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

Физико-математический факультет

Кафедра информатики и вычислительной техники

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Информационная безопасность в образовании

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

Профиль подготовки: Информатика. Математика

Форма обучения: Очная

Разработчики:
канд. физ.-мат. наук, доцент кафедры информатики и вычислительной техники Лапин К. С.
старший преподаватель кафедры информатики и вычислительной техники Зубрилина М.С.

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

Зав. кафедрой_____Вознесенская Н. В.

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

Зав. кафедрой_____Зубрилин А. А.

1. Цель и задачи изучения дисциплины

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

Задачи дисциплины:

- изучение основных направлений организации информационной безопасности (правового, технического, аппаратного) ;
- изучение основ правового регулирования информационной безопасности в России;
- формирование знаний о технических способах и средствах обеспечения защиты информации;
- изучение программных средств обеспечения информационной безопасности при работе на ПК и в сети Интернет;
- формирование умений аргументированного выбора и самостоятельной установки соответствующего программного обеспечения по защите данных на ПК;
- формирование умений по организации защиты файлов и отдельных данных в документах Microsoft;
- формирование умений разрабатывать и реализовывать политику информационной безопасности на предприятии, в частности в образовательном учреждении.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина К.М.06.ДВ.02.2 «Информационная безопасность в образовании» относится к части учебного плана, формируемой участниками образовательных отношений.

Дисциплина изучается на 4 курсе, в 8 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.
владеть понятием информация, знать свойства информации, распознавать информационные процессы и носители информации;
знать архитектуру ПК, классификацию программного обеспечения, структуру операционной системы Windows;
владеть программными продуктами Microsoft;

Изучению дисциплины К.М.06.ДВ.02.2 «Информационная безопасность в образовании» предшествует освоение дисциплин (практик):

ИКТ и медиаинформационная грамотность;
Информационные технологии в образовании.

Освоение дисциплины К.М.06.ДВ.02.2 «Информационная безопасность в образовании» является необходимой основой для последующего изучения дисциплин (практик):

Технология подготовки учащихся к олимпиадам по информатике;

Методика обучения информатике;

Защита информации в компьютерных сетях.

Область профессиональной деятельности, на которую ориентирует дисциплина «Технология и организация воспитательных практик», включает: 01 Образование и наука (в сфере дошкольного, начального общего, основного общего, среднего общего образования, профессионального обучения, профессионального образования, дополнительного образования).

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

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Компетенция в соответствии ФГОС ВО	
Индикаторы достижения компетенций	**Образовательные результаты**
ПК-11. Способен использовать теоретические и практические знания для постановки и решения исследовательских задач в предметной области (в соответствии с профилем и уровнем обучения) и в области образования.	
педагогическая деятельность	
ПК-11.1 Использует теоретические и практические знания для постановки и решения исследовательских задач в предметной области в соответствии с профилем и уровнем обучения и в области образования.	знать: - основные аспекты организации информационной безопасности в образовательных организациях; - нормативно-правовые основы информационной безопасности; - понятия информационной безопасности, изучаемые в школьном курсе информатики; уметь: - организовывать учебную деятельность для овладения способами защиты информации, изучаемые в школьном курсе информатики; - проектировать политику информационной безопасности в условиях определенной образовательной организации; владеть: - методами, средствами и формами организации информационной безопасности в соответствии с принятыми правовыми нормами РФ;- подходами к формированию умений использовать современные методы защиты информации.
ПК-11.2 Проектирует и решает исследовательские задачи в предметной области в соответствии с профилем и уровнем обучения и в области образования.	знать: - способы организации информационной безопасности, изучаемых в школьном курсе информатики; уметь: - определять оптимальный набор программных средств для обеспечения безопасной работы на ПК; - применять способы защиты информации в компьютерных сетях; владеть: - методами организации комплексной защиты информации различного вида;- методами защиты конфиденциальной информации в условиях образовательной организации.
ПК-14. Способен устанавливать содержательные, методологические и мировоззренческие связи предметной области (в соответствии с профилем и уровнем обучения) со смежными научными областями.	

