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)
«26» 09 2024 года

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Защита информации»

По направлению подготовки: 09.03.01 Информатика и вычислительная техника

Профиль: Компьютерные системы и сети

Северодонецк – 2024

Лист согласования РПУД

Рабочая программа учебной дисциплины «Защита информации» по направлению подготовки 09.03.01 Информатика и вычислительная техника (профиль «Компьютерные системы и сети») – 23 с.

Рабочая программа учебной дисциплины «Защита информации» разработана в соответствии федеральным государственным образовательным стандартом высшего образования – бакалавриат по направлению подготовки 09.03.01 Информатика и вычислительная техника, утвержденным приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. № 929 (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. и № 208 от 27.02.2023 г.).

СОСТАВИТЕЛЬ:
ст. преподаватель Кузнецова Е.В.

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

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 ОПОП ВО

Дисциплина входит в базовую часть профессионального цикла дисциплин подготовки студентов по направлению подготовки 09.03.01 Информатика и вычислительная техника.

Основывается на базе дисциплин: теория информации и кодирования; программирование; практикум по программированию.

Является основой для изучения следующих дисциплин: администрирование баз данных; веб-программирование; проблемно-ориентированные вычислительные системы.

3. Требования к результатам освоения содержания дисциплины

Код и наименование компетенции	Индикаторы достижений компетенции (по реализуемой дисциплине)	Перечень планируемых результатов
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.2 Способен учитывать основные требования информационной безопасности при решении стандартных задач профессиональной деятельности	**Знать**: понятие информации, способы ее представления, основные приемы получения, хранения, обработки информации; стандартные программные средства набора текста и баз данных; правовые акты в области защиты государственной тайны и информационной безопасности; правовые основы организации защиты государственной тайны и конфиденциальной информации; основные понятия информационной безопасности; основные принципы организации и алгоритмы функционирования систем безопасности в современных операционных системах и оболочках; возможности применения в работе современных системных программных средств: операционных систем, операционных оболочек, обслуживающих программ; основные принципы организации и алгоритмы функционирования операционных систем и оболочек; проблемы и направления развития системных программных средств. **Уметь**: использовать программные и аппаратные средства персонального компьютера; ориентироваться в современной

		системе источников информации; использовать современные информационные технологии в своей профессиональной деятельности; применять средства антивирусной защиты; анализировать информационную безопасность многопользовательских систем; пользоваться программными средствами, реализующими основные криптографические функции системы публичных ключей, цифровую подпись, разделение доступа; видеть и формулировать проблему, видеть конкретную ситуацию, прогнозировать и предвидеть, рассчитывать риски, ставить цели и задачи. **Владеть**: применения аппаратных и программных средств обеспечения информационной безопасности; противостояния типовым удаленным атакам; обеспечения безопасной работы на компьютере; поиска информации в глобальной информационной сети Интернет, работы с базами данных и Интернет-ресурсами; современной терминологией и методологией в области информационной безопасности.

4. Структура и содержание дисциплины

4.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем часов**	
	Очная форма	**Заочная форма**
Общая учебная нагрузка (всего)	**216 (6 зач. ед)**	**216 (6 зач. ед)**
Обязательная аудиторная учебная нагрузка (всего) в том числе:	**68**	**12**
Лекции	34	6
Семинарские занятия	-	-
Практические занятия	-	-
Лабораторные работы	34	6
Курсовая работа (курсовой проект)	36	36
Другие формы и методы организации образовательного процесса (*расчетнографические работы, групповые дискуссии, ролевые игры, тренинг, компьютерные симуляции, интерактивные лекции,* *семинары, анализ деловых ситуаций и т.п.)*	-	-
Самостоятельная работа студента (всего)	**112**	**168**
Итоговая аттестация	экзамен, курсовая работа	экзамен, курсовая работа

4.2. Содержание разделов дисциплины

ТЕМА 1 КЛАССИФИКАЦИЯ И ХАРАКТЕРИСТИКА УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ.

Понятие угроз безопасности. Классификация угроз информационной безопасности. Основная классификация угроз: угрозы нарушения конфиденциальности информации, угрозы нарушения целостности информации, угрозы нарушения доступности информации. Методы перечисления угроз. Случайные и преднамеренные угрозы. Технологические возможности злоумышленников по преодолению систем защиты информации. Признаки угрозы безопасности информации в распределенных вычислительных системах (РВС): по характеру воздействия; по цели воздействия; по условию начала осуществления воздействия; по наличию обратной связи с атакуемым объектом; по расположению субъекта атаки относительно атакуемого объекта; по уровню эталонной модели ISO/OSI, на котором осуществляется воздействие.

