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

Факультет педагогического и художественного образования
Кафедра информатики и вычислительной техники

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Основы управления информационной безопасностью в организации дополнительного образования

Направление подготовки: 44.03.01 Педагогическое образование
Профиль подготовки: Педагогика дополнительного образования
Форма обучения: Очная

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

Программа рассмотрена и утверждена на заседании кафедры информатики и вычислительной техники, протокол № 3 от 21.10.2021 года

Зав. кафедрой _____Зубрилин А. А.

1. Цель и задачи изучения дисциплины

Цель изучения дисциплины – подготовка бакалавров к деятельности, связанной с управлением информационной безопасностью, а также решением частных задач в области управления информационной безопасностью.

Задачи дисциплины:

– получение знаний о процессах, процедурах и элементах систем управления информационной безопасностью;

– овладение навыками проведения элементов анализа автоматизированных систем с точки зрения информационной безопасности;

– формирование практических навыков решения частных задач управления информационной безопасностью.

В том числе воспитательные задачи:

– формирование мировоззрения и системы базовых ценностей личности;

– формирование основ профессиональной культуры обучающегося в условиях трансформации области профессиональной деятельности.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина К.М.06.ДВ.06.01 «Основы управления информационной безопасностью в образовательной организации» относится к части учебного плана, формируемого участниками образовательных отношений.

Дисциплина изучается на 3 курсе, в 5 семестре.

Освоение дисциплины К.М.06.ДВ.06.01 «Основы управления информационной безопасностью в образовательной организации» является необходимой основой для последующего изучения дисциплин (практик):

Управление проектами в дополнительном образовании

Технология создания и продвижения медиа-проектов

Область профессиональной деятельности, на которую ориентирует дисциплина «Практикум по информационным технологиям», 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: - нормативные акты и стандарты в области управления информационной безопасностью; уметь: - выполнять планирование, идентификацию и анализ рисков, моделировать риски, проводить мониторинг; владеть: - навыками построения системы управления информационной безопасность предприятия в условиях

	применения современных информационных технологий.
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-12.2. Анализирует содержание, формы и выполняемые функции структурных элементов, входящих в систему познания предметной области (в соответствии с профилем и уровнем обучения)	знать: - формы организации конструктивного взаимодействия обучающихся в разных видах деятельности, условия для свободного выбора деятельности, участников совместной деятельности, материалов для достижения личностных, метапредметных и предметных результатов; уметь: - организовывать предметную и метапредметную деятельность воспитанников, необходимую для дальнейшей успешной траектории развития; владеть: - специализированным программным обеспечением; - пониманием структуры и системы взаимосвязи процессов управления информационной безопасностью.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	**Пятый семестр**
Контактная работа (всего)	**46**	**46**
Лекции	**16**	**16**
Практические	**30**	**30**
Самостоятельная работа (всего)	**26**	**26**
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. Система управления информационной безопасностью

Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии информационных ресурсов и защиты**.** Аудит информационной безопасности. Средства поддержки процессов управления информационной безопасностью. Сущность и задачи комплексной системы защиты информации.

Раздел 2. Управление комплексной системой защиты информации

Сущность и задачи комплексной системы защиты информации. Разработка модели комплексной системы защиты информации. Назначение, структура и содержание управления комплексной системой защиты информации. Оценка эффективности комплексной системой защиты информации. Методы и модели оценки эффективности комплексной системы защиты информации.

5.2. Содержание дисциплины: Лекции (16 ч.)

Раздел 1. Система управления информационной безопасностью (8 ч.)

Тема 1. Сущность и задачи комплексной системы защиты информации (2 ч.).

Разработка модели комплексной системы защиты информации. Назначение, структура

и содержание управления комплексной системой защиты информации.

Тема 2. Анализ объектазащиты (2 ч.).

Технология анализа объекта защиты. Типы информационных систем. Методы оценки ущерба от реализации угроз информационной безопасности. Комплекс стандартов в области информационной безопасности.

Тема 3. Модель угроз и модель нарушителя (4 ч.).

Подходы к формированию модели нарушителя и модели угроз. Требования регуляторов к формированию модели нарушителя и модели угроз.

Раздел 2. Управление комплексной системой защиты информации (8 ч.)

Тема 5. Оценка рисков информационнойбезопасности (2 ч.).

