МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (ОЦЕНОЧНЫЕ СРЕДСТВА)

Шифр	Наименование дисциплины (модуля)
Б1.В.01.ДВ.01	**Современные проблемы защиты данных в компьютерных сетях**

Код направления подготовки	44.04.01
Направление подготовки	Педагогическое образование
Наименование (я) ОПОП (направленность / профиль)	Информатика и робототехника в образовании
Уровень образования	магистр
Форма обучения	заочная

Разработчики:

Должность	Учёная степень, звание	Подпись	ФИО
Доцент	кандидат педагогических наук		Паршукова Наталья Борисовна

Рабочая программа рассмотрена и одобрена (обновлена) на заседании кафедры (структурного подразделения)

Кафедра	Заведующий кафедрой	Номер протокола	Дата протокола	Подпись
Кафедра информатики, информационных технологий и методики обучения информатике	Рузаков Андрей Александрович	10	13.06.2019	
Кафедра информатики, информационных технологий и методики обучения информатике	Рузаков Андрей Александрович	1	10.09.2020	

Раздел 1. Компетенции обучающегося, формируемые в результате освоения образовательной программы с указанием этапов их формирования

Таблица 1 - Перечень компетенций, с указанием образовательных результатов в процессе освоения дисциплины (в соответствии с РПД)

Формируемые компетенции			
Индикаторы ее достижения	**Планируемые образовательные результаты по дисциплине**		
	знать	**уметь**	**владеть**
ПК-4 способен проектировать и реализовывать программы общего, профессионального и дополнительного образования			
ПК.4.1 Знает теоретические и методические основы организации образовательного процесса в системе общего, профессионального и дополнительного образования	З.1 Знать основные понятия шифрования данных для защиты информации в компьютерных сетях		
ПК.4.2 Умеет организовать образовательный процесс в системе общего, профессионального и дополнительного образования		У.1 Уметь применять методы шифрования данных для защиты информации в компьютерных сетях для обучения криптографическим алгоритмам в системах общего, процессионального и дополнительного образования	
ПК.4.3 Владеет навыками организации образовательного процесса в системе общего, профессионального и дополнительного образования			В.1 Владеть технологией шифрования данных для демонстрации приемов защиты информации в компьютерных сетях
УК-5 способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия			
УК-5.1 Знает национальные, конфессиональные и этнокультурные особенности и национальные традиции; основные принципы и нормы межкультурного взаимодействия	З.2 Знать основные понятия в области защиты информации в процессе информационной коммуникации		
УК-5.2 Умеет грамотно, доступно излагать профессиональную информацию в процессе межкультурного взаимодействия; соблюдать этические нормы и права человека; анализировать особенности социального взаимодействия с учетом личностных, национально-этнических, конфессиональных и иных особенностей участников коммуникации		У.2 Уметь применять методы защиты информации при демонстрации алгоритмов шифрования в процессе обучения при работе в компьютерных сетях	

УК-5.3 Владеет способами выбора адекватной коммуникативной стратегии в зависимости от культурного контекста коммуникации и поставленных целей			В.2 Владеет технологией объяснения сложных алгоритмов, в том числе алгоритмов шифрования, в системе образования

Компетенции связаны с дисциплинами и практиками через матрицу компетенций согласно таблице 2.

Таблица 2 - Компетенции, формируемые в результате обучения

Код и наименование компетенции	
Составляющая учебного плана (дисциплины, практики, участвующие в формировании компетенции)	**Вес дисциплины в формировании компетенции (100 / количество дисциплин, практик)**
ПК-4 способен проектировать и реализовывать программы общего, профессионального и дополнительного образования	
Применение цифровых образовательных ресурсов в процессе обучения информатике	12,50
Теоретические и методические основы преподавания информатики в условиях профильного обучения	12,50
Применение дистанционных технологий в учебном процессе	12,50
Современные проблемы защиты данных в компьютерных сетях	**12,50**
Современные технологии создания Web-ресурсов	12,50
Образовательная робототехника	12,50
Web-дизайн	12,50
Детали модулей роботов и их конструирование	12,50
УК-5 способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	
Деловой иностранный язык	33,33
Современные проблемы защиты данных в компьютерных сетях	**33,33**
Web-дизайн	33,33

Таблица 3 - Этапы формирования компетенций в процессе освоения ОПОП

Код компетенции	**Этап базовой подготовки**	**Этап расширения и углубления подготовки**	**Этап профессионально-практической подготовки**
ПК-4	**Применение цифровых образовательных ресурсов в процессе обучения информатике, Теоретические и методические основы преподавания информатики в условиях профильного обучения, Применение дистанционных технологий в учебном процессе, Современные проблемы защиты данных в компьютерных сетях, Современные технологии создания Web-ресурсов, Образовательная робототехника, Web-дизайн, Детали модулей роботов и их конструирование**		

