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
Информационная безопасность в образовании

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

Профиль подготовки: Технология. Информатика

Форма обучения: очная

Разработчик:
Лапин К. С., канд. физ.-мат. наук, доцент кафедры информатики и вычислительной техники,
Сироткин В. А., старший преподаватель кафедры информатики и вычислительной техники

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 безопаснос (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.04.02 «Информационная безопасность в образовании» относится к части, формируемой участниками образовательных отношений.

Дисциплина изучается на 5 курсе, в 9 семестре.

Для изучения дисциплины требуется: знать определение понятия информации; свойства информации; информационные процессы; носители информации; архитектуру ПК; классификацию программного обеспечения; 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 К.М.06.ДВ.04.02 «Информационная безопасность в образовании» предшествует освоение дисциплин (практик):

ИКТ и медиаинформационная грамотность.

Освоение дисциплины К.М.06.ДВ.04.02 «Информационная безопасность в образовании» является необходимой основой для последующего изучения дисциплин (практик):

Основы защиты информации в компьютерных сетях.

Область профессиональной деятельности, на которую ориентирует дисциплина «Информационная безопасность в образовании», 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-11.6 Владеет современными информационными и коммуникационными технологиями с учетом требований информационного обеспечения к участникам образовательного процесса.	знать: - способы обеспечения информационной безопасности на современном оборудовании; уметь: - пользоваться программными средствами для обеспечения информационной безопасности; владеть: - навыки шифрованя данных и установка и использование программных средств для обеспечения информационной безопасности.
ПК-12. Способен выделять структурные элементы, входящие в систему познания предметной области (в соответствии с профилем и уровнем обучения), анализировать их в единстве содержания, формы и выполняемых функций.	

педагогическая деятельность

ПК-12.5 Проводит системный анализ современных проблем по информатике и вопросов связанных с информационной безопасностью всех участников образовательного процесса.	знать: - основы обеспечения информационной безопасности и методы шифрования; уметь: - уметь анализировать возможные риски информационных атак; - анализировать возможные программные средства защиты информации; владеть: - использования антивирусных программ;- навыки шифрования данных.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Девятый семестр
Контактная работа (всего)	**36**	**36**
Практические	36	36
Самостоятельная работа (всего)	**72**	**72**
Виды промежуточной аттестации		
Зачет		+
Общая трудоемкость часы	**108**	**108**
Общая трудоемкость зачетные единицы	**3**	**3**

5. Содержание дисциплины

5.1. Содержание разделов дисциплины

Раздел 1. Основы информационной безопасности:

Основные понятия информационной безопасности. Правовой аспект информационной безопасности. Оганизационный аспект информационной безопасности. Понятие информационной угрозы, виды угроз. Методы и средства защиты информации. Тестирование. Политика информационной безопасности в образовательной организации. Нормативные документы о защите детей в информационном простанстве. Формирование информационной культуры у детей при использовании сети интернет.

Раздел 2. Основы криптографии:

Информационная безопасность на уроках инофрматики. Коллоквиум. Тестирование. Аппаратно-программный аспект информационной безопасности. Понятие информационной угрозы, виды угроз. Брандмауэр. Антивирусные программы.

5.2. Содержание дисциплины: Практические (36 ч.)

Раздел 1. Основы информационной безопасности (18 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 информационной безопасности (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. 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 6. Тестирование (2 ч.)

Прохождение тестирование в системе Инфор-вуз

Тема 7. Политика информационной безопасности в образовательной организации (2 ч.)

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

Тема 8. Нормативные документы о защите детей в информационном простанстве (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 9. 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.

Раздел 2. Основы криптографии (18 ч.)

Тема 10. 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.

Тема 11. Информационная безопасность на уроках инофрматики (2 ч.)

Рассматривается содержание школьного курса информатики с точки зрения формирования понятий информационной безопасности. Рассматриваются задачи повышенного уровня сложности.

Тема 12. Коллоквиум (2 ч.) Проведение коллоквиума

Тема 13. Тестирование (2 ч.) Тестирование в системе Инфо-вуз

Тема 14. Аппаратно-программный аспект информационной безопасности (2 ч.) Выполнение лабораторной работы по теме «Программные средства защиты информации»

Тема 15. Понятие информационной угрозы, виды угроз (2 ч.) Выполнение лабораторной работы по теме «Виды угроз ИБ. Уязвимости»

Тема 16. Брандмауэр (2 ч.)

