных криптосистемах, овладение основами методологии обеспечения информационной безопасности.

Задачи: освоить методы и средства защиты информации; изучить документы в области обеспечения информационной безопасности, защиты государственной тайны и конфиденциальности информации.

2. Место дисциплины в структуре ООП ВО

Дисциплина «Защита информации» относится к части, формируемой участниками образовательных отношений, дисциплин подготовки студентов бакалавров по направлению подготовки 01.03.02 Прикладная математика и информатика.

Необходимыми условиями для освоения дисциплины являются: знания базовых понятий вычислительной техники, роли сетей и телекоммуникаций в науке и технике, умения применять вычислительную технику для решения практических задач, навыки работы на персональном компьютере и создания профессиональных программных продуктов.

Основывается на базе дисциплин: Информатика; Операционные системы; Сети телекоммуникации.

Является основой для изучения следующих дисциплин: Исследование операций; Исследование операций.

3. Требования к результатам освоения содержания дисциплины

Студенты, завершившие изучение дисциплины «Защита информации», должны

знать: методики поиска, сбора и обработки информации; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности; метод системного анализа; методы анализа и обобщения отечественного и международного опыта в области прикладной математики и информатики; различные виды наукометрических баз даннях;

уметь: применять методики поиска, сбора и обработки информации; осуществлять критический анализ и синтез информации, полученной из разных источников; применять системный подход для решения поставленных задач; осуществлять анализ информации в современных наукометрических базах данных; осуществлять сбор и проводить обработку научной и технической информации, в том числе применяя методы машинного обучения;

владеть: методами поиска, сбора и обработки критического анализа и синтеза информации; методикой системного подхода для решения поставленных задач; методы проведения вычислительных экспериментов, обобщения и обработки информации; методы сбора и обработки научной и

технической информации; навыками применять методы науки больших данных для сбора и обработки результатов научных экспериментов и исследований; способностью применять методы науки больших данных для проведения анализа информации в современных наукометрических базах данных и других облачных хранилищах больших данных.

Перечисленные результаты образования являются основой для формирования следующих компетенций (*в соответствии с государственными образовательными стандартами ВО и требованиями к результатам освоения основной профессиональной образовательной программы (ОПОП):*

универсальных:

УК-1 способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;

профессиональных:

ПК-2 способен проводить обработку и анализ научной и технической информации и результатов исследований.

4. Структура и содержание дисциплины

4.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем часов (зач. ед.)**		
	Очная форма	**Очно-заочная форма**	**Заочная форма**
Общая учебная нагрузка (всего)	**108 (3 зач. ед)**	**108 (3 зач. ед)**	**-**
Обязательная аудиторная учебная нагрузка (всего) в том числе:	**56**	**24**	**-**
Лекции	28	12	-
Семинарские занятия	-	-	-
Практические занятия	-	-	-
Лабораторные работы	28	12	-
Курсовая работа (курсовой проект)	-	-	-
Другие формы и методы организации образовательного процесса	-	-	-
Самостоятельная работа студента (всего)	**52**	**80**	**-**
Форма аттестации	Зачет 5	Зачет 5 (4 часа)	-

4.2. Содержание разделов дисциплины

Раздел 1 . Основные понятия информационной безопасности.

Тема 1. Основные понятия информационной безопасности. Основные составляющие. Важность проблемы.

Понятие информации и защиты информации. Категории информационной безопасности. Классификация угроз информационным системам.

Тема 2. Распространение объектно-ориентированного подхода на информационную безопасность

Основные понятия объектно-ориентированного подхода. Применение ООП к рассмотрению защищенных систем. Недостатки традиционного подхода к ИБ с объектной точки зрения

Тема 3. Наиболее распространенные угрозы.

Процесс передачи информации и его «узкие места». Отказ пользователей. Внутренний отказ информационной системы. Отказ поддерживающей инфраструктуры.

Тема 4. Законодательный уровень информационной безопасности.