ТЕМА 2. СТАНДАРТЫ И СПЕЦИФИКАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Понятие стандарта. Классификация стандартов в области информационной безопасности. «Оранжевая книга», ее структура и группы классов защищенности. Руководящие документы Гостехкомиссии России. Понятие несанкционированного доступа (НСД). Направления защиты от НСД. Основные способы НСД. Принципы защиты от НСД.

ТЕМА 3. АДМИНИСТРАТИВНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. УПРАВЛЕНИЕ РИСКАМИ. ПРОЦЕДУРНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Уровни защиты информации. Ключевые понятия информационной безопасности - политика безопасности и программа безопасности. Структура соответствующих документов, меры по их разработке и сопровождению. Этапы жизненного цикла информационных систем и меры безопасности. Методика, позволяющая сопоставить возможные потери от нарушений ИБ со стоимостью защитных средств. Оценка рисков: выбор анализируемых объектов и уровня детализации их рассмотрения; выбор методологии оценки рисков; идентификация активов; анализ угроз и их последствий, выявление уязвимых мест в защите; оценка рисков; выбор защитных мер; реализация и проверка выбранных мер; оценка остаточного риска.

ТЕМА 4. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ, УПРАВЛЕНИЕ ДОСТУПОМ.

Техническое обеспечение информационной безопасности. Понятие сервиса безопасности. Понятие архитектурной безопасности. Классификация сервисов безопасности. Средства идентификации и аутентификации пользователей. Идентификация и аутентификация, управление доступом. Парольная аутентификация. Одноразовые пароли. Система S/KEY компании Bellcore. Сервер аутентификации Kerberos. Идентификация/аутентификация с помощью биометрических данных. Управление доступом. Матрица доступа. Произвольное (или дискреционное) управление доступом. Принудительное (мандатное) управление доступом. Списки управления доступом. Ограничивающий интерфейс. Ролевое управление доступом. Статическое разделение обязанностей. Динамическое разделение обязанностей.

ТЕМА 5. МЕТОДЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ. ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ.

Основные понятия и классификация средств криптографической защиты информации. Криптографические методы защиты информации. Методы стеганографии. Аппаратно-

программные средства защиты информации: средства обеспечения конфиденциальности данных; средства аутентификации электронных данных и средства управления ключевой информацией. Классификация методов шифрования. Требования к современным шифрам. Методы симметричного шифрования. Блочное и потоковое шифрование. Классическая сеть Фейстеля. Алгоритм шифрования DES и его модификации. Абсолютно надежный шифр. Основные свойства симметричных криптосистем. Основные свойства асимметричных криптосистем.

Генерация и хранение ключей. Распределение ключей. Управление ключами в системах с открытым ключом. Алгоритм Диффи-Хелмана. Основные свойства хэшфункций. Основные свойства цифровой подписи. Алгоритм цифровой подписи RSA. Алгоритм цифровой подписи Эль Гамаля. Алгоритм цифровой подписи DSA. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-94. Схемы слепой подписи.

Схемы неоспоримой подписи. Защита информации при работе в сети

ТЕМА 6. ПРОТОКОЛИРОВАНИЕ И АУДИТ, КОНТРОЛЬ ЦЕЛОСТНОСТИ.

Протоколирование и аудит, их место в общей архитектуре безопасности. Активный аудит. Подозрительная активность. Сигнатура атаки. Функциональные компоненты, входящие в состав средств активного аудита. Применение аудита в ОС семейства Windows для отслеживания деятельности пользователей. Настройка политики аудита. Аудит в Windows Server 2008/2012.

ТЕМА 7. ЭКРАНИРОВАНИЕ, АНАЛИЗ ЗАЩИЩЕННОСТИ. ОБЕСПЕЧЕНИЕ ВЫСОКОЙ ДОСТУПНОСТИ. ТУННЕЛИРОВАНИЕ.

Понятие демилитаризованной зоны. Механизмы защиты, реализуемые межсетевым экраном (МЭ): фильтрация сетевого трафика; шифрование (создание VPN); трансляция адресов; аутентификация (дополнительная); противодействие некоторым сетевым атакам (наиболее распространённым); управление списками доступа на маршрутизаторах. Типы МЭ. Пакетные фильтры. Шлюзы уровня соединения. Шлюзы прикладного уровня.