Выполнение лабораторной работы по теме «Брандмауэр»

Тема 17. Антивирусные программы (2 ч.)

Выполнение лабораторной работы по теме «Антивирусные программы»

Тема 18. Тестирование (2 ч.)

Тестирование в системе Инфо-вуз

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

6.1 Вопросы и задания для самостоятельной работы

Девятый семестр (72 ч.)

Раздел 1. Основы информационной безопасности (36 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.Обоснуйте основные задачи системы информационной безопасности.

2. Обоснуйте этапы развития информационной безопасности.

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

4. Охарактеризуйте программные средства организации информационной безопасности при работе на компьютере. На примере одного приложения раскройте его

функциональные возможности по защите информации.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

19. 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.

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

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

22. Перечислите способы проникновения компьютерных вирусов на компьютер. Приведите примеры, опишите особенности их разрушительных действий.

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

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

25. Охарактеризуйте программные средства ограничения доступа в Интернет,

фильтрации информационных ресурсов. На примере одного приложения раскройте его функциональные возможности по ограничению доступа в Интернет.

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

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. Основы криптографии (24 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: *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

№ п/п	Оценочные средства	Компетенции, этапы их формирования
1.	Предметно-технологический модуль	ПК-11
2.	Предметно-методический модуль	ПК-12

8.2. Показатели и критерии оценивания компетенций, шкалы оценивания

Шкала, критерии оценивания и уровень сформированности компетенции			
2 (не зачтено) ниже порогового	3 (зачтено) пороговый	4 (зачтено) базовый	5 (зачтено) повышенный
ПК-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			
ПК-11.6 Владеет современными информационными и коммуникационными технологиями с учетом требований информационного обеспечения к участникам образовательного процесса.			

Не владеет современными информационными и коммуникационными технологиями с учетом требований информационного обеспечения к участникам образовательного процесса.	В целом успешно владеет современными информационными и коммуникационными технологиями с учетом требований информационного обеспечения к участникам образовательного процесса.	С отдельными недочетами владеет современными информационными и коммуникационными технологиями с учетом требований информационного обеспечения к участникам образовательного процесса.	В полном объеме владеет современными информационными и коммуникационными технологиями с учетом требований информационного обеспечения к участникам образовательного процесса.
ПК-12 Способен выделять структурные элементы, входящие в систему познания предметной области (в соответствии с профилем и уровнем обучения), анализировать их в единстве содержания, формы и выполняемых функций			
ПК-12.5 Проводит системный анализ современных проблем по информатике и вопросов связанных с информационной безопасностью всех участников образовательного процесса.			
Не способен проводить системный анализ современных проблем по информатике и вопросов связанных с информационной безопасностью всех участников образовательного процесса.	В целом успешно, но бессистемно проводит системный анализ современных проблем по информатике и вопросов связанных с информационной безопасностью всех участников образовательного процесса.	В целом успешно, но с отдельными недочетами проводит системный анализ современных проблем по информатике и вопросов связанных с информационной безопасностью всех участников образовательного процесса.	В полном объеме проводит системный анализ современных проблем по информатике и вопросов связанных с информационной безопасностью всех участников образовательного процесса.

Уровни сформированности компетенций

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	незачтено	Ниже 60%

8.3. Вопросы промежуточной аттестации

Девятый семестр (Зачет, ПК-11.6, ПК-12.5)

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 служит формой проверки усвоения учебного материала, готовности к практической деятельности и успешного решения студентами учебных задач.

Устный ответ на зачете

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

При оценке достижений студентов необходимо обращать особое внимание на:

– усвоение программного материала;

– умение излагать программный материал научным языком;

– умение связывать теорию с практикой;

– умение отвечать на видоизмененное задание;

– владение навыками поиска, систематизации необходимых источников литературы по изучаемой проблеме;

– умение обосновывать принятые решения;

– владение навыками и приемами выполнения практических заданий;

– умение подкреплять ответ иллюстративным материалом.

9. Перечень основной и дополнительной учебной литературы

Основная литература

1. 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. 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

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

2. http://www.securrity.ru - SecuRRity.Ru — « Информационная безопасность компьютерны систем и защита конфиденциальных данных»

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

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;

– 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 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, курсового проектирования (выполнения курсовых работ), № 14.

Помещение оснащено оборудованием и техническими средствами обучения.

Основное оборудование:

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, №101б.

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 (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