МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Луганский государственный университет имени Владимира Даля»
(ФГБОУ ВО «ЛГУ им. В. Даля»)

Северодонецкий технологический институт
Кафедра информационных технологий, приборостроения и электротехники

УТВЕРЖДАЮ:
Врио. директора СТИ (филиал)
ФГБОУ ВО «ЛГУ им. В. Даля»
_____ Ю.В. Бородач
(подпись)
«16» 09 2024 года

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Технологии защиты информации»

По направлению подготовки: 09.03.02 «Информационные системы и технологии»

Профиль «Информационные ситемы и технологии»

Северодонецк – 2024

Лист согласования РПУД

Рабочая программа учебной дисциплины «Технологии защиты информации» по направлению подготовки: 09.03.02 «Информационные системы и технологии» (программа бакалавриата «Информационные ситемы и технологии») – 21 с.

Рабочая программа учебной дисциплины «Технологии защиты информации» разработана в соответствии Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 09.03.02 «Информационные системы и технологии» утвержденный приказом Министерства науки и высшего образования Российской Федерации от 19 сентября 2017 г. № 926 (с изменениями и дополнениями в соответствии с приказами Министерства образования и науки Российской Федерации №1456 от 26.11.2020 г., №83 от 08.02.2021 г., №662 от 19.07.2022 г., №208 от 27.02.2023 г.).

СОСТАВИТЕЛЬ:
старший преподаватель Рогозян Е.А.

Рабочая программа дисциплины утверждена на заседании кафедры информационных технологий, приборостроения и электротехники «_05_» _сентября_ 2024 г., протокол №_1_.

Заведующий кафедрой ИТПЭ _____ В.Г. Чебан

Переутверждена: «____» _____ 20___г., протокол №___.

Рекомендована на заседании учебно-методической комиссии Северодонецкого технологического института (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Луганский государственный университет имени Владимира Даля» «_16_» _сентября_ 2024 г., протокол №_1_.

Председатель учебно-методической комиссии
СТИ (филиал) ФГБОУ ВО «ЛГУ им. В.Даля» _____ Ю.В. Бородач

Структура и содержание дисциплины

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

Цель изучения дисциплины – формирование у студентов знаний в области теоретических основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах. А также рассматриваются вопросы построения систем защиты информации от несанкционированного доступа.

Задачи:

– изучение наиболее распространенных угроз информационной безопасности;

– изучение основных алгоритмов шифрования;

– изучение основных стандартов и спецификаций информационной безопасности;

– изучение основных методов защиты распределенных информационных систем;

– изучение комплексного подхода к обеспечению информационной безопасности.

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

Дисциплина «Технологии защиты информации» входит в обязательную часть учебного плана по направлению подготовки 09.03.02 Информационные системы и технологии.

Необходимыми условиями для освоения дисциплины являются: знание основ информатики, умение использовать информационные технологии для обработки информации, навыки работы в Интернете, в среде операционной системы.

Содержание дисциплины является логическим продолжением содержания дисциплин математический анализ; теория информации и кодирования; операционные системы, среды и оболочки и служит основой для освоения дисциплин инфокоммуникационные системы и сети, информационные системы электронного документооборота, web-программирование и web-дизайн.

3. Требования к результатам освоения содержания дисциплины

Студенты, завершившие изучение дисциплины «Технологии защиты информации», должны

знать:

– основные категории и аспекты информационной безопасности;

– характеристики наиболее распространенных нарушений безопасности информационных систем;

– основные законодательные, процедурные, административные и программно-технические меры обеспечения информационной безопасности;

– содержание основных отечественных и международных стандартов и спецификаций, действующих в области информационной безопасности;

– основы построения криптосистем, а также средств создания электронных цифровых подписей и аутентификации;

– особенности защиты распределенных информационных систем;

уметь:

– организовать процесс защиты информационных систем в соответствии с отечественными и международными стандартами в области информационной безопасности;

– определить уязвимые места в защите информационной системы, выбрать необходимые и экономически обоснованные защитные мероприятия на административном, процедурном и программно-техническом уровнях обеспечения безопасности;

– осуществлять программную реализацию наиболее распространенных криптоалгоритмов самостоятельно или с применением существующих криптографических модулей;

– адаптировать и применять существующие системы защиты информации от несанкционированного доступа;

владеть навыками:

– контроля безопасности информационных систем;

– системного анализа информационных систем.

