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

«ЗАЩИТА ДАННЫХ В СЕТЯХ ЭВМ»

По направлению подготовки 09.04.01 Информатика и вычислительная техника

Программа магистратуры «Сети ЭВМ и телекоммуникации»

Луганск 2023

Лист согласования РПУД

Рабочая программа учебной дисциплины (модуля) «Защита данных в сетях ЭВМ». – 17 с.

Рабочая программа учебной дисциплины (модуля) «Защита данных в сетях ЭВМ» разработана с учетом Федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.04.01 Информатика и вычислительная техника, утвержденного приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 года № 918.

СОСТАВИТЕЛЬ:
ст. преп. кафедры компьютерных систем и сетей Аст С.А.

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 № _____

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

Цель изучения дисциплины - формирование у студентов знаний и умений по защите компьютерных сетей с применением современных средств; приобретение студентами умения проектировать системы защиты информации.

Задачи: предоставление студентам знаний о методах и средствах защиты информации в компьютерных сетях; изучение технологии межсетевого экранирования; изучение механизмов построения виртуальных частных сетей; рассмотрение способов анализа уровня защищенности информационных систем.

2. Место дисциплины в структуре ОПОП ВО. Требования к результатам освоения содержания дисциплины.

Курс входит в обязательную часть дисциплин подготовки студентов по направлению подготовки 09.04.01 Информатика и вычислительная техника.

Дисциплина реализуется кафедрой компьютерных систем и сетей.

Основывается на базе дисциплин: сети и телекоммуникации; администрирование вычислительных систем и сетей; защита информации.

Является основой для изучения следующих дисциплин: методы администрирования компьютерных сетей.

3. Требования к результатам освоения содержания дисциплины

ПК-1. Знание методов оптимизации и умение применять их при решении задач профессиональной деятельности.	ПК-1.1. Знать: основные методы оптимизации информационно-управляющих систем; особенности обеспечения информационной безопасности в распределенных системах и центрах обработки информации; основные понятия нечеткой логики и нечетких систем управления. ПК-1.2. Уметь: применять классические методы оптимизации при решении задач профессиональной деятельности; применять методы защиты удаленного доступа. ПК-1.3. Владеть: классическими методами оптимизации при решении задач профессиональной деятельности; методами принятия решений, применяемые в экспертных	Знать: основные методы оптимизации информационно-управляющих систем; особенности обеспечения информационной безопасности в распределенных системах и центрах обработки информации; основные понятия нечеткой логики и нечетких систем управления. Уметь: применять классические методы оптимизации при решении задач профессиональной деятельности; применять методы защиты удаленного доступа. Владеть: классическими методами оптимизации при решении задач профессиональной деятельности; методами принятия решений, применяемые в экспертных

	системах.	системах.
ПК-4. Способен осуществлять администрирование процесса поиска и диагностики ошибок сетевых устройств и программного обеспечения.	ПК-4.1. Знать: методы поиска и диагностики ошибок сетевых устройств и программного обеспечения. ПК-4.2. Уметь: определять ошибки сетевых устройств и операционных систем; документировать и устранять сбои и отказы сетевых устройств и операционных систем; работать с сетевыми протоколами. ПК-4.3. Владеть: навыками администрирования процесса поиска и диагностики ошибок сетевых устройств и программного обеспечения; методами работы с телекоммуникационными технологиями.	Знать: методы поиска и диагностики ошибок сетевых устройств и программного обеспечения. Уметь: определять ошибки сетевых устройств и операционных систем; документировать и устранять сбои и отказы сетевых устройств и операционных систем; работать с сетевыми протоколами. Владеть: навыками администрирования процесса поиска и диагностики ошибок сетевых устройств и программного обеспечения; методами работы с телекоммуникационными технологиями.

