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
Защита персональных данных

Направление подготовки: 44.03.05 Педагогическое образование (с двумя профилями подготовки)
Профиль подготовки: Менеджмент в образовании. Информационная безопасность в образовании
Форма обучения: Очная

Разработчики:
Голяев С.С., доцент кафедры информатики и вычислительной техники

Программа рассмотрена и утверждена на заседании кафедры, протокол № 9 от 17.03.2022 года

Зав. кафедрой_____Зубрилин А. А.

1. Цель и задачи изучения дисциплины

Цель изучения дисциплины - овладение студентами знаниями организации защиты персональных данных, а также технологий построения системы защиты информационных систем персональных данных в образовании. Реализовывать нормы материального и процессуального права в профессиональной деятельности с использованием ИТ.

Задачи дисциплины:

- изучение модели угроз в информационной системе персональных данных (ИСПДн);
- организация модели безопасности персональных данных в образовательных учреждениях;
- подбор и работа с кадрами в сфере защиты персональных данных;
- организация и обеспечение режима секретности;
- аттестация ИСПДн;

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.08.ДВ.02.02 «Защита персональных данных» относится к дисциплинам по выбору обязательной части учебного плана.

Изучению дисциплины «Защита персональных данных» предшествует освоение дисциплин (практик):

Основы информационной безопасности;

Безопасность информационных систем и баз данных;

Криптографические методы защиты информации;

Область профессиональной деятельности,на которую ориентирует дисциплина «Защита персональных данных», 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-1. Способен осваивать и использовать теоретические знания и практические умения и навыки в предметной области при решении профессиональных задач.	
ПК-1.1. Знает структуру, состав и дидактические единицы предметной области (преподаваемого предмета).	
ПК-1.1. Знает структуру, состав и дидактические единицы предметной области (преподаваемого предмета).	знать: - базовые понятия и определения, используемые в защите персональных данных; - Принципы и методы организации защиты персональных данных; уметь: - использовать нормативно-правовую базу и информационные ресурсы в организации защиты персональных данных; - разрабатывать документацию по защите персональных данных в образовательных организациях; владеть: - навыками применения различного инструментария при решении задач по защите персональных данных; - разработки и реализации методов защиты персональных данных.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Девятый семестр
Контактная работа (всего)	**34**	**34**
Лекции	**12**	**12**
Практические	**22**	**22**
Самостоятельная работа (всего)	**38**	**38**
Виды промежуточной аттестации		
зачет	+	+
Общая трудоемкость часы	**72**	**72**
Общая трудоемкость зачетные единицы	**2**	**2**

5. Содержание дисциплины

5.1. **Содержание разделов дисциплины**

Раздел 1. Основы теории защиты информации. Проблемы защиты информации.

Основные требования к информационной безопасности. Понятие угрозы безопасности информации и общие подходы к ее классификации. Классификация угроз безопасности информации по способам их возможного негативного воздействия. Принципы обеспечения условий безопасной жизнедеятельности. Нарушители безопасности информации. Происхождение угроз безопасности информации. Предпосылки появления угроз Понятие информационной безопасности. Важность и сложность проблемы информационной безопасности. Сервисные службы защиты. Нарушения. Принципы безопасности и целостности данных информационных систем и технологий обработки персональных данных.

Раздел 2. Правовые основы защиты персональных данных. Правовые документы основных органов, регулирующие процесс обработки персональных данных. Требование к документации образовательных организаций по защите персональных данных.

Правовые основы обеспечения условий безопасной жизнедеятельности. Изучение ФЗ № 152-ФЗ «О персональных данных». Система обеспечения информационной безопасности Российской Федерации. Государственная информационная политика. Государственная система защиты информации, состав, структура и функции. Функции и задачи органов исполнительной власти, уполномоченных в области ИБ (ФСО, ФСБ, ФСТЭК, Роскомнадзор).

Правовые документы обеспечения условий безопасной жизнедеятельности. Правовое обеспечение ЗИ. Основные правовые документы. Принципы, методы и способы правового регулирования защиты информации. Работа в программе Гарант. Поиск правовых документов в программе Гарант. Основные требования к правовым документам информационной безопасности.