Политика информационной безопасности. Основные положения стандартов в области управления рисками информационной безопасности.

Тема 6. Организация управления персоналом в контексте обеспечения информационнойбезопасности (2 ч.).

Основные положения стандартов в области регламентации обеспечения информационной безопасности. Управление инцидентами информационной безопасности

Тема 7. Основные положения стандартов в области управления инцидентами информационной безопасности (2 ч.).

Регламентация действий сотрудников привозникновении нештатных ситуаций.

Тема 7. Методы и модели оценки эффективности комплексной системы защиты информации (2 ч.).

Практические (30 ч.)

Раздел 1. Система управления информационной безопасностью (14 ч.).

Тема 1. Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии информационных ресурсов и защиты (2 ч.)

Введение. Основные понятия, определения и терминология. Базовые вопросы управления ИБ. Стандартизация в области управления ИБ. Общие положения организационной защиты. Особенности организационной защитыкомпьютерных информационных систем и сетей. Служба безопасности предприятия.

Тема 2. Процессный подход (2 ч.).

Понятие процесса. Методы формализации процессов. Цели и задачи формализации процессов. Понятие процессного подхода.

Тема 3. Областьдеятельности СУИБ (2 ч.)

Понятие области деятельности СУИБ. Механизм выбора области деятельности. Состав области деятельности (процессы, структурные подразделения организации, кадры). Описание области деятельности (структура и содержание документа).

Тема 4. Ролевая структура СУИБ (2 ч.).

Понятие роли. Использование ролевого принципа в рамках СУИБ. Преимущества использования ролевого принципа. Ролевая структура СУИБ (основные и дополнительные роли). Роль высшего руководства организации в СУИБ. Этапы разработки и функционирования СУИБ, на которых важно участие руководства организации. Суть участия руководства организации на этих этапах (утверждение документов, результатов анализа рисков и т.д.).

Тема 5. ПолитикаСУИБ (2 ч.).

Понятие Политики СУИБ. Цели Политики СУИБ. Структура и содержание политики СУИБ. Источники информации для разработки Политики СУИБ.

Источники информации об активах организации. Типы угроз ИБ и уязвимостей для выделенных на этапе инвентаризации активов.

Тема 6. Аудит информационной безопасности **(2 ч.).**

Средства поддержки процессов управления информационной безопасностью (2 ч.).

Сущность и задачи комплексной системы защиты информации.

Основыуправление рисками ИБ (2 ч.).

Анализ рисков ИБ. Основные определения и положения управление рисками ИБ. Цель процесса анализа рисков ИБ. Этапы и участники процесса анализа рисков ИБ.

Методики анализа рисков ИБ (2 ч.).

Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах организации. Типы угроз ИБ и уязвимостей для выделенных на этапе инвентаризации активов.

Тема 7. Планирование мер по обработкевыявленных рисков ИБ (2 ч.).

Оценка рисков ИБ. Утверждение результатов анализа рисков ИБ у высшего руководства. Использование результатов анализа рисков ИБ.

Раздел 2. Управление комплексной системой защиты информации (16 ч.).

Тема 1. Анализ объектазащиты (2 ч.)

Формальное описание структурыинформационной системы.

Модель угроз и модель нарушителя. Составление модели угрозинформационной системе. Система управления информационнойбезопасностью.

Тема 2. Формирование требований к системезащиты информации. Политика информационнойбезопасности (2 ч.)

Формирование требований к политикеинформационной безопасности.

Тема 3. Управление инцидентами информационнойбезопасности. (2 ч.)

Формирование регламента действий при возникновении нештатных ситуаций. Оценка эффективности комплексной системой защиты информации. Методы и модели оценки эффективности комплексной системы защиты информации.

Тема 4. Внедрениемер (контрольныхпроцедур) по обеспечению ИБ (2 ч.).

Категории контрольных процедур. Перечень контрольных процедур по обеспечению ИБ в соответствии с лучшими международными практиками. Содержание контрольных процедур по обеспечению ИБ в интерпретации лучших практик.

Тема 5. Экранирование,анализ защищенности (2 ч.).

Экранирование. Основные понятия. Архитектурные аспекты. Классификация межсетевых экранов. Анализ защищенности. Обеспечение высокой доступности.

Тема 6. Отказоустойчивость и зона риска (2 ч.).

