

**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

Безопасность образовательных Интернет-систем

Направление подготовки: 44.03.05 Педагогическое образование (с двумя профилями подготовки)

Профиль подготовки: Менеджмент в образовании. Информационная безопасность в образовании

Форма обучения: Очная

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

Программа рассмотрена и утверждена на заседании кафедры, протокол № 9 от 17.03.2022 года

Зав. кафедрой _____



_____Зубрилин А. А.

1. Цель и задачи изучения дисциплины

Цель изучения дисциплины – формирование у студентов навыков профессиональных компетенций в области информационной безопасности при организации образовательного процесса, эффективное использование полученных знаний в жизни и практической деятельности.

Задачи дисциплины:

- ознакомить студентов с теоретическими основами информационной безопасности при организации образовательного процесса в образовательных интернет-системах;
- ознакомить студентов с основными источниками и видами опасностей и угроз информационной безопасности при использовании образовательных интернет-систем;
- сформировать у студентов умения и навыки реализации методов обеспечения безопасности образовательных интернет-систем.

В том числе воспитательные задачи:

- формирование мировоззрения и системы базовых ценностей личности;
- формирование основ профессиональной культуры обучающегося в условиях трансформации области профессиональной деятельности.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина К.М.08.10 «Безопасность образовательных интернет-систем» относится к базовой части учебного плана.

Дисциплина изучается на 2 курсе, в 4 семестре.

Освоение дисциплины К.М.06.30 «Безопасность образовательных интернет-систем» является необходимой основой для последующего изучения дисциплин (практик):

Безопасность информационных систем и баз данных

Экосистема медийного пространства

Управление проектами в образовании

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Компетенция в соответствии ФГОС ВО	
Индикаторы достижения компетенций	Индикаторы достижения компетенций
ПК-1. Способен осваивать и использовать теоретические знания и практические умения и навыки в предметной области при решении профессиональных задач педагогическая деятельность	
ПК-1.3. Демонстрирует умение разрабатывать различные формы учебных занятий, применять методы, приемы и технологии обучения, в том числе информационные	ПК-1.3. Демонстрирует умение разрабатывать различные формы учебных занятий, применять методы, приемы и технологии обучения, в том числе информационные
ПК-8. Способен организовывать образовательный процесс с использованием современных образовательных технологий, в том числе дистанционных методическая деятельность	
ПК-8.1. Разрабатывает образовательные программы различных уровней в соответствии с современными методиками и технологиями.	ПК-8.1. Разрабатывает образовательные программы различных уровней в соответствии с современными методиками и технологиями.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	4 семестр
Контактная работа (всего)	36	36
Лекции	18	18
Практические	18	18
Самостоятельная работа (всего)	36	36
Виды промежуточной аттестации		
Зачет		+
Общая трудоемкость часы	72	72
Общая трудоемкость зачетные единицы	2	2

5. Содержание дисциплины

5.1. Содержание разделов дисциплины:

Раздел 1. Информационная безопасность образовательных интернет-систем

Информационные границы образования. Образовательные Интернет-системы. Нормативно-правовые аспекты защиты информации в образовательных организациях.

Раздел 2. Методы и средства реализации безопасности образовательных интернет-систем

Методологические подходы к организации безопасной информационно-образовательной среды. Особенности обеспечения информационной безопасности при организации образовательного процесса. Моделирование нарушения безопасности предприятия и поиск решений

5.2. Содержание дисциплины: Лекции (18 ч.)

Раздел 1. Информационная безопасность образовательных интернет-систем (8 ч.)

Тема 1. Информационные границы образования. Социально-информационное пространство эпохи информационного общества (2 ч.)

Образовательные Интернет-системы. Информационная безопасность обучающихся. Аспекты информационной безопасности - активная и пассивная формы.

Понятие и классификация образовательных интернет-систем

Тема 2. Основные понятия информационной безопасности. (2 ч.)

Концепция информационной безопасности; основные понятия: информационная безопасность, защита информации, угроза, утечка, уязвимость, отказ, сбой; виды защищаемой информации; информационная безопасность образовательного учреждения; способы несанкционированного доступа.

Тема 3. Нормативно-правовые аспекты защиты информации в образовательных организациях (2 ч.)

Виды защищаемой информации. основополагающие документы; обзор законов, указов, актов.

Персональные данные. Виды персональных данных; понятия субъекта и объекта персональных данных; обработка персональных данных; обязанности оператора персональных данных; принципы обработки персональных данных; ответственность за неправомерное использование персональных данных; полезная информация.

Раздел 2. Методы и средства реализации безопасности образовательных интернет-систем (10 ч.)

Тема 4. Методологические подходы к организации безопасной информационно-образовательной среды (2 ч.)