Категории и правовые аспекты защиты информации. Ответственность, предусмотренная за преступления в сфере защиты информации уголовным кодексом.

Раздел 2 . Стандарты и спецификации в области информационной безопасности.

Тема 5. Стандарты и спецификации в области информационной безопасности

Международные и национальные стандарты и спецификации в области ИБ - от "Оранжевой книги" до ISO 15408. Сильные и слабые стороны этих документов.

Тема 6. Административный уровень информационной безопасности

Основные понятия административного уровня информационной безопасности. Политика безопасности. Программа безопасности. Синхронизация программы безопасности с жизненным циклом систем.

Тема 7 Управление рисками

Этапы процесса управления рисками. Подготовительные этапы управления рисками.

Тема 8 Процедурный уровень информационной безопасности

Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ.

Раздел 3 . Современные криптосистемы.

Тема 9. Современные криптосистемы.

Симметричные и ассиметричные системы шифрования. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы.

Тема 10 Криптографические протоколы

Порядок выполнении протокола. Функции защиты и атаки на протоколы.

Тема 11 Основные программно-технические меры

Управление доступом. Протоколирование и аудит. Шифрование. Контроль целостности. Экранирование. Анализ защищенности. Обеспечение отказоустойчивости.

Раздел 4 . Экранирование, анализ защищенности.

Тема 12. Идентификация и проверка подлинности.

Системы идентификации (распознавания) и аутентификации (проверки подлинности) пользователей. Системы шифрования дисковых данных. Системы шифрования данных, передаваемых по сетям. Системы аутентификации электронных данных.

Тема 13 Протоколирование и аудит, шифрование, контроль целостности.

Протоколирование и аудит, а также криптографические методы защиты. Их место в общей архитектуре безопасности.

Тема 14 Экранирование, анализ защищенности

Модели компьютерных атак. Классификация атак. Системы обнаружения атак.

Тема 15. Обеспечение высокой доступности

Классификация информации. Категории защищаемой информации. Категорирование информации. Инвентаризация ресурсов

Тема 16. Туннелирование и управление.

туннелирование, конвертование, обертывание, конфиденциальность, конфиденциальность трафика.

4.3. Лекции

№ п/п	Название темы	Объем часов		
		Очная форма	Очно-заочная форма	Заочная форма
Тема 1.	Основные понятия информационной безопасности. Основные составляющие. Важность проблемы	2	1	-
Тема 2.	Распространение объектно-ориентированного подхода на информационную безопасность	2		-
Тема 3.	Наиболее распространенные угрозы	2	1	-
Тема 4.	Законодательный уровень информационной безопасности	2		-
Тема 5.	Стандарты и спецификации в области информационной безопасности	2	1	-
Тема 6.	Административный уровень информационной безопасности	2	1	-
Тема 7.	Управление рисками	2	1	-
Тема 8.	Процедурный уровень информационной безопасности	2	1	-
Тема 9.	Современные криптосистемы	2	1	-
Тема 10.	Криптографические протоколы	2	1	-
Тема 11.	Основные программно-технические меры	2	1	-
Тема 12.	Идентификация и проверка подлинности	2	1	-
Тема 13.	Протоколирование и аудит, шифрование, контроль целостности	2	1	-
Тема 14.	Экранирование, анализ защищенности	2	1	-
Итого:		***28***	***12***	**-**

4.4. Практические занятия – не предусмотрены рабочим учебным планом.