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

общепрофессиональных:

ОПК-2 Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности.

4. Структура и содержание дисциплины

4.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов (з.е.)		
	Очная форма	Очно-заочная форма	Заочная форма
Объем учебной дисциплины (всего)	144 (4 з.е.)	-	144 (4 з.е.)
Обязательная аудиторная учебная нагрузка дисциплины (всего) в том числе:	70	-	14
Лекции	28	-	6
Семинарские занятия	-	-	-

Практические занятия	-	-	-
Лабораторные работы	42	-	8
Курсовая работа (курсовой проект)	-	-	-
Индивидуальное задание	-	-	-
Самостоятельная работа студента (всего)	74	-	130
Форма аттестации	экзамен	-	экзамен

4.2. Содержание разделов дисциплины

Тема 1. Основы информационной безопасности и защиты информации

Содержание темы: информация и информационная безопасность, основные составляющие информационной безопасности, объекты защиты, категории и носители информации, средства защиты информации.

Тема 2. История криптографии

Содержание темы: введение, наивная криптография, формальная криптография, математическая криптография.

Тема 3. Основные термины и определения. Классификация шифров

Содержание темы: основные термины и определения, основные требования, предъявляемые к криптосистемам, классификация криптографических систем.

Тема 4. Шифры замены

Содержание темы: основы шифрования, шифры однозначной замены, полиграммные шифры, омофонические шифры, полиалфавитные шифры, нерегулярные шифры.

Тема 5. Шифры перестановки

Содержание темы: основы шифрования перестановками, шифры одинарной перестановки, шифры множественной перестановки.

Тема 6. Шифр гаммирования

Содержание темы: основы шифрования гаммирования, генерация гаммы, RC4.

Тема 7. Квантовое шифрование

Содержание темы: основы квантовой физики, основы квантового шифрования.

Тема 8. Шифрование с открытым ключом

Содержание темы: основы шифрования, алгоритм RSA, алгоритм на основе задачи об укладке ранца, вероятностное шифрование, алгоритм шифрования Эль-Гамаля, алгоритм на основе эллиптических кривых.

Тема 9. Хеш-функция

Содержание темы: основные понятия хеш-функции, MD5, применение шифрования для получения хеш-образа.

Тема 10. Протоколы аутентификации (идентификации)

Содержание темы: общие сведения о протоколах аутентификации, парольная идентификация/аутентификация, протокол идентификации/ аутентификации с использованием хеш-функции, протокол идентификации/ аутентификации на основе шифрования с открытым ключом, сервер аутентификации Kerberos.

Тема 11. Протоколы электронной цифровой подписи

Содержание темы: Общие сведения о протоколах ЭЦП, протокол на базе алгоритма RSA, алгоритм цифровой подписи ГОСТ 34.10-94, алгоритм цифровой подписи ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012, разновидности ЭЦП, юридические основания использования ЭЦП.

Тема 12. Защита информации средствами биометрических данных

Содержание темы: описание предметной области, биометрические системы защиты информации, классификация биометрических характеристик, применение биометрических параметров

Тема 13. Основы криптоанализа

Содержание темы: угрозы безопасности при использовании криптографии, краткая история криптоанализа, общие сведения о криптоанализе.

Тема 14. Стеганография

Содержание темы: общие сведения о стеганографии, классическая стеганография, компьютерная стеганография.

4.3. Лекции

№ п/п	Название темы	Объем часов		
		Очная форма	Очно-заочная форма	Заочная форма
1	Основы информационной безопасности и защиты информации	2	-	1
2	История криптографии	2	-	-
3	Основные термины и определения. Классификация шифров	2	-	1
4	Шифры замены	2	-	-
5	Шифры перестановки	2	-	-
6	Шифры гаммирования	2	-	-
7	Квантовое шифрование	2	-	-
8	Шифрование с открытым ключом	2	-	1
9	Хеш-функция	2	-	-
10	Протоколы аутентификации (идентификации)	2	-	1
11	Протоколы электронной цифровой подписи	2	-	-
12	Защита информации средствами биометрических данных	2	-	1
13	Основы криптоанализа	2	-	1
14	Стеганография	2	-	-
Итого:		28	-	6

4.4. Практические (семинарские) занятия

Не предусмотрены.

