Федеральное государственное бюджетное образовательное учреждение высшего образования «Мордовский государственный педагогический университет имени М.Е. Евсевьева»

Физико-математический факультет

Кафедра Информатики и вычислительной техники

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Информационная безопасность в сети Интернет

Направление подготовки: 44.04.01 Педагогическое образование

Профиль подготовки: Информатика и информационные технологии в образовании

Форма обучения: Очная

Разработчики:
канд. физ.-мат. наук, доцент кафедры Информатики и вычислительной техники Кормилицына Т. В.

Программа рассмотрена и утверждена на заседании кафедры, протокол № 11 от 16.05.2019 года

Зав. кафедрой _____Вознесенская Н. В.

Программа с обновлениями рассмотрена и утверждена на заседании кафедры, протокол № 1 от 31.08.2020 года

Зав. кафедрой _____Зубрилин А. А.

1. Цель и задачи изучения дисциплины

Цель изучения дисциплины - формирование у студентов информационного мировоззрения на основе знания аспектов защиты информации и воспитание информационной культуры для эффективного применения полученных знаний в профессиональной деятельности.

Задачи дисциплины:

- изучение основных направлений организации информационной безопасности (правового, технического, аппаратного);
- изучение основ правового регулирования информационной безопасности в России;
- формирование знаний о технических способах и средствах обеспечения защиты информации;
- изучение программных средств обеспечения информационной безопасности при работе на ПК и в сети Интернет;
- формирование умений разрабатывать и реализовывать политику информационной безопасности на предприятии, в частности в образовательном учреждении.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина К.М.05.ДВ.01.1 «Информационная безопасность в сети Интернет» относится к обязательной части учебного плана.

Дисциплина изучается на 2 курсе, в 4 семестре.

Для изучения дисциплины требуется: знание основ функционирования компьютерных сетей, современных тенденций электронного образования, теории и практики разработки информационных образовательных сред.

Изучению дисциплины К.М.05.ДВ.01.1 «Информационная безопасность в сети Интернет» предшествует освоение дисциплин (практик):

К.М.2 Современные тренды электронного обучения;

К.М.3 Теория и практика разработки электронной информационно-образовательной среды.

Освоение дисциплины К.М.05.ДВ.01.1 «Информационная безопасность в сети Интернет» является необходимой основой для последующего изучения дисциплин (практик):

К.М.2 Организация электронной информационно-образовательной среды;

К.М.5 Прикладные информационные технологии в деятельности педагога;

К.М.05.ДВ.01.2 Информационная безопасность в образовании.

Область профессиональной деятельности, на которую ориентирует дисциплина «Информационная безопасность в сети Интернет», включает: 01 Образование и наука (в сфере начального общего, основного общего, среднего общего образования, профессионального обучения, профессионального образования, дополнительного образования; в сфере научных исследований)
04 Культура, искусство (в сфере организации отдыха и развлечений, реализации зрелищно-развлекательной и культурно-просветительской деятельности).

Типы задач и задачи профессиональной деятельности, к которым готовится обучающийся, определены учебным планом.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Компетенция в соответствии ФГОС ВО	
Индикаторы достижения компетенций	**Образовательные результаты**
УК-2. Способен управлять проектом на всех этапах его жизненного цикла	

УК-2.1 Выстраивает этапы работы над проектом с учетом последовательности их реализации, определяет этапы жизненного цикла проекта.	знать: - этапы работы по обеспечению мер информационной безопасности образовательной организации; уметь: - проектировать этапы работы по обеспечению мер информационной безопасности образовательного учреждения; владеть: - навыком проектирования этапов работы по обеспечению мер информационной безопасности образовательной организации.
УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	
УК-3.3 Способен устанавливать разные виды коммуникации (устную, письменную, вербальную, невербальную, реальную, виртуальную, межличностную и др.) для руководства командой и достижения поставленной цели.	знать: - современные методы и средства коммуникации, используемые в сети Интернет; уметь: - использовать современные методы и средства коммуникации в при работе в Интернет-пространстве; владеть: - современными методами и средствами коммуникации .

ПК-3. Способен формировать у обучающихся умение применять средства информационно-коммуникационных технологий в решении задач там, где это эффективно.

