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

Гуманитарные аспекты информационной безопасности

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

Профиль подготовки: Менеджмент в образовании. Информационная безопасность в образовании

Форма обучения: Очная

Разработчики: 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 – формирование компетенций в области основных сведений об этике новых отношений, учитывающих массовую компьютеризацию всех сторон жизни и деятельности личности, общества и государства, в области социально-правовых проблем информатизации и обеспечения информационной безопасности, получение знаний о современных научных направлениях, связанных с решением этих проблем.

Задачи дисциплины:

– получение знаний об основных этапах и закономерностях исторического развития России и её своеобразии в парадигме проблем обеспечения информационной безопасности;

– формирование умений применения методов оценки роли страны в современном мире в контексте всеобщей истории.

– процессах, процедурах и элементах систем управления информационной безопасностью;

– овладение навыками проведения анализа актуальных проблем формирования информационной безопасности общества и гражданской позиции отдельного индивида.

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.06.02 «Гуманитарные аспекты информационной безопасности» относится к части учебного плана, формируемого участниками образовательных отношений.

Дисциплина изучается на 5 курсе, в 9 и 10 семестрах.

Освоение дисциплины К.М.06.ДВ.06.02 «Гуманитарные аспекты информационной безопасности» является необходимой основой для последующего изучения дисциплин (практик):

К.М.04.01 Управление качеством в образовании

К.М.06.29 Организация финансово-хозяйственной деятельности в образовательных организациях

К.М.06.ДВ.06.01 Основы управления информационной безопасностью в образовательной организации

К.М.08.04(У) Производственная (научно-исследовательская работа) практика

Компетенция в соответствии ФГОС ВО	
Индикаторы достижения компетенций	**Образовательные результаты**
УК-3. Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	
УК-3.3. Демонстрирует навыки работы с институтами и организациями в процессе осуществления социального взаимодействия	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. - навыками решения профессиональных задач в различных контекстах.
ПК-14 Способен устанавливать содержательные, методологические и мировоззренческие связи предметной области (в соответствии с профилем и уровнем обучения) со смежными научными областями	
педагогическая деятельность	
ПК-14.2. Осуществляет отбор	знать:

способов построения моделей в системе образования; владеет современными представлениями о программных продуктах, применяемых в образовании	- 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; - использовать информационные технологии в профессиональнойдеятельности; 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	**Девятый семестр**	**Десятый семестр**
Контактная работа (всего)	**70**	**22**	**48**
Лекции	**24**	**0**	**24**
Практические	**46**	**22**	**24**
Самостоятельная работа (всего)	**74**	**50**	**24**
Виды промежуточной аттестации			
Зачет		+	+
Общая трудоемкость часы	**144**	**72**	**72**
Общая трудоемкость зачетные единицы	**4**	**2**	**2**

5. Содержание дисциплины

5.1. Содержание разделов дисциплины:

Раздел 1. Информационное общество: общественный прогресс иновые реальности.

Содержание и взаимосвязи понятий «информационная безопасность» и «национальная безопасность». Национальная безопасность России в условиях информационного общества. Понятие международной информационной безопасности. Основные направления научных исследований в области обеспечения информационной безопасности Российской Федерации. Информационно-психологическая безопасность как составляющая информационной безопасности.

Раздел 2. Общие сведения об информационно-психологической безопасности.

Информационные взаимосвязи личности, общества и государства. Информационные воздействия на личность, общество и государство. Возможности применения информационных воздействий деструктивного характера для нанесения ущерба личности, обществу и государству. Понятие и структура информационно-психологической безопасности.

Раздел 3. Информационноепротивоборство и информационная война

Модели, ресурсы, технологии и мишени информационных воздействий. Основные типы и содержание технологий информационного воздействия. Понятие и примеры манипулирования в различных областях социального взаимодействия. Способы манипулирования в массовых информационных процессах, в ходе обсуждений и дискуссий, в межличностном общении. Ложь как средство манипулирования. Слухи и провокации как способы информационно-психологического воздействия.

Раздел 4. Информационные воздействия как инструмент скрытого управления

личностью и обществом

Технологии скрытого управления личностью и обществом с помощью информационных воздействий. Информационно-психологические операции как комплексные организационные технологии скрытого управления. Информационно-психологические операции в современных вооружённых конфликтах.

5.2. Содержание дисциплины: Лекции (24 ч.)

Раздел 3. Информационноепротивоборство и информационная война (12 ч.)

Тема 1. Общие сведения об информационно-психологической безопасности (2 ч.).

Информационное противоборство и информационная война. Понятия информационного и рефлексивного управления, их роль в информационном обществе.

Тема 2. Модели информационного и рефлексивного управления (2 ч.).

Понятия информационного и информационно-психологического противоборства. Теоретические основы информационного противоборства.

Тема 3. Информационная война как средство достижения политических целей (2 ч.).