Правовая документация обеспечения условий безопасной жизнедеятельности предприятия. Требования к правовым документам информационной безопасности. Порядок работы с персональными данными работника.

5.2 Содержание дисциплины: Лекции (12 ч.)

Раздел 1. Основы теории защиты информации. Проблемы защиты информации. (6 ч.)

Тема1. Проблемы защиты информации.(1 ч.)

Основные требования к информационной безопасности. Понятие угрозы безопасности информации и общие подходы к ее классификации. Классификация угроз безопасности информации по способам их возможного негативного воздействия. Принципы обеспечения условий безопасной жизнедеятельности. Нарушители безопасности информации. Происхождение угроз безопасности информации. Предпосылки появления угроз Понятие информационной безопасности. Важность и сложность проблемы информационной безопасности. Сервисные службы защиты. Нарушения. Принципы безопасности и целостности данных информационных систем и технологий обработки персональных данных.

Тема 2. Основы теории защиты информации. (1 ч.)

Основы теории защиты информации и требования к информационной безопасности. Сущность теории защиты информации, ее основные составляющие и задачи обеспечения условий безопасной жизнедеятельности. Моделирование процессов защиты информации. Стратегии защиты информации, безопасность и целостность данных информационных систем и технологий обработки персональных данных.

Тема 3. Роль стандартов и спецификаций в обеспечении информационной безопасности. (2 ч.)

Основные требования к информационной безопасности. Стандарты и спецификации в области информационной безопасности и их классификация. Общие сведения о стандартах и спецификациях в области информационной безопасности. «Оранжевая книга». Гармонизированные критерии Европейских стран. Руководящие документы (РД) Гостехкомиссии России. X.800 «Архитектура безопасности для взаимодействия открытых систем». Спецификация Internet-сообщества RFC 1510 «Сетевой сервис аутентификации Kerberos (V5)». FIPS 140-2 «Требования безопасности для криптографических модулей». «Обобщенный прикладной программный интерфейс службы безопасности». Технические спецификации IPsec [IPsec]. TLS. X.500 «Служба директорий: обзор концепций, моделей и сервисов». Рекомендация Internet-сообщества «Руководство по информационной безопасности предприятия». Рекомендация «Как выбирать поставщика».

Тема 4. Угрозы и методология оценки уязвимости информации. (2 ч.)

Методы обеспечения условий безопасной жизнедеятельности. Определение и содержание понятия угрозы информации в современных системах ее обработки. Возможные подходы к формированию множества угроз информации. Безопасность и целостность данных информационных систем и технологий. Цели и задачи оценки угроз информации. Классификация и содержание угроз информации. Методы и модели оценки уязвимости информации.

Раздел 2. Правовые основы защиты персональных данных. Правовые документы основных органов, регулирующие процесс обработки персональных данных. Требование к документации образовательных организаций по защите персональных данных. (6 ч.)

Тема 1. Правовые основы защиты персональных данных. (1 ч.)

Правовые основы обеспечения условий безопасной жизнедеятельности. Изучение ФЗ № 152-ФЗ «О персональных данных». Система обеспечения информационной безопасности Российской Федерации. Государственная информационная политика. Государственная система защиты информации, состав, структура и функции. Функции и задачи органов исполнительной власти, уполномоченных в области ИБ (ФСО, ФСБ, ФСТЭК, Роскомнадзор).

Тема 2. Правовые документы основных органов, регулирующие процесс обработки персональных данных. (1 ч.)

Правовые документы обеспечения условий безопасной жизнедеятельности. Правовое обеспечение ЗИ. Основные правовые документы. Принципы, методы и способы правового регулирования защиты информации. Работа в программе Гарант. Поиск правовых документов в программе Гарант. Основные требования к правовым документам информационной безопасности.

Тема 3. Требование к документации предприятия по защите персональных данных. (1 ч.)

Правовая документация обеспечения условий безопасной жизнедеятельности предприятия. Требования к правовым документам информационной безопасности. Порядок работы с персональными данными работника.

Тема 4. Требование к документации юридических лиц по защите персональных данных. (1 ч.)

Требования к документации обеспечения условий безопасной жизнедеятельности по защите персональных данных. Планирование мероприятий по защите персональных данных. Изучение методов обезличивания персональных данных. Требования к правовым документам информационной безопасности.

