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

Физико-математический факультет

Кафедра информатики и вычислительной техники

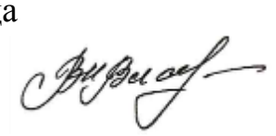
РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Наименование дисциплины (модуля): Информационная безопасность в образовании
Уровень ОПОП: Бакалавриат

Направление подготовки: 44.03.05 Педагогическое образование (с двумя профилями подготовки)
Профиль подготовки: Информатика. Математика
Форма обучения: Очная

Разработчики:
Лапин К. С., канд. физ.-мат. наук, доцент
Зубрилин А. А., канд. филос. наук, зав. кафедрой

Программа рассмотрена и утверждена на заседании кафедры, протокол № 10 от 19.05.2016 года



Зав. кафедрой _____Вознесенская Н. В.

Программа с обновлениями рассмотрена и утверждена на заседании кафедры, протокол № 15 от 21.06.2018 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 - изучение основ информационной безопасности, формирование у студентов информационного мировоззрения на основе знания аспектов защиты информации с использованием естественнонаучных и математических знаний для реализации образовательных программ по информатике; воспитание информационной культуры для эффективного применения полученных знаний в профессиональной деятельности и достижения личностных, метапредметных и предметных результатов обучения и обеспечения качества учебно-воспитательного процесса.

Задачи дисциплины:

- изучение основных направлений организации информационной безопасности (правового, технического, аппаратного) для реализации образовательных программ по информатике;
- изучение основ правового регулирования информационной безопасности в России для реализации образовательных программ по информатике;
- формирование представлений о технических способах и средствах обеспечения защиты информации с использованием естественнонаучных и математических знаний для ориентирования в современном образовательном пространстве;
- изучение программных средств обеспечения информационной безопасности при работе на ПК и в сети Интернет с использованием возможностей образовательной среды для достижения личностных, метапредметных и предметных результатов обучения и обеспечения качества учебно-воспитательного процесса;
- формирование умений аргументированного выбора и самостоятельной установки соответствующего программного обеспечения по защите данных на ПК для реализации образовательных программ по информатике;
- формирование умений по организации защиты файлов и отдельных данных в документах Microsoft для реализации образовательных программ по информатике;
- формирование умений разрабатывать и реализовывать политику информационной безопасности на предприятии, в частности в образовательном учреждении.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина Б1.В.ДВ.03.02 «Информационная безопасность в образовании» относится к вариативной части учебного плана.

Дисциплина изучается на 3 курсе, в 6 семестре.

Для изучения дисциплины требуется:

знать:

определение понятия информации;
свойства информации;
информационные процессы;
носители информации;
архитектуру ПК;
классификацию программного обеспечения;
структуру операционной системы Windows;
понятие правового пространства, уровни законодательства в России;
основы дистанционных образовательных технологий;

уметь:

применять свободное программное обеспечение, служащие для выполнения вспомогательных операций обработки данных или обслуживания компьютеров;
применять дистанционные технологии в образовании;

владеть:

программными продуктами Microsoft.

Изучению дисциплины «Информационная безопасность в образовании» предшествует освоение дисциплин (практик):

Информационные технологии в образовании;
Практикум по информационным технологиям.

Освоение дисциплины «Информационная безопасность в образовании» является необходимой основой для последующего изучения дисциплин (практик):

Интернет-технологии;
Методика обучения информатике;
Защита информации в компьютерных сетях.

Область профессиональной деятельности, на которую ориентирует дисциплина «Информационная безопасность в образовании», включает: образование, социальную сферу, культуру.

Освоение дисциплины готовит к работе со следующими объектами профессиональной деятельности:

- обучение;
- воспитание;

- развитие;
- просвещение;
- образовательные системы.

В процессе изучения дисциплины студент готовится к видам профессиональной деятельности и решению профессиональных задач, предусмотренных ФГОС ВО и учебным планом.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование компетенций и трудовых функций (профессиональный стандарт Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель), утвержден приказом Министерства труда и социальной защиты №544н от 18.10.2013).

Выпускник должен обладать следующими общекультурными компетенциями (ОК):

ОК-3. способностью использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве	
ОК-3 способностью использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве	знать: - фундаментальные понятия информационной безопасности для формирования способности для формирования способности использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве; - естественнонаучные и математические факты, в том числе основные аспекты информационной безопасности для ориентирования в современном информационном пространстве; уметь: - определять оптимальный набор программных средств для обеспечения безопасной работы на компьютере для безопасного ориентирования в современном информационном пространстве; владеть: - методами организации комплексной защиты информации (компьютерной, конфиденциальной) для ориентирования в современном информационном пространстве с помощью естественнонаучных и математических знаний.