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)	**144 (4 зач. ед)**	**-**	**144 (4 зач. ед)**
Обязательная аудиторная учебная нагрузка (всего) в том числе:	**56**	**-**	**12**
Лекции	28	-	6
Семинарские занятия	-	-	-
Практические занятия	28	-	6
Лабораторные работы	-	-	-
Курсовая работа (курсовой проект)	-	-	-
Другие формы и методы организации образовательного процесса (*расчетно-графические работы, групповые дискуссии, ролевые игры, тренинг, компьютерные симуляции, интерактивные лекции, семинары, анализ деловых ситуаций и т.п.)*	-	-	-
Самостоятельная работа студента (всего)	**52**	**-**	**123**
Форма аттестации:	-	-	-
Экзамен (семестр 2)	36	-	9

4.2. Содержание разделов дисциплины

В разделе приводится полный перечень дидактических единиц, подлежащих усвоению при изучении данной дисциплины, структурированный по разделам дисциплины.

Тема 1. Общие вопросы информационной безопасности

Основные понятия и определения. Понятия информации,

информатизации, информационной системы, информационной безопасности. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, понятие тайны, средства защиты информации. Международные стандарты информационного обмена. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Требования к защите информации. Комплексность системы защиты информации.

Тема 2. Государственная система информационной безопасности

Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Структура государственной системы информационной безопасности. Структура законодательной базы по вопросам информационной безопасности. Механизмы лицензирования и сертификации в области защиты информации. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.

Тема 3. Угрозы безопасности

Понятие угрозы. Виды противников или «нарушителей». Классификация и виды угроз информационной безопасности. Основные нарушения. Характер происхождения угроз (умышленные и естественные факторы). Источники и предпосылки появления угроз. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации.

Тема 4. Теоретические основы методов защиты информационных систем.

Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Методы защиты средств вычислительной техники. Использование защищенных компьютерных систем. Аппаратные и программные средства для защиты компьютерных систем от несанкционированного доступа. Основы криптографии. Методы криптографии. Симметричное и асимметричное шифрование. Алгоритмы шифрования.

Тема 5. Архитектура защищенных экономических систем

Основные технологии построения защищенных экономических информационных систем. Функции защиты информации. Классы задач защиты информации. Архитектура систем защиты информации. Ядро и ресурсы средств защиты информации. Стратегии защиты информации. Особенности экономических информационных систем.

Тема 6. Алгоритмы привязки программного обеспечения к аппаратному окружению

Индивидуальные параметры вычислительной системы. Блок

проверки аппаратного окружения. Технология HASP, эмуляторы. Временные метки и запись в реестр. Обеспечение требуемого количества запусков (trial version). Технология spyware. Виды распространения программного обеспечения. Шифрование и запутывание исполняемого кода.

4.3. Лекции

№ п/п	Название темы	Объем часов		
		Очная форма	Очно-заочная форма	Заочная форма
Семестр 2		**28**	**-**	**6**
1	Общие вопросы информационной безопасности	4	-	
2	Государственная система информационной безопасности	4	-	2
3	Угрозы безопасности	4	-	2
4	Теоретические основы методов защиты информационных систем.	4	-	2
5	Архитектура защищенных экономических систем	6	-	
6	Алгоритмы привязки программного обеспечения к аппаратному окружению	6	-	
Итого		**28**	**-**	**6**

4.4. Практические (семинарские) занятия

№ п/п	Название темы	Объем часов		
		Очная форма	Очно-заочная форма	Заочная форма
Семестр 2		**28**	**-**	**6**
1	Восстановление зараженных файлов	2	-	2
2	Профилактика проникновения «троянских программ»	2	-	
3	Настройка безопасности почтового клиента	2	-	
4	Настройка параметров аутентификации	2	-	
5	Создание VPN-подключения	4	-	
6	Знакомство с сертифицированными программными и программно-аппаратными средствами защиты информации и контроля доступа. Аппаратные и программные средства защиты информации»	4	-	2
7	Защита программ и файлов от несанкционированного доступа	4	-	
8	Шифрование информации средствами операционной системы	4	-	
9	Настройка, изучение режимов работы и сравнение различных антивирусных пакетов. Антивирусное программное обеспечение.	2	-	2
10	Криптографические методы защиты информации.	4	-	
Итого		**28**	**-**	**6**

4.5. Лабораторные работы

Лабораторные работы не предусмотрены рабочим учебным планом.