Тема 5. Требования к документации по обработке персональных данных работников. (2 ч.)

Требования к документации обеспечения условий безопасной жизнедеятельности по защите персональных данных. Изучение ФЗ № 149-ФЗ «Об информации, информационных технологиях и о защите информации» Изучение функций и задач органов исполнительной власти, уполномоченных в области ИБ. Требования к правовым документам информационной безопасности.

5.3 Содержание дисциплины: Практические занятия (22 ч.)

Раздел 1. Основы теории защиты информации. Проблемы защиты информации. (10 ч.)

Тема1. Проблемы защиты информации.(2 ч.)

Основные требования к информационной безопасности. Понятие угрозы безопасности информации и общие подходы к ее классификации. Классификация угроз безопасности информации по способам их возможного негативного воздействия. Принципы обеспечения условий безопасной жизнедеятельности. Нарушители безопасности информации. Происхождение угроз безопасности информации. Предпосылки появления угроз Понятие информационной безопасности. Важность и сложность проблемы информационной безопасности. Сервисные службы защиты. Нарушения. Принципы безопасности и целостности данных информационных систем и технологий обработки персональных данных.

Тема 2. Основы теории защиты информации. (2 ч.)

Основы теории защиты информации и требования к информационной безопасности. Сущность теории защиты информации, ее основные составляющие и задачи обеспечения условий безопасной жизнедеятельности. Моделирование процессов защиты информации. Стратегии защиты информации, безопасность и целостность данных информационных систем и технологий обработки персональных данных.

Тема 3. Роль стандартов и спецификаций в обеспечении информационной безопасности. (2 ч.)

Основные требования к информационной безопасности. Стандарты и спецификации в области информационной безопасности и их классификация. Общие сведения о стандартах и спецификациях в области информационной безопасности. «Оранжевая книга». Гармонизированные критерии Европейских стран. Руководящие документы (РД) Гостехкомиссии России. X.800 «Архитектура безопасности для взаимодействия открытых систем». Спецификация Internet-сообщества RFC 1510 «Сетевой сервис аутентификации Kerberos (V5)». FIPS 140-2 «Требования безопасности для криптографических модулей». «Обобщенный прикладной программный интерфейс службы безопасности». Технические спецификации IPsec [IPsec]. TLS. X.500 «Служба директорий: обзор концепций, моделей и сервисов». Рекомендация Internet-сообщества «Руководство по информационной безопасности предприятия». Рекомендация «Как выбирать поставщика».

Тема 4. Угрозы и методология оценки уязвимости информации. (4 ч.)

Методы обеспечения условий безопасной жизнедеятельности. Определение и содержание понятия угрозы информации в современных системах ее обработки. Возможные подходы к формированию множества угроз информации. Безопасность и целостность данных информационных систем и технологий. Цели и задачи оценки угроз информации. Классификация и содержание угроз информации. Методы и модели оценки уязвимости информации.

Раздел 2. Правовые основы защиты персональных данных. Правовые документы основных органов, регулирующие процесс обработки персональных данных. Требование к документации образовательных организаций по защите персональных данных. (12 ч.)

Тема 1. Правовые основы защиты персональных данных. (2 ч.)

Правовые основы обеспечения условий безопасной жизнедеятельности. Изучение ФЗ № 152-ФЗ «О персональных данных». Система обеспечения информационной безопасности

Российской Федерации. Государственная информационная политика. Государственная система защиты информации, состав, структура и функции. Функции и задачи органов исполнительной власти, уполномоченных в области ИБ (ФСО, ФСБ, ФСТЭК, Роскомнадзор).

Тема 2. Правовые документы основных органов, регулирующие процесс обработки персональных данных. (2 ч.)

Правовые документы обеспечения условий безопасной жизнедеятельности. Правовое обеспечение ЗИ. Основные правовые документы. Принципы, методы и способы правового регулирования защиты информации. Работа в программе Гарант. Поиск правовых документов в программе Гарант. Основные требования к правовым документам информационной безопасности.

Тема 3. Требование к документации предприятия по защите персональных данных. (2 ч.)

Правовая документация обеспечения условий безопасной жизнедеятельности предприятия. Требования к правовым документам информационной безопасности. Порядок работы с персональными данными работника.

