МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (ОЦЕНОЧНЫЕ СРЕДСТВА)

Шифр	Наименование дисциплины (модуля)
Б1.В	**Организационно-правовое обеспечение информационной безопасности образовательной организации**

Код направления подготовки	44.04.04
Направление подготовки	Профессиональное обучение (по отраслям)
Наименование (я) ОПОП (направленность / профиль)	Управление информационной безопасностью в профессиональном образовании
Уровень образования	магистр
Форма обучения	очная

Разработчики:

Должность	Учёная степень, звание	Подпись	ФИО
Старший преподаватель	кандидат педагогических наук		Гафарова Елена Аркадьевна

Рабочая программа рассмотрена и одобрена (обновлена) на заседании кафедры (структурного подразделения)

Кафедра	Заведующий кафедрой	Номер протокола	Дата протокола	Подпись
транспорта, информационных технологий и методики обучения техническим дисциплинам	Руднев Валерий Валентинович	10	13.06.2019	
транспорта, информационных технологий и методики обучения техническим дисциплинам	Руднев Валерий Валентинович	1	13.09.2020	

Раздел 1. Компетенции обучающегося, формируемые в результате освоения образовательной программы с указанием этапов их формирования

Таблица 1 - Перечень компетенций, с указанием образовательных результатов в процессе освоения дисциплины (в соответствии с РПД)

Формируемые компетенции			
Индикаторы ее достижения	**Планируемые образовательные результаты по дисциплине**		
	знать	**уметь**	**владеть**
ПК-16 способен применять инженерно-технические и программно-аппаратные средства обеспечения информационной безопасности			
ПК.16.1 Знает научные тенденции отечественных и зарубежных исследований перспективных технологий применения инженерно-технических и программно-аппаратных средств обеспечения информационной безопасности в практике ВО, современного профессионального образования, ДПО и ДПП	З.1 основные принципы и подходы при организации защиты ифнормации		
ПК.16.2 Умеет применять перспективные технологические разработки инженерно-технических и программно-аппаратных средств обеспечения информационной безопасности в практике ВО, современного профессионального образования, ДПО и ДПП		У.1 ппримен‍ять основыне нормативно-правоые акты в области ИБ	
ПК.16.3 Владеет научными основами практики применения перспективных технологические разработки инженер-но-технических и программно-аппаратных средств обеспечения информационной безопасности в практике ВО, сов-ременного профессионального образования, ДПО и ДПП			В.1 владеет опытом применения нормативно-правовых актов в области ИБ
УК-5 способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия			
УК.5.1 Знает особенности непосредственной и опосредованной коммуникации с представителями различных культур и социальных групп (субкультур); основы обеспечения различных типов коммуникации с учетом личностных, национально-этнических, конфессиональных и иных особенностей участников коммуникации; правила межкультурной коммуникации	З.2 инженерно-технические и программно-аппаратные средства обеспечение ИБ		

УК.5.2 Умеет грамотно, доступно излагать профессиональную информацию в процессе межкультурного взаимодействия; соблюдать этические нормы и права человека; анализировать особенности социального взаимодействия с учетом личностных, национально-этнических, конфессиональных и иных особенностей участников коммуникации; выявлять барьеры в межкультурном взаимодействии, находить способы их преодоления или устранения		У.2 умение аргументртировать свою позицию по организации защиты информации	
УК.5.3 Владеет навыками подготовки и преобразования информации, выбора форм и средств ее представления для обеспечения взаимопонимания в процессе межкультурного взаимодействия; навыками активного слушания, наблюдения и интерпретации поведения представителей разных культур и социальных групп; навыками выбора адекватной коммуникативной стратегии в зависимости от культурного контекста коммуникации и поставленных целей			В.2 опыт подготовки обзора и анализа номративно-правоых документво в области ИБ

Компетенции связаны с дисциплинами и практиками через матрицу компетенций согласно таблице 2.