4.5. Лабораторные работы

№ п/п	Название темы	Объем часов		
		Очная форма	Очно-заочная форма	Заочная форма
1	Защита информации с помощью пароля	2	-	1
2	Стеганографическое программное обеспечение	2	-	-
3	Классические криптографические системы	4	-	1
4	Методы сжатия информации	4	-	1
5	Дешифрирование шифра простой замены (симметричный алгоритм)	4	-	1
6	Криптографический алгоритм «методом перестановок»	4	-	1
7	Симметричная криптография. Простые шифры	4	-	1
8	Криптографический алгоритм serpent	2	-	-
9	Антивирусные программные продукты	4	-	-
10	Технология защиты сетевых компьютеров. Брандмауэр	4	-	-
11	Настройка параметров безопасности интернет - браузера	4	-	1
12	Средства защиты информации и обеспечения безопасности операционной системы	4	-	1
Итого:		42	-	8

4.6. Самостоятельная работа студентов

№ п/п	Название темы	Вид СРС	Объем часов		
			Очная форма	Очно-заочная форма	Заочная форма
1	Основы информационной безопасности и защиты информации	Подготовка к защите лабораторной работы Изучение дополнительного теоретического материала	4	-	8
2	История криптографии	Подготовка к защите лабораторной работы Изучение дополнительного теоретического материала	4	-	8
3	Основные термины и определения. Классификация шифров	Подготовка к защите лабораторной работы Изучение дополнительного теоретического материала	7	-	10
4	Шифры замены	Подготовка к защите лабораторной работы Изучение дополнительного теоретического материала	5	-	10
5	Шифры перестановки	Подготовка к защите лабораторной работы Изучение дополнительного теоретического материала	5	-	9
6	Шифры гаммирования	Подготовка к защите лабораторной работы	5	-	8

		Изучение дополнительного теоретического материала			
7	Квантовое шифрование	Подготовка к защите лабораторной работы Изучение дополнительного теоретического материала	5	-	8
8	Шифрование с открытым ключом	Подготовка к защите лабораторной работы Изучение дополнительного теоретического материала	7	-	10
9	Хеш-функция	Подготовка к защите лабораторной работы Изучение дополнительного теоретического материала	5	-	9
10	Протоколы аутентификации (идентификации)	Подготовка к защите лабораторной работы Изучение дополнительного теоретического материала	5	-	10
11	Протоколы электронной цифровой подписи	Подготовка к защите лабораторной работы Изучение дополнительного теоретического материала	5	-	9
12	Защита информации средствами биометрических данных	Подготовка к защите лабораторной работы Изучение дополнительного теоретического материала	7	-	12
13	Основы криптоанализа	Подготовка к защите лабораторной работы Изучение дополнительного теоретического материала	5	-	10
14	Стеганография	Подготовка к защите лабораторной работы Изучение дополнительного теоретического материала	5	-	9
Итого:			74	-	130

4.7. Курсовые работы/проекты.

Не предусмотрены.

5. Образовательные технологии

Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

– традиционные объяснительно-иллюстративные технологии, которые обеспечивают доступность учебного материала для большинства студентов, системность, отработанность организационных форм и привычных методов, относительно малые затраты времени;

– технологии проблемного обучения, направленные на развитие познавательной активности, творческой самостоятельности студентов и предполагающие последовательное и целенаправленное выдвижение перед студентом познавательных задач, разрешение которых позволяет студентам активно усваивать знания (используются поисковые методы; постановка познавательных задач);

– технологии развивающего обучения, позволяющие ориентировать учебный процесс на потенциальные возможности студентов, их реализацию и развитие;

– технологии концентрированного обучения, суть которых состоит в создании максимально близкой к естественным психологическим особенностям человеческого восприятия структуры учебного процесса и которые дают возможность глубокого и системного изучения содержания учебных дисциплин за счет объединения занятий в тематические блоки;

– технологии модульного обучения, дающие возможность обеспечения гибкости процесса обучения, адаптации его к индивидуальным потребностям и особенностям обучающихся (применяются, как правило, при самостоятельном обучении студентов по индивидуальному учебному плану);

– технологии дифференцированного обучения, обеспечивающие возможность создания оптимальных условий для развития интересов и способностей студентов, в том числе и студентов с особыми образовательными потребностями, что позволяет реализовать в культурно-образовательном пространстве университета идею создания равных возможностей для получения образования;

– технологии активного (контекстного) обучения, с помощью которых осуществляется моделирование предметного, проблемного и социального содержания будущей профессиональной деятельности студентов (используются активные и интерактивные методы обучения) и т.д.