Доступность. Основные понятия. Меры по обеспечению высокой доступности. Отказоустойчивость и зона риска. Обеспечение отказоустойчивости. Программное обеспечениепромежуточного слоя. Обеспечение обслуживаемости.

Тема 7. Туннелирование и управление (2 ч.).

Тождественно истинные и тождественно ложные команды. Передача через сеть пакетов, принадлежащих протоколу, который в данной сети не поддерживается. Обеспечения слабой формы конфиденциальности (сокрытие истинных адресов и другой служебной информации).

Тема 8. Обеспечения конфиденциальности и целостности передаваемых данных при использовании вместе с криптографическими сервисами (2 ч.).

Мониторинг компонентов. Выдача и реализация управляющих воздействий. Координация работы компонентов системы.

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

6.1 Вопросы и задания для самостоятельной работы

Пятый семестр (26 ч.)

Раздел 1. Система управления информационной безопасностью (12 ч.)

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

Темы проектов:

1. Основные составляющие информационной безопасности.

2. Управление информационной безопасностью.
3. Важность и сложность проблемы информационной безопасности
4. Основные определения и критерии классификации угроз.
5. Основные угрозы доступности.
6. Основные угрозы целостности.
7. Основные угрозы конфиденциальности.
8. Вредительские программы
9. Роль стандартов ИБ.
10. Обоснование необходимости инвестиций в информационную безопасность компании.
11. Методика FRAP (фреп).
12. Методика OCTAVE (октэйв)
13. Методика Risk Watch (риск вэтч).
14. Основные направления обеспечения информационной безопасности.
15. Законодательно-правовая база обеспечения информационной безопасности на предприятии.
16. Нормативные акты предприятия по информационной безопасности.
17. Формы правовой защиты информации на предприятии.
18. Другие документы предприятия, в которых отражаются вопросы обеспечения информационной безопасности.
19. Общие положения организационной защиты.

Раздел 2. Управление комплексной системой защиты информации (14 ч.)

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

Темы проектов:

1. Оранжевая книга" как оценочный стандарт.
2. Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем.
3. Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Их основные положения.
4. Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования".
5. Сертификация СУИБ на соответствие ISO 27001.
6. Метод оценки рисков на основе модели угроз и уязвимостей
7. Расчет рисков по угрозе информационной безопасности
8. Задание контрмер
9. Качественные методики управления рисками.
10. Количественные методики управления рисками. Метод CRAMM.
11. Особенности организационной защиты компьютерных информационных систем и сетей.
12. Служба безопасности предприятия.
13. Основные программно-технические меры.
14. Идентификация и аутентификация.
15. Управление доступом
16. Протоколирование и аудит
17. Активный аудит.
18. Шифрование.
19. Контроль целостности.
20. Цифровые сертификаты.

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-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-11.1. 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.			
Не 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	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	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	Способен в полном объеме 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-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-12.2. Анализирует содержание, формы и выполняемые функции структурных элементов, входящих в систему познания предметной области (в соответствии с профилем и уровнем обучения)			
Не способен анализировать содержание, формы и выполняемые функции структурных элементов, входящих в систему познания предметной области (в соответствии с профилем и уровнем обучения)	В целом успешно, но бессистемно анализирует содержание, формы и выполняемые функции структурных элементов, входящих в систему познания предметной области (в соответствии с профилем и уровнем обучения)	В целом успешно, но с отдельными недочетами анализирует содержание, формы и выполняемые функции структурных элементов, входящих в систему познания предметной области (в соответствии с профилем и уровнем обучения)	Способен в полном объеме анализировать содержание, формы и выполняемые функции структурных элементов, входящих в систему познания предметной области (в соответствии с профилем и уровнем обучения)

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

Пятый семестр (Зачет, ПК-11.1, ПК-12.2)

