МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования
«Поволжский государственный университет сервиса» (ФГБОУ ВО «ПВГУС»)

Колледж креативных индустрий и предпринимательства

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОП.15 «ЗАЩИТА ИНФОРМАЦИИ»

Специальность
09.02.01 «Компьютерные системы и комплексы»

Тольятти 2024

Рабочая программа дисциплины «Защита информации» разработана в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 09.02.01 «Компьютерные системы и комплексы», утвержденным приказом Министерства просвещения России от 25 мая 2022 года № 362.

Разработчик РПД:

преподаватель	А.К. Попов
(ученая степень, ученое звание)	(ФИО)

Рассмотрена на заседании предметно-цикловой комиссии по образовательной программе 09.02.01 Компьютерные системы и комплексы
Протокол от «22» ноября 2024 г., № 3
Председатель ПЦК И.У. Каримов, преподаватель
(ФИО, должность, ученая степень, ученое звание)

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Цель освоения дисциплины

Целью освоения дисциплины является формирование у обучающихся следующих компетенций:

Код компетенции	Наименование компетенции
ОК 01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности
ПК 3.1	Проводить контроль параметров, диагностику и восстановление работоспособности цифровых устройств компьютерных систем и комплексов

1.2. Планируемые результаты освоения дисциплины

В результате освоения дисциплины обучающийся должен:

иметь практический опыт:

- использования мероприятий по защите информации в компьютерных системах и комплексах;

уметь:

- решать задачи по защите информации в компьютерных системах и комплексах;
- проводить контроль, диагностику и восстановление работоспособности компьютерных систем и комплексов; выявлять угрозы информационной безопасности;

знать:

- основные понятия и определения защиты информации в компьютерных системах, комплексах и сетях; источники риска и форм атак на компьютерную информацию;
- политику и стандарты безопасности; аппаратные и программные средства контроля и диагностики компьютерных систем и комплексов;
- методы и средства обеспечения информационной безопасности компьютерных систем.

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Защита информации» относится к общепрофессиональному циклу основной профессиональной образовательной программы.

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объём дисциплины и виды учебной работы

Общая трудоёмкость дисциплины составляет **72 часа.** Их распределение по видам работ представлено в таблице:

Виды учебных занятий и работы обучающихся	Трудоемкость, час
Общая трудоемкость дисциплины	**72**
Объем работы обучающихся во взаимодействии с преподавателем по видам учебных занятий (всего), в т.ч.:	**46**
лекции	24
практические работы	22
Самостоятельная работа	**26**
Контроль (часы на контрольную работу)	**-**
Консультация перед экзаменом	**-**
Промежуточная аттестация	**Зачет**

2.2. Содержание дисциплины, структурированное по темам

Коды компетенций, формированию которых способствует элемент программы	Наименование разделов, тем	Виды учебной работы				Формы текущего контроля (наименование оценочного средства)
		Работа во взаимодействии с преподавателем			Самостоятельная работа, час	
		Лекции, час	Лабораторные работы, час	Практические занятия, час		
ОК 01, ОК 02, ПК 3.1	**Тема 1. Проблемы информационной безопасности компьютерных сетей.** - Модель ISO/OSI и стек протоколов TCP/IP как основной стандарт построения компьютерных сетей - Угрозы сетевой безопасности и проблемы безопасности IP-сетей - Угрозы безопасности беспроводным сетям и уязвимости беспроводных сетей - Обеспечение информационной безопасности компьютерных сетей	4				Конспектирование лекционного материала
	Самостоятельная работа: поиск материала по теме.				4	
ОК 01, ОК 02, ПК 3.1	**Тема 2. Криптографическая защита информации в компьютерных сетях.** - Основные понятия криптографической защиты информации - Симметричные криптосистемы шифрования - Асимметричные криптосистемы шифрования - Функция хэширования - Электронная цифровая подпись	4				Конспектирование лекционного материала Отчет по практическим работам
	Практическая работа 1. Количественная оценка стойкости парольной защиты. Шифрование информации. Практическая работа 2. Изучение методов шифрования. Шифры замены и шифры перестановки.			6		
	Самостоятельная работа: подготовка к практическим работам, поиск материала по теме.				4	
ОК 01, ОК 02, ПК 3.1	**Тема 3. Идентификация, аутентификация и управление доступом** - Аутентификация, авторизация и администрирование действий пользователей в компьютерных сетях - Аутентификация на основе многоразовых паролей - Аутентификация на основе одноразовых паролей - Биометрическая аутентификация пользователей	4				Конспектирование лекционного материала Отчет по практическим работам