Технологии Proxy и Stateful inspection. Концепция построения защищённых виртуальных частных сетей VPN. Функции и компоненты сети VPN. VPN решения для построения защищённых корпоративных сетей.

Два вида средств поддержания высокой доступности: обеспечение отказоустойчивости (нейтрализация отказов, живучесть) и обеспечение безопасного и быстрого восстановления после отказов (обслуживаемость).

ТЕМА 8. ЗАЩИТА КОМПЬЮТЕРНЫХ СИСТЕМ ОТ ВИРУСОВ И ВРЕДОНОСНЫХ ПРОГРАММ

Классификация компьютерных вирусов и вредоносных программ. Файловые, загрузочные и сетевые вирусы. Методы и средства борьбы с вирусами и вредоносными программами. Профилактика заражения вирусами компьютерных систем и порядок действий пользователей в случае заражения. Механизмы распространения вирусов. Каналы распространения вирусов. Классические компьютерные вирусы. Макровирусы. Троянские программы. Сетевые черви. Антивирусное ПО. Обнаружение компьютерных вирусов. Комплексная система защиты информации.

4.3. Лекции

№ п/п	Название темы	Объем часов	
		Очная форма	Заочная форма
1	Тема 1 Классификация и характеристика угроз безопасности информации	4	0,5
2	Тема 2. Стандарты и спецификации в области информационной безопасности	4	0,5
3	Тема 3. Административный уровень информационной безопасности. Управление рисками. Процедурный уровень информационной безопасности	4	0,5
4	Тема 4. Идентификация и аутентификация, управление доступом	4	0,5
5	Тема 5. Методы криптографической защиты информации. Электронная цифровая подпись	4	1
6	Тема 6. Протоколирование и аудит, контроль целостности	4	1
7	Тема 7. Экранирование, анализ защищенности. Обеспечение высокой доступности. Туннелирование	6	1
8	Тема 8. Защита компьютерных систем от вирусов и вредоносных программ	4	1
Итого:		**34**	**6**

4.4. Практические (семинарские) занятия

Практические занятия не предусмотрены.

4.5. Лабораторные работы

№ п/п	Название темы	Объем часов	
		Очная форма	Заочная форма
1	Лабораторная работа № 1 Аудит реестра в операционной системе Windows	2	0,5
2	Лабораторная работа № 2 Получение информации о настройках протокола TCP/IP и выполнение его настройки	2	0,5
3	Лабораторная работа № 3 Разграничение прав пользователей в защищенных версиях операционной системы Windows	4	0,5
4	Лабораторная работа № 4 Реализация политики безопасности в защищенных версиях операционной системы Windows	4	0,5
5	Лабораторная работа № 5 Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows	4	1
6	Лабораторная работа № 6 Использование программной системы PGP для обеспечения конфиденциальности и целостности информационных ресурсов	4	1
7	Лабораторная работа № 7 Использование программных средств контроля и анализа выполнения политики безопасности на примере операционной системы Windows	4	1
8	Лабораторная работа № 8 Изучение штатных средств операционной системы Windows, предназначенных для обеспечения информационной безопасности при использовании глобальных вычислительных сетей	10	1
Итого:		**34**	**6**

4.6. Самостоятельная работа студентов

№ п/п	Название темы	Вид СРС	Объем часов	
			Очная форма	Заочная форма
1	Тема 1 Классификация и характеристика угроз безопасности информации	Подготовка к лабораторным работам и оформление отчетов	8	15
2	Тема 2. Стандарты и спецификации в области информационной безопасности	Подготовка к лабораторным работам и оформление отчетов	9	16
3	Тема 3. Административный уровень информационной безопасности. Управление рисками. Процедурный уровень информационной безопасности	Подготовка к лабораторным работам и оформление отчетов	9	16
4	Тема 4. Идентификация и аутентификация, управление доступом	Подготовка к лабораторным работам и оформление отчетов	9	16
5	Тема 5. Методы криптографической защиты информации. Электронная цифровая подпись	Подготовка к лабораторным работам и оформление отчетов	9	16
6	Тема 6. Протоколирование и аудит, контроль целостности	Подготовка к лабораторным работам и оформление отчетов	9	16
7	Тема 7. Экранирование, анализ защищенности. Обеспечение высокой доступности. Туннелирование	Подготовка к лабораторным работам и оформление отчетов	9	16
8	Тема 8. Защита компьютерных систем от вирусов и вредоносных программ	Подготовка к лабораторным работам и оформление отчетов	9	16
9	Курсовая работа	Выполнение курсовой работы	36	36
Итого:			**107**	**163**

4.7. Курсовые работы/проекты.