1. Раскройте понятие информационной безопасности.
2. Выделите основные составляющие информационной безопасности.
3. Обоснуйте важность и сложность проблемы информационной безопасности.
4. Выделите недостатки традиционного подхода к информационной безопасности с объектной точки зрения.
5. Раскройте основные определения и критерии классификации угроз.
6. Выделите наиболее распространенные угрозы доступности.
7. Приведите примеры угроз доступности информации.
8. Расскажите о вредоносном программном обеспечении.
9. Выделите основные угрозы целостности конфиденциальности информации.
10. Сделайте обзор российского законодательства в области информационной безопасности. Расскажите о правовых актах общего назначения, затрагивающих вопросы информационной безопасности.
11. Раскройте важность Закона «Об информации, информационных технологиях и о защите информации» с точки зрения организации информационной безопасности на предприятии.
12. Раскройте оценочные стандарты и технические спецификации.
13. Расскажите о классах безопасности.
14. Расскажите о сетевых сервисах безопасности.
15. Выделите требования доверия безопасности.
16. Выделите подготовительные этапы управления рисками. Расскажите об основных этапах управления рисками на предприятии.
17. Раскройте понятия идентификации и аутентификации в компьютерной сети.
18. Расскажите о парольной аутентификации.
19. Раскройте особенности идентификации/аутентификации с помощью биометрических данных.
20. Расскажите об управлении доступом в компьютерной сети предприятия.
21. Расскажите об экранировании в компьютерной сети.
22. Дайте классификации межсетевых экранов.
23. Расскажите о методах «социальной инженерии» и укажите способы защиты от них.
24. Перечислите этапы оценки рисков информационной безопасности автоматизированных систем.
25. Проведите типизацию информационных систем. Какие данные об информационной системе необходимы для построения модели документооборота?
26. Какие подходы к разграничению доступа существуют в рамках организации. Какова структура документов, регламентирующих разграничение доступа.
27. Опишите подходы к построению модели нарушителя.
28. Проведите классификацию нарушителей (ФСТЭК).
29. Проведите классификация угроз безопасности персональных данных (ФСТЭК).
30. Прокомментируйте основные положения методики определения актуальных угроз (ФСТЭК).
31. Какова методика оценки ущерба, нанесённого при реализации угроз информационной

безопасности.

32. Перечислите угрозы информационной безопасности, источником которых является персонал организации.

33. Расскажите о туннелировании. Приведите примеры

34. Перечислите обязанности сотрудников службы безопасности при приёме сотрудников на работу.

35. Перечислите основные требования по организации парольной защиты.

36. Перечислите основные положения инструкции по организации антивирусной защиты.

37. Перечислите основные положения инструкции по работе с электронной почтой.

38. Приведите примеры источников информации об инцидентах информационной безопасности.

39. Перечислите аспекты анализа инцидентов информационной безопасности, направленные на совершенствование системы управления информационной безопасностью.

40. Приведите требования к формированию политики информационной безопасности организации и учитываемые в ней категории безопасности.

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

Промежуточная аттестация проводится в форме зачета.

Зачет позволяет оценить сформированность универсальных, общепрофессиональных и профессиональных компетенций, теоретическую подготовку студента, его способность к творческому мышлению, готовность к практической деятельности, приобретенные навыки самостоятельной работы, умение синтезировать полученные знания и применять их при решении практических задач.

При балльно-рейтинговом контроле знаний итоговая оценка выставляется с учетом набранной суммы баллов.

Собеседование (устный ответ) на зачете

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

При оценке достижений студентов необходимо обращать особое внимание на:

– усвоение программного материала;

– умение излагать программный материал научным языком;

– умение связывать теорию с практикой;

– умение отвечать на видоизмененное задание;

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

– умение обосновывать принятые решения;

– владение навыками и приемами выполнения практических заданий;

– умение подкреплять ответ иллюстративным материалом.

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

– в тестовом задании закрытой формы с выбором ответа выбран правильный ответ;

– по вопросам, предусматривающим множественный выбор правильных ответов, выбраны все правильные ответы;

– в тестовом задании открытой формы дан правильный ответ;

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

– в тестовом задании на установление соответствия сопоставление произведено верно

для всех пар.

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

Критерии оценки

До 60% правильных ответов – оценка «неудовлетворительно».

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

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

Свыше 90% правильных ответов – оценка «отлично».

9. Перечень основной и дополнительной учебной литературы

Основная литература

1. Моргунов А. В. ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2019. – 83 с. : ил., табл. – URL: https://biblioclub.ru/index.php?page=book&id=576726. – Библиогр.: с. 64. – ISBN 978-5-7782-3918-0. – Текст : электронный

2. 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. – URL: https://biblioclub.ru/index.php?page=book&id=493175. – Библиогр. в кн. – ISBN 978-5-9275-2364-1. – Текст : электронный.