Выпускник должен обладать следующими профессиональными компетенциями (ПК) в соответствии с видами деятельности:

ПК-1. готовностью реализовывать образовательные программы по учебным предметам в соответствии с требованиями образовательных стандартов	
педагогическая деятельность	
ПК-1 готовностью реализовывать образовательные программы по учебным предметам в соответствии с требованиями образовательных стандартов	знать: - понятия информационной безопасности, изучаемые в школьном курсе информатики с целью реализации образовательных программ по информатике в соответствии с требованиями образовательных стандартов; уметь: - использовать способы защиты информации, изучаемые в школьном курсе информатики в условиях реализации образовательных программ по информатике в соответствии с требованиями образовательных стандартов;; владеть: - современными методами защиты информации с целью реализации образовательных программ по информатике в соответствии с требованиями образовательных стандартов..
ПК-4. способностью использовать возможности образовательной среды для достижения личностных, метапредметных и предметных результатов обучения и обеспечения качества учебно-воспитательного процесса средствами преподаваемых учебных предметов	
педагогическая деятельность	
ПК-4 способностью использовать возможности образовательной среды для достижения личностных, метапредметных и предметных результатов обучения и обеспечения качества учебно-воспитательного процесса	знать: - нормативные документы, отражающие концепцию информационной безопасности в РФ для достижения личностных, метапредметных и предметных результатов обучения и обеспечения качества учебно-воспитательного процесса средствами преподаваемых учебных предметов; уметь: - проектировать политику информационной безопасности в условиях определенной образовательной организации с использованием возможностей

средствами преподаваемых учебных предметов	информационно-образовательной среды; владеть: - методами, средствами и формами организации информационной безопасности в соответствии с принятыми правовыми нормами РФ для достижения личностных, метапредметных и предметных результатов обучения и обеспечения качества учебно-воспитательного процесса.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Шестой 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 модулей дисциплины

Модуль 1. Аспекты информационной безопасности в образовании:

Основные понятия информационной безопасности. Правовой аспект защиты информации. Организационный аспект информационной безопасности. Понятие информационной угрозы, виды угроз. Методы и средства защиты информации.

Модуль 2. Организация защиты информации в образовательных организациях:

Политика информационной безопасности в образовательной организации. Нормативные документы о защите детей в информационном пространстве. Формирование информационной культуры у детей при использовании сети интернет. Информационная безопасность на уроках информатики.

5.2. Содержание дисциплины: Лекции (18 ч.)

Модуль 1. Аспекты информационной безопасности в образовании (10 ч.)

Тема 1. Основные понятия информационной безопасности (2 ч.)

Общие вопросы информационной безопасности. Аспекты информационной безопасности: доступность, целостность и конфиденциальность. Основные задачи информационной безопасности. Исторический аспект информационной безопасности.

Тема 2. Правовой аспект защиты информации (2 ч.)

Законодательная основа информационной 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 3. Организационный аспект информационной безопасности (2 ч.)

Раскрываются особенности организационного направления по обеспечению информационной безопасности. Рассматриваются вопросы политики ИБ и методические рекомендации по обеспечению ИБ.

Тема 4. Понятие информационной угрозы, виды угроз (2 ч.)

Понятие информационной угрозы, виды угроз. Средства защиты информации. Вредоносные программы, их виды. Классификация компьютерных вирусов. Классические компьютерные вирусы. Файловые вирусы. Макровирусы. Троянские программы. Руткиты. Сетевые черви. Антивирусные программы.

Тема 5. Методы и средства защиты информации (2 ч.)

Рассматриваются основные методы и средства защиты информации правого, организационного и программного характера. Аппаратно-технические и программные средства обеспечения сетевой защиты и защиты компьютерной информации. Идентификация и аутентификация пользователей, виды аутентификации. Криптографическая защита данных. Межсетевые экраны. VPN-технологии. Раскрывается криптографический метод защиты информации. Рассматриваются основные понятия криптографии. Методы криптографии. Предмет и задачи криптографии, требования к криптографическим системам защиты информации, исторические сведения об основных этапах развития криптографии как науки. Понятие криптографического протокола. Основные направления шифрования. Алгоритмы и ключи. Методы криптографии. Стандарты шифрования. Пример простейшего шифра, на основе которого поясняются сформулированные понятия и тезисы.

Модуль 2. Организация защиты информации в образовательных организациях (8 ч.)

Тема 6. Политика информационной безопасности в образовательной организации (2 ч.)