Создание безопасной информационной среды образовательного комплекса как необходимое условия обеспечения качества образования. ЦОС образовательной организации

Тема 5. Угрозы информационной безопасности образовательной организации Виды угроз информационной безопасности (2 ч.)

Понятие угроз информационной безопасности; классификация угроз; угрозы информационной безопасности в образовательной организации; угрозы доступности по компонентам информационных систем; способы несанкционированного доступа.

Тема 6. Особенности обеспечения информационной безопасности при организации

образовательного процесса (2 ч.)

Информационная безопасность в образовательном учреждении как система обязательных контекстов социальной ситуации развития Применение средств информационных и коммуникационных технологий (ИКТ) в учебном процессе

Тема 7. Основные угрозы безопасности (2 ч.)

Кибербуллинг: понятие, признаки. Информационные угрозы и информационная безопасность. Задачи образовательной организации в обеспечении информационной безопасности. Угрозы аддиктивного поведения в электронной среде. Интернет-зависимость. основные показатели, характерные для Интернет-зависимости). Профилактика терроризма и экстремизма в образовательной среде

Тема 8. Моделирование нарушения безопасности предприятия и поиск решений (4 ч.)

Примеры программных и технических средств защиты информации Виды нарушений информационной безопасности. Особенности нарушения информационной безопасности на предприятии.

Социальная инженерия как инструмент нарушения информационной безопасности на предприятии.

Практические (18 ч.)

Раздел 1. Информационная безопасность образовательных интернет-систем (8 ч.)

Тема 1. Законодательство РФ в области информационной безопасности. Конституция Российской Федерации (2 ч.)

Доктрина информационной безопасности Российской Федерации. Федеральные законы в области информации и информационной безопасности. Указы президента РФ и постановления правительства РФ в области информации и информационной безопасности. Правовые вопросы защиты информации с использованием технических средств.

Тема 2. Система сертификации средств криптографической защиты информации (2 ч.)

Виды и схемы сертификации средств криптографической защиты информации.

Функции органов, лабораторий и заявителей в системе сертификации криптографической защиты информации.

Особенности подготовки и проведения сертификации криптографических средств защиты информации.

Контроль и надзор за проведением сертификации криптографических средств защиты информации и стабильностью характеристик сертифицированной продукции.

Тема 3. Информационная безопасность обучающихся разных возрастных групп (2 ч.)

Работа с персональными данными в образовательной организации (формат представления работы – аналитическая справка). Федеральный закон от 29 декабря 2010 года № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»: обзор статей про информационную продукцию для детей разных возрастных групп; примеры, ссылки на интересные материалы;

Тема 4. Контрольная аттестация (2 ч.)

Раздел 2. Методы и средства реализации безопасности образовательных интернет-систем (10 ч.)

Тема 5. Задачи педагогического характера для организации мероприятий по информационной безопасности (2 ч.)

Методы и средства разработки заданий по проверке знаний правил и реализации требований к информационной безопасности

Угрозы информационной безопасности образовательной организации Анализ сайта образовательной организации на наличие данных об информационной безопасности

Тема 6. Формирование культуры безопасного взаимодействия в сети Интернет: основы воспитательной работы (2 ч.)

Мировой уровень цифровой культуры по результатам исследования DCI; понятия информационной грамотности, информационной культуры, медиаграмотности; секреты информационной безопасности; цели Интернет-общения и правила его организации

Тема 7. Правила работы в виртуальном пространстве (4 ч.)

Особенности поиска и применения информации в облачных хранилищах (работа с

лектронными библиотеками, научными базами данных и т.д.)

Тема 8. Контрольная аттестация (2 ч.)

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

6.1 Вопросы и задания для самостоятельной работы

Четвертый семестр (36 ч.)

Раздел 1. Информационная безопасность образовательных интернет-систем (16 ч.)

Вид СРС: *Выполнение индивидуальных заданий

Вариант индивидуального задания

Подготовьте материал для консультации по вопросам информационной безопасности:

1. Дайте определение аттестации объектов информатизации по требованиям безопасности информации.
2. Виды аттестации помещений по требованиям безопасности информации.
3. Какие помещения подлежат обязательной аттестации?
4. Порядок проведения аттестации помещений по требованиям безопасности информации.
5. Какая документация представляется органу по аттестации?
6. Содержание заключения аттестационной проверки помещения.
7. Содержание протокола аттестационных испытаний помещения.

Раздел 2. Методы и средства реализации безопасности образовательных интернет-систем (20 ч.)