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

Дополнительная литература

1. Кияев, В. Безопасность информационных систем: курс : [16+] / В. Кияев, О. Граничин. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 192 с. : ил. – URL: https://biblioclub.ru/index.php?page=book&id=429032. – Текст : электронный.

2. Кришталюк, А. Н. Правовые аспекты системы безопасности: курс лекций / А. Н. Кришталюк ; Межрегиональная академия безопасности и выживания. – Орел : Межрегиональная академия безопасности и выживания, 2014. – 204 с. : табл., схем. – URL: https://biblioclub.ru/index.php?page=book&id=428612. – Библиогр. в кн. – Текст : электронный.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

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

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

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

11. Методические указания обучающимся по освоению дисциплины (модуля)

При освоении материала дисциплины необходимо:

– спланировать и распределить время, необходимое для изучения дисциплины;

– конкретизировать для себя план изучения материала;

– ознакомиться с объемом и характером внеаудиторной самостоятельной работы для полноценного освоения каждой из тем дисциплины.

Сценарий изучения курса:

– проработайте каждую тему по предлагаемому ниже алгоритму действий;

– изучив весь материал, выполните итоговый тест, который продемонстрирует готовность к сдаче зачета.

Алгоритм работы над каждой темой:

– изучите содержание темы вначале по лекционному материалу, а затем по другим источникам;

– прочитайте дополнительную литературу из списка, предложенного преподавателем;

– составьте краткий план ответа по каждому вопросу, выносимому на обсуждение на практическом занятии;

– выучите определения терминов, относящихся к теме;

– продумайте примеры и иллюстрации к ответу по изучаемой теме.

Рекомендации по работе с литературой:

– ознакомьтесь с аннотациями к рекомендованной литературе и определите основной метод изложения материала того или иного источника;

– составьте собственные аннотации к другим источникам на карточках, что поможет при подготовке рефератов, текстов речей, при подготовке к зачету;

– выберите те источники, которые наиболее подходят для изучения конкретной темы.

12. Перечень информационных технологий

Реализация учебной программы обеспечивается доступом каждого студента к информационным ресурсам – электронной библиотеке и сетевым ресурсам Интернет. Для использования ИКТ в учебном процессе используется программное обеспечение, позволяющее осуществлять поиск, хранение, систематизацию, анализ и презентацию информации, экспорт информации на цифровые носители, организацию взаимодействия в реальной и виртуальной образовательной среде. Индивидуальные результаты освоения дисциплины студентами фиксируются.

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

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

12.2 Перечень информационно-справочных систем (обновление выполняется еженедельно)

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

12.3 Перечень современных профессиональных баз данных

1. Профессиональная база данных «Открытые данные Министерства образования и науки РФ» (http://xn----8sblcdzzacvuc0jbg.xn--80abucjiibhv9a.xn--p1ai/opendata/)
2. Электронная библиотечная система Znanium.com(http://znanium.com/)
3. Единое окно доступа к образовательным ресурсам (http://window.edu.ru

13. Материально-техническое обеспечение дисциплины(модуля)

Для проведения аудиторных занятий необходим стандартный набор специализированной учебной мебели и учебного оборудования, а также мультимедийное оборудование для демонстрации презентаций на лекциях. Для проведения практических занятий, а также организации самостоятельной работы студентов необходим компьютерный класс с рабочими местами, обеспечивающими выход в Интернет. Индивидуальные результаты освоения дисциплины студентами фиксируются в информационной системе 1 С:Университет. Реализация учебной программы обеспечивается доступом каждого студента к информационным ресурсам – электронной библиотеке и сетевым ресурсам Интернет. Для использования ИКТ в учебном процессе необходимо наличие программного обеспечения, позволяющего осуществлять поиск информации в сети Интернет, систематизацию, анализ и презентацию информации, экспорт информации на цифровые носители.

Учебная аудитория для проведения учебных занятий.

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

Учебная аудитория для проведения учебных занятий.

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

Лаборатория вычислительной техники.

Помещение оснащено оборудованием и техническими средствами обучения.

Основное оборудование:

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

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

Учебно-наглядные пособия:

Презентации.

Помещение для самостоятельной работы

Читальный зал электронных ресурсов.

Основное оборудование:

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

Мультимедийный проектор, многофункциональное устройство, принтер.

Учебно-наглядные пособия:

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