Информационное оружие. Взгляды иностранных государств на информационную войну. Информационные войны в новейшей истории. Основы государственной информационной политики в условиях информационно-психологической войны.

Тема 4. Информационные воздействия как инструмент скрытого управления личностью и обществом (4 ч.).

Информационные воздействия различных коммуникативных ситуациях.

Модели, ресурсы, технологии и мишени информационных воздействий. Основные типы.

Тема 5. Контрольная аттестация (2 ч.)

Раздел 4. Информационные воздействия как инструмент скрытого управления личностью и обществом (12 ч.)

Тема 1. Технологии скрытого управления личностью и обществом с помощью информационных воздействий (2 ч.).

Информационно-психологические операции как комплексные организационные технологии скрытого управления. Информационно-психологические операции в современных вооружённых конфликтах.

Информационно-психологические операции в избирательных кампаниях.

Тема 2. «Кризисные» технологии как вид информационно-психологических операций (2 ч.).

Технология постепенного изменения общественного сознания (модель «окна Овертона»). Политика ненасильственных действий как метод влияния на внутриполитические отношения.

Тема 3. Технологии управления личностью, применяемые в тоталитарных сектах и деструктивных культах(2 ч.).

Информационные операции в сети Интернет.

Тема 4. Содержание технологий информационного воздействия (2 ч.).

Понятие и примеры манипулирования в различных областях социального взаимодействия. Способы манипулирования в массовых информационных процессах, в ходе обсуждений и дискуссий, в межличностном общении. Ложь как средство манипулирования. Слухи и провокации как способы информационно-психологического воздействия.

Тема 5. Глобальная сеть Интернет как среда реализации информационных воздействий деструктивного характера (2 ч.).

Тема 6. Контрольная аттестация (2 ч.)

Практические (46 ч.)

Раздел 1. Информационное общество: общественный прогресс и новые реальности (12 ч.).

Тема 1. Гуманитарныепроблемы информационнойбезопасности (4 ч.).

Информационное общество: общественный прогресс и новые реальности. Содержание и взаимосвязи понятий «информационная безопасность» и «национальная безопасность». Национальная безопасность России в условиях информационного общества. Понятие международной информационной безопасности. Основные направления научных исследований в области обеспечения информационной безопасностиРоссийской Федерации.

Тема 2. Информационно-психологическая безопасность как составляющая информационной безопасности (2 ч.).

Информационная сфера как системообразующий факторжизни общества.

Тема 3. Доктрина информационной безопасности Российской Федерации (2 ч.). Информационное обеспечение государственной политики. Сохранение культурно-нравственных ценностей российского народа. Подходы к оцениванию информационной безопасности России.

Тема 4. Информационные взаимосвязи личности, общества и государства (2 ч.).

Информационные воздействия на личность, общество и государство. Возможности применения информационных воздействий деструктивного характера для нанесения ущерба личности, обществу и государству. Понятие и структура информационно-психологической безопасности. Субъекты, объекты и источники угроз информационно-психологической безопасности.

Тема 5. Контрольная аттестация (2 ч.).

Раздел 2. Общие сведения об информационно-психологической безопасности (10 ч.).

Тема 1. Общие сведения об информационно-психологической безопасности (2 ч.).

Информационное противоборство и информационная война. Понятия информационного и рефлексивного управления, их роль в информационном обществе.

Тема 2. Основы обеспечения информационно-психологическойбезопасности личности (2 ч.).

Общие сведения об информационно-психологической защите личности. Основные направления обеспеченияинформационно-психологической безопасности личности.

Тема 3. Информационная война как средство достижения политических целей (2 ч.).

Информационное оружие. Взгляды иностранных государств на информационную войну. Информационные войны в новейшей истории. Основы государственной информационной политики в условиях информационно-психологической войны.

Тема 4. Информационные воздействия как инструмент скрытого управления личностью и обществом (2 ч.).

Информационные воздействия различных коммуникативных ситуациях. Модели, ресурсы, технологии и мишени информационных воздействий

Тема 5. Контрольная аттестация (2 ч.)

Раздел 3. Информационноепротивоборство и информационная война (12 ч.)

Тема 1. Общие сведения об информационно-психологической безопасности (2 ч.).

Информационное противоборство и информационная война. Понятия информационного и рефлексивного управления, их роль в информационном обществе.

Тема 2. Модели информационного и рефлексивного управления (2 ч.).

Понятия информационного и информационно-психологического противоборства. Теоретические основы информационного противоборства.

Тема 3. Информационная война как средство достижения политических целей (2 ч.).

Информационное оружие. Взгляды иностранных государств на информационную войну. Информационные войны в новейшей истории. Основы государственной информационной политики в условиях информационно-психологической войны.

Тема 4. Информационные воздействия как инструмент скрытого управления личностью и обществом (4 ч.).