Таблица 2 - Компетенции, формируемые в результате обучения

Код и наименование компетенции	
Составляющая учебного плана (дисциплины, практики, участвующие в формировании компетенции)	**Вес дисциплины в формировании компетенции (100 / количество дисциплин, практик)**
ПК-16 способен применять инженерно-технические и программно-аппаратные средства обеспечения информационной безопасности	
Программно-аппаратное обеспечение информационной безопасности	33,33
Организационно-правовое обеспечение информационной безопасности образовательной организации	**33,33**
Цифровизация и квалиметрическая оценка учебных достижений в образовательной организации	33,33
УК-5 способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	
производственная практика (педагогическая)	20,00
Иностранный язык в профессиональной коммуникации	20,00
Организационно-правовое обеспечение информационной безопасности образовательной организации	**20,00**
Русский язык в сфере профессиональной деятельности	20,00
Технологии свободно распространяемого программного обеспечения	20,00

Таблица 3 - Этапы формирования компетенций в процессе освоения ОПОП

Код компетенции	Этап базовой подготовки	Этап расширения и углубления подготовки	Этап профессионально-практической подготовки
ПК-16	**Программно-аппаратное обеспечение информационной безопасности, Организационно-правовое обеспечение информационной безопасности образовательной организации, Цифровизация и квалиметрическая оценка учебных достижений в образовательной организации**		
УК-5	**производственная практика (педагогическая), Иностранный язык в профессиональной коммуникации, Организационно-правовое обеспечение информационной безопасности образовательной организации, Русский язык в сфере профессиональной деятельности, Технологии свободно распространяемого программного обеспечения**		производственная практика (педагогическая)

Раздел 2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Таблица 4 - Показатели оценивания компетенций на различных этапах их формирования в процессе освоения учебной дисциплины (в соответствии с РПД)

№	Раздел	
	Формируемые компетенции	
	Показатели сформированности (в терминах «знать», «уметь», «владеть»)	**Виды оценочных средств**
1	Информационная безопасность и ее обеспечение	
	ПК-16	
	Знать основные принципы и подходы при организации защиты ифнормации	Тест
	Уметь ппримен‌ять основыне нормативно-правоые акты в области ИБ	Опрос
2	Правовое обеспечение информационной безопасности	
	ПК-16	
	Владеть владеет опытом применения нормативно-правовых актов в области ИБ	Проект
3	Организационное обеспечение информационной безопасности.	
	УК-5	
	Знать инженерно-технические и программно-аппаратные средства обеспечение ИБ	Тест
4	Концепция информационной безопасности организации профессионального образования	
	УК-5	
	Уметь умение аргуменртировать свою позицию по организации защиты информации	Кейс-задачи
5	Построение частной модели угроз безопасности персональных данных при их обработке в информационной системе	
	УК-5	
	Владеть опыт подготовки обзора и анализа номративно-правоых документво в области ИБ	Проект

Таблица 5 - Описание уровней и критериев оценивания компетенций, описание шкал оценивания

Код	**Содержание компетенции**			
Уровни освоения компетенции	**Содержательное описание уровня**	**Основные признаки выделения уровня (критерии оценки сформированности)**	**Пятибалльная шкала (академическая оценка)**	**% освоения (рейтинговая оценка)**
ПК-16	ПК-16 способен применять инженерно-технические и программно-аппаратные средства обеспечения информационной безопасности			
УК-5	УК-5 способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия			

Раздел 3. Типовые контрольные задания и (или) иные материалы, необходимые для оценки планируемых результатов обучения по дисциплине (модулю)

1. Оценочные средства для текущего контроля

Раздел: Информационная безопасность и ее обеспечение

Задания для оценки знаний

1. Тест:

1. К каким мерам защиты относится политика безопасности?
а) к административным;
б) к законодательным;
в) к программно-техническим;
г) к процедурным.

2. В каком из представлений матрицы доступа наиболее просто определить пользователей, имеющих доступ к определенному файлу?
а) CL;
б) списки полномочий субъектов;
в) атрибутные схемы.

3. Как называется свойство информации, означающее отсутствие неправомочных, и не предусмотренных ее владельцем изменений?
а) целостность;
б) апеллируемость;
в) доступность;
г) конфиденциальность;
д) аутентичность.