Информационная безопасность в образовательной организации. Рассматривается политика ИБ в образовательной организации, компьютерная безопасность с точки зрения пользователя ПК и сети интернет. Основные методы и средства защиты информации образовательной организации.

Тема 7. Нормативные документы о защите детей в информационном пространстве (2 ч.)

Рассматриваются нормативные документы федерального и регионального уровня. направленные на обеспечение защиты детей от противоправного контента в сети интернет, а также на сохранение психического и физического здоровья детей.

Тема 8. Формирование информационной культуры у детей при использовании сети интернет (2 ч.)

Рассматриваются компоненты, составляющие информационную культуру. Особенности законного поведения в социальных сетях с целью не причинения вреда себе и другим пользователям соцсетей.

Тема 9. Информационная безопасность на уроках инофрматики (2 ч.)

Рассматривается содержание школьного курса информатики с точки зрения формирования понятий информационной безопасности. Изучаются методические особенности формирования этих понятий.

5.3. Содержание дисциплины: Практические (18 ч.)

Модуль 1. Аспекты информационной безопасности в образовании (10 ч.)

Тема 1. Возможности ОС Windows по организации защиты информации (2 ч.)

Задания практической работы направлены на выявление возможностей операционных систем, ориентированных на организацию защиты информации.

Тема 2. Организации защиты информации. Браузеры (2 ч.)

Задания практической работы направлены на проведения сравнительного анализа возможностей популярных браузеров по организации защиты информации.

Тема 3. Антивирусные программы (2 ч.)

Задания практической работы направлены на проведения сравнительного анализа возможностей популярных антивирусных программ по организации защиты информации.

Тема 4. Организация защиты офисных документов_Word (2 ч.)

Задания практической работы направлены на выявление возможностей текстовых редакторов по организации защиты информации, а также на изучение функционала и инструментов MS Word. позволяющих различными способами организовать сохранность текстовой информации, передачу и преобразование.

Тема 5. Криптографические методы защиты информации (2 ч.)

Рассматриваются криптографические методы защиты информации. Выполняется реализация шифрования средствами MS Excel.

Модуль 2. Организация защиты информации в образовательных организациях (8 ч.)

Тема 6. Классификатор российского ПО, программное обеспечение для реализации информационной безопасности (2 ч.)

Рассматривается российский классификатор программного обеспечения. Изучаются программные средства обеспечения информационной безопасности российских правообладателей.

Тема 7. Исторические шифры (2 ч.)

Задания практической работы направлены на изучение исторических подходов шифрования текстовой информации.

Тема 8. Позиционные системы счисления (2 ч.)

Задания практической работы направлены на изучение математических основ криптографии, которые лежат в основе гаммирования и других современных методов криптографииl.

Тема 9. Гаммирование (2 ч.)

Задания практической работы направлены на реализацию метода гаммирования.

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

6.1 Вопросы и задания для самостоятельной работы

Шестой семестр (36 ч.)

Модуль 1. Аспекты информационной безопасности в образовании (18 ч.)

Вид СРС: *Выполнение индивидуальных заданий

Подготовить реферат по заданной теме.

Темы рефератов

1. Политика ИБ в образовательном учреждении (отразить концепцию ИБ образовательного учреждения и перечень мероприятий).

2. Организация защиты электронной почты.

3. Организация защиты ПК в образовательном учреждении.

4. Нормативно-правовой аспект защиты информации в образовательном учреждении.

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, сети).

9. Угрозы ИБ, виды угроз, способы защиты.

10. Вирусная атака, ее механизм реализации.

Вид СРС: *Подготовка к коллоквиуму

Вопросы к коллоквиуму:

1. Раскройте различные подходы к определению понятия «информационная безопасность». Привести примеры нарушения информационной безопасности в быту и на предприятии.

2. Обоснуйте основные задачи системы информационной безопасности.

3. Обоснуйте этапы развития информационной безопасности.

4. Раскройте понятие «защита информации» и обоснуйте основные аспекты защиты информации.

5. Охарактеризуйте программные средства организации информационной безопасности при работе на компьютере. На примере одного приложения раскройте его функциональные возможности по защите информации.

6. Охарактеризуйте программные средства организации информационной безопасности в компьютерной сети. На примере одного приложения раскройте его функциональные возможности по защите информации.

7. Охарактеризуйте аппаратные средства организации информационной безопасности при работе на компьютере. Приведите примеры аппаратных средств защиты информации.

8. Охарактеризуйте аппаратные средства организации информационной безопасности в компьютерной сети. Приведите примеры аппаратных средств защиты информации.

9. Укажите основные направления организации информационной безопасности. Сформулируйте рекомендации для организации информационной безопасности при работе на ПК для сотрудников образовательного учреждения.