педагогический деятельность

ПК-3.1 Знает: нормы законодательства РФ, регламентирующие использование ИКТ и электронного обучения при реализации основных и дополнительных образовательных программ; требования к использованию ИТ-методов, инструментов и технологий для создания электронной информационно-образовательной среды.	знать: - правовые особенности применения норм законодательства РФ в области использования ИКТ и электронного обучения при реализации основных и дополнительных образовательных программ; уметь: - применять основные принципы безопасной работы в Интернет; владеть: - навыками безопасной работы в Интернет.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Четвертый семестр
Контактная работа (всего)	**10**	**10**
Практические	10	10
Самостоятельная работа (всего)	**62**	**62**
Виды промежуточной аттестации		
Зачет с оценкой		+
Общая трудоемкость часы	**72**	**72**
Общая трудоемкость зачетные единицы	**2**	**2**

5. Содержание дисциплины

5.1. Содержание разделов дисциплины

Раздел 1. Основы информационной безопасности:

Правовой аспект информационной безопасности. Понятие информационной угрозы, виды угроз.

Раздел 2. Практические вопросы организации информационной безопасности в сети:

Системы защиты от угроз нарушения доступности информации. Основные классы мер процедурного уровня. Идентификация и аутентификация.

5.2. Содержание дисциплины: Практические (10 ч.)

Раздел 1. Основы информационной безопасности (4 ч.)

Тема 1. Правовой аспект информационной безопасности (2 ч.)

Практическое занятие направлено на изучение нормативно-правовой базы по вопросам информационной безопасности. Законодательная основа информацооной безопасности. Информационное право в России. Структура законодательства России в области защиты информации. Нормативно-правовые документы на всех государственных уровнях, регламентирующих организацию защиты информации в РФ. Конфиденциальная информация, государственная тайна. Нарушение информационной безопасности и их последствия.

Тема 2. Понятие информационной угрозы, виды угроз (2 ч.)

Основные определения и критерии классификации угроз
Наиболее распространенные угрозы доступности
Некоторые примеры угроз доступности
Вредоносное программное обеспечение
Основные угрозы целостности
Основные угрозы конфиденциальности

Раздел 2. Практические вопросы организации информационной безопасности в сети (6 ч.)

Тема 3. Системы защиты от угроз нарушения доступности информации (2 ч.)

Оценочные стандарты и технические спецификации. "Оранжевая книга" как оценочный стандарт. Механизмы безопасности. Классы безопасности.
Информационная безопасность распределенных систем. Сетевые сервисы безопасности. Сетевые механизмы безопасности. Администрирование средств безопасности. Стандарт ISO/IEC 15408 " Критерии оценки безопасности информационных технологий"

Тема 4. Основные классы мер процедурного уровня (2 ч.)

Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ.

Тема 5. Идентификация и аутентификация (2 ч.)

Основные понятия. Парольная аутентификация. Одноразовые пароли
Идентификация/аутентификация с помощью биометрических данных

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (разделу)

6.1 Вопросы и задания для самостоятельной работы

Четвертый семестр (41,333333333333333332 ч.)

Раздел 1. Основы информационной безопасности (31 ч.)

Вид СРС: *Подготовка письменных работ (эссе, рефератов, докладов)

Подготовьте реферат по заданной теме.

Темы рефератов

1. Политика информационной на предприятии.
2. Организация защиты электронной почты.
3. Организация защиты ПК на предприятии.
4. Нормативно-правовой аспект защиты информации на предприятии.

5. Организация защиты баз данных.
6. Ответственность за нарушения в сфере информационного права.
7. Конфиденциальная информация, ее виды и способы защиты.
8. Программные средства защиты (ПК, локальной компьютерной сети).

Вид СРС: *Работа с электронными ресурсами и информационными системами

Прохождение онлайн курса:

"Основы информационной безопасности при работе на компьютере" http://www.intuit.ru/studies/courses/680/536/info

Раздел 2. Практические вопросы организации информационной безопасности в сети (31 ч.)

Вид СРС: *Работа с электронными ресурсами и информационными системами

Прохождение онлайн-курса "Основы криптографии". - URL https://www.intuit.ru/studies/courses/691/547/info

Вид СРС: *Выполнение индивидуальных заданий

Подготовьте реферат по заданной теме.

Темы рефератов

1. Электронная цифровая подпись.
2. Киберпреступность в России и в других странах.
3. Криптографические системы защиты данных.
4. Исторические шифры.
5. Современный шифры.

7. Тематика курсовых работ(проектов)

Курсовые работы (проекты) по дисциплине не предусмотрены.