ПК-14.4 Формирует междисциплинарные связи методики обучения информатике с педагогическими, психологическими и гуманитарными дисциплинами, в том числе на основе интеграции деятельности в области информатики и методики обучения информатики.	знать: - методы организации учебной деятельности при изучении понятий инофрмационной безопасности курса информатики; - этапы формирования понятий информационной безопасности на уроках информатики; уметь: - организовывать учебную деятельность для овладения способами защиты инофрмации, изучаемые в школьном курсе информатики; - проектировать политику информационной безопасности в условиях определенной образовательной организации; владеть: - методами, средствами и формами организации информационной безопасности в соответствии с принятыми правовыми нормами РФ;- подходами к формированию умений использовать современные методы защиты информации.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Восьмой семестр
Контактная работа (всего)	**40**	**40**
Лабораторные	40	40
Самостоятельная работа (всего)	**32**	**32**
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. Основы информационной безопасности:

Правовой аспект информационной безопасности. Понятие информационной угрозы, виды угроз. Компьютерные вирусы. Организационный аспект информационной безопасности. Классификатор российского ПО, программное обеспечение для реализации информационной безопасности. Криптографические методы защиты информации. Исторические шифры: замена и перестановка. Математическая модель шифра замены. Математические основы современных шифров. Шифры гаммирования.

Раздел 2. Информационная безопасность в образовательной организации:

Антивирусные программы. Настройки браузеров для организации защиты информации. Аппаратно-программный аспект информационной безопасности. Доктрина информационной безопасности. Технологии обработки конфиденциальных документов.

Интернет-мошенничества. Аспекты социальной инженерии. Формирование информационной культуры у детей при использовании сети интернет. Нормативные документы о защите детей в информационном пространстве. Информационная безопасность на уроках информатики.

5.2. Содержание дисциплины: Лабораторные (40 ч.) Раздел 1. Основы информационной безопасности (20 ч.)

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

Практическое занятие направлено на изучение нормативно-правовой базы по вопросам информационной безопасности. 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 2. Понятие информационной угрозы, виды угроз (2 ч.)

Понятие информационной угрозы, виды угроз. Средства и методы защиты информации.

Тема 3. Компьютерные вирусы (2 ч.)

Вредоносные программы, их виды. Классификация компьютерных вирусов. Классические компьютерные вирусы. Файловые вирусы. Макровирусы. Троянские программы. Руткиты. Сетевые черви. Антивирусные программы.

Тема 4. 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 5. 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 6. Криптографические методы защиты информации (2 ч.)

Рассматриваются криптографические методы защиты информации. Исторические шифры, шифрования с использованием MS Excel

Тема 7. Исторические шифры: замена и перестановка (2 ч.)

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

Тема 8. Математическая модель шифра замены (2 ч.)

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

Тема 9. Математические основы современных шифров (2 ч.)

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

Тема 10. Шифры гаммирования (2 ч.)

Задания практической работы направлены на изучение алгоритма гаммирования и его реализацию.

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

Тема 11. Антивирусные программы (2 ч.)

Задания практической работы направлены на изучение функционала популярных антивирусных программ.

Тема 12. Настройки браузеров для организации защиты информации (2 ч.)

Задания практической работы направлены на проведения сравнительного анализа функционала популярных браузеров. направленного на защиту информации.

Тема 13. Аппаратно-программный аспект информационной безопасности (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.

Тема 14. Доктрина информационной безопасности (2 ч.)

Практическое занятие направлено на выявление особенностей организации информационной безопасности в общеобразовательных учреждениях.

Тема 15. Технологии обработки конфиденциальных документов (2 ч.)

Практическое занятие направлено на изучение правил работы с конфиденциальной

информацией в общеобразовательных учреждениях.

Тема 16. Интернет-мошенничества (2 ч.)

Практическое занятие направлено на выявление способов мошенничества в сети интернет и разработку рекомендаций по защите от мошенничества для родителей и детей.

Тема 17. Аспекты социальной инженерии (2 ч.)

Практическое занятие направлено на изучение аспектов социальной инженерии как нового направления информационной безопасности. Задания лабораторной работы направлены на разработку методических рекомендаций по защите от психологического воздействия пользователей сети Интернет.

Тема 18. Формирование информационной культуры у детей при использовании сети интернет (2 ч.)

Практическое занятие направлено на выявление особенностей информационной культуры личности ребенка.

Тема 19. 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 20. Информационная безопасность на уроках информатики (2 ч.)

Рассматривается содержание курса школьной информатики (продвинутый уровень) с точки зрения формирования понятий информационной безопасности. Изучаются методические особенности формирования этих понятий.

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

6.1 Вопросы и задания для самостоятельной работы

Восьмой семестр (32 ч.)

Раздел 1. Основы информационной безопасности (16 ч.)