4.6. Самостоятельная работа студентов

№ п/п	Название темы	Вид СРС	Объем часов		
			Очная форма	Очно-заочная форма	Заочная форма
Семестр 2			**52**	**-**	**123**
Тема 1	Общие вопросы информационной безопасности	Изучение теоретического материала. Поиск дополнительного материала по теме.	8	-	20
Тема 2	Государственная система информационной безопасности	Изучение теоретического материала. Поиск дополнительного материала по теме.	8	-	20
Тема 3	Угрозы безопасности	Изучение теоретического материала. Поиск дополнительного материала по теме.	8	-	20
Тема 4	Теоретические основы методов защиты информационных систем.	Изучение теоретического материала. Поиск дополнительного материала по теме.	8	-	20
Тема 5	Архитектура защищенных экономических систем	Изучение теоретического материала. Поиск дополнительного материала по теме.	10	-	20
Тема 6	Алгоритмы привязки программного обеспечения к аппаратному окружению	Изучение теоретического материала. Поиск дополнительного материала по теме.	10	-	23
Итого			**52**	**-**	**123**

4.7. Курсовые работы/проекты.

Курсовые работы или проекты не предусмотрены рабочим учебным планом.

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 практических заданий, самостоятельная работа с электронными образовательными

ресурсами (электронный конспект, размещенный во внутренней сети) при подготовке к лекциям, практическим занятиям; интерактивные лекции (презентации).

6. Формы контроля освоения дисциплины

Текущая аттестация студентов производится в дискретные временные интервалы лектором и преподавателем(ями), ведущими практические занятия по дисциплине в следующих формах:

- выполнение практических работ;
- защита практических 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 письменного экзамена, включающего теоретические вопросы.

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 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 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 чёткие 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. Кияев В.И., Безопасность информационных систем / Кияев В.И., Граничин О.Н. - М.: Национальный Открытый Университет "ИНТУИТ", 2016. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : http://www.studentlibrary.ru/book/intuit_040.html

2. Бахаров Л.Е., Информационная безопасность и защита информации (разделы криптография и стеганография) : практикум / Л.Е. Бахаров. - М. : МИСиС, 2019. - 59 с. - ISBN 978-5-906953-94-0 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : http://www.studentlibrary.ru/book/ISBN9785906953940.html

б) дополнительная литература:

1. Малюк А.А., Теория защиты информации / Малюк А.А. - М. : Горячая линия - Телеком, 2012. - 184 с. - ISBN 978-5-9912-0246-6 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : http://www.studentlibrary.ru/book/ISBN9785991202466.html

2. Шаньгин В.Ф., Защита компьютерной информации. Эффективные методы и средства / Шаньгин В.Ф. - М. : ДМК Пресс, 2010. - 544 с. - ISBN 978-5-94074-518-1 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : http://www.studentlibrary.ru/book/ISBN9785940745181.html

3. Ботуз С.П., УПРАВЛЕНИЕ УДАЛЕННЫМ ДОСТУПОМ / Защита интеллектуальной собственности в сети Internet / Ботуз С.П. - М. : СОЛОН-ПРЕСС, 2008. - 256 с. - ISBN 5-98003-289-4 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : http://www.studentlibrary.ru/book/ISBN5980032894.html

4. Шаньгин В.Ф., Защита компьютерной информации. Эффективные методы и средства / Шаньгин В.Ф. - М. : ДМК Пресс, 2010. - 544 с. - ISBN 978-5-94074-518-1 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : http://www.studentlibrary.ru/book/ISBN9785940745181.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 обеспечение дисциплины

Освоение дисциплины «Защита данных в сетях ЭВМ» 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).

Практические занятия: 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
Почтовый клиент	Mozilla Thunderbird	http://www.mozilla.org/ru/thunderbird
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
Антивирус	Kaspersky Free	https://www.kaspersky.ru/free-antivirus

9. Оценочные средства по дисциплине

Паспорт
оценочных средств по учебной дисциплине
«Защита данных в сетях ЭВМ»

Перечень компетенций (элементов компетенций), формируемых в результате освоения учебной дисциплины (модуля) или практики