Коды компетенций, формированию которых способствует элемент программы	Наименование разделов, тем	Виды учебной работы				Формы текущего контроля (наименование оценочного средства)
		Работа во взаимодействии с преподавателем			Самостоятельная работа, час	
		Лекции, час	Лабораторные работы, час	Практические занятия, час		
	Практическая работа 3. Аппаратно-программные средства защита компьютерной информации.			4		
	Самостоятельная работа: подготовка к практическим работам, поиск материала по теме.				4	
ОК 01, ОК 02, ПК 3.1	**Тема 4.Безопасность операционных систем** - Угрозы безопасности операционной системы - Понятие защищенной операционной системы	4				Конспектирование лекционного материала Отчет по практическим работам
	Практическая работа №4. Организация безопасного обмена трафиком.			4		
	Самостоятельная работа: подготовка к практическим работам, поиск материала по теме.				4	
ОК 01, ОК 02, ПК 3.1	**Тема 5. Современные подходы к обеспечению анонимности работы в сети Интернет** - Прокси-серверы - Виртуальные частные сети (VPN/SSH) - Сеть анонимизации TOR - Сеть анонимизации I2P	4				Конспектирование лекционного материала Отчет по практическим работам
	Практическая работа №5. Проверка целостности файла. Практическая работа №6. Шифрование файлов.			4		
	Самостоятельная работа: подготовка к практическим работам, поиск материала по теме.				4	
ОК 01, ОК 02, ПК 3.1	**Тема 6. Вредоносные программы и спам** - Классификация вредоносных программ - Рекомендации по безопасной работе в сети Интернет	4				Конспектирование лекционного материала Отчет по практическим работам
	Практическая работа №7. Защита wifi соединения. Практическая работа №8. Настройка ACL-списка.			4		
	Самостоятельная работа: подготовка к практическим работам, поиск материала по теме.				6	
	ИТОГО	**24**		**22**	**26**	

2.3. Формы и критерии текущего контроля успеваемости (технологическая карта для студентов очной формы обучения)

Формы текущего контроля	Количество контрольных точек	Количество баллов за 1 контр. точку	Макс. возм. кол-во баллов
Конспектирование лекционного материала	6	6	36
Отчет по практическим работам	8	8	64
Итого по дисциплине			**100 баллов**

2.4. Шкала оценки результатов освоения дисциплины, сформированности результатов обучения

Форма проведения промежуточной аттестации	Условия допуска	Шкалы оценки уровня сформированности результатов обучения		Шкала оценки уровня освоения дисциплины		
		Уровневая шкала оценки компетенций	100 бальная шкала, %	100 бальная шкала, %	5-балльная шкала, дифференцированная оценка/балл	недифференцированная оценка
Зачет (по накопительному рейтингу или компьютерное тестирование)	допускаются все студенты	допороговый	ниже 61	ниже 61	«неудовлетворительно» / 2	не зачтено
		пороговый	61-85,9	61-69,9	«удовлетворительно» / 3	зачтено
				70-85,9	«хорошо» / 4	зачтено
		повышенный	86-100	86-100	«отлично» / 5	зачтено

3. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

3.1. Общие методические рекомендации по освоению дисциплины, образовательные технологии

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

Контактная работа может быть аудиторной, внеаудиторной, а также проводиться в электронной информационно-образовательной среде университета (далее - ЭИОС). В случае проведения части контактной работы по дисциплине в ЭИОС (в соответствии с расписанием учебных занятий), трудоемкость контактной работа в ЭИОС эквивалентна аудиторной работе.