10. Раскройте понятие «сетевые атаки». Приведите примеры сетевых атак. Укажите способы несанкционированного проникновения на сетевой компьютер и охарактеризуйте пути противодействия им.

11. Раскройте понятие «информационная угроза» с позиции проблемы обеспечения информационной безопасности. Охарактеризуйте виды угроз. Приведите примеры угроз различных видов.

12. Раскройте суть нормативно-правового аспекта защиты информации. Охарактеризуйте структуру законодательства России в области защиты информации.

13. Дайте определение государственной тайне. Перечислите основные статьи в Законе о государственной тайне.

14. Дайте определение понятиям «авторское право» и «коммерческая тайна». Укажите их отличительные особенности. Охарактеризуйте способы защиты авторских прав и коммерческой тайны.

15. Перечислите виды конфиденциальной информации. Приведите примеры конфиденциальной информации и укажите способы ее защиты.

16. Перечислите нормативно-правовые документы, ориентированные на обеспечение информационной безопасности. Охарактеризуйте нарушения, представленные в этих документах и меру наказания.

17. Охарактеризуйте организационные меры защиты информации. Обоснуйте основные организационные мероприятия информационной безопасности.

18. Охарактеризуйте технологические меры информационной безопасности. Обоснуйте классификацию средств технологической защиты информации.

19. Охарактеризуйте аппаратные средства защиты информации, укажите основания для их классификации. Приведите примеры аппаратных средств защиты информации.

20. Опишите суть программной защиты информации. Перечислите основные средства программной защиты информации, обоснуйте их классификацию. На примере одного приложения раскройте его функциональные возможности по защите информации.

21. Перечислите антивирусные программные средства. На примере конкретного приложения продемонстрируйте настройку безопасности.

22. Раскройте понятие «компьютерный вирус». Перечислите виды компьютерных вирусов. Приведите примеры, опишите способы их проникновения и особенности разрушительных действий.

23. Перечислите способы проникновения компьютерных вирусов на компьютер.

Приведите примеры, опишите особенности их разрушительных действий.

24. Раскройте суть технология антивирусной защиты сетевого компьютера. Приведите примеры антивирусных приложений и укажите особенности их функционала.

25. Охарактеризуйте вредоносные программы и их виды. Перечислите способы борьбы с ними.

26. Охарактеризуйте программные средства ограничения доступа в Интернет, фильтрации информационных ресурсов. На примере одного приложения раскройте его функциональные возможности по ограничению доступа в Интернет.

27. Укажите виды мошенничества в сети Интернет. Перечислите способы противодействия Интернет-мошенникам. Охарактеризуйте поведение при возникновении угрозы Интернет-мошенников.

Вид СРС: *Подготовка к промежуточной аттестации

Изучение основной и дополнительной литературы по данному модулю.

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

Модуль 2. Организация защиты информации в образовательных организациях (18 ч.)

Вид СРС: *Выполнение индивидуальных заданий

Подготовить 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.

Вид СРС: *Подготовка к промежуточной аттестации

Изучение основной и дополнительной литературы по данному модулю.

Вид СРС: *Работа с электронными ресурсами и информационными системами

Прохождение онлайн курса:

"Технологии и продукты Microsoft в обеспечении информационной безопасности " http://www.intuit.ru/studies/courses/600/456/info.

7. Тематика курсовых работ(проектов)

Курсовые работы (проекты) по дисциплине не предусмотрены.

8. Оценочные средства для промежуточной аттестации

8.1. Компетенции и этапы формирования

Коды компетенций	Этапы формирования		
	Курс, семестр	Форма контроля	Модули (разделы) дисциплины
ОК-3 ПК-4	3 курс, Шестой семестр	Зачет	Модуль 1: Аспекты информационной безопасности в образовании.
ПК-1	3 курс, Шестой семестр	Зачет	Модуль 2: Организация защиты информации в образовательных организациях.

Сведения об иных дисциплинах, участвующих в формировании данных компетенций:

Компетенция ОК-3 формируется в процессе изучения дисциплин:

Естественнонаучная картина мира, Защита информации в компьютерных сетях, Информационная безопасность в образовании, Информационные технологии в образовании, Искусственный интеллект и экспертные системы, Основы математической обработки информации, Подготовка к сдаче и сдача государственного экзамена.