8. Оценочные средства

8.1. Компетенции и этапы формирования

№ п/п	Оценочные средства	Компетенции, этапы их формирования

8.2. Показатели и критерии оценивания компетенций, шкалы оценивания

Шкала, критерии оценивания и уровень сформированности компетенции			
2 (не зачтено) ниже порогового	3 (зачтено) пороговый	4 (зачтено) базовый	5 (зачтено) повышенный
ПК-3 Способен проектировать содержание учебных дисциплин и конкретных моделей обучения			
ПК-3.1 Знает: нормы законодательства РФ, регламентирующие использование ИКТ и электронного обучения при реализации основных и дополнительных образовательных программ; требования к использованию ИТ-методов, инструментов и технологий для создания электронной информационно-образовательной среды.			

Не знает нормы законодательства РФ, регламентирующие использование ИКТ и электронного обучения при реализации основных и дополнительных образовательных программ; требования к использованию ИТ-методов, инструментов и технологий для создания электронной информационно-образовательной среды.	В целом успешно, но бессистемно знает нормы законодательства РФ, регламентирующие использование ИКТ и электронного обучения при реализации основных и дополнительных образовательных программ; требования к использованию ИТ-методов, инструментов и технологий для создания электронной информационно-образовательной среды.	В целом успешно, но с отдельными недочетами знает нормы законодательства РФ, регламентирующие использование ИКТ и электронного обучения при реализации основных и дополнительных образовательных программ; требования к использованию ИТ-методов, инструментов и технологий для создания электронной информационно-образовательной среды.	В полном объеме знае нормы законодательства РФ, регламентирующие использование ИКТ и электронного обучения при реализации основных и дополнительных образовательных программ; требования к использованию ИТ-методов, инструментов и технологий для создания электронной информационно-образовательной среды.
УК-2 Способен управлять проектом на всех этапах его жизненного цикла			
УК-2.1 Выстраивает этапы работы над проектом с учетом последовательности их реализации, определяет этапы жизненного цикла проекта.			
Не способен выстраивать этапы работы над проектом с учетом последовательности их реализации, определяет этапы жизненного цикла проекта.	В целом успешно, но бессистемно выстраивает этапы работы над проектом с учетом последовательности их реализации, определяет этапы жизненного цикла проекта.	В целом успешно, но с отдельными недочетами выстраивает этапы работы над проектом с учетом последовательности их реализации, определяет этапы жизненного цикла проекта.	Способен в полном объеме выстраивать этапы работы над проектом с учетом последовательности их реализации, определяет этапы жизненного цикла проекта.
УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели			
УК-3.3 Способен устанавливать разные виды коммуникации (устную, письменную, вербальную, невербальную, реальную, виртуальную, межличностную и др.) для руководства командой и достижения поставленной цели.			
Не способен устанавливать разные виды коммуникации (устную, письменную, вербальную, невербальную, реальную, виртуальную, межличностную и др.) для руководства командой и достижения поставленной цели.	В целом успешно, но бессистемно устанавливает разные виды коммуникации (устную, письменную, вербальную, невербальную, реальную, виртуальную, межличностную и др.) для руководства командой и достижения поставленной цели.	В целом успешно, но с отдельными недочетами устанавливает разные виды коммуникации (устную, письменную, вербальную, невербальную, реальную, виртуальную, межличностную и др.) для руководства командой и достижения поставленной цели.	Способен в полном объеме устанавливать разные виды коммуникации (устную, письменную, вербальную, невербальную, реальную, виртуальную, межличностную и др.) для руководства командой и достижения поставленной цели.

Уровень сформированности компетенции	Шкала оценивания для промежуточной аттестации		Шкала оценивания по БРС
	Экзамен (дифференцированный зачет)	Зачет	
Повышенный	5 (отлично)	зачтено	90 – 100%
Базовый	4 (хорошо)	зачтено	76 – 89%
Пороговый	3 (удовлетворительно)	зачтено	60 – 75%
Ниже порогового	2 (неудовлетворительно)	незачтено	Ниже 60%

8.3. Вопросы промежуточной аттестации

Четвертый семестр (Зачет с оценкой, ПК-3.1, УК-2.1, УК-3.3)

