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

Факультет естественно-технологический
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: Технология. Информатика
Форма обучения: Очная

Разработчики:
Лапин К. С., канд. физ.-мат. наук, доцент
Харитонова А. А., канд. пед. наук, доцент

Программа рассмотрена и утверждена на заседании кафедры, протокол № 13 от 17.05.2018 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.12.02 «Информационная безопасность в образовании» относится к вариативной части учебного плана.

Дисциплина изучается на 4 курсе, в 8 семестре.

Для изучения дисциплины требуется: знание школьного курса информатики.

Изучению дисциплины Б1.В.ДВ.12.02 «Информационная безопасность в образовании» предшествует освоение дисциплин (практик):

Информационные технологии в образовании;

Практикум по информационным технологиям;

Свободное программное обеспечение в образовании;

Свободное офисное программное обеспечение.

Освоение дисциплины Б1.В.ДВ.12.2 «Информационная безопасность в образовании» является необходимой основой для последующего изучения дисциплин (практик):

Основы защиты информации в компьютерных сетях;

Методика обучения информатике.

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;
- образовательные системы.

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

планом:

педагогическая деятельность

- изучение возможностей, потребностей, достижений обучающихся в области образования;

- обучение и воспитание в сфере образования в соответствии с требованиями образовательных стандартов;

- использование технологий, соответствующих возрастным особенностям обучающихся и отражающих специфику предметных областей;

- формирование образовательной среды для обеспечения качества образования, в том числе с применением информационных технологий.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование компетенций и трудовых функций (профессиональный стандарт Педагог (педагогическая деятельность в дошкольном, начальном общем, основном общем, среднем общем образовании) (воспитатель, учитель), утвержден приказом Министерства труда и социальной защиты №544н от 18.10.2013).

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; - основные аспекты организации информационной безопасности в образовательных организациях с целью реализации образовательных программ по информатике в соответствии с требованиями образовательных стандартов;; - нормативно-правовые основы информационной безопасности с целью реализации образовательных программ по информатике в соответствии с требованиями образовательных стандартов;; - понятия информационной безопасности, изучаемые в школьном курсе информатики с целью реализации образовательных программ по информатике в соответствии с требованиями образовательных стандартов; - нормативно-правовые основы информационной безопасности 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; - организовывать учебную деятельность для овладения способами защиты информации, изучаемые в школьном курсе информатики с целью реализации образовательных программ по информатике в соответствии с требованиями образовательных стандартов; - проектировать политику информационной безопасности в условиях определенной образовательной организации с целью 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. - методами, средствами и формами организации информационной безопасности в соответствии с принятыми правовыми нормами РФ с целью реализации образовательных программ по информатике в соответствии с требованиями образовательных стандартов;; - подходами к формированию умений использовать современные методы защиты информации с целью реализации образовательных программ по информатике в соответствии с требованиями образовательных стандартов.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Восьмой семестр
Контактная работа (всего)	**38**	**38**
Практические	38	38
Самостоятельная работа (всего)	**70**	**70**
Виды промежуточной аттестации		
Зачет		+
Общая трудоемкость часы	**108**	**108**
Общая трудоемкость зачетные единицы	**3**	**3**

5. Содержание дисциплины

5.1. Содержание модулей дисциплины

Модуль 1. Основы информационной безопасности:

Общие вопросы информационной безопасности. Аспекты информационной безопасности. 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. 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 ин-формационной безопасности и их последствия. Аппаратно-технические и программные средства обеспечения сетевой защиты и защиты компьютер-ной информации. Идентификация и аутентификация пользователей, виды аутентификации. Криптографическая защита данных. Межсетевые экраны. VPN-технологии.

Модуль 2. Информационная безопасность в образовательной организации:

Традиционные вопросы криптографии. Современные приложения криптографии. Понятие криптографического протокола. Основные направления шифрования. Исторические шифры. Алгоритмы и ключи. Методы криптографии. Стандарты шифрования. Симметричное и асимметричное шифрование. Технология электронно-цифровой подписи. Компьютерные алгоритмы шифрования. Парольная защита. Приложения шифрования (дешифрования) данных.

5.2. Содержание дисциплины: Практические (38 ч.)

Модуль 1. Основы информационной безопасности (18 ч.)

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

Лабораторная работа по теме "Антивирусная программа". Общие вопросы информационной безопасности. Аспекты информационной безопасности:

доступность, целостность и конфиденциальность. Основные задачи инофрмационной безопасности. Исторический аспект инорфмационной безопасности.

Тема 2. Аспекты информационной безопасности (2 ч.)

Законодательная основа информациооной 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. Лабораторная работа по теме "Нормативно-правовые документы по облеспечению информационной безопасности в РФ"

Тема 3. 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. Лабораторная работа по теме "Вредоносное ПО"

Тема 4. Правовой аспект информационной безопасности (4 ч.)