4. К основным принципам построения системы защиты АИС относятся:
а) открытость;
б) взаимозаменяемость подсистем защиты;
в) минимизация привилегий;
г) комплексность;

5. Диспетчер доступа...
а) ... использует базу данных защиты, в которой хранятся правила разграничения доступа;
б) ... использует атрибутные схемы для представления матрицы доступа;
в) ... выступает посредником при всех обращениях субъектов к объектам;
г) ... фиксирует информацию о попытках доступа в системном журнале;

6. Какие предположения включает неформальная модель нарушителя?
а) о возможностях нарушителя;
б) о категориях лиц, к которым может принадлежать нарушитель;
в) о привычках нарушителя;
г) о предыдущих атаках, осуществленных нарушителем;
д) об уровне знаний нарушителя.

Задания для оценки умений

1. Опрос:

1. Каковы основные разделы правовых документов в СПС «КонсультантПлюс»?
2. Что включается в иную официальную правовую информацию?
3. Перечислите основные инструменты поиска данной системы.
4. Как найти списки документов, регламентирующих конкретный правовой вопрос?
5. Из каких подразделов состоят разделы «Законодательство», «Судебная практика»?
6. В каком из разделов можно посмотреть тематические обзоры по проблемным правовым вопросам?
7. Как организована обратная связь с пользователями в данной системе?
8. Для чего применяется функция закладок в СПС «КонсультантПлюс»

Задания для оценки владений

Раздел: Правовое обеспечение информационной безопасности

Задания для оценки знаний

Задания для оценки умений

Задания для оценки владений

1. Проект:

Учебный проект: разработка концепции безопасности конкретного учреждения по приведенному развернутому плану-шаблону.
Концепция обеспечения информационной безопасности предприятия
Содержание
- Общие положения
- Описание объекта защиты
  - Назначение и основные функции информационной системы
  - Группы задач, решаемых в информационной системе
  - Классификация пользователей системы
  - Организационная структура обслуживающего персонала
  - Структура и состав комплекса программно-технических средств
  - Корпоративная сеть предприятия
    - Серверы
    - Рабочие станции
    - Линии связи и активное сетевое оборудование
    - Виды информационных ресурсов, хранимых и обрабатываемых в системе
    - Структура информационных потоков
    - Внутренние информационные потоки
    - Внешние информационные потоки
    - Характеристика каналов взаимодействия с другими системами и точек входа
- Основные факторы, влияющие на информационную безопасность предприятия
- Основные принципы обеспечения информационной безопасности
- Организация работ по защите информации
- Меры обеспечения информационной безопасности
  - Меры обеспечения информационной безопасности организационного уровня
  - Меры обеспечения информационной безопасности процедурного уровня
- Распределение ответственности и порядок взаимодействия
- Порядок категорирования защищаемой информации
- Модель нарушителя информационной безопасности
  - Внутренние нарушители
  - Внешние нарушители
- Модель угроз информационной безопасности
  - Защита информационных компонентов и группы угроз
  - Угрозы, реализуемые с использованием технических средств
  - Угрозы, реализуемые с использованием программных средств
  - Угрозы утечки информации по техническим каналам связи
- Требования по обеспечению информационной безопасности
  - Требования к составу основных подсистем СОИБ
  - Требования к подсистеме управления политикой безопасности
  - Требования к подсистеме анализа и управления рисками
  - Требования к подсистеме идентификации и аутентификации
  - Требования к подсистеме разграничения доступа
  - Требования к подсистеме протоколирования и пассивного аудита
  - Требования к подсистеме активного аудита безопасности
  - Требования к подсистеме контроля целостности
  - Требования к подсистеме контроля защищенности
  - Требования к подсистеме «удостоверяющий центр»
  - Требования к подсистеме сегментирования и межсетевого экранирования
  - Требования к подсистеме VPN

- Требования к подсистеме антивирусной защиты
- Требования к подсистеме фильтрации контента
- Требования к подсистеме управления безопасностью
- Требования к подсистеме предотвращения утечки информации по техническим каналам
- Технические требования к смежным подсистемам
- Требования к структурированной кабельной системе
- Требования по физической защите
- Ответственность сотрудников за нарушение безопасности
- Механизм реализации концепции

Раздел: Организационное обеспечение информационной безопасности.