1. Определите понятие информационной безопасности. Укажите место вопросов информационной безопасности в системе обеспечения национальной безопасности.
2. Перечислите основные составляющие и аспекты информационной безопасности.
3. Проведите классификацию угроз информационной безопасности: для личности, для общества, для государства.
4. Перечислите основные задачи в сфере обеспечения информационной безопасности и приведите способы их решения.
5. Опишите отечественные стандарты в области информационной безопасности.
6. Опишите зарубежные стандарты в области информационной безопасности.
7. Раскройте понятие защиты информации.
8. Опишите основные критерии оценки надежности: политика безопасности и гарантированность.
9. Расскажите об основных конституционных гарантиях по охране и защите прав и свобод в информационной сфере.
10. Дайте понятие надежности информации в автоматизированных системах обработки данных. Что понимается под системной защитой информации.
11. Укажите причины уязвимости информации в автоматизированных системах обработки данных.
12. Дайте описание элементов и объектов защиты в автоматизированных системах обработки данных.
13. Приведите примеры использования методов защиты информации от преднамеренного доступа.
14. Расскажите о процессе реализации защиты информации от копирования.
15. Опишите криптографические методы защиты информации в автоматизированных системах.
16. Расскажите об основных направлениях использования криптографических методов. Симметричные криптосистемы. Системы с открытым ключом.
17. Объясните назначение электронной (цифровой) подписи. Выделите цели ее применения.
18. Введите понятие криптостойкости шифра, перечислите требования к криптографическим системам защиты информации.
19. Перечислите способы опознавания (аутентификации) пользователей и используемых компонентов обработки информации и дайте их краткую характеристику.
20. Укажите признаки для классификации компьютерных вирусов.
21. Укажите способы заражения программ, выделите стандартные методы заражения.
22. Расскажите о функционирования компьютерного вируса. Опишите методы защиты от компьютерных вирусов.
23. Назовите антивирусные программы: программы-детекторы, программы-доктора. Опишите их назначение и возможности.

24. Назовите антивирусные программы: антивирусы-полифаги, эвристические анализаторы. Опишите их назначение и возможности.

25. Назовите антивирусные программы: программы-ревизоры, программы-фильтры. Опишите их назначение и возможности.

26. Сформулируйте цели, функции и задачи защиты информации в компьютерных сетях. Перечислите угрозы безопасности для сетей передачи данных.

27. Опишите задачи защиты в сетях передачи данных.

28. Составьте инструкцию по безопасной работе на компьютере для сотрудника предприятия.

29. Составьте инструкцию по безопасной работе в сети Интернет для сотрудника предприятия.

30. Перечислите обязанности администратора образовательного учреждения по соблюдению требований информационной безопасности на предприятии.

8.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Промежуточная аттестация проводится в форме зачета с оценкой.

Зачет позволяет оценить сформированность универсальных, общепрофессиональных и профессиональных компетенций, теоретическую подготовку студента, его способность к творческому мышлению, готовность к практической деятельности, приобретенные навыки самостоятельной работы, умение синтезировать полученные знания и применять их при решении практических задач.

При балльно-рейтинговом контроле знаний итоговая оценка выставляется с учетом набранной суммы баллов.

Устный ответ на зачете

Для оценки сформированности компетенции посредством собеседования (устного ответа) студенту предварительно предлагается перечень вопросов или комплексных заданий, предполагающих умение ориентироваться в проблеме, знание теоретического материала, умения применять его в практической профессиональной деятельности, владение навыками и приемами выполнения практических заданий.

При оценке достижений студентов необходимо обращать особое внимание на:

– усвоение программного материала;

– умение излагать программный материал научным языком;

– умение связывать теорию с практикой;

– умение отвечать на видоизмененное задание;

– владение навыками поиска, систематизации необходимых источников литературы по

изучаемой проблеме;
– умение обосновывать принятые решения;
– владение навыками и приемами выполнения практических заданий;
– умение подкреплять ответ иллюстративным материалом.

9. Перечень основной и дополнительной учебной литературы

Основная литература

1. Башлы, П.Н. Информационная безопасность : учебно-практическое пособие / П.Н. Башлы, Е.К. Баранова, А.В. Бабаш. – Москва : Евразийский открытый институт, 2011. – 375 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=90539 (дата обращения: 28.04.2020). – ISBN 978-5-374-00301-7. – Текст : электронный.

2. Ковалев, Д.В. Информационная безопасность : учебное пособие / Д.В. Ковалев, Е.А. Богданова ; Министерство образования и науки РФ, Южный федеральный университет. – Ростов-на-Дону : Южный федеральный университет, 2016. – 74 с. : схем., табл., ил. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=493175. – ISBN 978-5-9275-2364-1. – Текст : электронный.