1. Защита систем трансляции, передачи сообщений и электропитания.
2. Защита помещения от утечки акустической информации через акустоэлектрические преобразователи телефонной цепи и аппарата.
3. Акустопреобразовательные элементы с передачей информативного сигнала радиоизлучением.
4. Акустоэлектрические преобразователи, технические характеристики акустопреобразовательного канала.
5. Криптографическая защита телефонных сообщений.
6. Активные способы защиты телефонных линий.
7. Пассивные способы защиты телефонных линий.
8. Телефонная линия как канал утечки информации, индуктивный и бесконтактный съем информации с телефонной линии.
9. Комбинированные способов технической защиты телефонных линий.
10. Способы технической защиты в IP телефонии.
11. Радиозакладные устройства.

12. Сетевые закладные устройства.
13. Средства и способы обнаружения радиозакладных устройств.
14. Комплексы мониторинга технических каналов утечки информации.
15. Активное противодействие закладным радиоустройствам.
16. Акустические устройства перехвата информации.
17. Защита конфиденциальной акустической информации от несанкционированной аудио записи.
18. Портативные средства аудиозаписи, способы и средства противодействия.
19. Переносные средства аудиозаписи, способы и средства противодействия.
20. Способы и средства проверки звукоизоляции помещений.
21. Средства контроля эффективности акустической защиты.
22. Аппаратно-программные комплексы виброакустических измерений.
23. Пассивные способы защиты акустической информации.
24. Активные способы защиты акустической информации.
25. Комплексные системы защиты акустической информации.
26. Защита конфиденциальной информации от несанкционированной видео записи.
27. Портативные средства видеозаписи, способы и средства противодействия.
28. Переносные средства видеозаписи, способы и средства противодействия.
29. Технические каналы утечки информации.
30. Технические средства информационной разведки и промышленного шпионажа.

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. Учебно-методическое и программно-информационное обеспечение дисциплины:

а) основная литература:

1. Ищейнов В.Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации. - М.: Форум : ИНФРА-М, 2014.

2. Мельников В. П. Информационная безопасность и защита информации. - М.: Академия, 2008.

3. Информационная безопасность открытых систем. - М.: Горячая линия-Телеком, 2008.

б) дополнительная литература:

1. Леванский В.А. Моделирование в социально-правовых исследованиях. М.: Наука, 1986. 160 с.

2. Наумов В.Б. Право и Интернет: Очерки теории и практики. - М.: Книжный дом «Университет», 2002.

3. Норткатт С., Новак Д. Обнаружение вторжений в сеть. Настольная книга специалиста по системному анализу, Москва - Лори, 2001.

4. Овчинский А.С. Информация и оперативно-розыскная деятельность. –М.: ИнфраМ, 2002. 97 с.

в) интернет-ресурсы:

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

2. Министерства природных ресурсов и экологии Российской Федерации – http://www.mnr.gov.ru

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

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

5. Министерство природных ресурсов и экологической безопасности ЛНР – https://www.mprlnr.su

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

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

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

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

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

Электронные библиотечные системы и ресурсы:

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

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

3. Научная электронная библиотека eLIBRARI.RU» – http://elibrary.ru

4. ЭБС Издательства «ЛАНЬ» – https://e.lanbook.com

Информационный ресурс библиотеки образовательной организации

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

7. Материально-техническое обеспечение дисциплины

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

Прочее: рабочее место преподавателя, оснащенное компьютером с доступом в Интернет; для проведения лекционных занятий требуется аудитория на курс, оборудованная мультимедийным проектором с экраном; для проведения лабораторных работ требуется компьютерный класс, подключенный к 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/

8. Оценочные средства по учебной дисциплине Паспорт фонда оценочных средств по учебной дисциплине

Защита информации

(наименование учебной дисциплины)

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

№ п/п	Код контроли-руемой компетенции	Формулировка контролируемой компетенции	Индикаторы достижений компетенции (по реализуемой дисциплине)	Контроли-руемые разделы (темы) учебной дисциплины (модуля), практики	Этапы формирования (семестр изучения)
1.	ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.2 Способен учитывать основные требования информационной безопасности при решении стандартных задач профессиональной деятельности	Тема 1. Тема 2. Тема 3. Тема 4. Тема 5. Тема 6. Тема 7. Тема 8.	5