Задания для оценки знаний

1. Тест:

1. К каким мерам защиты относится политика безопасности?
а) к административным;
б) к законодательным;
в) к программно-техническим;
г) к процедурным.

2. В каком из представлений матрицы доступа наиболее просто определить пользователей, имеющих доступ к определенному файлу?
а) ACL;
б) списки полномочий субъектов;
в) атрибутные схемы.

3. Как называется свойство информации, означающее отсутствие неправомочных, и не предусмотренных ее владельцем изменений?
а) целостность;
б) апеллируемость;
в) доступность;
г) конфиденциальность;
д) аутентичность.

4. К основным принципам построения системы защиты АИС относятся:
а) открытость;
б) взаимозаменяемость подсистем защиты;
в) минимизация привилегий;
г) комплексность;
д) простота.

5. Диспетчер доступа...
а) ... использует базу данных защиты, в которой хранятся правила разграничения доступа;
б) ... использует атрибутные схемы для представления матрицы доступа;
в) ... выступает посредником при всех обращениях субъектов к объектам;
г) ... фиксирует информацию о попытках доступа в системном журнале;

Задания для оценки умений

Задания для оценки владений

Раздел: Концепция информационной безопасности организации профессионального образования

Задания для оценки знаний

Задания для оценки умений

1. Кейс-задачи:

• Задача №7

Юрист Бурков , работая в адвокатской фирме «Норма» помощником генерального директора, в свободное от работы время несанкционированно получал доступ к чужим программам, базам данных и постоянно пользовался ими.

Информацию, полученную из них, Бурков часто использовал не по назначению, продавал ее своим клиентам. При этом из-за несанкционированного проникновения помощника генерального директора в названные программы и базы данных в них стали появляться сбои. Впоследствии собственники информационных ресурсов установили причины сбоев и потребовали строгого наказания Буркова .

Дайте правовую оценку действиям Буркова.

• Задача №8

Химический завод г.Д. осуществил выброс ядовитых веществ в реку N. Городские власти, получив от санэпидемслужбы города соответствующую информацию, не оповестили граждан об опасности. В результате купания в реке дети — пять мальчиков и одна девочка — получили серьезные кожные заболевания.

Оцените ситуацию. Кто должен нести ответственность за сокрытие данной информации?

• Задача №9

Желая помочь своим коллегам, программист Сальников и адвокат Сабуров — работники нотариальной конторы «ОКС» — внесли изменения в программу «Акты и документы о недвижимости». В результате этих действий была уничтожена информация, касающаяся опыта работы конторы в области регистрации объектов недвижимости за последний год и нарушена работа ПЭВМ.

Руководитель нотариальной конторы обратился к прокурору с заявлением о возбуждении уголовного дела против Сальникова и Сабурова.

Есть ли в действиях Сальникова и Сабурова состав преступления?

• Задача №10

Инженер Смыслов был приглашен на работу в акционерное общество «Оптрон» для организации выпуска нового вида продукции. В процессе работы Смыслов обратил внимание на то, что сведения о переходе предприятия на выпуск новых изделий и их характеристики известны многим работникам и никаких мер по защите этой информации руководство общества не принимает. Смыслов поделился своими сомнениями с бывшим работником «Оптрона» Недремовым.

Вскоре акционерное общество «Кулон», где работал Недремов, освоило производство указанных выше новых изделий, тем самым опередив по всем параметрам предприятие «Оптрон». Руководство «Оптрона» обвинило Смыслова в разглашении коммерческой тайны и пожаловалось на него в прокуратуру города.

Можно ли вменить Смыслову разглашение коммерческой тайны?