Законодательная основа информациооной 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. Лабораторная работа по теме "Персональные данные"

Тема 5. Оганизационный аспект информационной безопасности (4 ч.)

Раскрываются особенности организационного направления по обеспечению информационной безопасности. Рассматриваются вопросы политики ИБ и методические рекомендации по обеспечению ИБ. Лабораторная работа по теме "Политики информационной безопасности"

Тема 6. Аппаратно-программный аспект информационной безопасности (4 ч.)

Задания практической работы направлены на проведения сравнительного анализа возможностией популярных антивирусных программ по организации защиты информации. Лабораторная работа по теме "Способы защиты документов в Microsoft Office"

Модуль 2. Информационная безопасность в образовательной организации (20 ч.)

Тема 7. 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. Криптографи-ческая 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.

Тема 8. Основы криптографии (2 ч.)

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

Тема 9. Основные направления шифрования (2 ч.)

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

Тема 10. Технология электронно-цифровой подписи (2 ч.)

Изучается технология использования электронно-цифровой подписи в различных

организациях.

Тема 11. Компьютерные алгоритмы шифрования (4 ч.)

Лабораторная работа по теме "Современные криптосистемы". Использования в программной реализации шифра Цезаря и шифра Вижинера.

Тема 12. Компьютерные алгоритмы шифрования (4 ч.)

Лабораторная работа по теме "Современные криптосистемы". Изучение современных криптосистем и использование их в реальной жизни.

Тема 13. Тестирование (4 ч.)

Тестирование в Инфор-вузе.

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

6.1 Вопросы и задания для самостоятельной работы

Восьмой семестр (70 ч.)

Модуль 1. Основы информационной безопасности (34 ч.)

Вид СРС: *Выполнение индивидуальных заданий

Создать с использованием любых программных средств продукт (видеоролик, интерактивная презентация, фотогалерея и пр.), наглядно демонстрирующий механизмы проникновения, особенности поведения, цикл жизнедеятельности вредоносного ПО (вирус, червь, троян и др.) и способы защиты от него.

Например

Жизненный цикл вредоносных программ:

Процесс размножения

вирусов

может быть условно разделен на несколько стадий:

1) активация вируса;

2) поиск объектов для заражения;

3) подготовка вирусных копий;

4) внедрение вирусных копий;

Жизненный цикл

Червей можно разделить на определенные стадии:

1) проникновение в систему;

2) активация;

3) поиск «жертв»;

4) подготовка копий;

5) распространение копий;

У троянов вследствие отсутствия функций размножения и распространения, их жизненный цикл меньше чем у вирусов – всего три стадии:

1) проникновение на компьютер;

2) активация;

3) выполнение заложенных функций.

Но это не означает, что времени жизни троянов мало. Напротив, троян может незаметно находиться в памяти компьютера длительное время, никак не выдавая своего присутствия, до тех пор, пока не выполнит свою вредоносную функцию будет обнаружен антивирусными средствами.

Виды вредоносного ПО:

Вирусы (Viruses).

Черви (Worms).

Троянские программы (Trojans).

Спам (Spam).

Фишинг (Phishing).

Рекламные закладки.

Шпионские программы.

Руткиты (Rootkit).

Зобми компьютер (Zombie).

Ботнет (Botnet).

Требования:

Время демонстрации не более 5 минут.

Использовать свободное ПО, реализуемое на любом ПК, например: программы для создания анимации (онлайн сервисы и редакторы)

http://www.newart.ru/htm/flash/risovalka_7.htm

Отчет ИДЗ включает:

1) описание вредоносного ПО (в соответствии с вариантом)

2) сценарий представленной анимации

3) файл с продуктом.

Модуль 2. Информационная безопасность в образовательной организации (36 ч.)

Вид СРС: *Выполнение индивидуальных заданий

1. Пройти онлайн-курсы по ИБ (ИНТУИТ)

1) «Основы информационной безопасности при работе на компьютере»

http://www.intuit.ru/studies/courses/680/536/info

2)«Обеспечение безопасности персональных данных»

http://www.intuit.ru/studies/courses/697/553/info

3)Технологии и продукты Microsoft в обеспечении информационной безопасности (СР «Разработка политики ИБ для вузов/факультета/кафедры»)

http://www.intuit.ru/studies/courses/600/456/info

2. Подготовить сообщение по темам:

Безопасность персональных данных.

Признаки заражения ПК.

Антивирусные программы.

Файерволлы.

Безопасность банковских карт.

Организацию безопасности при использовании Интернет.

Социальные аспекты информационной безопасности.

Защита от вирусных угроз.

Защита от сетевых атак на основе межсетевого экранирования.

Аудит информационной безопасности.

Организационно-правовые аспекты информационной безопасности.

Обзор функций безопасности

Windows

.Криптографические механизмы

Windows

.