УК-5	**Деловой иностранный язык, Современные проблемы защиты данных в компьютерных сетях, Web-дизайн**		

Раздел 2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Таблица 4 - Показатели оценивания компетенций на различных этапах их формирования в процессе освоения учебной дисциплины (в соответствии с РПД)

№	Раздел	
	Формируемые компетенции	
	Показатели сформированности (в терминах «знать», «уметь», «владеть»)	**Виды оценочных средств**
1	Современные проблемы защиты данных в компьютерных сетях	
	ПК-4 УК-5	
	Знать знать основные понятия шифрования данных для защиты информации в компьютерных сетях Знать знать основные понятия в области защиты информации в процессе информационной коммуникации	Отчет по лабораторной работе
	Уметь уметь применять методы шифрования данных для защиты информации в компьютерных сетях для обучения криптографическим алгоритмам в системах общего, процессионального и дополнительного образования Уметь уметь применять методы защиты информации при демонстрации алгоритмов шифрования в процессе обучения при работе в компьютерных сетях	Отчет по лабораторной работе
	Владеть владеть технологией шифрования данных для демонстрации приемов защиты информации в компьютерных сетях Владеть владеет технологией объяснения сложных алгоритмов, в том числе алгоритмов шифрования, в системе образования	Доклад/сообщение

Таблица 5 - Описание уровней и критериев оценивания компетенций, описание шкал оценивания

Код	**Содержание компетенции**			
Уровни освоения компетенции	**Содержательное описание уровня**	**Основные признаки выделения уровня (критерии оценки сформированности)**	**Пятибалльная шкала (академическая оценка)**	**% освоения (рейтинговая оценка)**
ПК-4	ПК-4 способен проектировать и реализовывать программы общего, профессионального и дополнительного образования			
УК-5	УК-5 способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия			

Раздел 3. Типовые контрольные задания и (или) иные материалы, необходимые для оценки планируемых результатов обучения по дисциплине (модулю)

1. Оценочные средства для текущего контроля

Раздел: Современные проблемы защиты данных в компьютерных сетях

Задания для оценки знаний

1. Отчет по лабораторной работе:

Выступление с докладами и участие в дискуссии по современным способам защиты информации в компьютерных сетях.
Примерные вопросы:
1. Способы защиты аккаунтов от взлома.
2. Как хранятся пароли в информационных системах.
3. Фишинг как современный способ мошенничества и рекомендации как не попасться на удочку к мошенникам.
4. Роль социальной инженерии при доступе к конфиденциальной информации.
5. Биометрические параметры человека как средство защиты информации

Приложение 1.
Задание 1.
Найдите и обсудите в сети интернет рекомендации, как можно отличить фишинговое сообщение в почтовом ящике от настоящего. Сформулируйте рекомендации по действиям пользователя в таком случае.
Примеры фишинговых сообщений в почте

Задание 2.
Рассмотрите и обсудите методы социальной инженерии для получения важных сведений. Например, получить важные сведения о персональных данных сотрудников, данных из информационных систем и других конфиденциальных сведений.
Дополните следующий список мероприятий по противодействию методов социального инжиниринга:
1. Не фотографируйте и не выкладывайте в общий доступ важные данные, тем более персональные (паспортные данные, карточки, идентификационные номера, штрих-коды, билеты и др.). Помните, что даже мессенджеры с частной перепиской могут быть взломаны или их данные могут быть переданы третьим лицам.
2. Не используйте один и тот же пароль для различных сервисов. Не используйте пароль, который содержит часть персональных данных (дату рождения, имя, фамилию).
3. Подчиняйтесь протоколам и правилам, которые сформулировал отдел информационной безопасности той организации, в которой вы учитесь или работаете. Например, если нельзя пользоваться внешними почтовыми ящиками в организации, а использовать только корпоративный ящик. Например, нельзя копировать на собственные носители и выносить конфиденциальную информацию.
4. Не переходите по ссылкам из писем, особенно тем, где от вас просят ввести какие-то данные: номер карты, email и пароль, коды от карт.
5. Используйте двухфакторную аутентификацию в платежных системах, интернет-магазинах и др.
6. Не отключайте по чьей-либо просьбе сетевой экран (брандмауэр) на рабочем компьютере, если вы работаете с конфиденциальной информацией и это действие противоречит политике информационной безопасности вашей организации.
7. Не старайтесь всегда и во всем помогать людям, прежде всего малознакомым: сначала могут спросить, как пройти в какой-то отдел, потом могут уточнить конфиденциальную информацию. Должен быть всегда трезвый контроль тех действий и информации, которую вы сообщаете человеку, которого видите впервые или не знаете его имени.
8. Критически относитесь к действиям, которые выполняют большое количество людей. Если вам рассказывают, что большинство людей уже извлекли финансовую выгоду из какого-то мероприятия, к которому склоняют и вас – перепроверьте эту информацию или возьмите время на раздумье. А лучше откажитесь.