При проведении учебных занятий по дисциплине обеспечивается развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплины в форме курса, составленного на основе результатов научных исследований, проводимых университетом, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

- *балльно-рейтинговая технология оценивания;*
- *электронное обучение;*
- *репродуктивные технологии;*
- *технологии развивающего обучения;*
- *практико-ориентированные технологии.*

Для оценки знаний, умений, навыков и уровня сформированности компетенции по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. В основу балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего контроля успеваемости. Максимальное количество баллов в семестре – 100.

По итогам текущей успеваемости студенту может быть выставлена оценка по промежуточной аттестации в соответствии за набранными за семестр баллами. Студентам, набравшим в ходе текущего контроля успеваемости по дисциплине от 61 до 100 баллов и выполнившим все обязательные виды запланированных учебных занятий, по решению преподавателя без прохождения промежуточной аттестации выставляется оценка в соответствии со шкалой оценки результатов освоения дисциплины.

Результат обучения считается сформированным (повышенный уровень), если теоретическое содержание курса освоено полностью; при устных собеседованиях студент исчерпывающе, последовательно, четко и логически стройно излагает учебный материал; свободно справляется с задачами, вопросами и другими видами заданий, требующих применения знаний, использует в ответе дополнительный материал; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 86 до 100, что соответствует повышенному уровню сформированности результатов обучения.

Результат обучения считается сформированным (пороговый уровень), если теоретическое содержание курса освоено полностью; при устных собеседованиях студент последовательно, четко и логически стройно излагает учебный материал; справляется с задачами, вопросами и другими видами заданий, требующих применения знаний; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено

числом баллов от 61 до 85,9, что соответствует пороговому уровню сформированности результатов обучения.

Результат обучения считается несформированным, если студент при выполнении заданий не демонстрирует знаний учебного материала, допускает ошибки, неуверенно, с большими затруднениями выполняет задания, не демонстрирует необходимых умений, качество выполненных заданий не соответствует установленным требованиям, качество их выполнения оценено числом баллов ниже 61, что соответствует допороговому уровню.

3.2. Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обеспечивает подготовку обучающегося к аудиторным занятиям и мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине. Результаты этой подготовки проявляются в активности обучающегося на занятиях и в качестве выполненных практических заданий и других форм текущего контроля.

При выполнении заданий для самостоятельной работы рекомендуется проработка материалов лекций по каждой пройденной теме, а также изучение рекомендуемой литературы, представленной в Разделе 4.

В процессе самостоятельной работы при изучении дисциплины студенты могут использовать в специализированных аудиториях для самостоятельной работы компьютеры, обеспечивающему доступ к программному обеспечению, необходимому для изучения дисциплины, а также доступ через информационно-телекоммуникационную сеть «Интернет» к электронной информационно-образовательной среде университета (ЭИОС) и электронной библиотечной системе (ЭБС), где в электронном виде располагаются учебные и учебно-методические материалы, которые могут быть использованы для самостоятельной работы при изучении дисциплины.

Для обучающихся по заочной форме обучения самостоятельная работа является основным видом учебной деятельности.

4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

4.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Васильков, А. В. Безопасность и управление доступом в информационных системах : учеб. пособие для сред. проф. образования / А. В. Васильков, И. А. Васильков. - Документ read. - Москва : ФОРУМ [и др.], 2022. - 367 с. : ил., табл. - (Среднее профессиональное образование). - Предм. указ. - URL: https://znanium.ru/read?id=399436 (дата обращения: 14.03.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-91134-360-6. - 978-5-16-012933-4. - 978-5-16-104336-3. - Текст : электронный..

2. Нестеров, С. А. Основы информационной безопасности : учеб. пособие / С. А. Нестеров. - Изд. 5-е, стер. - Документ Reader. - Санкт-Петербург [и др.] : Лань, 2022. - 322 с. - (Учебники для вузов. Специальная литература). - URL: https://reader.lanbook.com/book/206279 (дата обращения: 20.10.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-8114-4067-2. - Текст : электронный..

3. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений : учеб. пособие / С. Н. Никифоров. - Изд. 5-е, стер. - Документ Reader. - Санкт-Петербург [и др.] : Лань, 2023. - 93 с. - Прил. - URL: https://reader.lanbook.com/book/288974 (дата обращения: 06.12.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-507-45868-4. - Текст : электронный.

4. Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование : учеб. пособие / С. Н. Никифоров. - Изд. 4-е, стер. - Документ Reader. - Санкт-Петербург [и др.] : Лань, 2022. - 121 с. - Прил. - URL: https://reader.lanbook.com/book/200483 (дата обращения: 20.10.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-8114-9563-4. - Текст : электронный.

5. Никифоров, С. Н. Методы защиты информации. Шифрование данных : учеб. пособие / С. Н. Никифоров. - Изд. 2-е, стер. - Документ Reader. - Санкт-Петербург [и др.] : Лань, 2022. - 158 с. - (Учебники для вузов. Специальная литература). - URL: https://reader.lanbook.com/book/206285 (дата обращения: 20.10.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-8114-4042-9. - Текст : электронный.

6. Никифоров, С. Н. Методы защиты информации. Защищенные сети : учеб. пособие / С. Н. Никифоров. - Документ Reader. - Санкт-Петербург [и др.] : Лань, 2021. - 94 с. - (Учебники для вузов. Специальная литература). - URL: https://e.lanbook.com/reader/book/169311/#1 (дата обращения: 07.04.2021). - Режим доступа: для авториз. пользователей. - ISBN 978-5-8114-3099-4. - Текст : электронный.

7. Баланов, А. Н. Защита информационных систем. Кибербезопасность : учеб. пособие / А. Н. Баланов. - Изд. 2-е, стер. - Документ read. - Санкт-Петербург [и др.] : Лань, 2025. - 277 с. - Прил. - URL: https://reader.lanbook.com/book/438971 (дата обращения: 14.11.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-507-50467-1. - Текст : электронный.

Дополнительная литература:

1. Защита информации : учеб. пособие для вузов по направлению подгот. Инфокоммуникац. технологии и системы связи квалификации (степ.) "бакалавр" и квалификации (степ.) "магистр" / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. - 3-е изд. - Документ read. - Москва : РИОР [и др.], 2024. - 400 с. - (Высшее образование). - URL: https://znanium.ru/read?id=443251 (дата обращения: 05.04.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-369-01759-3. - 978-5-16-013801-5. - 978-5-16-106478-8. - Текст : электронный.

2. Сычев, Ю. Н. Защита информации и информационная безопасность : учеб. пособие для студентов высш. учеб. заведений по направлению подгот. 10.03.01.

"Информационная безопасность" (квалификация (степень) "бакалавр") / Ю. Н. Сычев. - Документ read. - Москва : ИНФРА-М, 2022. - 201 с. - (Высшее образование - бакалавриат). - Прил. - URL: https://znanium.com/read?id=388766 (дата обращения: 26.05.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-16-107471-8. - Текст : электронный.

3. Петренко, В. И. Защита персональных данных в информационных системах. Практикум : учеб. пособие / В. И. Петренко, И. В. Мандрица. - Изд. 6-е, стер. - Документ Reader. - Санкт-Петербург [и др.] : Лань, 2025. - 105 с. - URL: https://reader.lanbook.com/book/437192 (дата обращения: 14.11.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-507-50458-9. - Текст : электронный.

4. Назаров, А. В. Эксплуатация объектов сетевой инфраструктуры : учеб. для проф. образоват. орг. по специальности 09.02.02 "Компьютер. сети" / А. В. Назаров, А. Н. Енгалычев, В. П. Мельников. - Документ Bookread2. - Москва : Курс [и др.], 2023. - 360 с. - (Среднее профессиональное образование) (Среднее профессиональное образование). - URL: https://znanium.ru/read?id=428836 (дата обращения: 17.01.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-906923-06-6. - 978-5-16-105198-6. - Текст : электронный.