Тема 4. Требование к документации юридических лиц по защите персональных данных. (2 ч.)

Требования к документации обеспечения условий безопасной жизнедеятельности по защите персональных данных. Планирование мероприятий по защите персональных данных. Изучение методов обезличивания персональных данных. Требования к правовым документам информационной безопасности.

Тема 5. Требования к документации по обработке персональных данных работников. (4 ч.)

Требования к документации обеспечения условий безопасной жизнедеятельности по защите персональных данных. Изучение ФЗ № 149-ФЗ «Об информации, информационных технологиях и о защите информации» Изучение функций и задач органов исполнительной власти, уполномоченных в области ИБ. Требования к правовым документам информационной безопасности.

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

6.1 Вопросы и задания для самостоятельной работы

Девятый семестр семестр (38 ч.)

Раздел 1. Основы теории защиты информации. Проблемы защиты информации. (20 ч.)

Вид СРС: *Подготовка к практическим занятиям Перечень контрольных вопросов по модулю " Основы теории защиты информации. Проблемы защиты информации."

1. Случайные угрозы информации в КС.
2. Преднамеренные угрозы информации в КС.
3. Назначение и функции аппаратных устройств защиты ПЭВМ.
4. Идентификация и аутентификация пользователей.
5. Разграничение доступа к информации и компонентам ее обработки.
6. Организационно-распорядительные документы по защите персональных данных.
7. Защита ИСПДн при межсетевом экранировании.
8. Защита ПДн криптографическими методами и средствами.
9. Защита информации в КС от случайных угроз.
10. Защита информации в КС от преднамеренных угроз.
11. Физическая защита ПЭВМ от НСД.
12. Способы криптографического закрытия информации на ВЗУ и в процессе обработки.
13. Подсистема аудита.
14. Обеспечение защиты информации средствами VPN.
15. Системы анализа защищенности.
16. Системы обнаружения атак.
17. Организация аудита ресурсов и событий системы защиты.
18. Угрозы безопасности информации в компьютерных сетях.

19. Задачи и направления обеспечения информационной безопасности в сетях передачи данных.

Вид СРС: *Работа с электронными ресурсами и информационными системами

Пройти дистанционное обучение по указанному курсу.

Корнилова, А. А. Защита персональных данных : учебное пособие : [16+] / А. А. Корнилова, Д. С. Юнусова, А. С. Исмагилова ; Башкирский государственный университет. – Уфа : Башкирский государственный университет, 2020. – 119 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=611314. – Библиогр. в кн. – Текст : электронный.

Данное учебное пособие является введением в общий контекст защиты персональных данных как одной из задач информационной безопасности. Особое внимание уделено анализу нормативно-правового регулирования защиты, обработки персональных данных, выявлению структурных элементов, а также характеристике стратегий защиты персональных данных.

Вид СРС: *Подготовка к контрольной работе. С использованием информационно-справочной системы «Гарант» решите и обоснуйте решение следующих задач.

Задача 1. При проведении проверки первичной документации по учёту труда и его оплаты было обнаружено, что в личном деле одного из референтов федерального агентства отсутствуют сведения из налоговой службы об имущественном положении, а также данные дактилоскопической регистрации. Инспектор труда потребовал предъявить указанные документы.

Правомерны ли требования инспектора труда?

Задача 2. Семенов обратился в ОАО «Решение» с просьбой принять его на работу в качестве ведущего специалиста отдела продаж. Начальник кадровой службы направил запрос в психоневрологический диспансер по месту жительства Семенова, в котором просил сообщить сведения о состоянии психологического здоровья и о фактах обращения Семенова за психиатрической помощью, поскольку организации необходимо решить вопрос о пригодности Семенова для выполнения работы.

Законны ли действия начальника кадровой службы?

Задача 3. Начальник отдела кадров Дубовцева распространяла среди своих знакомых сведения об образовании и данные медицинского осмотра заведующего складом Мамонтова, которые, по её мнению, порочили его честь и достоинство. Мамонтов потребовал от директора организации защитить его персональные данные от неправомерного использования и привлечь Дубовцеву к административной ответственности. Директор оштрафовал Дубовцеву на сумму, равную трем минимальным размера оплаты труда.