Задание 3.
Рассмотрите тест по информационной безопасности. Самостоятельно или в группах пройдите тести и обсудите вопросы теста.
https://иб-диктант.рф

Задания для оценки умений

1. Отчет по лабораторной работе:

Выступление с докладами и участие в дискуссии по современным способам защиты информации в компьютерных сетях.
Примерные вопросы:
1. Способы защиты аккаунтов от взлома.
2. Как хранятся пароли в информационных системах.
3. Фишинг как современный способ мошенничества и рекомендации как не попасться на удочку к мошенникам.
4. Роль социальной инженерии при доступе к конфиденциальной информации.
5. Биометрические параметры человека как средство защиты информации

Приложение 1.
Задание 1.
Найдите и обсудите в сети интернет рекомендации, как можно отличить фишинговое сообщение в почтовом ящике от настоящего. Сформулируйте рекомендации по действиям пользователя в таком случае.
Примеры фишинговых сообщений в почте

Задание 2.
Рассмотрите и обсудите методы социальной инженерии для получения важных сведений. Например, получить важные сведения о персональных данных сотрудников, данных из информационных систем и других конфиденциальных сведений.
Дополните следующий список мероприятий по противодействию методов социального инжиниринга:
1. Не фотографируйте и не выкладывайте в общий доступ важные данные, тем более персональные (паспортные данные, карточки, идентификационные номера, штрих-коды, билеты и др.). Помните, что даже мессенджеры с частной перепиской могут быть взломаны или их данные могут быть переданы третьим лицам.
2. Не используйте один и тот же пароль для различных сервисов. Не используйте пароль, который содержит часть персональных данных (дату рождения, имя, фамилию).
3. Подчиняйтесь протоколам и правилам, которые сформулировал отдел информационной безопасности той организации, в которой вы учитесь или работаете. Например, если нельзя пользоваться внешними почтовыми ящиками в организации, а использовать только корпоративный ящик. Например, нельзя копировать на собственные носители и выносить конфиденциальную информацию.
4. Не переходите по ссылкам из писем, особенно тем, где от вас просят ввести какие-то данные: номер карты, email и пароль, коды от карт.
5. Используйте двухфакторную аутентификацию в платежных системах, интернет-магазинах и др.
6. Не отключайте по чьей-либо просьбе сетевой экран (брандмауэр) на рабочем компьютере, если вы работаете с конфиденциальной информацией и это действие противоречит политике информационной безопасности вашей организации.
7. Не старайтесь всегда и во всем помогать людям, прежде всего малознакомым: сначала могут спросить, как пройти в какой-то отдел, потом могут уточнить конфиденциальную информацию. Должен быть всегда трезвый контроль тех действий и информации, которую вы сообщаете человеку, которого видите впервые или не знаете его имени.
8. Критически относитесь к действиям, которые выполняют большое количество людей. Если вам рассказывают, что большинство людей уже извлекли финансовую выгоду из какого-то мероприятия, к которому склоняют и вас – перепроверьте эту информацию или возьмите время на раздумье. А лучше откажитесь.

Задание 3.
Рассмотрите тест по информационной безопасности. Самостоятельно или в группах пройдите тести и обсудите вопросы теста.
https://иб-диктант.рф

Задания для оценки владений

1. Доклад/сообщение:

Представить отчет по лабораторной работе "Простейшие методы шифрования с закрытым ключом", в котором выполнить решение следующих алгоритмов
1. Шифрование и дешифрование по алгоритму "Скитала"
2. Шифрование и дешифрование по алгоритму "Цезаря"
3. Шифрование и дешифрование по алгоритму "Виженера"
4. Метод гаммирования при шифровании данных
5. Блочные алгоритмы шифрования.
6. Симметричное шифрование.