Вид СРС: *Выполнение индивидуальных заданий

Выполните следующие задания

1. Выделить нормативно-правовые акты, регулирующие циркулирование информации в организации (из списка организаций).
2. Выявить категории персональных данных и порядок обращения с ними в ситуации обращения за услугой в организацию (из списка ситуаций).
3. Выделить нормативно-правовые акты, закрепляющие недопустимость сокрытия или ограничения доступа к информации (из списка организаций).
4. Выявить угрозы информационной безопасности в предлагаемой ситуации (общение в социальной сети, передача логина пароля специалисту обслуживающей организации).
5. Оценить действия сотрудника предприятия, приведшие к инциденту, связанному с угрозой информационной безопасности (в предлагаемой ситуации).
6. Установка, настройка антивируса, проверка его работоспособности путем создания тестового вирусного файла.
7. Проектирование модели угроз путем сопоставления угроз и методов их парирования (в предлагаемой ситуации).

Вид СРС: *Подготовка к тестированию*

Типовые вопросы теста

1. Что такое защита информации?
1) защита от несанкционированного доступа к информации;
2) выпуск бронированных коробочек для дискет;
3) комплекс мероприятий, направленных на обеспечение информационной безопасности.
2. К какой группе мер по защите информации относится шифрование информации?
1) организационным;
2) техническим;
3) аппаратным;

4) программным.

3. Укажите принципы создания комплексной системы защиты информации:

1) неизменности;

2) прозрачности;

3) модульности;

4) рациональности;

5) доступности.

4. Внешние техногенные угрозы информационной безопасности обусловлены:

1) средствами связи и помехами от них;

2) близко расположенными опасными производствами;

3) некачественными программными средствами;

4) взаимодействием технических средств.

5. К какой группе угроз информационной безопасности относятся ошибки программного обеспечения?

1) стихийные;

2) техногенные;

3) антропогенные.

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

Раздел 2. Информационная безопасность в образовательной организации (16 ч.)

Вид СРС: *Выполнение индивидуальных заданий

Выполните следующие задания

1 Изучить документ "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации". Укажите, какие типы НСД рассмотрены в документе. Составить презентацию на тему «Классы защищённости СВТ».

2. Воспользуйтесь поиском для составления сводной таблицы документов, регламентирующих требования к информационной безопасности. Укажите, какие документы необходимо учитывать при проектировании защиты документации на электронном носителе. Смоделируйте последовательность действий для защиты от копирования информации.

3. Изучить ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Изучить основные термины и определения. Составить глоссарий для памятки по информационной безопасности.

4. На основе ГОСТ Р 53114-2008 составить памятку об информационной безопасности для заведения, использующего электронный документооборот. Обосновать достаточность предлагаемых пунктов безопасности. На примере продемонстрировать необходимость соблюдения правил информационной безопасности.

5. Провести анализ защищенности объекта защиты информации по следующим разделам: Виды возможных угроз; Характер происхождения угроз; Классы каналов несанкционированного получения информации.

6. Предложить анализ увеличения защищенности объекта защиты информации; определить требования к защите информации. Классифицировать автоматизированную систему.

7. Пользуясь учебником, опишите виды и схемы сертификации средств защиты информации; функции ФСТЭК в области сертификации средств защиты информации.

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.

Вид СРС: *Подготовка к тестированию*

Типовые вопросы теста

1. Политика безопасности:
1) строится на основе общих представлений об информационной системе организации;
2) строится на основе изучения политик родственных организаций;
3) строится на основе анализа рисков;
4) фиксирует правила разграничения доступа;
5) отражает подход организации к защите своих информационных активов;
6) описывает способы защиты руководства организации.
2. Оценка рисков позволяет ответить на следующие вопросы:
1) Как спроектировать надежную защиту?
2) Какую политику безопасности предпочесть?
3) Какие защитные средства экономически целесообразно использовать?
4) Чем рискует организация, используя информационную систему?
5) Чем рискуют пользователи информационной системы?
6) Чем рискуют системные администраторы?
7) Существующие риски приемлемы?
8) Кто виноват в том, что риски неприемлемы?
9) Что делать, чтобы риски стали приемлемыми?
3. Нужно ли включать в число ресурсов по информационной безопасности серверы с информацией о методах использования уязвимостей?
1) да, поскольку знание таких методов помогает ликвидировать уязвимости;
2) нет, поскольку это плодит новых злоумышленников;
3) не имеет значения, поскольку если информация об использовании уязвимостей понадобится, ее легко найти.
4. Риск является функцией:
1) вероятности реализации угрозы;
2) стоимости защитных средств;
3) числа уязвимостей в системе.
5. В число принципов физической защиты входят:
1) беспощадный отпор;
2) непрерывность защиты в пространстве и времени;
3) минимизация защитных средств.