Законно ли действие работодателя? Какие виды юридической ответственности установлены законодательством России за нарушение норм, регулирующих сбор, обработку, хранение, распространение и защиту персональных данных работника.

Задача 4. Работник Падерин, ознакомившись со своими персональными данными, хранящимися в организации, потребовал от директора ООО «Аквамарин» исключить устаревшие и исправить неверные, а также известить всех лиц, которым они ранее были сообщены, обо всех исправлениях или дополнениях. Директор не выполнил требования работника.

Правомерен ли отказ директора? Какие права по защите своих персональных данных, хранящихся у работодателя, закон предоставляет работнику?

Раздел 2. Правовые основы защиты персональных данных. Правовые документы основных органов, регулирующие процесс обработки персональных данных. Требование к документации образовательных организаций по защите персональных данных. (18 ч.)

Вид СРС: *Подготовка к практическим занятиям Перечень контрольных вопросов по модулю " Правовые основы защиты персональных данных. Правовые документы основных органов, регулирующие процесс обработки персональных данных. Требование к документации образовательных организаций по защите персональных данных."

1. Нормативная база обработки ПДн.
2. Принципы обработки ПДн.
3. Права субъекта персональных данных.
4. Требования ФСТЭК России по защите персональных данных.

5. Обязанности оператора ИСПДн.
6. Обеспечение безопасности ПДн при их обработке.
7. Классификация ПДн.
8. Организация работ по обработке персональных данных.
9. Базовая модель угроз безопасности ПДн.
10. Частная модель угроз безопасности ПДн.
11. Организационные меры защиты информации в КС.
12. Методы обнаружения известных и неизвестных вирусов.
13. Действия пользователя при обнаружении заражения КС вирусами.
14. Средства восстановления работоспособности КС.
15. Функции администратора по созданию и управлению учетными записями пользователей.
16. Классификация и применение межсетевых экранов.
17. Системы контроля содержания.
18. Схема работы электронной подписи.
19. Основные сведения об Инфраструктуре открытых ключей.
20. Хэш - функция и ее использование в системах цифровой подписи.
21. Состав и функции удостоверяющего центра.
22. Понятие симметричной и асимметричной криптографии. Приведите примеры.

Вид СРС: *Работа с электронными ресурсами и информационными системами

Пройти дистанционное обучение по указанному курсу.

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. – Текст : электронный.

В курсе рассматриваются основные термины в области информационной безопасности: уязвимость, атака, угроза, злоумышленник. Излагаются ключевые аспекты федеральных законов и других нормативно-методических документов в области обеспечения безопасности персональных данных: понятия оператора и субъекта персональных данных, их права и обязанности. Порядок классификации информационных систем персональных данных в зависимости от количества субъектов, данные которых обрабатываются, и категории персональных данных. Рассмотрены этапы построения системы защиты персональных данных и соответствующие им организационно-технические мероприятия. Порядок аттестации, сертификации и лицензирования в области обеспечения безопасности персональных данных.

Регуляторы и способы контроля за соблюдением требований законодательства.

Вид СРС: *Подготовка к контрольной работе. С использованием информационно-справочной системы «Гарант» решите и обоснуйте решение следующих задач.

Задача 1. Перевалов обратился в центр занятости по месту жительства в целях поиска подходящей работы. Инспектор центра занятости потребовал от гражданина предоставить сведения о последнем месте работы, о составе его семьи, его религиозных убеждениях и принадлежности к политическим партиям. Считая такие требования незаконными, Перевалов обратился с жалобой к руководителю центра занятости.

Законны ли требования инспектора. Какое решение по жалобе должен принять руководитель центра занятости?

Задача 2. 20.01.2015 менеджер проектов ООО «Ответ» Фалалеева сделала запрос о предоставлении персональных данных юриста ЗАО «Квадратный метр» Оленевой, в связи с осуществлением совместного проекта. Директор ЗАО «Квадратный метр» без согласования с Оленевой предоставил запрашиваемые данные.

Правомерны ли действия директора ЗАО? Какие требования установлены для передачи персональных данных работника?