5. Зверева, В. П. Участие в планировании и организации работ по обеспечению защиты объекта : учеб. для сред. проф. образования по специальности 10.02.01 "Орг. и технология защиты информации" / В. П. Зверева, А. В. Назаров. - Документ read. - Москва : Курс [и др.], 2020. - 320 с. - (Среднее профессиональное образование). - URL: https://znanium.com/read?id=347024 (дата обращения: 10.12.2020). - Режим доступа: для авториз. пользователей. - ISBN 978-5-16-012302-8. - 978-5-16-105204-4. - Текст : электронный.

6. Учебно-методическое пособие по дисциплине "Защита информации" : для студентов специальности 09.02.01 "Компьютер. системы и комплексы" / Поволж. гос. ун-т сервиса (ФГБОУ ВО "ПВГУС"), Каф. "Информ. и электрон. сервис" ; сост. Г. П. Жуков. - Документ Adobe Acrobat. - Тольятти : ПВГУС, 2018. - 4,38 МБ, 144 с. : ил. - Прил. - URL: http://elib.tolgas.ru/publ/Metod_ZIspo_SPOKSK_29.03.2018.pdf (дата обращения: 21.10.2020). - Режим доступа: для авториз. пользователей. - 0-00. - Текст : электронный.

4.2. Профессиональные базы данных, информационно-справочные системы, интернет-ресурсы

1. eLIBRARY.RU : научная электронная библиотека : сайт. – Москва, 2000 - . – URL : https://elibrary.ru (дата обращения: 03.12.2021). – Режим доступа: для зарегистрир. пользователей. – Текст: электронный.

2. Единое окно доступа к образовательным ресурсам : сайт. - URL : http://window.edu.ru/ (дата обращения: 03.12.2021). - Текст : электронный.

3. Университетская информационная система РОССИЯ : сайт. - URL : http://uisrussia.msu.ru (дата обращения: 03.12.2021). - Текст : электронный.

4. Федеральная служба государственной статистики : сайт. - Москва, 1999 - . - URL: http://www.gks.ru/ (дата обращения: 03.12.2021). - Текст: электронный.

5. Электронная библиотечная система Поволжского государственного университета сервиса : сайт / ФГБОУ ВО «ПВГУС». – Тольятти, 2010 - . - URL : http://elib.tolgas.ru (дата обращения 03.12.2021). - Режим доступа: для авториз. пользователей. - Текст : электронный.

6. Электронно-библиотечная система Znanium.com : сайт / ООО "ЗНАНИУМ". – Москва, 2011 - . – URL : https://znanium.com/ (дата обращения 03.12.2021). - Режим доступа: для авториз. пользователей. - Текст : электронный.

7. Электронно-библиотечная система Лань : сайт / ООО "ЭБС ЛАНЬ". - Москва, 2011 - . - URL: https://e.lanbook.com/ (дата обращения 03.12.2021). - Режим доступа: для авториз. пользователей. - Текст : электронный.

4.3. Программное обеспечение

Информационное обеспечение учебного процесса по дисциплине осуществляется с использованием следующего программного обеспечения (лицензионного и свободно распространяемого), в том числе отечественного производства:

№ п/п	Наименование	Условия доступа
1	Microsoft Windows	из внутренней сети университета (лицензионный договор)
2	Microsoft Office	из внутренней сети университета (лицензионный договор)
3	КонсультантПлюс	из внутренней сети университета (лицензионный договор)
4	СДО MOODLE	из любой точки, в которой имеется доступ к сети Интернет (лицензионный договор)

5. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Специальные помещения представляют собой учебные аудитории для проведения занятий всех видов, предусмотренных образовательной программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы, мастерские и лаборатории, оснащенные оборудованием, техническими средствами обучения и материалами, учитывающими требования международных стандартов.

Занятия лекционного типа. Учебные аудитории для занятий лекционного типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук), учебно-наглядные пособия (презентации по темам лекций), обеспечивающие тематические иллюстрации, соответствующие данной программе дисциплины.