4.5. Лабораторные работы

№ п/п	Название темы	Объем часов		
		Очная форма	Очно-заочная форма	Заочная форма
Тема 1.	Управление локальными параметрами безопасности ОС.	2	1	-
Тема 2.	Шифрование файлов. Защита архивов паролем.	2	1	-
Тема 3.	Антивирусные программы	2	1	-
Тема 4.	Шифры замены	2	1	-

Тема 5.	Шифр Виженера	4	1	-
Тема 6.	Шифр перестановки	2	1	-
Тема 7.	Шифр простой замены	4	1	-
Тема 8.	Аддитивные шифры	2	1	-
Тема 9.	Шифрование с открытым ключом	2	1	-
Тема 10.	Комбинированные шифры	2	1	-
Тема 11.	Перехват и анализ сетевых пакетов.	4	2	-
Итого:		***28***	***12***	**-**

4.6. Самостоятельная работа студентов

№ п/п	Название темы	Вид СРС	Объем часов		
			Очная форма	Очно-заочная форма	Заочная форма
Тема 1.	Основные понятия информационной безопасности. Основные составляющие. Важность проблемы	Изучение теоретического материала. Поиск дополнительного материала по теме	2	4	-
Тема 2.	Распространение объектно-ориентированного подхода на информационную безопасность	Изучение теоретического материала. Поиск дополнительного материала по теме	2	4	-
Тема 3.	Наиболее распространенные угрозы	Изучение теоретического материала. Поиск дополнительного материала по теме	4	6	-
Тема 4.	Законодательный уровень информационной безопасности	Изучение теоретического материала. Поиск дополнительного материала по теме	4	6	-
Тема 5.	Стандарты и спецификации в области информационной безопасности	Изучение теоретического материала. Поиск дополнительного материала по теме	4	6	-
Тема 6.	Административный уровень информационной безопасности	Изучение теоретического материала. Поиск дополнительного материала по теме	4	6	-
Тема 7.	Управление рисками	Изучение теоретического материала. Поиск дополнительного материала по теме	4	6	-
Тема 8.	Процедурный уровень информационной безопасности	Изучение теоретического материала. Поиск дополнительного материала по теме	4	6	-

Тема 9.	Современные криптосистемы	Изучение теоретического материала. Поиск дополнительного материала по теме	4	6	-
Тема 10.	Криптографические протоколы	Изучение теоретического материала. Поиск дополнительного материала по теме	4	6	-
Тема 11.	Основные программно-технические меры	Изучение теоретического материала. Поиск дополнительного материала по теме	4	6	-
Тема 12.	Идентификация и проверка подлинности	Изучение теоретического материала. Поиск дополнительного материала по теме	4	6	-
Тема 13.	Протоколирование и аудит, шифрование, контроль целостности	Изучение теоретического материала. Поиск дополнительного материала по теме	4	6	-
Тема 14.	Экранирование, анализ защищенности	Изучение теоретического материала. Поиск дополнительного материала по теме	4	6	-
Итого:			***52***	***80***	**-**

4.7. Курсовые работы/проекты

Курсовые работы/проекты по дисциплине не предусмотрены.

5. Образовательные технологии

С целью формирования и развития профессиональных навыков обучающихся преподавание дисциплины ведется с применением технологии объяснительно-иллюстративного и проблемного обучения в сочетании с современными информационными технологиями обучения (различные демонстрации с использованием проекционного мультимедийного оборудования).

В процессе проведения аудиторных занятий используются следующие активные и интерактивные методы и формы обучения: проблемная лекция, совместная работа студентов в группе при выполнении лабораторных работ, самостоятельная работа с электронными образовательными ресурсами (электронный конспект, размещенный во внутренней сети) при подготовке к лекциям, лабораторным работам; интерактивные лекции (презентации).

6. Формы контроля освоения дисциплины

Текущая аттестация студентов производится в дискретные временные интервалы лектором или преподавателем, ведущим практические занятия по дисциплине в следующих формах:

- лабораторные работы;
- защита лабораторных работ.

Фонды оценочных средств, включающие типовые задания и методы контроля, позволяющие оценить результаты текущей и промежуточной аттестации 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. Зачет для всех форм обучения выставляется по результатам текущего контроля знаний при всех положительно выполненных контрольных мероприятиях (лабораторных работ, защит лабораторных работ) и не предусматривает обязательного присутствия студента.