Задача 3. В ОАО «Решение» было разработано и утверждено приказом директора Положение о порядке обработки и хранения персональных данных работников. Директор поручил своему заместителю ознакомить с положением всех работников под расписку.

Правомерно ли действие директора ОАО? Кто по законодательству имеет право вырабатывать меры защиты персональных данных работников, порядок их сбора, хранения и использования?

Задача 4. Администрация МУП г. Ижевска «Банно-прачечный комбинат» обратилась в органы ФСБ России с просьбой предоставить необходимые персональные данные на работника МУП Шатунова.

Законно ли обращение администрации? Какой порядок получения персональных данных работника установлен ТК РФ?

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
	Предметно-методический модуль "Информационная безопасность в образовании".	ПК-1, ПК-1.1

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-1 Способен осваивать и использовать теоретические знания и практические умения и навыки в предметной области при решении профессиональных задач			
ПК-1.1. Знает структуру, состав и дидактические единицы предметной области (преподаваемого предмета).			
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.

Уровень сформированности компетенции	Шкала оценивания для промежуточной аттестации	Шкала оценивания по БРС
	Экзамен (дифференцированный зачет)	
Повышенный	5 (отлично)	90 – 100%
Базовый	4 (хорошо)	76 – 89%
Пороговый	3 (удовлетворительно)	60 – 75%
Ниже порогового	2 (неудовлетворительно)	Ниже 60%

8.2.1 Вопросы промежуточной аттестации

Девятый семестр (Зачет, ПК-1, ПК-1.1)

1. Назовите случайные угрозы информации в КС.
2. Назовите преднамеренные угрозы информации в КС.
3. Охарактеризуйте назначение и функции аппаратных устройств защиты ПЭВМ.
4. Дайте понятие идентификации и аутентификации пользователей.
5. Охарактеризуйте процесс разграничения доступа к информации и компонентам ее обработки.
6. Приведите примеры оформления организационно-распорядительных документов по защите персональных данных.
7. Дайте понятие защиты ИСПДн при межсетевом экранировании.
8. Дайте понятие защиты ПДн криптографическими методами и средствами.
9. Дайте понятие защиты информации в КС от случайных угроз.
10. Дайте понятие защиты информации в КС от преднамеренных угроз.
11. Дайте понятие физической защиты ПЭВМ от НСД.
12. Охарактеризуйте способы криптографического закрытия информации на ВЗУ и в процессе обработки.
13. Дайте понятие подсистемы аудита.
14. Охарактеризуйте процесс обеспечения защиты информации средствами VPN.
15. Дайте понятие системы анализа защищенности.
16. Приведите примеры систем обнаружения атак.
17. Охарактеризуйте процесс организации аудита ресурсов и событий системы защиты.
18. Дайте понятие угрозы безопасности информации в компьютерных сетях.
19. Охарактеризуйте задачи и направления обеспечения информационной безопасности в сетях передачи данных.
20. Опишите нормативную базу обработки ПДн.
21. Охарактеризуйте принципы обработки ПДн.
22. Дайте понятие права субъекта персональных данных.
23. Расскажите о требованиях ФСТЭК России по защите персональных данных.
24. Расскажите об обязанностях оператора ИСПДн.
25. Охарактеризуйте процесс обеспечения безопасности ПДн при их обработке.
26. Приведите классификацию ПДн.
27. Охарактеризуйте процесс организации работ по обработке персональных данных.
28. Охарактеризуйте базовой модели угроз безопасности ПДн.
29. Охарактеризуйте частную модель угроз безопасности ПДн.
30. Приведите примеры организационных мер защиты информации в КС.
31. Назовите методы обнаружения известных и неизвестных вирусов.
32. Перечислите действия пользователя при обнаружении заражения КС вирусами.
33. Охарактеризуйте средства восстановления работоспособности КС.
34. Назовите функции администратора по созданию и управлению учетными записями пользователей.
35. Приведите виды классификации и применения межсетевых экранов.
36. Охарактеризуйте системы контроля содержания.
37. Опишите схему работы электронной подписи.
38. Расскажите об основных сведениях Инфраструктуры открытых ключей.
39. Дайте понятие Хэш - функции и ее использование в системах цифровой подписи.
40. Охарактеризуйте состав и функции удостоверяющего центра.
41. Дайте понятие симметричной и асимметричной криптографии. Приведите примеры.