Вид СРС: *Выполнение проектов и заданий поисково-исследовательского характера

1. Разработать систему классных часов, внеклассных мероприятий, уроков и занятий по формированию безопасной информационной среды учреждения и позитивного и критического мышления участников.
 2. Разработать методические рекомендации по организации классных часов, внеклассных мероприятий, уроков и занятий, направленных на реализацию цели проекта.
 3. Разработать и апробировать методики и технологии формирования безопасной информационной среды с использованием ресурсов медиаобразования;
 4. Выполнить поиск информации в сети Интернет. Описать работу с мобильными устройствами (2ГИС, Госуслуги, Википедия, эл.книги, фотоколлаж, Компас, диктофон, Калькулятор и пр.).
- Оформите реферат по результатам выполнения задания.

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
1	Предметно-методический модуль	УК-9; ОПК-1; ОПК-2; ПК-3; ОПК-9; ПК-1; ПК-8

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-1. Способен осваивать и использовать теоретические знания и практические умения и навыки в предметной области при решении профессиональных задач			
ПК-1.3. Демонстрирует умение разрабатывать различные формы учебных занятий, применять методы, приемы и технологии обучения, в том числе информационные			
Не способен разрабатывать различные формы учебных занятий, применять методы, приемы и технологии обучения, в том числе информационные	В целом успешно, но бессистемно способен разрабатывать различные формы учебных занятий, применять методы, приемы и технологии обучения, в том числе информационные	В целом успешно, но с отдельными недочетами способен разрабатывать различные формы учебных занятий, применять методы, приемы и технологии обучения, в том числе информационные	Способен в полном объеме разрабатывать различные формы учебных занятий, применять методы, приемы и технологии обучения, в том числе информационные
ПК-8. Способен организовывать образовательный процесс с использованием современных образовательных технологий, в том числе дистанционных			
ПК-8.3. Разрабатывает план коррекции образовательного процесса в соответствии с результатами диагностических и мониторинговых мероприятий			
Не способен разработать план коррекции образовательного процесса в соответствии с результатами диагностических и мониторинговых мероприятий	В целом успешно, но бессистемно разрабатывает план коррекции образовательного процесса в соответствии с результатами диагностических и мониторинговых мероприятий	В целом успешно, но с отдельными недочетами разрабатывает план коррекции образовательного процесса в соответствии с результатами диагностических и мониторинговых мероприятий	Способен в полном объеме разработать план коррекции образовательного процесса в соответствии с результатами диагностических и мониторинговых мероприятий

Уровень сформированности компетенции	Шкала оценивания для промежуточной аттестации	Шкала оценивания по БРС
	Зачет	
Повышенный	зачтено	90 – 100%
Базовый	зачтено	76 – 89%
Пороговый	зачтено	60 – 75%
Ниже порогового	Не зачтено	Ниже 60%

8.3. Вопросы промежуточной аттестации

Четвертый семестр (Зачет, ПК-1, ПК-8)

1. Какие положения составляют основу теории и методики обеспечения информационной безопасности человека во всех видах его деятельности?
2. Проведите классификацию образовательных интернет-систем, выбрав самостоятельно определенный критерий.
3. Составьте регламент работы с персональными данными в образовательной организации.
4. Какие методы и средства разработки заданий по проверке знаний правил и реализации требований к информационной безопасности Вы знаете?
5. Опишите угрозы информационной безопасности образовательной организации.
6. Проведите анализ сайта образовательной организации на наличие данных об информационной безопасности.
7. Проведите оценку мирового уровня цифровой культуры.
8. Расшифруйте понятия информационной грамотности, информационной культуры, медиаграмотности.

9. Перечислите цели безопасного Интернет-общения и правила его организации.
10. Укажите особенности поиска и применения информации в облачных хранилищах.
11. Какие рекомендации Вы дадите пользователям для безопасной работы с электронными библиотеками, научными базами данных и т.д.
12. Назовите виды и схемы сертификации средств криптографической защиты информации и дайте их характеристику.
13. Перечислите функции органов, лабораторий и заявителей в системе сертификации криптографической защиты информации.
14. Какие особенности подготовки и проведения сертификации криптографических средств защиты информации необходимо учитывать?
15. Контроль и надзор за проведением сертификации криптографических средств защиты информации и стабильностью характеристик сертифицированной продукции.
16. В чем заключается главная идея концепции обеспечения информационной безопасности образовательного процесса?
17. Перечислите и раскройте задачи мероприятий по обеспечению безопасности информационной безопасности образовательного учреждения.
18. Рассмотрите и охарактеризуйте основные элементы системы информационной безопасности образовательного учреждения.
19. Перечислите законодательные акты, составляющие правовую основу системы безопасности в Образовательной организации.
20. Предложите план мероприятий по формированию безопасной информационной среды учреждения и позитивного и критического мышления участников образовательного процесса.

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

Промежуточная аттестация проводится в форме зачета.

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.

Собеседование (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.