Информационные воздействия различных коммуникативных ситуациях.

Модели, ресурсы, технологии и мишени информационных воздействий. Основные типы.

Тема 5. Контрольная аттестация (2 ч.)

Раздел 4. Информационные воздействия как инструмент скрытого управления личностью и обществом (12 ч.)

Тема 1. Понятие и виды психологической защиты личности (2 ч.).

Понятие и структура системы психологической защиты личности. Инструментарий оценки информационно-психологической защищенности личности.

Тема 2. Модели информационного и рефлексивного управления (2 ч.).

Понятия информационного и информационно-психологического противоборства. Теоретические основы информационного противоборства

Тема 3. Алгоритмические основы психологической самозащитыличности (2 ч.).

Основные формы психологической самозащиты. Основы психологической самозащиты в межличностных, контакт-коммуникативных, масс- коммуникативных ситуациях и при работе в глобальнойсети Интернет.

Тема 4. Способы повышения стрессоустойчивости личности (2 ч.).

Алгоритмический подход к организации психологической самозащиты.

Тема 5. Контрольная аттестация (2 ч.)

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

6.1 Вопросы и задания для самостоятельной работы

Девятый семестр (50 ч.)

Раздел 1. Информационное общество: общественный прогресс иновые реальности (26 ч.)

Вид СРС: *Выполнение практико-ориентированного задания.

Составьте словарь с трактовкой следующих понятий учебного курса:

Манипулирование

Понятийное логическое мышление

Аналитическое мышление

Фрагментарное (клиповое) сознание

Правильное мышление

Правильное логическое мышление

Аргумент

Демонстрация

Дискуссия

Доказательство

Критерий

Полемика

Содержание и форма

Софизм

Спор

Тезис

Оформите задание в виде текста с гиперссылками. Подготовьте презентацию для иллюстрации применения понятий курса (не менее 20 слайдов). Включите исторический материал по теме эссе.

Раздел 2. Общие сведения об информационно-психологической безопасности (24 ч.)

Вид СРС: Подготовить учебное эссе по мотивам одной истем:

Информационное воздействие на человека и манипуляция сознанием. Особенности строения головного мозга человека.

История изучения воздействия СМИ и основные тенденции (20е – 30е годы прошлого столетия).

Концепции опосредованного воздействия СМИ на аудиторию (40-50е годы)

Альтернативные тенденции: таблоидизация и специализация масс-медиа.

Тенденции освещения экстремальных событий в СМИ.

Способы привлечения массовой и специализированной аудиторий

Десятый семестр (24 ч.)

Раздел 3. Информационноепротивоборство и информационная война (12 с.)

Вид СРС: Подготовить учебное эссе по мотивам одной истем:

Семантическая сеть знаний.

«Спираль молчания».

Манипуляция сознанием.

Язык образов.

Эмоциональное воздействие как предпосылка манипуляции.

Раздел 4. Информационныевоздействия как инструмент скрытого управления личностью и обществом (12 ч.)

Вид СРС: Подготовить учебное эссе по мотивам одной истем:

1. Манипуляция сознанием, признаки выявления манипуляции, методы противодействия манипуляции
2. Манипуляция сознанием в деструктивных культах и техника религиозной безопасности.
3. Основные теории информационного психологического воздействия. Основные положения теории семантических сетей знаний В.Я. Розенберга.
4. Пример построения модели знаний человека на основе семантических сетей.
5. Методы фильтрации информации.
6. Основные положения теории информационно-психологического воздействия.

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	УК-3 , 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
УК-3. Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде			
УК-3.3. Демонстрирует навыки работы с институтами и организациями в процессе осуществления социального взаимодействия			
Не способен демонстрировать навыки работы с институтами и организациями в процессе осуществления социального взаимодействия	В целом успешно, но бессистемно демонстрирует навыки работы с институтами и организациями в процессе осуществления социального взаимодействия	В целом успешно, но с отдельными недочетами демонстрирует навыки работы с институтами и организациями в процессе осуществления социального взаимодействия	Способен в полном объеме демонстрировать навыки работы с институтами и организациями в процессе осуществления социального взаимодействия
ПК-14 Способен устанавливать содержательные, методологические и мировоззренческие связи предметной области (в соответствии с профилем и уровнем обучения) со смежными научными областями			
ПК-14.2. Осуществляет отбор способов построения моделей в системе образования; владеет современными представлениями о программных продуктах, применяемых в образовании.			
Не способен осуществлять отбор способов построения моделей в системе образования; владеет современными представлениями о программных продуктах, применяемых в образовании.	В целом успешно, но бессистемно осуществляет отбор способов построения моделей в системе образования; владеет современными представлениями о программных продуктах, применяемых в образовании..	В целом успешно, но с отдельными недочетами осуществляет отбор способов построения моделей в системе образования; владеет современными представлениями о программных продуктах, применяемых в	Способен в полном объеме осуществлять отбор способов построения моделей в системе образования; владеет современными представлениями о программных продуктах, применяемых в образовании.