Занятия семинарского типа. Для проведения практических занятий используется учебная аудитория, укомплектованная мебелью и техническими средствами обучения, служащими для представления учебной информации (переносной набор демонстрационного оборудования (проектор, экран, /ноутбук).

Промежуточная аттестация. Для проведения промежуточной аттестации по дисциплине используются компьютерные классы, оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду университета и/или учебные аудитории, укомплектованные мебелью и техническими средствами обучения.

Самостоятельная работа. Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде университета. Для организации самостоятельной работы обучающихся используются: компьютерные классы университета; библиотека (медиазал), имеющая места для обучающихся, оснащенные компьютерами с доступом к базам данных и сети Интернет.

Электронная информационно-образовательная среда университета (ЭИОС). Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде университета (ЭИОС) http://sdo.tolgas.ru/ из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет», как на территории университета, так и вне ее.

6. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБУЧЕНИЯ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

При необходимости рабочая программа может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе для дистанционного обучения. Для этого требуется заявление студента (его законного представителя) и заключение психолого-медико-педагогической комиссии (ПМПК).

К предметным результатам освоения дисциплины дополнительно относятся:

1) для слепых, слабовидящих обучающихся:

- сформированность навыков письма на брайлевской печатной машинке;

2) для глухих, слабослышащих, позднооглохших обучающихся:

- сформированность и развитие основных видов речевой деятельности обучающихся - слухозрительного восприятия (с использованием слуховых аппаратов и (или) кохлеарных имплантов), говорения, чтения, письма;

3) для обучающихся с расстройствами аутистического спектра:

-овладение основными стилистическими ресурсами лексики и фразеологии языка, основными нормами литературного языка, нормами речевого этикета; приобретение опыта их использования в речевой и альтернативной коммуникативной практике при создании устных, письменных, альтернативных высказываний; стремление к возможности выразить собственные мысли и чувства, обозначить собственную позицию.

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, в том числе с применением электронного обучения и дистанционных технологий:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.

- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (ФОНД ОЦЕНОЧНЫХ СРЕДСТВ) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7.1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта в ходе текущего контроля успеваемости

7.1.1. Типовые задания к практическим (семинарским) занятиям

Практическая работа № 1. Количественная оценка стойкости парольной защиты. Шифрование информации. Цель работы — оценить устойчивость различных паролей к атакам и изучить методы шифрования данных. Задание состоит в проведении тестов на стойкость паролей и применении различных алгоритмов шифрования для защиты информации. Рассматриваемые вопросы: методы подбора паролей, атаки на пароли, принципы работы симметричного и асимметричного шифрования.

Практическая работа № 2. Изучение методов шифрования. Шифры замены и шифры перестановки. Цель работы — изучить основные типы шифров, такие как шифры замены и шифры перестановки, а также их применение для защиты информации. Задание состоит в анализе и реализации простых методов шифрования и расшифровки. Рассматриваемые вопросы: принципы работы с шифрами, их уязвимости и методы усиления безопасности.

Практическая работа № 3. Аппаратно-программные средства защиты компьютерной информации. Цель работы — ознакомиться с основными аппаратными и программными средствами для защиты данных в компьютерных системах. Задание включает изучение работы антивирусного ПО, фаерволов и средств защиты от несанкционированного доступа. Рассматриваемые вопросы: методы защиты информации на уровне операционной системы, принципы работы фаерволов и систем антивирусной защиты.

Практическая работа № 4. Организация безопасного обмена трафиком. Цель работы — изучить методы обеспечения безопасности при передаче данных по сети. Задание заключается в настройке защищенного канала связи и оценке его безопасности. Рассматриваемые вопросы: протоколы шифрования трафика (SSL/TLS), VPN-технологии, методы защиты от атак на сети.