Компетенция ПК-1 формируется в процессе изучения дисциплин:

3D моделирование, Алгебра, Вводный курс математики, Внеурочная деятельность учащихся по информатике, Геометрия, Задачи с параметрами и методы их решения, Защита информации в компьютерных сетях, Интернет-технологии, Информационные системы, Искусственный интеллект и экспертные системы, Исследовательская и проектная деятельность в обучении математике, Исследовательская и проектная деятельность учащихся по информатике, Компетентностный подход в обучении математики, Компьютерная алгебра, Компьютерная графика, Компьютерное моделирование, Компьютерные сети, Математический анализ, Математическое моделирование, Методика обучения информатике, Методика обучения математике, Методика обучения математике в профильных классах, Методология обучения математике, Методы аксиоматического построения алгебраических

систем, Методы решения задач государственной итоговой аттестации по математике, Методы решения задач по информатике, Моделирование в системах динамической математики, Нестандартные методы решения математических задач, Общая теория линейных операторов и ее приложение к решению геометрических задач, Оптимизация и продвижение сайтов, Практикум по информационным технологиям, Применение систем динамической математики в образовании, Программирование, Проектирование информационно-образовательной среды, Разработка приложений в Microsoft Visual Studio, Разработка электронных образовательных ресурсов и методика их оценки, Реализация прикладной направленности в обучении математике, Решение задач основного государственного экзамена по математике, Решение задач повышенного уровня сложности по алгебре, Решение задач повышенного уровня сложности по геометрии, Решение задач профильного уровня единого государственного экзамена по математике, Решение олимпиадных задач по информатике, Свободные инструментальные системы, Системы компьютерной математики, Современные средства оценивания результатов обучения, Теоретические основы информатики, Теория рядов и ее приложения, Технология обучения математическим понятиям в школе, Технология обучения учащихся решению математических задач, Технология разработки и методика проведения элективных курсов по математике, Формы и методы работы с одаренными детьми, Численные методы, Элементарная математика, Элементы конструктивной геометрии в школьном курсе математики, Элементы функционального анализа, Проектирование в системах автоматизированного проектирования, Исторический подход в обучении математике.

Компетенция ПК-4 формируется в процессе изучения дисциплин:

3D моделирование, Защита информации в компьютерных сетях, Интернет-технологии, Информационные системы, Информационные технологии в научных исследованиях, Исследовательская и проектная деятельность в обучении математике, Компьютерная графика, Компьютерная обработка результатов научного исследования, Компьютерное моделирование, Компьютерные сети, Математическое моделирование, Методика обучения информатике, Методика обучения математике, Методика обучения математике в профильных классах, Методика подготовки учащихся к государственной итоговой аттестации по информатике, Методы решения задач государственной итоговой аттестации по математике, Методы решения задач по информатике, Моделирование в системах динамической математики, Нестандартные методы решения математических задач, Практикум по информационным технологиям, Применение систем динамической математики в образовании, Программирование, Проектирование информационно-образовательной среды, Разработка приложений в Microsoft Visual Studio, Разработка электронных образовательных ресурсов и методика их оценки, Решение задач повышенного уровня сложности по алгебре, Решение задач повышенного уровня сложности по геометрии, Решение олимпиадных задач по информатике, Свободные инструментальные системы, Системы компьютерной математики, Теоретические основы информатики, Технология разработки и методика проведения элективных курсов по информатике, Технология разработки и методика проведения элективных курсов по математике, Формы и методы работы с одаренными детьми, Численные методы, Проектирование в системах автоматизированного проектирования.

8.2. Показатели и критерии оценивания компетенций, шкалы оценивания

В рамках изучаемой дисциплины студент демонстрирует уровни овладения компетенциями:

Повышенный уровень:

знает и понимает теоретическое содержание дисциплины; творчески использует ресурсы (технологии, средства) для решения профессиональных задач; владеет навыками решения практических задач.

Базовый уровень:

знает и понимает теоретическое содержание; в достаточной степени сформированы умения применять на практике и переносить из одной научной области в другую теоретические знания; умения и навыки демонстрируются в учебной и практической деятельности; имеет навыки оценивания собственных достижений; умеет определять проблемы и потребности в конкретной области профессиональной деятельности.

Пороговый уровень:

понимает теоретическое содержание; имеет представление о проблемах, процессах, явлениях; знаком с терминологией, сущностью, характеристиками изучаемых явлений; демонстрирует практические умения применения знаний в конкретных ситуациях профессиональной деятельности.

Уровень ниже порогового:

имеются пробелы в знаниях основного учебно-программного материала, студент допускает принципиальные ошибки в выполнении предусмотренных программой заданий, не способен продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.