№ п/п	Код контролируемой компетенции	Формулировка контролируемой компетенции	Индикаторы достижений компетенции (по реализуемой дисциплине	Контролируемые темы учебной дисциплины, практики	Этапы формирования (семестр изучения)
1.	ПК-1.	Знание методов оптимизации и умение применять их при решении задач профессиональной деятельности.	ПК-1.1. Знать: основные методы оптимизации информационно-управляющих систем; особенности обеспечения информационной безопасности в распределенных системах и центрах обработки информации; основные понятия нечеткой логики и нечетких систем управления. ПК-1.2. Уметь: применять классические методы оптимизации при решении задач профессиональной деятельности; применять методы защиты удаленного доступа. ПК-1.3. Владеть: классическими методами оптимизации при решении задач	Тема 1. Общие вопросы информационной безопасности	2
				Тема 2. Государственная система информационной безопасности	2
				Тема 3. Угрозы безопасности	2
				Тема 4. Теоретические основы методов защиты информационных систем.	2
				Тема 5. Архитектура защищенных экономических систем	2

			профессиональной деятельности; методами принятия решений, применяемые в экспертных системах.	Тема 6. Алгоритмы привязки программного обеспечения к аппаратному окружению	2
2.	ПК-4.	Способен осуществлять администрирование процесса поиска и диагностики ошибок сетевых устройств и программного обеспечения.	ПК-4.1. Знать: методы поиска и диагностики ошибок сетевых устройств и программного обеспечения. ПК-4.2. Уметь: определять ошибки сетевых устройств и операционных систем; документировать и устранять сбои и отказы сетевых устройств и операционных систем; работать с сетевыми протоколами. ПК-4.3. Владеть: навыками администрирования процесса поиска и диагностики ошибок сетевых устройств и программного обеспечения; методами работы с телекоммуникационными технологиями.	Тема 1. Общие вопросы информационной безопасности	2
				Тема 2. Государственная система информационной безопасности	2
				Тема 3. Угрозы безопасности	2
				Тема 4. Теоретические основы методов защиты информационных систем.	2
				Тема 5. Архитектура защищенных экономических систем	2
				Тема 6. Алгоритмы привязки программного обеспечения к аппаратному окружению	2

Показатели и критерии оценивания компетенций, описание шкал оценивания

№ п/п	Код контролируемой компет	Индикаторы достижений компетенции (по реализуемой	Перечень планируемых результатов	Контролируемые темы учебной дисциплины	Наименование оценочного средства

	енции	дисциплине)			
1.	ПК-1.	ПК-1.1. Знать: основные методы оптимизации информационно-управляющих систем; особенности обеспечения информационной безопасности в распределенных системах и центрах обработки информации; основные понятия нечеткой логики и нечетких систем управления. ПК-1.2. Уметь: применять классические методы оптимизации при решении задач профессиональной деятельности; применять методы защиты удаленного доступа. ПК-1.3. Владеть: классическими методами оптимизации при решении задач профессиональной деятельности; методами принятия решений, применяемые в экспертных системах.	Знать: основные методы оптимизации информационно-управляющих систем; особенности обеспечения информационной безопасности в распределенных системах и центрах обработки информации; основные понятия нечеткой логики и нечетких систем управления. Уметь: применять классические методы оптимизации при решении задач профессиональной деятельности; применять методы защиты удаленного доступа. Владеть: классическими методами оптимизации при решении задач профессиональной деятельности; методами принятия решений, применяемые в экспертных системах.	Тема 1, Тема 2, Тема 3, Тема 4, Тема 5, Тема 6.	Практические работы, защита практических работ
2.	ПК-4.	ПК-4.1. Знать: методы поиска и диагностики ошибок сетевых устройств и программного обеспечения. ПК-4.2. Уметь: определять ошибки сетевых устройств и операционных систем; документировать и устранять сбои и отказы сетевых устройств и операционных систем;	Знать: методы поиска и диагностики ошибок сетевых устройств и программного обеспечения. Уметь: определять ошибки сетевых устройств и операционных систем; документировать и устранять сбои и отказы сетевых устройств и операционных систем; работать с сетевыми	Тема 1, Тема 2, Тема 3, Тема 4, Тема 5, Тема 6.	Практические работы, защита практических работ

		работать с сетевыми протоколами. ПК-4.3. Владеть: навыками администрирования процесса поиска и диагностики ошибок сетевых устройств и программного обеспечения; методами работы с телекоммуникационными технологиями.	протоколами. Владеть: навыками администрирования процесса поиска и диагностики ошибок сетевых устройств и программного обеспечения; методами работы с телекоммуникационными технологиями.		