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

Характеристика знания предмета и ответов	Зачеты
Студент глубоко и в полном объёме 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 лабораторных работ.	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 лабораторных работ.	
Студент знает только основной программный материал, допускает неточности, недостаточно чёткие формулировки, непоследовательность в ответах, излагаемых в устной или письменной форме. При этом недостаточно владеет умениями и навыками при выполнении лабораторных работ. 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 информационное обеспечение дисциплины:

а) основная литература:

1. Гусева Е.Н., Информатика / Е.Н. Гусева, И.Ю. Ефимова, Р.И. Коробков, К.В. Коробкова, И.Н. Мовчан, Л.А. Савельева - М. : ФЛИНТА, 2016. - 260 с. - ISBN 978-5-9765-1194-1 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL :

http://www.studentlibrary.ru/book/ISBN9785976511941.html

2. Проскуряков А.В., Компьютерные сети. Основы построения компьютерных сетей и телекоммуникаций : учебное пособие / Проскуряков А. В. - Ростов н/Д : Изд-во ЮФУ, 2018. - 201 с. - ISBN 978-5-9275-2792-2 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : http://www.studentlibrary.ru/book/ISBN9785927527922.html

б) дополнительная литература:

1. Алиев В.К., Информатика в задачах, примерах, алгоритмах / Алиев В.К. - М. : СОЛОН-ПРЕСС, 2009. - 144 с. - ISBN 5-93455-119-1 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : http://www.studentlibrary.ru/book/ISBN5934551191.html

2. Губарев В.В., Информатика: прошлое, настоящее, будущее / Губарев В.В. - М. : Техносфера, 2011. - 432 с. - ISBN 978-5-94836-288-5 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : http://www.studentlibrary.ru/book/ISBN9785948362885.html

3. Девянин П.Н., Модели безопасности компьютерных систем. Управление доступом и информационными потоками : Учебное пособие для вузов / Девянин П.Н. - М. : Горячая линия - Телеком, 2012. - 320 с. - ISBN 978-5-9912-0147-6 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : http://www.studentlibrary.ru/book/ISBN9785991201476.html

4. Иванова Н.Ю., Системное и прикладное программное обеспечение : Учебное пособие / Иванова Н.Ю., Маняхина В.Г. - М. : Прометей, 2011. - 202 с. - ISBN 978-5-4263-0078-1 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : http://www.studentlibrary.ru/book/ISBN9785426300781.html

в) интернет-ресурсы:

Министерство образования и науки Российской Федерации – http://минобрнауки.рф

Федеральная служба по надзору в сфере образования и науки – http://obrnadzor.gov.ru

Министерство образования и науки Луганской Народной Республики – https://minobr.su

Народный совет Луганской Народной Республики – https://nslnr.su

Портал Федеральных государственных образовательных стандартов высшего образования – http://fgosvo.ru

Федеральный портал «Российское образование» – http://www.edu.ru/

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

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

Электронные библиотечные системы и ресурсы

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

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

Информационный ресурс библиотеки образовательной организации
Научная библиотека имени А. Н. Коняева – http://biblio.dahluniver.ru/

8. Материально-техническое и программное обеспечение дисциплины

Освоение дисциплины «Защита информации» предполагает использование академических аудиторий, соответствующих действующим санитарным и противопожарным правилам и нормам.

Лекционные занятия: комплект электронных презентаций/слайдов; аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук).

Лабораторные работы: компьютерный класс, презентационная техника (проектор, экран, компьютер/ноутбук), пакеты ПО общего и специализированного назначения (операционная система, текстовые редакторы, графические редакторы, и т.п.).

Прочее: рабочее место преподавателя, оснащенное компьютером с доступом в Интернет.

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	Firefox Mozilla	http://www.mozilla.org/ru/firefox/fx
Браузер	Opera	http://www.opera.com
Почтовый клиент	Mozilla Thunderbird	http://www.mozilla.org/ru/thunderbird
Файл-менеджер	Far Manager	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/