Показатели и критерии оценивания компетенций, описание шкал оценивания

№ п/п	Код контроли-руемой компетенции	Индикаторы достижений компетенций (по реализуемой дисциплине)	Перечень планируемых результатов	Контроли-руемые разделы (темы) учебной дисциплины (модуля), практики	Наименование оценочного средства
1	ОПК-3	ОПК-3.2	**Знать**: понятие информации, способы ее представления, основные приемы получения, хранения, обработки информации; стандартные программные средства набора текста и баз данных; правовые акты в области защиты государственной тайны и информационной безопасности; правовые основы организации защиты государственной тайны и конфиденциальной	Тема 1. Тема 2. Тема 3. Тема 4. Тема 5. Тема 6. Тема 7. Тема 8.	Собеседование (устный или письменный опрос), контрольная работа.

			информации; основные понятия информационной безопасности; основные принципы организации и алгоритмы функционирования систем безопасности в современных операционных системах и оболочках; возможности применения в работе современных системных программных средств: операционных систем, операционных оболочек, обслуживающих программ; основные принципы организации и алгоритмы функционирования операционных систем и оболочек; проблемы и направления развития системных программных средств. **Уметь**: использовать программные и аппаратные средства персонального компьютера; ориентироваться в современной системе источников информации; использовать современные информационные технологии в своей профессиональной деятельности; применять средства антивирусной защиты; анализировать информационную безопасность многопользовательских систем; пользоваться программными средствами, реализующими основные криптографические функции системы публичных ключей, цифровую подпись, разделение доступа; видеть и формулировать проблему, видеть конкретную ситуацию, прогнозировать и предвидеть, рассчитывать риски, ставить цели и задачи. **Владеть**: применения аппаратных и программных средств обеспечения		

			информационной безопасности; противостояния типовым удаленным атакам; обеспечения безопасной работы на компьютере; поиска информации в глобальной информационной сети Интернет, работы с базами данных и Интернет-ресурсами; современной терминологией и методологией в области информационной безопасности		

Фонды оценочных средств по дисциплине «Защита информации»

Перечень вопросов (для проведения собеседования (устный или письменный опрос))

1. Стандарты в области информационной безопасности.
2. Международные стандарты информационного обмена.
3. Понятие угрозы, атаки.
4. Понятие нарушителя информационной безопасности.
5. Понятие государственной, коммерческой, личной тайны.
6. Основные нормативные документы в этой области.
7. Порядок рассекречивания документов.
8. Уровень тайны.
9. Понятие угрозы нарушения режима безопасности.
10. Причины нарушения информационной безопасности.
11. Предпосылки угроз
12. Аудит событий в рамках информационной системы.
13. Реализация законодательного уровня защиты информации в РФ. Конституция.
14. Закон об информатизации.
15. Закон о цифровой подписи.
16. Уголовный кодекс РФ о незаконном использовании объектов авторского права и смежных прав.
17. Международные и отечественные требования по защите информации и их стандартизация.
18. Уровни безопасности информации. Требования к криптографическим алгоритмам и системам.

Критерии и шкала оценивания по оценочному средству собеседование (устный или письменный опрос)

Шкала оценивания (интервал баллов)	Критерий оценивания
5	собеседование (устный или письменный опрос) прошел на высоком уровне (студент в полном объеме осветил рассматриваемый вопрос, владеет профильным понятийным (категориальным) аппаратом и т.п.)

4	собеседование (устный или письменный опрос) прошел на среднем уровне (студент в целом осветил рассматриваемый вопрос, владеет профильным понятийным (категориальным) аппаратом и т.п.)
3	собеседование (устный или письменный опрос) на низком уровне (студент допустил существенные неточности, изложил материал с ошибками, не владеет в достаточной степени профильным категориальным аппаратом и т.п.)
2	собеседование (устный или письменный опрос) прошел на неудовлетворительном уровне или не представлен (студент не готов, не выполнил задание и т.п.)

Задания к контрольным работам

1 Используя алгоритмы двойной перестановки строк и столбцов выполнить шифрование следующих фраз (ключ выбирать самостоятельно, номер варианта выбрать по номеру в списке группы):

1. Он досрочно завалил экзамен.
2. Закон суров, но это закон.
3. Умному легче доказать, что он дурак.
4. И у дурака вырастает зуб мудрости.
5. Свободу симулировать нельзя.
6. Подумай, прежде чем подумать.
7. Каждый век имеет свое средневековье.
8. Брюки протираются даже на троне.
9. Окно в мир можно закрыть газетой.
10. Чаще всего выход там, где был вход.
11. Безграмотные вынуждены диктовать.
12. Хлеб открывает любой рот.
13. Деньги не пахнут, но улетучиваются.
14. Сны зависят от положения спящего.
15. Труднее всего поджечь ад.
16. Ужасен кляп, смазанный медом.
17. Не пиши кредо на заборе.
18. Беззубым многое легче выговаривать.
19. И регалии звенят по разному.
20. Лицемерный палач ослабляет петлю.
21. Интеллектуальная узость ширится.
22. Вписывайся во влиятельные круги.
23. Иные ступени карьеры ведут на виселицу.
24. И маятник идет в ногу со временем.