Оценочные средства по дисциплине «Защита данных в сетях ЭВМ»

Типовые задания для практических работ

Практическая работа 1

Тема: Восстановление зараженных файлов.

Цель работы: Научиться восстанавливать файл, заражённый макровирусом.

Практическая работа 2

Тема: Профилактика проникновения «троянских программ».

Цель работы: Освоить методику проверки потенциальных мест записей «троянских программ» в системном реестре операционной системы.

Практическая работа 3

Тема: Настройка безопасности почтового клиента.

Цель работы: Разработать систему правил по управлению входящими сообщениями в почтовом клиенте и настроить его для передачи сообщений с электронной цифровой подписью.

Практическая работа 4

Тема: Настройка параметров аутентификации.

Цель работы: Настроить параметры локальной политики безопасности операционной системы.

Практическая работа 5

Тема: Создание VPN-подключения.

Цель работы: Создать VPN-подключение и выполнить его настройку.

Практическая работа 6

Тема: Знакомство с сертифицированными программными и программно-аппаратными средствами защиты информации и контроля доступа. Аппаратные и программные средства защиты информации».

Цель работы: Ознакомится с современными аппаратными и программными средствами защиты информации.

Практическая работа 7

Тема работы: Защита программ и файлов от несанкционированного доступа.

Цель работы: Научиться устанавливать пароль для доступа к информации в текстовом файле.

Практическая работа 8

Тема: Шифрование информации средствами операционной системы.

Цель работы: Научиться шифровать файлы используя средства операционной системы.

Практическая работа 9

Тема: Настройка, изучение режимов работы и сравнение различных антивирусных пакетов. Антивирусное программное обеспечение.

Цель работы: Познакомиться с антивирусными программами. Научиться проверять компьютер на наличие вирусов.

Практическая работа 10

Тема: Криптографические методы защиты информации.

Цель работы: Изучить алгоритмы шифрования информации.

Критерии и шкала оценивания по оценочному средству «практические задания»

Шкала оценивания (интервал баллов)	Критерий оценивания
5	Задание по работе выполнено в полном объеме. Обучающийся свободно ориентируется в предложенном решении, может его модифицировать при изменении условия задачи. Отчет выполнен аккуратно и в соответствии с предъявляемыми требованиями.
4	Задание по работе выполнено в полном объеме. Обучающийся ориентируется в предложенном решении. Качество оформления отчета к работе не полностью соответствует требованиям
3	Обучающийся правильно выполнил задание к работе. Составил отчет в установленной форме, представил решения большинства заданий, предусмотренных в работе. Обучающийся не может полностью объяснить полученные результаты.
2	Обучающийся не выполнил все задания работы и не может объяснить полученные результаты.

Оценочные средства для промежуточной аттестации (экзамен)

ЛУГАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМ. В. ДАЛЯ

Кафедра компьютерных систем и сетей

Факультет: *КСИТ*

Дисциплина: *Защита данных в сетях ЭВМ*

Билет №1

1. Понятие информационной безопасности, ее цель. *1 балл*

2. Классификация каналов несанкционированного получения информации. *1 балл*

3. Применимость мер защиты. Надежность и восстановление ЭВМ. *1 балл*
4. Брандмауэры. Основные понятия. *1 балл*
5. Межсетевой экран. Классификация межсетевых экранов. *1 балл*

Утверждено на заседании кафедры КСС, протокол № от 20 г.

Заведующий кафедрой *доц. Попов С.В.*

Лектор *Аст С.А.*

Форма аттестации по результатам освоения дисциплины проходит в форме письменного экзамена, включающего теоретические вопросы.

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 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 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 чёткие 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.

Лист изменений и дополнений

№ п/п	Виды дополнений и изменений	Дата и номер протокола заседания кафедры (кафедр), на котором были рассмотрены и одобрены изменения и дополнения	Подпись (с расшифровкой) заведующего кафедрой (заведующих кафедрами)