		образовании.	

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

Девятый семестр (Зачет, УК-3.3, ПК-14.2)

1. Выполните анализ гуманитарных проблем информационнойбезопасности
2. Раскройте содержание и взаимосвязи понятий «информационная безопасность» и «национальная безопасность».
3. Дайте трактовку понятия международной информационной безопасности. Перечислите и дайте характеристику основных направлений научных исследований в области обеспечения информационной безопасностиРоссийской Федерации.
4. Проанализируйте Доктрину информационной безопасности Российской Федерации.
5. Как, на Ваш взгляд, реализовать сохранение культурно-нравственных ценностей российского народа.
6. Перечислите подходы к оцениванию информационнойбезопасности России.
7. Укажите информационные взаимосвязи личности, общества и государства.
8. Как происходят информационные воздействия на личность, общество и государство.
9. Приведите примеры информационного противоборства и информационной войны на конкретном примере.
10. Приведите примеры информационного обеспечения государственной политики на примере Республики Мордовия.
11. Назовите субъекты, объекты и источники угроз информационно- психологической безопасности
12. Прокомментируйте понятия информационного и информационно-психологического противоборства.
13. Приведите примеры информационного воздействия в различных коммуникативных ситуациях.
14. Приведите пример применения современного информационного оружия.
15. Составьте памятку для детей по правилам поведения в сети Интернет.
16. Перечислите основные проблемы общения в социальных сетях.
17. Назовите механизмы защиты от информационных угроз в социальных сетях.
18. Определите понятие и приведите примеры манипулирования в различных областях социального взаимодействия.
19. Какие способы манипулирования в массовых информационных процессах, в ходе обсуждений и дискуссий, вмежличностном общении.
20. Дайте характеристику основным направлениям обеспечения информационно-психологической безопасности личности.

Десятый семестр (Зачет, УК-3.3, ПК-14.2)

1. Укажите возможности применения информационных воздействий деструктивного арактера для нанесения ущерба личности, обществу и государству.
2. Определите понятие и опишите структуру информационно-психологической езопасности.
3. Приведите примеры влияния информационной сферы на жизнь современного бщества.
4. Приведите примеры из реальности, как слухи и провокации используются как способы нформационно-психологического воздействия.
5. Приведите пример информационной войны в новейшей истории.
6. Перечислите технологий информационного воздействия и подробно раскройте одержание одной из них (на выбор).

7. Опишите виды мошенничества в социальных сетях и укажите меры защиты от него.

8. Как используют глобальную сеть Интернет для реализации информационных оздействий деструктивного характера?

9. Как влияют моральные нормы на интернет-отношения? Приведите примеры.

10. Приведите пример формирования имиджа (положительного/отрицательного) тдельной личности или некоторого явления посредством целенаправленной оммуникационной политики.

11. Дайте понятие цифровой гигиены. Как Вы планируете ее соблюдать?

12. Проведите анализ правовых норм работы в виртуальном пространстве.

13. Как, на Ваш взгляд, интернет и телевидение влияют на нравственность российского бщества? Ответ аргументируйте.

14. Проведите обзор технологий управления личностью, применяемые в эталитарныхсектах и деструктивных культах. Приведите примеры.

15. Как Вы соблюдаете сетевой интернет? Приведите примеры.

16. Как оградить себя от буллинга в социальных сетях?

17. Дайте рекомендации для человека старшего поколения по правилам ведения елефонных разговоров.

18. Перечислите методы и способы защиты от несанкционированного использования нформационных ресурсов.

19. Приведите примеры организации информационных операций в сети Интернет.

20. Оцените модель «окна Овертона» как угрозу современному обществу.

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. Полякова, Т. А. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс] : учеб. и практикум для СПО / отв. ред. Т. А. Полякова, А. А. Стрельцов. - Москва : Юрайт, 2017. Режим доступа: по подписке. – URL: https://urait.ru/book/organizacionnoe-i-pravovoe-obespechenie-informacionnoy-bezopasnosti-414389 – Текст : электронный.

2. Моргунов, А. В. ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2019. – 83 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=576726 (дата обращения: 16.10.2021). – Библиогр.: с. 64. – ISBN 978-5-7782-3918-0. – Текст : электронный

3. 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. – URL: https://biblioclub.ru/index.php?page=book&id=493175 (дата обращения: 16.10.2021). – Библиогр. в кн. – ISBN 978-5-9275-2364-1. – Текст : электронный.

4. 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. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=234794 (дата обращения: 16.10.2021). – 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. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=429032 (дата обращения: 16.10.2021). – 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. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=428612 (дата обращения: 16.10.2021). – 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.