2. Оценочные средства для промежуточной аттестации

1. Зачет

Вопросы к зачету:

1. Предмет и задачи криптографии
2. Основные определения
3. Реализация криптографических методов
4. Криптографические атаки
5. Пример шифра Юлия Цезаря
6. Криптографический протокол
7. Общая схема симметричного шифрования
8. Методы замены
9. Одноалфавитная замена
10. Пропорциональные шифры
11. Многоалфавитные подстановки
12. Методы гаммирования
13. Методы перестановки
14. Перестановка с фиксированным периодом
15. Перестановка по таблице
16. Понятие композиционного шифра
17. Операции, используемые в блочных алгоритмах симметричного шифрования
18. Структура блочного алгоритма симметричного шифрования
19. Сеть Фейштеля
20. Требования к блочному алгоритму шифрования
21. Понятие хеш-функции
22. Использование блочных алгоритмов шифрования для формирования хеш-функции
23. Обзор алгоритмов формирования хеш-функций
24. Алгоритмы шифрования с открытым ключом
25. Цифровая подпись на основе алгоритмов с открытым ключом
26. Стандарты на алгоритмы цифровой подписи
27. Применение электронно-цифровой подписи
28. Новый отечественный стандарт электронной цифровой подписи
29. Аутентификация
30. Идентификация
31. Защита при администрировании систем
32. Обработка регистрационных журналов
33. Определение прав доступа к ресурсам
34. Запуск системы защиты на ЭВМ
35. Брандмауэры как средство защиты данных при работе в компьютерных сетях
36. Понятие фишинга в сети интернет
37. Социальный инжиниринг как способ доступа злоумышленника к конфиденциальной информации
38. Информационная безопасность в сети интернет
39. Роль антивирусного программного обеспечения в системе информационной безопасности при работе в компьютерных сетях
40. Аппаратные, программные и административные способы защиты информации в компьютерных сетях

Раздел 4. Методические материалы, определяющие процедуры оценивания значни, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

1. Для текущего контроля используются следующие оценочные средства:

1. Доклад/сообщение

Доклад − развернутое устное (возможен письменный вариант) сообщение по определенной теме, сделанное публично, в котором обобщается информация из одного или нескольких источников, представляется и обосновывается отношение к описываемой теме.
Основные этапы подготовки доклада:
1. четко сформулировать тему;
2. изучить и подобрать литературу, рекомендуемую по теме, выделив три источника библиографической информации:
− первичные (статьи, диссертации, монографии и т. д.);
− вторичные (библиография, реферативные журналы, сигнальная информация, планы, граф-схемы, предметные указатели и т. д.);
− третичные (обзоры, компилятивные работы, справочные книги и т. д.);
3. написать план, который полностью согласуется с выбранной темой и логично раскрывает ее;
4. написать доклад, соблюдая следующие требования:
− структура доклада должна включать краткое введение, обосновывающее актуальность проблемы; основной текст; заключение с краткими выводами по исследуемой проблеме; список использованной литературы;
− в содержании доклада общие положения надо подкрепить и пояснить конкретными примерами; не пересказывать отдельные главы учебника или учебного пособия, а изложить собственные соображения по существу рассматриваемых вопросов, внести свои предложения;
5. оформить работу в соответствии с требованиями.

2. Отчет по лабораторной работе

При составлении и оформлении отчета следует придерживаться рекомендаций, представленных в методических указаниях по выполнению лабораторных работ по дисциплине.

2. Описание процедуры промежуточной аттестации

Оценка за зачет/экзамен может быть выставлена по результатам текущего рейтинга. Текущий рейтинг – это результаты выполнения практических работ в ходе обучения, контрольных работ, выполнения заданий к лекциям (при наличии) и др. видов заданий.

Результаты текущего рейтинга доводятся до студентов до начала экзаменационной сессии.

Цель зачета − проверка и оценка уровня полученных студентом специальных знаний по учебной дисциплине и соответствующих им умений и навыков, а также умения логически мыслить, аргументировать избранную научную позицию, реагировать на дополнительные вопросы, ориентироваться в массиве информации.

Зачет может проводиться как в формате, аналогичном проведению экзамена, так и в других формах, основанных на выполнении индивидуального или группового задания, позволяющего осуществить контроль знаний и полученных навыков.

Подготовка к зачету начинается с первого занятия по дисциплине, на котором обучающиеся получают предварительный перечень вопросов к зачёту и список рекомендуемой литературы, их ставят в известность относительно критериев выставления зачёта и специфике текущей и итоговой аттестации. С самого начала желательно планомерно осваивать материал, руководствуясь перечнем вопросов к зачету и списком рекомендуемой литературы, а также путём самостоятельного конспектирования материалов занятий и результатов самостоятельного изучения учебных вопросов.

По результатам сдачи зачета выставляется оценка «зачтено» или «не зачтено».