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%

Критерии оценки знаний студентов по дисциплине

Оценка	Показатели
Зачтено	Студент знает: фундаментальные понятия информационной безопасности; аспекты информационной безопасности; основные подходы к разработке политики информационной безопасности; нормативно-правовые документы на всех государственных уровнях, регламентирующих организацию защиты информации в РФ; функционал аппаратно-программного обеспечения и сервисы Интернет с целью организации защиты компьютерной информации в процессе профессиональной деятельности; правила предостережения от интернет-мошенничества; основные способы защиты компьютерной информации; способы шифрования данных Владеет средствами обеспечения информационной безопасности при работе за персональным компьютером и в компьютерных сетях; криптографическими методами защиты информации; методами организации комплексной защиты информации (компьютерной, конфиденциальной)
Не зачтено	Студент демонстрирует незнание основных понятий содержания дисциплины, обнаруживая существенные пробелы в знаниях учебного материала, допускает принципиальные ошибки в выполнении практических заданий; затрудняется делать выводы и отвечать на дополнительные вопросы преподавателя.

8.3. Вопросы, задания текущего контроля

Модуль 1: Аспекты информационной безопасности в образовании

ОК-3 способностью использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве

Сформулируйте механизмы обеспечения ИБ, опишите способ разграничения доступа.

Сформулируйте механизмы обеспечения ИБ, опишите суть процедур идентификация и аутенфикация.

Сформулируйте рекомендации для защиты от вирусов.

Сформулируйте определения основных понятий ИБ, изучаемых курсе информатики (укажите основные разделы курса школьной информатики).

Разработайте кейс-задачи для школьников, направленные на формирование криптографических способов защиты информации.

ПК-4 способностью использовать возможности образовательной среды для достижения личностных, метапредметных и предметных результатов обучения и обеспечения качества учебно-воспитательного процесса средствами преподаваемых учебных предметов

1. Опишите построение корпоративной системы обеспечения ИБ

2. Охарактеризуйте особенности организации ИБ компьютерны сетей образовательных организаций

3. Опишите административный уровень обеспечения ИБ.

4. Сформулируйте определение защиты информации, укажите основные аспекты защиты информации и обоснуйте их целесообразность.

5. Раскройте понятие «сетевые атаки». Приведите примеры сетевых атак. Укажите способы несанкционированного проникновения на сетевой компьютер и охарактеризуйте пути противодействия им.

Модуль 2: Организация защиты информации в образовательных организациях

ПК-1 готовностью реализовывать образовательные программы по учебным предметам в соответствии с требованиями образовательных стандартов

1. Раскройте основные аспекты ИБ, изучаемые на уроках информатики (укажите основные разделы курса школьной информатики).

2. Сформулируйте вопросы ИБ, целесообразные для организации внеурочной деятельности (внеклассные мероприятия).

3. Разработайте кейс-задачи для школьников для разработки политики ИБ.

4. Разработайте кейс-задачи для школьников, направленные на формирование информационной культуры (поведение в социальных сетях).

5. Разработайте кейс-задачи для школьников, направленные на формирование

информационной культуры (платежные системы).

6. Разработайте кейс-задачи для школьников, направленные на формирование информационной культуры (дистанционные государственные услуги).

8.4. Вопросы промежуточной аттестации

Шестой семестр (Зачет, ОК-3, ПК-1, ПК-4)

1. Раскройте различные подходы к определению понятия «информационная безопасность». Приведите примеры нарушения информационной безопасности в быту и в образовательном учреждении.

2. Перечислите и обоснуйте основные задачи системы информационной безопасности.

3. Укажите и обоснуйте этапы развития информационной безопасности.

4. Сформулируйте определение защиты информации, укажите основные аспекты защиты информации и обоснуйте их целесообразность.

5. Охарактеризуйте программные средства, необходимые для организации информационной безопасности при работе на компьютере. На примере одного программного средства раскройте его функциональные возможности по защите информации.

6. Охарактеризуйте программные средства, необходимые для организации информационной безопасности в компьютерной сети. На примере одного программного средства раскройте его функциональные возможности по защите информации.

7. Охарактеризуйте аппаратные средства, необходимые для организации информационной безопасности. Приведите примеры аппаратных средств защиты информации.

8. Охарактеризуйте аппаратные средства, необходимые для организации информационной безопасности в компьютерной сети. Приведите примеры аппаратных средств защиты информации.

9. Укажите основные направления организации информационной безопасности. Сформулируйте рекомендации для организации информационной безопасности при работе на ПК для сотрудников образовательного учреждения.

10. Раскройте понятие «сетевые атаки». Приведите примеры сетевых атак. Укажите способы несанкционированного проникновения на сетевой компьютер и охарактеризуйте пути противодействия им.