2 Используя алгоритмы двойной перестановки строк и столбцов выполнить дешифрование шифрограмм, приведенные в таблице 3.1 (номер варианта выбрать по последней цифре номера шифра). В шифротексте следует обратить внимание на наличие пробелов в тексте, длина текста по всем вариантам равняется 25 символам:

Таблица 3.1

Номер вар-та	Шифротекст	Ключ 1	Ключ 2
1	**В ОН, Т ОЭЗКНОА УОРСЗКНОА**	КРУТО	СТУЖА
2	**ЗВАОЛИ ЛАН ОДОРОНЧСАЧТЕЗ**	ВЕСНА	ОСЕНЬ
3	**ПАЙРДЕЕЖ М ЧЕДАТУМЬДУПОМ**	ОСЕНЬ	ДОСУГ
4	**ДОВХЫМА Т ЕД Г ДО ХВ ИИЩ**	ТРАВА	ДОСУГ
5	**!Т РОЙОЛЮБ БХЛЕ ТВАЕЫРОТК**	ПРАВО	ТРАВА
6	**Ь ДА ОЖЧЕДТУНДРЕ СВЕЕОП Г**	КРУТО	ПРАВО
7	**ЕН ПОЕРД ЕОБР!ЗАН А ШИИК**	СПОРТ	КРУТО
8	**Е ВГОБЫ-М БЕУЗЗ ЛЧЕГОРЬИТ**	ВЕТЕР	СПОРТ
9	**ГАЛЕР ЗВИИОМУНЗЯТ НЕ РАОП**	СТУЖА	ВЕТЕР
10	**СЯТООН ОН УЫЖННЫПЕН ЕЖННУ**	ДРЕВО	СТУЖА

3 Используя магический квадрат (таблица 3.2) расшифровывать следующие шифрограммы (шифрограммы приведены в таблице 3.3, номер варианта выбрать по числу букв в фамилии):

Таблица 3.2

11	24	7	20	3
4	12	25	8	16
17	5	13	21	9
10	18	1	14	22
23	6	19	2	15

Таблица 3.3

Вариант	Шифротекст
1	ОЛ ЕЛ ОДУЛА-СЕЛЯС МЕЛЙДГ
2	ВТТЙЕБА КЛЮ Е РЫБХТРОООЛ
3	ОЕР Д ТОАЛОЗЗЧНИОААЧСЛНВ
4	УЗУНОБЛЯСВАОИЕИМТСРЛЬДЬВО
5	ЕТЙДДУЖЬ ЧЕМДУПРМПЕМАА О
6	ЕАЕЕУДГД ПОНОЧВСДТ Ь ЕЖР
7	КРШЗ РЕИ НПЕА АНДБОИ ЕО
8	ОНЫ НУСЫЕННЖТН ПОНОУЖН ЕЯ
9	ЕМИАГАНУ ПОЛЯЗЗВ РТНОИРЕ
10	НУУ З Е!ДЛЬТ РА КБТЫБРОЕО

4 Используя шифр многоалфавитной замены шифровать фразу из п. 1 (исключив пробелы и знаки препинания), используя в качестве ключа «Ключ 1» в таблице 3.1. Для шифрования использовать алфавит замены из таблицы 3.5.

5 Используя шифр многоалфавитной замены дешифровать фразу, используя «Ключ» (шифрограммы и ключи приведены в таблице 3.4, номер варианта выбрать по последней цифре суммы числа букв в имени и фамилии).