• Задача №11

По заявлению истца компании «Запад» о выдаче исполнительного листа на принудительное исполнение решения к ответчику акционерному обществу «Восток» арбитражным судом было вынесено решение о принудительном взыскании суммы основного долга и процентов за пользование денежными средствами с ответчика.

Однако в процессе совместной работы ответчик заключил договор на обслуживание своего расчетного счета с другим банком, реквизиты которого не сообщил партнеру по коммерческим соображениям, а отношения с банком, указанным в договоре с компанией «Запад», прекратил. Кредитор истца обратился с заявлением в арбитражный суд, в котором просил направить в адрес налоговой инспекции по месту нахождения ответчика информацию о расчетных счетах партнера по коммерческим отношениям.

В ответ на запрос арбитражного суда налоговая инспекция сообщила, что, исходя из учредительных документов акционерного общества «Восток», информация о нахождении и состоянии расчетных счетов ответчика является коммерческой тайной и поэтому она не может быть передана истцу.

Дайте информационно-правовую оценку действиям налоговой инспекции на запрос арбитражного суда.

Задания для оценки владений

Раздел: Построение частной модели угроз безопасности персональных данных при их обработке в информационной системе

Задания для оценки знаний

Задания для оценки умений

Задания для оценки владений

1. Проект:

Порядок выполнения работы

1. Изучить исходные условия существующей ИСПДн
2. Копировать шаблон частной модели угроз
3. Заполнить шаблон частной модели угроз по исходным условиям информационной систем обработки персональным данным.
4. Защитить свой проект частной модели угроз ИСПДн.

2. Оценочные средства для промежуточной аттестации

1. Зачет

Вопросы к зачету:

1. • Информация как объект правоотношений. Структура информационной сферы и характеристика ее элементов. В иды защищаемой информации по законодательству РФ.
2. • Защита интеллектуальных прав. Юридическая ответственность за нарушение авторских прав.
3. • Конституционные гарантии прав граждан в информационной сфере и механизм их реализации.
4. • Понятие информационной безопасности. Субъекты и объекты правоотношений в области информационной безопасности. Система нормативных правовых актов, регулирующих обеспечение информационной безопасности в РФ.
5. • Уровни ИБ: законодательный, административный, процедурный
6. • Правовые режимы конфиденциальной информации: особенности и содержание.
7. • Законодательный уровень ИБ в РФ: обзор основных правовых документов.
8. • Управление доступом. Объектно-ориентированный подход к управлению доступом. Матрица доступа. Программно-аппаратная реализация матрицы доступа.
9. • Административный уровень ИБ. Концепция и политика безопасности учреждения/предприятия.
10. • Основные понятия и критерии в классификации угроз.
11. • Стандарты и спецификации в области ИБ.
12. • Правовой режим защиты государственной тайны. Государственная тайна как особый вид защищаемой информации, и ее характерные признаки.
13. • Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну.
14. • Понятие конфиденциальной информации, основные виды конфиденциальной информации: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, тайна следствия и судопроизводства, профессиональная тайна.
15. • Юридическая ответственность за нарушения правовых режимов конфиденциальной информации - дисциплинарная, гражданско-правовая, административная, уголовная.
16. • Понятие лицензирования по законодательству РФ. Виды деятельности, подлежащие лицензированию.
17. • Правовые режимы конфиденциальной информации: особенности и содержание.
18. • Правовая регламентация лицензионной деятельности в области обеспечения ИБ.
19. • Правовая регламентация сертификационной деятельности в области обеспечения ИБ. Объекты сертификации. Органы сертификации и их полномочия.
20. • Законодательство РФ об интеллектуальных правах. Понятие и виды интеллектуальных прав.
21. • Преступления в сфере компьютерной информации: виды, состав. Основы расследования преступлений в сфере компьютерной информации. Иные преступления в информационной сфере.
22. • Сущность организационных методов защиты информации. Соотношение организационных методов защиты информации с правовыми и техническими.
23. • Понятие «режим защиты информации». Режим защиты информации как составная часть организационной защиты информации.
24. • Объекты обеспечения физической безопасности: сооружения, предметы, люди. Проектирование здания. Охрана территории. Охрана здания. Сигнализация. Противостояние взлому: двери, замки, запоры, ограждения.
25. • Идентификация и аутентификация. Парольная аутентификация, меры по усилению парольной аутентификации. Биометрическая идентификация и аутентификация, достоинства и недостатки.
26. • Протоколирование и аудит ИС. Активный аудит.
27. • Порядок доступа и допуска к государственной тайне. Основные принципы допускной работы. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления и утверждения.
28. • Технологическая схема обработки информации. Основные каналы утечки информации при обработке на компьютерах.
29. • Административный уровень ИБ. Концепция и политика безопасности учреждения/предприятия.
30. • Справочно-поисковые системы «Консультант» и «Гарант»: сфера применения, основные функции

31. • Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну.

32. • Контроль доступа, средства поиска и досмотра. Системы контроля доступа. Технологии считывания электронных ключей, электронных пропусков.

33. • Предварительная защита документов. Приборы и методы контроля документов. Хранилища. Сейфы. Запирающие устройства.

34. • Физическая защита неподвижных объектов. Пропускной режим.

35. • Проблема безопасности технологии. Организация работы персонала. Система инструкций и правил

36. • Правовая охрана баз данных, топологий интегральных схем и единых технологий.

37. • Защита интеллектуальных прав. Юридическая ответственность за нарушение авторских прав.

38. • Безопасность при транспортировке носителей информации. Личная безопасность сотрудников и членов их семей.

39. • Защита документов от подделок. Обнаружение фальсификации документов. Предварительная защита документов. Приборы и методы контроля документов. Хранилища. Сейфы. Запирающие устройства.

40. • Национальная доктрина информационной безопасности РФ

2. Экзамен

Вопросы к экзамену:

1. • Информация как объект правоотношений. Структура информационной сферы и характеристика ее элементов. В иды защищаемой информации по законодательству РФ.

2. • Защита интеллектуальных прав. Юридическая ответственность за нарушение авторских прав.

3. • Конституционные гарантии прав граждан в информационной сфере и механизм их реализации.

4. • Понятие информационной безопасности. Субъекты и объекты правоотношений в области информационной безопасности. Система нормативных правовых актов, регулирующих обеспечение информационной безопасности в РФ.

5. • Уровни ИБ: законодательный, административный, процедурный

6. • Правовые режимы конфиденциальной информации: особенности и содержание.

7. • Законодательный уровень ИБ в РФ: обзор основных правовых документов.

8. • Управление доступом. Объектно-ориентированный подход к управлению доступом. Матрица доступа. Программно-аппаратная реализация матрицы доступа.

9. • Административный уровень ИБ. Концепция и политика безопасности учреждения/предприятия.

10. • Основные понятия и критерии в классификации угроз.

11. • Стандарты и спецификации в области ИБ.

12. • Правовой режим защиты государственной тайны. Государственная тайна как особый вид защищаемой информации, и ее характерные признаки.

13. • Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну.

14. • Понятие конфиденциальной информации, основные виды конфиденциальной информации: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, тайна следствия и судопроизводства, профессиональная тайна.

15. • Юридическая ответственность за нарушения правовых режимов конфиденциальной информации - дисциплинарная, гражданско-правовая, административная, уголовная.

16. • Понятие лицензирования по законодательству РФ. Виды деятельности, подлежащие лицензированию.

17. • Правовые режимы конфиденциальной информации: особенности и содержание.

18. • Правовая регламентация лицензионной деятельности в области обеспечения ИБ.

19. • Правовая регламентация сертификационной деятельности в области обеспечения ИБ. Объекты сертификации. Органы сертификации и их полномочия.

20. • Законодательство РФ об интеллектуальных правах. Понятие и виды интеллектуальных прав.

21. • Преступления в сфере компьютерной информации: виды, состав. Основы расследования преступлений в сфере компьютерной информации. Иные преступления в информационной сфере.

22. • Сущность организационных методов защиты информации. Соотношение организационных методов защиты информации с правовыми и техническими.