Максимальная эффективность педагогического процесса достигается путем конструирования оптимального комплекса педагогических технологий и (или) их элементов на личностно-ориентированной, деятельностной, диалогической основе и использования необходимых современных средств обучения.

6. Формы контроля освоения дисциплины

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

- лабораторные работы;
- защита лабораторных работ.

Фонды оценочных средств, включающие типовые задания, контрольные работы, 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».

Промежуточная аттестация по результатам освоения дисциплины проходит в форме письменного экзамена, включающего теоретические вопросы и практические задания. В случае неполного, спорного или некорректного выполнения задания письменного экзамена, допускается уточняющий устный опрос студента, на основании которого возможна корректировка оценки результатов промежуточной аттестации. Допуск к

промежуточной аттестации производится на основании положительных результатов по всем формам текущего контроля.

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 объеме 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 четкие 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. Костин В.Н., Методы и средства защиты компьютерной информации: законодательные и нормативные акты по защите информации: учеб. пособие / В.Н. Костин - М : МИСиС, 2017. - 26 с. - ISBN 978-5-906846-

87-7 - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: http://www.studentlibrary.ru/book/ISBN9785906846877.html

2. Малюк А.А., Защита информации в информационном обществе: Учебное пособие для вузов. / А.А. Малюк - М.: Горячая линия - Телеком, 2015. - 230 с. - ISBN 978-5-9912-0481-1 - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: http://www.studentlibrary.ru/book/ISBN9785991204811.html

3. Краковский Ю.М., Защита информации : учебное пособие / Ю.М. Краковский - Ростов н/Д: Феникс, 2016. - 347 с. (Высшее образование) - ISBN 978-5-222-26911-4 - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: http://www.studentlibrary.ru/book/ISBN9785222269114.html

4. Кирпичников А.П., Криптографические методы защиты компьютерной информации: учебное пособие / Кирпичников А. П. - Казань: Издательство КНИТУ, 2016. - 100 с. - ISBN 978-5-7882-2052-9 - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: http://www.studentlibrary.ru/book/ISBN9785788220529.html

б) дополнительная литература:

1. Аверченков В.И., Криптографические методы защиты информации / Аверченков В.И. - М.: ФЛИНТА, 2017. - 215 с. - ISBN 978-5-9765-2947-2 - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: http://www.studentlibrary.ru/book/ISBN9785976529472.html

2. Моделирование криптосистем / Левина А.Б. - СПб.: ИЦ Интермедия, 2017. - ISBN 978-5-4383-0136-3 - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: http://www.studentlibrary.ru/book/ISBN9785438301363.html

3. Антивирусная защита компьютерных систем / - М.: Национальный Открытый Университет "ИНТУИТ", 2016. - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: http://www.studentlibrary.ru/book/intuit032.html

в) Интернет-ресурсы:

Портал по информационной безопасности: http://infosecurity.report.ru/

Российский криптографический портал: http://www.cryptography.ru/

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 «Технологии защиты информации» предполагает использование академических аудиторий, соответствующих действующим санитарным и противопожарным правилам и нормам.

Лекционные занятия: проекционное оборудование для проведения лекционных занятий.

Лабораторные работы: лаборатория информационных систем и технологий, оснащенная компьютерной сетью, специализированным ПО, шаблоны отчетов по лабораторным работам.

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/

Паспорт
фонда оценочных средств по учебной дисциплине
«Технологии защиты информации»

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

№ п/п	Код контролируемой компетенции	Формулировка контролируемой компетенции	Контролируемые темы учебной дисциплины	Этапы формирования (семестр изучения)
1	ОПК-2	Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности	Тема 1. Основы информационной безопасности и защиты информации Тема 2. История криптографии Тема 3. Основные термины и определения. Классификация шифров Тема 4. Шифры замены Тема 5. Шифры перестановки Тема 6. Шифры гаммирования Тема 7. Квантовое шифрование Тема 13. Основы криптоанализа Тема 14. Стеганография	начальный (5)
			Тема 8. Шифрование с открытым ключом Тема 9. Хеш-функция Тема 10. Протоколы аутентификации (идентификации) Тема 11. Протоколы электронной цифровой подписи Тема 12. Защита информации средствами биометрических данных	продвинутый (5)