Таблица 3.4

Номер вар-та	Шифротекст	Ключ
1	РПЮЫВОНБЩОИТЯФАМХМЯЬЕЕШТТРО	ВЕСНА
2	ПЦМРМОЭУЯЙЙЦЗИЙБЧЙТЙЙХНЧОЬУЕЯШ	ОСЕНЬ
3	ЩЩЦФСЦШБОЕДУГЮБЕЬЪГСЦ	ДОСУГ
4	ГЭЫЙАФШСБТАВПРЛАЦЕПИСБПБЩЧУО	ТРАВА
5	РХЗЙБРЛМОЫЭУОЗЩФУЧЗРКУОДОЯШВВАЛ	ПРАВО
6	ХШЙЧЪПААНЧЩРЮТЕШБЮТПХПШДЭПВЮР	КРУТО
7	ЩЬАХЭЬФШВЕСЪКЭТРВХЮГГЛЖШВЩБЯП	СПОРТ
8	ДФЪЦЛДЕЬЩПДУФРШБЧЧРМПАЧПАХИЬ	ВЕТЕР
9	УБЫЧЫУТЬЧЯУАХСИРДШСЬЮНШРРДХЫ	СТУЖА
10	МЬЕБАСШПКТЙВЗПЬЗГЦРРФХСЗЫЙЬ	ДРЕВО

Дешифрованный текст привести с пробелами.

	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
А	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Б	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А
В	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б
Г	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В
Д	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г
Е	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д
Ж	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е
З	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж
И	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З
Й	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И
К	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й
Л	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К
М	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л
Н	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М
О	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н
П	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О
Р	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
С	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р
Т	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
У	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
Ф	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У
Х	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Ц	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
Ч	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
Ш	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч

Ш	Ш	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
Ъ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
Ы	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
Ь	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы
Э	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь
	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я

Оценочные средства для промежуточной аттестации (зачет)
Теоретические вопросы

1. Свойства защищаемой информации.
2. Доступность.
3. Конфиденциальность.
4. Целостность
5. Понятие Информационной безопасности и безопасности информации.
6. Понятие защита информации.
7. Виды носителей информации.
8. Угрозы защищаемой информации по видам носителей.
9. Возможные предпосылки нарушений свойств информационной безопасности.
10. Возможные злоумышленники.
11. Каналы утечки информации.
12. Анализ угроз защищаемой информации по видам носителей.
13. Понятие криптография.
14. Понятие криптоанализ.
15. Понятие стеганография.
16. Шифрование.
17. Дешифрование.
18. Кодирование.
19. Обзор основных методов шифрования и дешифрования.
20. Обзор основных методов кодирования.
21. Обзор основных методов криптоанализа.
22. Обзор основных методов стеганографии.
23. Симметричные системы шифрования с одним ключом.
24. Достоинства и недостатки шифров с одним ключом.
25. Создание шифров на основе блочных алгоритмом перестановки.
26. Стандарты шифрования DES, 3DES и ГОСТ.
27. Стандарт шифрования AES.
28. Асимметричные системы шифрования с открытым ключом.
29. Достоинства и недостатки шифров с открытым ключом.
30. Способы передачи секретного ключа.
31. Создание ключа на основе псевдослучайных последовательностей.
32. Примеры шифров на основе алгоритма Эль-Гамаля и алгоритма RSA.
33. Аутентификация (подмена данных, хэш-функция, защита от подмены данных).

34. Цифровая подпись (создание цифровой подписи, атаки и защита цифровой подписи).
35. Стандарты на электронно-цифровую подпись: DSS и ГОСТ Р 34.10-94.
36. Цифровая подпись на базе шифра RSA и шифра Эль-Гамаля.
37. Системы по отпечаткам пальцев. На основании каких физических характеристик пальца можно составить биометрический шаблон?
38. Преимущества и недостатки метода отпечатка пальцев.
39. Системы по голосу. Какие физические характеристики входят в основу шаблона? Преимущества и недостатки.
40. Системы по радужной оболочке глаза. Преимущества и недостатки.
41. Основные подсистемы системы идентификации по радужной оболочке глаза.

Статистические характеристики метода.

42. Системы идентификации и аутентификации по изображению лица. Классификация методов.
43. Системы идентификации и аутентификации по 2-d изображению лица. Преимущества и недостатки.
44. Особенности систем по 3-d распознаванию лица. Классификация систем и особенности.
45. Системы идентификации по геометрии руки. Виды систем. Преимущества и недостатки метода.
46. Метод распознавания по сетчатке глаза. Статистические показатели. Преимущества и недостатки.
47. Метод аутентификации и идентификации по венозному рисунку руки.
48. Статистические показатели.
49. Классификация методов распознавания по почерку. Преимущества и недостатки.
50. Система электронного носа.
51. Система распознавания по форме ушной раковины.
52. Перспективные методы БСЗИ.
53. Применение биометрии в подсистемах безопасности и ИБ.
54. Механизм генерации ЭП с помощью биометрии.
55. Система BioLink Cl.
56. Применение технологий БСЗИ в картах Государственных систем социального обеспечения.
57. Возможности видеоаналитики в мониторинговых системах.
58. Компьютерная система.
59. Основные угрозы безопасности информации в компьютерной системе.
60. Основные механизмы защиты информации в компьютерных системах.
61. Защита компьютерной системы на физическом уровне.
62. Идентификация и аутентификация пользователей.
63. Парольная аутентификация
64. Атрибутивная аутентификация
65. Биометрическая аутентификация
66. Разграничение доступа пользователей к ресурсам.
67. Дискретная модель.
68. Мандатная модель.
69. Верификационная модель.
70. Проблемы безопасности сетей.