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
ПК-1	4 курс, Восьмой семестр	Зачет	Модуль 1: Основы информационной безопасности.
ПК-1	4 курс,	Зачет	Модуль 2: Информационная безопасность в

	Восьмой семестр		образовательной организации

Сведения об иных дисциплинах, участвующих в формировании данных компетенций:

Компетенция ПК-1 формируется в процессе изучения дисциплин:

3D моделирование, Администрирование компьютерных сетей, Биотехнологические производства Республики Мордовия, Инженерная графика в технологическом образовании, Информационные системы, История и методология информатики и вычислительной техники, Компьютерное моделирование, Математика, Математические методы в конструировании, Методика обучения информатике, Методика обучения технологии, Метрология и техническое законодательство, Обустройство и дизайн дома, Организация и технология предприятий бытового обслуживания, Основы защиты информации в компьютерных сетях, Основы конструирования, Основы материаловедения и технологии обработки материалов, Основы микроэлектроники, Основы моделирования в швейном производстве, Основы моделирования машин и механизмов, Основы нанотехнологий, Основы рационального природопользования, Основы сельского хозяйства, Основы теории машин и механизмов, Основы теории технологической подготовки, Практикум по информационным технологиям, Практикум по кулинарии, Практикум по швейному производству, Программирование, Проектирование в системах автоматизированного проектирования, Разработка приложений в Microsoft Visual Studio, Разработка электронных образовательных ресурсов и методика их оценки, Свободные инструментальные системы, Современные проблемы биотехнологии, Социальная экология, Специальное рисование, Стандартизация и сертификация в современном производстве, Теория графов в информатике, Техническое черчение, Технологии обработки металла и дерева, Технологии переработки сельскохозяйственной продукции, Технологии современных производств, Технология обработки ткани и пищевых продуктов, Физика, Химические производства Республики Мордовия, Химический мониторинг состояния окружающей среды, Химия, Химия в пищевой промышленности, Химия в текстильной промышленности, Экологический мониторинг состояния окружающей среды, Электротехнические и радиотехнические устройства.

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: основные понятия изучаемой предметной области; аспекты информационной безопасности, виды информационные угроз и способы защиты; Демонстрирует умение решения практико-ориентированных задач; Владеет терминологией изучаемой предметной области, способностью к решению профессиональных задач в области информационной безопасности. Ответ логичен и последователен, отличается глубиной и полнотой раскрытия темы, выводы аргументированы
Незачтено	Студент демонстрирует незнание основного содержания дисциплины, обнаруживая существенные пробелы в знаниях учебного материала, допускает принципиальные ошибки в выполнении предлагаемых заданий; затрудняется делать выводы и отвечать на дополнительные вопросы преподавателя.

8.3. Вопросы, задания текущего контроля

Модуль 1: Основы информационной безопасности

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)

.Модуль 2: Информационная безопасность в образовательной организации

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).

8.4. Вопросы промежутосной аттестации

Восьмой семестр (Зачет, ПК-1)

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

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.

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.

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.

9. Перечень основной и дополнительной учебной литературы

Основная 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 ://biblioclub.ru/index.php?page=book&id=428605

2. 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 ://biblioclub.ru/index.php?page=book&id=276557

3. Заика, А. Компьютерная безопасность [Электронный ресурс] / А. Заика. - М. : Рипол Классик, 2013. – 160 с. – (Компьютер — это просто). – Режим доступа : //biblioclub.ru/index.php?page=book&id=227317

4. 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 ://biblioclub.ru/index.php?page=book&id=363040

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

3. http://edu-top.ru/katalog - Университетская библиотека онлайн [Электронный ресурс]. – М. : Издательство «Директ-Медиа». – Режим доступа: http://biblioclub.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;
– прочитайте дополнительную литературу из списка, предложенного преподавателем;
– выпишите в тетрадь основные категории и персоналии по теме, 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 лабораторном занятии;
– выучите определения терминов, относящихся к теме;
– продумайте примеры и иллюстрации к ответу по изучаемой теме;
– подберите цитаты ученых, общественных деятелей, публицистов, уместные с точки зрения обсуждаемой проблемы;
– продумывайте высказывания по темам, предложенным к лабораторному 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

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/opendata/)
2. Профессиональная база данных «Портал открытых данных Министерства культуры Российской Федерации» (http://opendata.mkrf.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 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.

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, курсового проектирования (выполнения курсовых работ), № 14.

Помещение укомплектовано специализированной мебелью и техническими средствами обучения.

Основное оборудование:

Наборы демонстрационного оборудования: автоматизированное рабочее место в составе (системный блок, монитор, клавиатура, мышь, гарнитура); интерактивная система информации; AverVision F55 (документ-камера).

Учебно-наглядные пособия:

Презентации.

Помещение для самостоятельной работы.

Читальный зал электронных ресурсов, № 101 б

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 12 шт., мультимедийны проектор 1 шт., многофункциональное устройство 1 шт., принтер 1 шт.).

Учебно-наглядные пособия:

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