Показатели и критерии оценивания компетенций, описание шкал оценивания

№ п/п	Код контролируемой компетенции	Показатель оценивания (знания, умения, навыки)	Контролируемые темы учебной дисциплины	Наименование оценочного средства
1	ОПК-2	Знать: принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности; Уметь: выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности; Иметь навыки: применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.	Тема 1, Тема 2, Тема 3, Тема 4, Тема 5, Тема 6, Тема 7, Тема 8, Тема 9, Тема 10, Тема 11, Тема 12, Тема 13, Тема 14	Защита лабораторных работ, контрольные работы, промежуточная аттестация (экзамен)

Фонды оценочных средств по дисциплине «Технологии защиты информации»

Фонд оценочных средств по дисциплине «Технологии защиты информации» предназначен для аттестации обучающихся на соответствие их персональных достижений поэтапным требованиям образовательной программы, в том числе рабочей программы дисциплины «Технологии защиты информации», для оценивания результатов обучения: знаний, умений, владений и уровня приобретенных компетенций.

Фонд оценочных средств по дисциплине «Технологии защиты информации» включает:

1. Оценочные средства для проведения текущего контроля успеваемости:

– комплект заданий репродуктивного уровня для выполнения на лабораторных занятиях, позволяющих оценивать и диагностировать знание фактического материала (базовые понятия, законы, принципы, факты) и умение правильно использовать терминологию и понятия, распознавание объектов изучения в рамках определенного раздела дисциплины;

– контрольные работы;

– перечень вопросов для защиты отчётов по лабораторным работам.

2. Оценочные средства для промежуточной аттестации.

Оценочные средства для текущего контроля знаний по дисциплине «Технологии защиты информации»

В целях закрепления практического материала и углубления теоретических знаний по разделам дисциплины «Технологии защиты информации» предполагается выполнение лабораторных работ, что позволяет углубить процесс познания, раскрыть понимание прикладной значимости осваиваемой дисциплины.

Критерии и шкала оценивания лабораторных работ

Шкала оценивания (интервал баллов)	Критерии оценивания
отлично (5)	Задание выполнено полностью, в представленном отчете обоснованно получено правильное выполненное задание.
хорошо (4)	Задание выполнено полностью, но нет достаточного обоснования или при верном решении допущена незначительная ошибка, не влияющая на правильную последовательность рассуждений.
удовлетворительно (3)	Задания выполнены частично.
неудовлетворительно (2)	Задание не выполнено.

Вопросы для защиты отчётов по лабораторным работам

1. Какие виды атак на пароль Вы знаете?
2. Какие правила должны соблюдаться при использовании аутентификации на основе паролей?
3. Что такое плохой пароль? Что такое хороший пароль?
4. Как можно противостоять атаке полным перебором?
5. Как длина пароля влияет на вероятность раскрытия пароля?
6. Какие правила снижения уязвимости паролей, направленные на противодействие известным атакам на них?

7. Дайте определение стеганографии и компьютерной стеганографии.
8. Назовите принципы и методы стеганографического программного обеспечения для защиты информации.
9. Какие современные стеганографические программные пакеты Вы знаете?
10. Какое стеганографическое программное обеспечение использовалось Вами в данной работе?
11. Дайте названия классических криптографических систем.
12. Назовите классические криптографические алгоритмы.
13. Что называют сжатием информации?
14. Что такое кодирование и декодирование информации?
15. Что означает термин «эффективное кодирование» информации?
16. В чем суть основной теоремы Шеннона для канала без помех?
17. Приведите примеры использования формулы Хартли
18. Что означает закон аддитивности информации?
19. Опишите алгоритм эффективного кодирования по Шеннону
20. Что означает избыточность кода?
21. Опишите алгоритм эффективного кодирования по Хаффману
22. От чего зависит возможность дешифрования какого-либо шифра?
23. Каковы наиболее устойчивые закономерности открытого сообщения?
24. Назовите 10 наиболее вероятных букв русского языка.
25. Что такое биграмма? Какова наиболее часто встречаемая биграмма?
26. Опишите алгоритм дешифрования шифра простой замены.
27. Каковы недостатки шифра простой замены?
28. Дайте определения криптоанализа.
29. Что такое ключ?
30. Какие методы шифрования используются в лабораторной работе?
31. Каковы наиболее устойчивые закономерности открытого сообщения?
32. На чем основан метод «вскрытия» шифров двойной перестановки?
33. Какой шифр называется шифром подстановки?
34. Какой шифр называется шифром перестановки?
35. Какой шифр называется поворотной решеткой?
36. Какой шифр называется шифром вертикальной перестановки?
37. К какому классу шифров относится шифр Цезаря?
38. Что такое гамма и гаммирование?
39. В чем заключается шифрование по Вижинеру?