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	ПК-11, ПК-14
2.	Учебно-исследовательский модуль	ПК-11, ПК-14

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

<table>
<tr><td colspan="4">ПК-11 Способен использовать теоретические и практические знания для постановки и решения исследовательских задач в предметной области (в соответствии с профилем и уровнем обучения) и в области образования</td></tr>
<tr><td colspan="4">ПК-11.1 Использует теоретические и практические знания для постановки и решения исследовательских задач в предметной области в соответствии с профилем и уровнем обучения и в области образования.</td></tr>
<tr><td>Не способен Использует теоретические и практические знания для постановки и решения исследовательских задач в предметной области в соответствии с профилем и уровнем обучения и в области образования.</td><td>В целом успешно, но бессистемно Использует теоретические и практические знания для постановки и решения исследовательских задач в предметной области в соответствии с профилем и уровнем обучения и в области образования.</td><td>В целом успешно, но с отдельными недочетами Использует теоретические и практические знания для постановки и решения исследовательских задач в предметной области в соответствии с профилем и уровнем обучения и в области образования.</td><td>Способен в полном объеме Использует теоретические и практические знания для постановки и решения исследовательских задач в предметной области в соответствии с профилем и уровнем обучения и в области образования.</td></tr>
<tr><td colspan="4">ПК-11.2 Проектирует и решает исследовательские задачи в предметной области в соответствии с профилем и уровнем обучения и в области образования.</td></tr>
<tr><td>Не способен Проектирует и решает исследовательские задачи в предметной области в соответствии с профилем и уровнем обучения и в области образования.</td><td>В целом успешно, но бессистемно Проектирует и решает исследовательские задачи в предметной области в соответствии с профилем и уровнем обучения и в области образования.</td><td>В целом успешно, но с отдельными недочетами Проектирует и решает исследовательские задачи в предметной области в соответствии с профилем и уровнем обучения и в области образования.</td><td>Способен в полном объеме Проектирует и решает исследовательские задачи в предметной области в соответствии с профилем и уровнем обучения и в области образования.</td></tr>
<tr><td colspan="4">ПК-14 Способен устанавливать содержательные, методологические и мировоззренческие связи предметной области (в соответствии с профилем и уровнем обучения) со смежными научными областями</td></tr>
<tr><td colspan="4">ПК-14.4 Формирует междисциплинарные связи методики обучения информатике с педагогическими, психологическими и гуманитарными дисциплинами, в том числе на основе интеграции деятельности в области информатики и методики обучения информатики.</td></tr>
</table>

Не способен Формирует междисциплинарные связи методики обучения информатике с педагогическими, психологическими и гуманитарными дисциплинами, в том числе на основе интеграции деятельности в области информатики и методики обучения информатики.	В целом успешно, но бессистемно Формирует междисциплинарные связи методики обучения информатике с педагогическими, психологическими и гуманитарными дисциплинами, в том числе на основе интеграции деятельности в области информатики и методики обучения информатики.	В целом успешно, но с отдельными недочетами Формирует междисциплинарные связи методики обучения информатике с педагогическими, психологическими и гуманитарными дисциплинами, в том числе на основе интеграции деятельности в области информатики и методики обучения информатики.	Способен в полном объеме Формирует междисциплинарные связи методики обучения информатике с педагогическими, психологическими и гуманитарными дисциплинами, в том числе на основе интеграции деятельности в области информатики и методики обучения информатики.

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

Восьмой семестр (Зачет, ПК-11.1, ПК-11.2, ПК-14.4)

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 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.

8.4. 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 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 : http://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 доступаhttp://biblioclub.ru/index.php?page=book&id=276557

3. 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

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

Дополнительная литература

1.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. – UR http://biblioclub.ru/index.php?page=book&id=493175

2.Технологии защиты информации в компьютерных сетях [Электронный ресурс] / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 369 с. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=428820

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://school-collection.edu.ru - Единая коллекция Цифровых Образовательных [Электронный ресурс]. - URL: http://school-collection.edu.ru

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

3. http://www.informika.ru - Федеральное государственное автономное учреждение «Государственный научно-исследовательский институт информационных технологий и телекоммуникаций» [Электронный ресурс] / М.: Informika.ru, 2002 - 2016. - Режим доступ http://www.informika.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.

11. 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 информационно-справочных систем

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

12.2 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 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 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 – 24 шт.).

Учебно-наглядные пособия:

Презентации.

Помещение для самостоятельной работы.

Помещение оснащено оборудованием и техническими средствами обучения.

Основное оборудование:

Компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду университета (персональный компьютер 10 шт.).

Учебно-наглядные пособия:

Презентации.

Помещение для самостоятельной работы.

Читальный зал.

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.