11. Раскройте понятие «информационная угроза» с позиции проблемы обеспечения информационной безопасности. Охарактеризуйте виды угроз, приведите примеры.

12. Раскройте суть нормативно-правового аспекта защиты информации. Охарактеризуйте структуру законодательства России в области защиты информации.

13. Дайте определение государственной тайны. Перечислите основные статьи в Федеральном Законе о государственной тайне.

14. Дайте определение понятиям «авторское право» и «коммерческая тайна». Укажите их отличительные особенности. Охарактеризуйте способы защиты авторских прав и коммерческой тайны.

15. Перечислите виды конфиденциальной информации. Приведите примеры конфиденциальной информации и укажите способы ее защиты.

16. Перечислите нормативно-правовые документы, ориентированные на обеспечение информационной безопасности в России. Охарактеризуйте нарушения, представленные в этих документах и меру наказания.

17. Охарактеризуйте организационные меры защиты информации в образовательном учреждении. Обоснуйте основные организационные мероприятия информационной безопасности.

18. Охарактеризуйте технологические меры информационной безопасности в образовательном учреждении. Обоснуйте классификацию средств технологической защиты информации.

19. Охарактеризуйте аппаратные средства защиты информации, и их классификации. Приведите примеры аппаратных средств защиты информации в образовательной организации.

20. Охарактеризуйте программные средства защиты информации, и их классификации. Перечислите основные средства программной защиты информации. На примере одного приложения раскройте его функциональные возможности по защите информации.

21. Перечислите антивирусные программные средства. На примере конкретного приложения продемонстрируйте настройку безопасности.

22. Раскройте понятие «компьютерный вирус». Перечислите виды компьютерных вирусов. Приведите примеры, опишите способы их проникновения и особенности разрушительных действий.

23. Перечислите способы проникновения компьютерных вирусов на ПК и опишите механизм их реализации. Приведите примеры, опишите особенности их разрушительных действий.

24. Раскройте технологию антивирусной защиты сетевого компьютера. Приведите примеры антивирусных приложений и укажите особенности их функционала.

25. Охарактеризуйте вредоносные программы и их виды. Перечислите способы борьбы с ними.

26. Охарактеризуйте программные средства ограничения доступа в Интернет, фильтрации информационных ресурсов. На примере одного приложения раскройте его функциональные возможности по ограничению доступа в Интернет.

27. Укажите виды мошенничества в сети Интернет. Перечислите способы противодействия Интернет-мошенникам. Охарактеризуйте поведение при возникновении угрозы Интернет-мошенников.

28. Раскройте цели и задач криптографии как научной области. Перечислите основные направления использования криптографических методов для защиты информации.

29. Охарактеризуйте современные криптосистемы. Продемонстрируйте модели симметричных и асимметричных криптосистем. Приведите примеры.

30. Охарактеризуйте методы криптографического закрытия информации. Опишите суть стойкости метода и трудоемкости метода.

31. Перечислите популярные исторические шифры. Опишите суть шифра Цезаря и шифра Вижинера. Приведите пример открытого текста и шифрограммы, полученной с помощью этих шифров.

32. Раскройте понятие шифра, укажите типы шифров. На конкретных примерах укажите преимущества и недостатки различных типов шифров.

33. Охарактеризуйте современные способы шифрования данных.

34. Охарактеризуйте программные средства шифрования данных. Раскройте технологию шифрования на примере конкретного приложения.

35. Раскройте особенность парольной защиты информации. Укажите достоинства и недостатки парольной защиты информации. Назовите примеры программных средств для создания и хранения паролей.

36. Раскройте суть электронной цифровой подписи. Охарактеризуйте правовой и технический аспекты. Сформулируйте рекомендации для использования электронной цифровой подписи.

37. Сформулируйте рекомендации для обеспечения безопасности в приложениях MS Word и MS Excel. Опишите способы защиты информации в БД на примере MS Access.

38. Раскройте суть идентификация и аутентификация при входе в информационную систему. Сформулируйте рекомендации по использованию парольных схем в компьютерных сетях. Укажите недостатки парольных схем.

39. Раскройте технологию функционирования брандмауэров. Объясните настройку брандмауэра на примере конкретного приложения.

40. Сформулируйте методические рекомендации для изучения основ информационной безопасности в школьном курсе информатики.

8.5. 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 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 устного ответа студенту предварительно предлагается перечень вопросов и заданий, выявляющих 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.

Тесты

При определении уровня достижений студентов с помощью тестового контроля необходимо обращать особое внимание на следующее:

– оценивается полностью правильный ответ;

– преподавателем должна быть определена максимальная оценка за тест, включающий определенное количество вопросов;

– преподавателем может быть определена максимальная оценка за один вопрос теста;

– по вопросам, предусматривающим множественный выбор правильных ответов, оценка определяется исходя из максимальной оценки за один вопрос теста.