Критерии и шкала оценивания по оценочному средству защита лабораторных работ

Шкала оценивания (интервал баллов)	Критерии оценивания
отлично (5)	Ответ на вопрос раскрыт полностью, в представленном ответе обоснованно получен правильный ответ
хорошо (4)	Ответ дан полностью, но нет достаточного обоснования или при верном ответе допущена незначительная ошибка, не влияющая на правильную последовательность рассуждений
удовлетворительно (3)	Ответы даны частично
неудовлетворительно (2)	Ответ неверен или отсутствует

Оценочные средства для промежуточной аттестации (экзамен)

Теоретические вопросы

1. Информация. Виды информации. Ценность информации.
2. Защита информации средствами голосовой биометрии.
3. Объект, предмет защиты информации.
4. Защита информации средствами биометрических параметров человека (сетчатка глаза).
5. Угрозы информационной безопасности.
6. Защита информации средствами биометрических параметров человека (радужная оболочка глаза).
7. Основные способы защиты информации.
8. Защита информации средствами биометрических параметров человека (отпечаток пальца).
9. Шифр Гая Юлия Цезаря.
10. Защита информации средствами биометрических параметров человека (форма лица).
11. Шифр перестановки.
12. Защита информации средствами биометрических параметров человека (форма ладони).
13. Прибор Сцитала.
14. Сравнительная характеристика защиты информации средствами биометрических параметров человека.
15. Квадрат Полибия.
16. Защита информации средствами биометрических параметров человека (сетчатка глаза).
17. Классификация вторжений в ВС.
18. Защита информации средствами голосовой биометрии.
19. Потенциальные угрозы в сети.
20. Защита информации средствами биометрических параметров человека (радужная оболочка глаза).
21. Классы защиты информации в ВС.

22. Защита информации средствами биометрических параметров человека (отпечаток пальца).
23. Физическая защита данных в сети.
24. Защита информации средствами биометрических параметров человека (форма лица).
25. Аутентификация. Авторизация.
26. Защита информации средствами биометрических параметров человека (форма ладони).
27. Брандмауэры. Архитектура брандмауэров
28. Сравнительная характеристика защиты информации средствами биометрических параметров человека.
29. Криптография. Криптоанализ.
30. Защита информации средствами биометрических параметров человека (сетчатка глаза).
31. Электронная цифровая подпись.
32. Защита информации средствами голосовой биометрии
33. Шифр простой замены
34. Защита информации средствами биометрических параметров человека (радужная оболочка глаза).
35. Стеганография.
36. Защита информации средствами биометрических параметров человека (отпечаток пальца).
37. Методы сжатия информации (Шеннон - Фоно).
38. Защита информации средствами биометрических параметров человека (форма лица).
39. Методы сжатия информации (Хаффмана).
40. Защита информации средствами биометрических параметров человека (форма ладони).
41. Вирусы.
42. Сравнительная характеристика защиты информации средствами биометрических параметров человека
43. Фрактальное сжатие изображения.
44. Защита информации средствами биометрических параметров человека (сетчатка глаза).
45. Программные методы защиты информации.
46. Защита информации средствами голосовой биометрии.
47. Основные требования, предъявляемые к системе защиты от копирования.
48. Защита информации средствами биометрических параметров человека (радужная оболочка глаза).

Типовой экзаменационный билет:

ФГБОУ ВО «ЛУГАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ ВЛАДИМИРА ДАЛЯ»

Кафедра Информационных и управляющих систем
Дисциплина «Информационные технологии»
Семестр 5

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Информация. Виды информации. Ценность информации.
2. Защита информации средствами голосовой биометрии.

Утверждено на заседании кафедры ___.___._____ г.
Протокол № ____

Зав.кафедрой_____доц.Горбунов А.И. Экзаменатор_____доц.Черных В.В.

Критерии и шкала оценивания по оценочному средству промежуточная аттестация (экзамен)

Шкала оценивания (интервал баллов)	Критерий оценивания
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)