3. Прохорова, О.В. Информационная безопасность и защита информации : учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». – Самара : Самарский государственный архитектурно-строительный университет, 2014. – 113 с. : табл., схем., ил. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=438331. – Библиогр. в кн. – ISBN 978-5-9585-0603-3. – Текст : электронный

Дополнительная литература

1. Сычев, Ю.Н. Основы информационной безопасности : учебно-практическое пособие / Ю.Н. Сычев. – Москва : Евразийский открытый институт, 2010. – 328 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=90790. – ISBN 978-5-374-00381-9. – Текст : электронный

2. Голиков, А.М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А.М. Голиков ; Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 284 с. : схем., табл., ил. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=480637. – Библиогр. в кн. – Текст : электронный

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://www.intuit.ru - Интернет-Университет Информационных Технологий [Электронный ресурс] / Бесплатные учебные курсы по информационным технологиям. – М. : НОУ «ИНТУИТ»,

2. http://www.securitylab.ru - Security Lab by Positive Technologies [Электронный ресурс] . URL: http://www.securitylab.ru

3. http://all-ib.ru - Информационная безопасность. Защита информации

11. Методические указания обучающимся по освоению дисциплины (модуля)

При освоении материала дисциплины необходимо:
– спланировать и распределить время, необходимое для изучения дисциплины;
– конкретизировать для себя план изучения материала;
– ознакомиться с объемом и характером внеаудиторной самостоятельной работы для полноценного освоения каждой из тем дисциплины.

Сценарий изучения курса:
– проработайте каждую тему по предлагаемому ниже алгоритму действий;
– изучив весь материал, выполните итоговый тест, который продемонстрирует готовность к

сдаче зачета и экзамена.

Алгоритм работы над каждой темой:

– изучите содержание темы вначале по теоретическому материалу, а затем по другим источникам;

– ознакомьтесь с дополнительной литературой из списка, предложенного преподавателем;

– выпишите в тетрадь основные категории и понятия по вопросам информационной безопасности, используя лекционный материал или словари, что поможет быстро повторить материал при подготовке к зачету;

– составьте краткий план ответа по каждому вопросу, выносимому на обсуждение на практическом занятии;

– выучите определения терминов, относящихся к теме;

– продумайте примеры и иллюстрации к ответу по изучаемой теме;

– продумывайте высказывания по темам, предложенным к практическому занятию.

Рекомендации по работе с литературой:

– ознакомьтесь с аннотациями к рекомендованной литературе и определите основной метод изложения материала того или иного источника;

– составьте собственные аннотации к другим источникам на карточках, что поможет при подготовке рефератов, текстов речей, при подготовке к зачету;

– выберите те источники, которые наиболее подходят для изучения конкретной темы.

12. Перечень информационных технологий

Реализация учебной программы обеспечивается доступом каждого студента к информационным ресурсам – электронной библиотеке и сетевым ресурсам Интернет. Для использования ИКТ в учебном процессе используется программное обеспечение, позволяющее осуществлять поиск, хранение, систематизацию, анализ и презентацию информации, экспорт информации на цифровые носители, организацию взаимодействия в реальной и виртуальной образовательной среде.

Индивидуальные результаты освоения дисциплины студентами фиксируются в информационной системе 1С:Университет.

12.1 Перечень программного обеспечения (обновление призводится по мере появления новых версий программы)

1. Microsoft Windows 7 Pro
2. Microsoft Office Professional Plus 2010
3. 1С: Университет ПРОФ

12.2 Перечень информационных справочных систем (обновление выполняется еженедельно)

1. Информационно-правовая система "ГАРАНТ" (http://www.garant.ru)
2. Справочная правовая система «КонсультантПлюс» (http://www.consultant.ru)

12.3 Перечень современных профессиональных баз данных

1. Профессиональная база данных «Открытые данные Министерства образования и науки РФ» (http://xn----8sblcdzzacvuc0jbg.xn--80abucjiibhv9a.xn--p1ai/ope
2. Единое окно доступа к образовательным ресурсам (http://window.edu.ru)
3. Международная реферативная база данных Scopus (http://www.scopus.com/)

13. Материально-техническое обеспечение дисциплины(модуля)

Для проведения аудиторных занятий необходим стандартный набор специализированной учебной мебели и учебного оборудования, а также мультимедийное оборудование для демонстрации презентаций на лекциях. Для проведения практических занятий, а также организации самостоятельной работы студентов необходим компьютерный класс с рабочими местами, обеспечивающими выход в Интернет.

При изучении дисциплины используется интерактивный комплекс Flipbox для

проведения презентаций и видеоконференций, система iSpring в процессе проверки знаний п
электронным тест-тренажерам.

Оснащение аудиторий

1. Доска магнитно-маркерная эконом - 1 шт.
2. АРМ (в составе: персональный компьютер) - 1 шт.
3. Интерактивная доска - 1 шт.
4. АРМ-9 - 13 шт.
5. Проектор EPSON - 1 шт.