71. Уровни безопасности сетевых систем.
72. Источники угроз в сетях.
73. Виды сетевых угроз и противодействие им.
74. Атаки на сетевые системы.
75. ПЭМИН каналов связи.
76. Удаленные атаки через сеть Internet.
77. Уязвимости протоколов и служб Internet.
78. Задачи и уровни защиты в сетях передачи данных.
79. Механизмы современной защиты информации в каналах связи.
80. Организационные мероприятия по защите информации в сетях.
81. Политика сетевой безопасности.
82. Методы и средства защиты информации от побочного электромагнитного излучения и наводок информации.
83. Управление доступом к информации в сетях передачи данных.
84. Межсетевые экраны (МЭ). Компоненты МЭ.
85. Основные схемы защиты на базе МЭ. Модули МЭ.
86. Программные методы защиты, реализуемые МЭ.
87. Антивирусная защита.
88. Системы обнаружения сетевых вторжений.
89. Принципы построения СЗИ в АС.
90. Уровни защиты информации в ИС
91. Физический уровень.
92. Уровень данных.
93. Уровень программ.
94. Уровень локальной сети
95. Межсетевой уровень
96. Организационный уровень.
97. Методы проектирования СЗИ.
98. План-график проектирования СЗИ.
99. Инструментарий для разработки проектов СЗИ в ИС по уровням.

Критерии и шкала оценивания к промежуточной аттестации «экзамен»

Национальная шкала	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

9. Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости рабочая программа учебной дисциплины может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе с применением электронного обучения и дистанционных образовательных технологий.

Для этого требуется заявление студента (его законного представителя) и заключение психолого-медико-педагогической комиссии (ПМПК). В случае необходимости обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося), а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида могут предлагаться следующие варианты восприятия учебной информации с учетом их индивидуальных психофизических особенностей:

– создание текстовой версии любого нетекстового контента для его возможного преобразования в альтернативные формы, удобные для различных пользователей;

– создание контента, который можно представить в различных видах без потери данных или структуры, предусмотреть возможность масштабирования текста и изображений без потери качества, предусмотреть доступность управления контентом с клавиатуры;

– создание возможностей для обучающихся воспринимать одну и ту же информацию из разных источников, например, так, чтобы лица с нарушениями слуха получали информацию визуально, с нарушениями зрения – аудиально;

– применение программных средств, обеспечивающих возможность освоения навыков и умений, формируемых дисциплиной (модулем), за счёт альтернативных способов, в том числе виртуальных лабораторий и симуляционных технологий;

– применение электронного обучения, дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем, в том числе вебинаров, которые могут быть использованы для проведения виртуальных лекций с возможностью взаимодействия всех участников дистанционного обучения, проведения семинаров, выступления с докладами и защиты выполненных работ, проведения тренингов, организации коллективной работы;

– применение электронного обучения, дистанционных образовательных технологий для организации форм текущего и промежуточного контроля;

– увеличение продолжительности сдачи обучающимся инвалидом или лицом с ограниченными возможностями здоровья форм промежуточной аттестации по отношению к установленной продолжительности их сдачи:

– продолжительность сдачи зачёта или экзамена, проводимого в письменной форме, – не более чем на 90 минут;

– продолжительность подготовки обучающегося к ответу на зачёте или экзамене, проводимом в устной форме, – не более чем на 20 минут; – продолжительность выступления обучающегося при защите курсовой работы – не более чем на 15 минут.

Лист изменений и дополнений

№ п/п	Виды дополнений и изменений с указанием страниц	Дата и номер протокола заседания кафедры (кафедр), на котором были рассмотрены и одобрены изменения и дополнения	Подпись (с расшифровкой) заведующего кафедрой (заведующих кафедрами)
1.			
2.			
3.			
4.			