Практическая работа № 5. Проверка целостности файла. Цель работы — изучить методы проверки целостности данных и их защиты от изменений. Задание состоит в применении хеш-функций для обеспечения целостности файлов и проверке их подлинности. Рассматриваемые вопросы: алгоритмы хеширования, цифровые подписи, методы защиты файлов от подмены и повреждений.

Практическая работа № 6. Шифрование файлов. Цель работы — изучить различные методы шифрования файлов для защиты информации. Задание включает практическое применение алгоритмов шифрования для защиты данных. Рассматриваемые вопросы: симметричное и асимметричное шифрование, алгоритмы AES и RSA, создание и использование ключей для шифрования.

Практическая работа № 7. Защита wifi соединения. Цель работы — изучить методы защиты беспроводных сетей Wi-Fi от несанкционированного доступа. Задание включает настройку защищенной Wi-Fi сети и анализ угроз безопасности. Рассматриваемые вопросы: стандарты защиты WPA/WPA2, методы подбора паролей, атаки на Wi-Fi сети.

Практическая работа № 8. Настройка ACL-списка. Цель работы — научиться настраивать списки контроля доступа (ACL) для ограничения прав доступа к ресурсам сети. Задание состоит в создании и настройке ACL для управления доступом в компьютерных сетях. Рассматриваемые вопросы: принципы работы с ACL, типы списков, методы реализации безопасности на уровне сетевых устройств.

7.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта в ходе промежуточной аттестации

Форма проведения промежуточной аттестации по дисциплине: зачет (по результатам накопительного рейтинга или в форме компьютерного тестирования).

Контроль и оценка результатов освоения дисциплины в части сформированности общих компетенций и их частей (ОК 1, ОК 2) осуществляется преподавателем в ходе текущего контроля успеваемости (в процессе проведения практических работ, тестирования).

В ходе проведения промежуточной аттестации осуществляется контроль и оценка результатов освоения профессиональных компетенций и их частей.

Вопросы для подготовки к промежуточной аттестации (зачет)

ПК 3.1 Проводить контроль параметров, диагностику и восстановление работоспособности цифровых устройств компьютерных систем и комплексов

1. Что такое диагностика компьютерных систем, и какие основные этапы включает этот процесс?
2. Какие методы используются для контроля параметров работы операционной системы с точки зрения безопасности?
3. Каковы основные признаки неисправностей в цифровых устройствах компьютерных систем?
4. Чем отличается диагностика аппаратных и программных неисправностей в компьютерных системах?
5. Какие средства диагностики могут использоваться для проверки целостности данных в компьютерных системах?
6. Какие параметры компьютерной сети должны быть проверены для выявления проблем с безопасностью?
7. Как можно оценить состояние защищённости компьютера на уровне операционной системы?
8. Какие инструменты можно использовать для анализа логов безопасности и выявления подозрительной активности?
9. Какие способы восстановления работоспособности компьютерных систем существуют при сбоях в аппаратной части?
10. Как проводится диагностика и восстановление информации после сбоя в жестком диске?
11. Что такое RAID-массивы, и как они помогают в восстановлении данных в случае выхода из строя отдельных устройств хранения?
12. Какие методы используются для тестирования и восстановления работоспособности устройств ввода-вывода в компьютере?
13. Как проводится восстановление информации в случае вирусной атаки, если данные были повреждены или уничтожены?
14. Какие параметры и состояния оборудования следует контролировать для предупреждения перегрева процессора или других критичных компонентов?
15. Как можно диагностировать утечку памяти в программном обеспечении и какие действия предпринимать для её устранения?
16. Какие инструменты могут быть использованы для восстановления работоспособности системы после сбоя в сети (например, при проблемах с маршрутизацией)?
17. Что такое криптографическое восстановление ключей, и как это связано с безопасностью компьютерных систем?
18. Какие признаки могут указывать на атаку типа "отказ в обслуживании" (DoS), и как восстановить нормальную работу системы в таких случаях?
19. Как проверить эффективность работы системы защиты от несанкционированного доступа и какие действия предпринять при выявлении уязвимостей?
20. Как проводится диагностика работы антивирусных программ и их эффективность в защите от новых угроз?