Контекстная учебная задача, проблемная ситуация, ситуационная задача, кейсовое задание могут быть включены в зачет.

При определении уровня достижений студентов при решении учебных практических задач необходимо обращать особое внимание на следующее:

– способность определять и принимать цели учебной задачи, самостоятельно и творчески планировать ее решение как в типичной, так и в нестандартной ситуации;

– систематизированные, глубокие и полные знания по всем разделам программы; – точное использование научной терминологии, стилистически грамотное, логически правильное изложение ответа на вопросы и задания;

– владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке и решении учебных задач; – грамотное использование основной и дополнительной литературы;

– умение использовать современные информационные технологии для решения учебных задач, использовать научные достижения других дисциплин;

– творческая самостоятельная работа на практических занятиях, активное участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

9. Перечень основной и дополнительной учебной литературы

Основная литература

1. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации [Электронный ресурс] : учебное пособие / Ю. Н. Загинайлов. – М. ; Берлин : Директ-Медиа, 2015. – 253 с. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=276557.

2. Котова, Л. В. Сборник задач по дисциплине «Методы и средства защиты информации» [Электронный ресурс] : учебное пособие / Л. В. Котова ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Московский педагогический государственный университет». – Москва : МПГУ, 2015. – 44 с. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=469877.

3. Нестеров, С. А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / С. А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. – СПб. : Издательство Политехнического университета, 2014. – 322 с. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=363040.

4. Прохорова, О. В. Информационная безопасность и защита информации [Электронный ресурс] : 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. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=438331.

Дополнительная литература

1. Артемов, А. В. Информационная безопасность [Электронный ресурс] : курс лекций / А. В. Артемов ; Межрегиональная Академия безопасности и выживания. – Орел : МАБИВ, 2014. – 257 с. – Режим доступа http://biblioclub.ru/index.php?page=book&id=428605.

2. Спицын, В.Г. Информационная безопасность вычислительной техники [Электронный ресурс] : учебное пособие / В.Г. Спицын ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). – Томск : Эль Контент, 2011. – 148 с. Режим доступа : http://biblioclub.ru/index.php?page=book&id=208694.

3. Мэйволд, Э. Безопасность сетей [Электронный ресурс] / Э. Мэйволд. – 2-е изд., испр. – М. : Национальный Открытый Университет «ИНТУИТ», 2016. – 572 с. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=429035.

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.informika.ru - Федеральное государственное автономное учреждение «Государственный научно-исследовательский институт информационных технологий и

телекоммуникаций» [Электронный ресурс] / М.: Informika.ru, 2002 - 2016. - Режим доступа: http://www.informika.ru/

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

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

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;

– 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 электронной информационно-образовательной среде университета.

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» (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/opendata/)
2. Профессиональная база данных «Портал открытых данных Министерства культуры Российской Федерации» (http://opendata.mkrf.ru/)
3. Электронная библиотечная система Znanium.com (http://znanium.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.

Индивидуальные результаты освоения дисциплины фиксируются в электронной информационно-образовательной среде университета.

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.

Оснащение аудиторий

Лаборатория вычислительной техники.

Помещение укомплектовано специализированной мебелью и техническими средствами обучения.

Основное оборудование:

Наборы демонстрационного оборудования: автоматизированное рабочее место в составе (учебный методический комплекс трибуна, проектор, экран), маркерная доска, колонки SVEN.

Лабораторное оборудование: автоматизированное рабочее место (компьютеры – 13 шт.).

Учебно-наглядные пособия:

Презентации.

Лабораторное оборудование: автоматизированное рабочее место (компьютеры – 13 шт.).

Учебно-наглядные пособия:

Презентации.

Помещения для самостоятельной работы.

Лаборатория вычислительной техники.

Помещение укомплектовано специализированной мебелью и техническими средствами обучения.

Основное оборудование:

Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета (компьютер 10 шт., проектор с экраном 1 шт.).

Учебно-наглядные пособия:

Презентации.

Помещение для самостоятельной работы.

Читальный зал.

Помещение укомплектовано специализированной мебелью и техническими средствами обучения.

Основное оборудование:

Компьютерная техника с возможностью подключения к сети .«Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета (компьютер 10 шт., проектор с экраном 1 шт., многофункциональное устройство 1 шт., принтер 1 шт.)

Учебно-наглядные пособия:

Учебники и учебно-методические пособия, периодические издания, справочная литература.

Стенды с тематическими выставками..