23. • Понятие «режим защиты информации». Режим защиты информации как составная часть организационной защиты информации.

24. • Объекты обеспечения физической безопасности: сооружения, предметы, люди. Проектирование здания. Охрана территории. Охрана здания. Сигнализация. Противостояние взлому: двери, замки, запоры, ограждения.

25. • Идентификация и аутентификация. Парольная аутентификация, меры по усилению парольной аутентификации. Биометрическая идентификация и аутентификация, достоинства и недостатки.

26. • Протоколирование и аудит ИС. Активный аудит.

27. • Порядок доступа и допуска к государственной тайне. Основные принципы допускной работы. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления и утверждения.
28. • Технологическая схема обработки информации. Основные каналы утечки информации при обработке на компьютерах.
29. • Административный уровень ИБ. Концепция и политика безопасности учреждения/предприятия.
30. • Справочно-поисковые системы «Консультант» и «Гарант»: сфера применения, основные функции
31. • Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну.
32. • Контроль доступа, средства поиска и досмотра. Системы контроля доступа. Технологии считывания электронных ключей, электронных пропусков.
33. • Предварительная защита документов. Приборы и методы контроля документов. Хранилища. Сейфы. Запирающие устройства.
34. • Физическая защита неподвижных объектов. Пропускной режим.
35. • Проблема безопасности технологии. Организация работы персонала. Система инструкций и правил
36. • Правовая охрана баз данных, топологий интегральных схем и единых технологий.
37. • Защита интеллектуальных прав. Юридическая ответственность за нарушение авторских прав.
38. • Безопасность при транспортировке носителей информации. Личная безопасность сотрудников и членов их семей.
39. • Защита документов от подделок. Обнаружение фальсификации документов. Предварительная защита документов. Приборы и методы контроля документов. Хранилища. Сейфы. Запирающие устройства.
40. • Национальная доктрина информационной безопасности РФ

Раздел 4. Методические материалы, определяющие процедуры оценивания значни, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

1. Для текущего контроля используются следующие оценочные средства:

1. Кейс-задачи

Кейс – это описание конкретной ситуации, отражающей какую-либо практическую проблему, анализ и поиск решения которой позволяет развивать у обучающихся самостоятельность мышления, способность выслушивать и учитывать альтернативную точку зрения, а также аргументировано отстаивать собственную позицию.

Рекомендации по работе с кейсом:

1. Сначала необходимо прочитать всю имеющуюся информацию, чтобы составить целостное представление о ситуации; не следует сразу анализировать эту информацию, желательно лишь выделить в ней данные, показавшиеся важными.
2. Требуется охарактеризовать ситуацию, определить ее сущность и отметить второстепенные элементы, а также сформулировать основную проблему и проблемы, ей подчиненные. Важно оценить все факты, касающиеся основной проблемы (не все факты, изложенные в ситуации, могут быть прямо связаны с ней), и попытаться установить взаимосвязь между приведенными данными.
3. Следует сформулировать критерий для проверки правильности предложенного решения, попытаться найти альтернативные способы решения, если такие существуют, и определить вариант, наиболее удовлетворяющий выбранному критерию.
4. В заключении необходимо разработать перечень практических мероприятий по реализации предложенного решения.
5. Для презентации решения кейса необходимо визуализировать решение (в виде электронной презентации, изображения на доске и пр.), а также оформить письменный отчет по кейсу.

2. Опрос

Опрос представляет собой совокупность развернутых ответов студентов на вопросы, которые они заранее получают от преподавателя. Опрос может проводиться в устной и письменной форме.

Подготовка к опросу включает в себя:

- изучение конспектов лекций, раскрывающих материал, знание которого проверяется опросом;
- повторение учебного материала, полученного при подготовке к семинарским, практическим занятиям и во время их проведения;
- изучение дополнительной литературы, в которой конкретизируется содержание проверяемых знаний;
- составление в мысленной форме ответов на поставленные вопросы.

3. Проект

Проект – это самостоятельное, развёрнутое решение обучающимся, или группой обучающихся какой-либо проблемы научно-исследовательского, творческого или практического характера.