При определении уровня достижений студентов с помощью тестового контроля ответ считается правильным, если:

- в тестовом задании закрытой формы с выбором ответа выбран правильный ответ;
- по вопросам, предусматривающим множественный выбор правильных ответов, выбраны все правильные ответы;
- в тестовом задании открытой формы дан правильный ответ;

– в тестовом задании на установление правильной последовательности установлена правильная последовательность;

– в тестовом задании на установление соответствия сопоставление произведено верно для всех пар.

При оценивании учитывается вес вопроса (максимальное количество баллов за правильный ответ устанавливается преподавателем в зависимости от сложности вопроса). Количество баллов за тест устанавливается посредством определения процентного соотношения набранного количества баллов к максимальному количеству баллов.

Критерии оценки

До 60% правильных ответов – оценка «неудовлетворительно».

От 60 до 75% правильных ответов – оценка «удовлетворительно».

От 75 до 90% правильных ответов – оценка «хорошо».

Свыше 90% правильных ответов – оценка «отлично».

9. Перечень основной и дополнительной учебной литературы

Основная литература

А. В. Моргунов ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2019. – 83 с. : ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=576726> (дата обращения: 16.10.2021). – Библиогр.: с. 64. – ISBN 978-5-7782-3918-0. – Текст : электронный

Ковалев, Д. В. Информационная безопасность : учебное пособие : [16+] / Д. В. Ковалев, Е. А. Богданова ; Южный федеральный университет. – Ростов-на-Дону : Южный федеральный университет, 2016. – 74 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=493175> (дата обращения: 16.10.2021). – Библиогр. в кн. – ISBN 978-5-9275-2364-1. – Текст : электронный.

Скрипник, Д. А. Обеспечение безопасности персональных данных: курс / Д. А. Скрипник ; Национальный Открытый Университет "ИНТУИТ". – Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2011. – 109 с. : ил., схем. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=234794> (дата обращения: 16.10.2021). – Текст : электронный.

Дополнительная литература

Кияев, В. Безопасность информационных систем: курс : [16+] / В. Кияев, О. Граничин. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 192 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=429032> (дата обращения: 16.10.2021). – Текст : электронный.

Кришталюк, А. Н. Правовые аспекты системы безопасности: курс лекций / А. Н. Кришталюк ; Межрегиональная академия безопасности и выживания. – Орел : Межрегиональная академия безопасности и выживания, 2014. – 204 с. : табл., схем. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=428612> (дата обращения: 16.10.2021). – Библиогр. в кн. – Текст : электронный.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Единая коллекция цифровых образовательных ресурсов [Электронный ресурс]. – URL: <http://scool-collection.edu.ru>

Единое окно доступа к образовательным ресурсам [Электронный ресурс]. – URL: <http://window.edu.ru>

Издательство «Лань» [Электронный ресурс]: электронно-библиотечная система. – URL: <http://e.lanbook.com/>

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.

Алгоритм работы над каждой темой:

- изучите содержание темы вначале по лекционному материалу, а затем по другим источникам;
- прочитайте дополнительную литературу из списка, предложенного преподавателем;
- 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.

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

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

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

12.2 Перечень информационно-справочных систем (обновление выполняется еженедельно)

1. Информационно-правовая система "ГАРАНТ"
2. Справочная правовая система «КонсультантПлюс»

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/opendata/>)
2. Электронная библиотечная система Znanium.com(<http://znanium.com/>)
3. Единое окно доступа к образовательным ресурсам (<http://window.edu.ru>)

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. Индивидуальные результаты освоения дисциплины студентами фиксируются в информационной системе 1 С:Университет. Реализация учебной программы обеспечивается доступом каждого студента к информационным ресурсам – электронной библиотеке и сетевым ресурсам Интернет. Для использования ИКТ в учебном процессе необходимо наличие программного обеспечения, позволяющего осуществлять поиск информации в сети Интернет, систематизацию, анализ и

презентацию информации, экспорт информации на цифровые носители.

Учебная аудитория для проведения учебных занятий.

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Учебная аудитория для проведения учебных занятий.

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Лаборатория вычислительной техники.

Помещение оснащено оборудованием и техническими средствами обучения.

Основное оборудование:

Автоматизированное рабочее место в составе (системный блок, монитор, клавиатура, мышь, гарнитура, проектор, интерактивная доска), магнитно-маркерная доска.

Лабораторное оборудование: автоматизированное рабочее место (компьютеры – 10 шт.).

Учебно-наглядные пособия:

Презентации.

Помещение для самостоятельной работы

Читальный зал электронных ресурсов.

Основное оборудование:

Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета: автоматизированные рабочие места (компьютер – 12 шт.).

Мультимедийный проектор, многофункциональное устройство, принтер.

Учебно-наглядные пособия:

Презентации, электронные диски с учебными и учебно-методическими пособиями.