Этапы в создании проектов.

1. Выбор проблемы.
2. Постановка целей.
3. Постановка задач (подцелей).
4. Информационная подготовка.
5. Образование творческих групп (по желанию).
6. Внутригрупповая или индивидуальная работа.
7. Внутригрупповая дискуссия.
8. Общественная презентация – защита проекта.

4. Тест

Тест это система стандартизированных вопросов (заданий), позволяющих автоматизировать процедуру измерения уровня знаний и умений обучающихся. Тесты могут быть аудиторными и внеаудиторными. Преподаватель доводит до сведения студентов информацию о проведении теста, его форме, а также о разделе (теме) дисциплины, выносимой на тестирование.

При самостоятельной подготовке к тестированию студенту необходимо:

− проработать информационный материал по дисциплине. Проконсультироваться с преподавателем по вопросу выбора учебной литературы;

− выяснить все условия тестирования заранее. Необходимо знать, сколько тестов вам будет предложено, сколько времени отводится на тестирование, какова система оценки результатов и т.д.

− работая с тестами, внимательно и до конца прочесть вопрос и предлагаемые варианты ответов; выбрать правильные (их может быть несколько); на отдельном листке ответов выписать цифру вопроса и буквы, соответствующие правильным ответам. В случае компьютерного тестирования указать ответ в соответствующем поле (полях);

− в процессе решения желательно применять несколько подходов в решении задания. Это позволяет максимально гибко оперировать методами решения, находя каждый раз оптимальный вариант.

− решить в первую очередь задания, не вызывающие трудностей, к трудному вопросу вернуться в конце.

− оставить время для проверки ответов, чтобы избежать механических ошибок.

2. Описание процедуры промежуточной аттестации

Оценка за зачет/экзамен может быть выставлена по результатам текущего рейтинга. Текущий рейтинг – это результаты выполнения практических работ в ходе обучения, контрольных работ, выполнения заданий к лекциям (при наличии) и др. видов заданий.

Результаты текущего рейтинга доводятся до студентов до начала экзаменационной сессии.

Цель зачета − проверка и оценка уровня полученных студентом специальных знаний по учебной дисциплине и соответствующих им умений и навыков, а также умения логически мыслить, аргументировать избранную научную позицию, реагировать на дополнительные вопросы, ориентироваться в массиве информации.

Зачет может проводиться как в формате, аналогичном проведению экзамена, так и в других формах, основанных на выполнении индивидуального или группового задания, позволяющего осуществить контроль знаний и полученных навыков.

Подготовка к зачету начинается с первого занятия по дисциплине, на котором обучающиеся получают предварительный перечень вопросов к зачёту и список рекомендуемой литературы, их ставят в известность относительно критериев выставления зачёта и специфике текущей и итоговой аттестации. С самого начала желательно планомерно осваивать материал, руководствуясь перечнем вопросов к зачету и списком рекомендуемой литературы, а также путём самостоятельного конспектирования материалов занятий и результатов самостоятельного изучения учебных вопросов.

По результатам сдачи зачета выставляется оценка «зачтено» или «не зачтено».

Экзамен преследует цель оценить работу обучающегося за определенный курс: полученные теоретические знания, их прочность, развитие логического и творческого мышления, приобретение навыков самостоятельной работы, умения анализировать и синтезировать полученные знания и применять их для решения практических задач.

Экзамен проводится в устной или письменной форме по билетам, утвержденным заведующим кафедрой (или в форме компьютерного тестирования). Экзаменационный билет включает в себя два вопроса и задачи. Формулировка вопросов совпадает с формулировкой перечня вопросов, доведенного до сведения обучающихся не позднее чем за один месяц до экзаменационной сессии.

В процессе подготовки к экзамену организована предэкзаменационная консультация для всех учебных групп.

При любой форме проведения экзаменов по билетам экзаменатору предоставляется право задавать студентам дополнительные вопросы, задачи и примеры по программе данной дисциплины. Дополнительные вопросы также, как и основные вопросы билета, требуют развернутого ответа.