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

Промежуточная аттестация проводится в форме зачета.

Зачет по дисциплине или ее части имеет цель оценить сформированность компетенций, теоретическую и практическую подготовку студента, его способность к творческому мышлению, приобретенные им навыки самостоятельной работы, умение синтезировать полученные знания и применять их при решении практических задач.

Устный ответ на зачете

При определении уровня достижений студентов на зачете необходимо обращать особое внимание на следующее:

– дан полный, развернутый ответ на поставленный вопрос;

– показана совокупность осознанных знаний об объекте, проявляющаяся в свободном оперировании понятиями, умении выделить существенные и несущественные его признаки, причинно-следственные связи;

– знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей;

– ответ формулируется в терминах науки, изложен грамотным литературным языком, логичен, доказателен, демонстрирует авторскую позицию студента;

– теоретические постулаты подтверждаются примерами из практики.

Вопросы и задания для устного опроса

При определении уровня достижений студентов при устном ответе необходимо обращать особое внимание на следующее:

– дан полный, развернутый ответ на поставленный вопрос;

– показана совокупность осознанных знаний об объекте, проявляющаяся в свободном оперировании понятиями, умении выделить существенные и несущественные его признаки, причинно-следственные связи;

– знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей;

– ответ формулируется в терминах науки, изложен литературным языком, логичен, доказателен, демонстрирует авторскую позицию студента;

– теоретические постулаты подтверждаются примерами из практики. Оценка за опрос определяется простым суммированием баллов:

Критерии оценки ответа

Правильность ответа – 1 балл.

Всесторонность и глубина (полнота) ответа – 1 балл.

Наличие выводов – 1 балл.

Соблюдение норм литературной речи – 1 балл. Владение профессиональной лексикой – 1 балл. Итого: 5 баллов.

Практические задания

При определении уровня достижений студентов при выполнении практического задания необходимо обращать особое внимание на следующее:

– задание выполнено правильно;

– показана совокупность осознанных знаний об объекте, проявляющаяся в свободном оперировании понятиями, умении выделить существенные и несущественные его признаки, причинно-следственные связи;

– умение работать с объектом задания демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей;

– ответ формулируется в терминах науки, изложен литературным языком, логичен, доказателен, демонстрирует авторскую позицию студента;

– выполнение задания теоретически обосновано.

Оценка за опрос определяется простым суммированием баллов:

Критерии оценки ответа

Правильность выполнения задания – 1 балл.

Всесторонность и глубина (полнота) выполнения – 1 балл.

Наличие выводов – 1 балл.

Соблюдение норм литературной речи – 1 балл. Владение профессиональной лексикой – 1 балл. Итого: 5 баллов.

Контрольная работа

Виды контрольных работ: аудиторные, домашние, текущие, экзаменационные, письменные, графические, практические, фронтальные, индивидуальные. Система заданий письменных контрольных работ должна:

– выявлять знания студентов по определенной дисциплине (разделу дисциплины);
– выявлять понимание сущности изучаемых предметов и явлений, их закономерностей;
– выявлять умение самостоятельно делать выводы и обобщения;
– творчески использовать знания и навыки.

Требования к контрольной работе по тематическому содержанию соответствуют устному ответу.

Также контрольные работы могут включать перечень практических заданий.

Критерии оценки ответа

Правильность ответа – 1 балл.

Всесторонность и глубина (полнота) ответа – 1 балл.

Наличие выводов – 1 балл.

Соблюдение норм литературной письменной речи – 1 балл. Владение профессиональной лексикой – 1 балл.

Итого: 5 баллов.

9. Перечень основной и дополнительной учебной литературы

Основная литература

1. Корнилова, А. А. Защита персональных данных : учебное пособие : [16+] / А. А. Корнилова, Д. С. Юнусова, А. С. Исмагилова ; Башкирский государственный университет. – Уфа : Башкирский государственный университет, 2020. – 119 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=611314. – Библиогр. в кн. – Текст : электронный.

2. 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. – Текст : электронный.

Дополнительная литература

1. Буянова, М. О. Трудовое право России : учебник / М. О. Буянова, О. Б. Зайцева ; под общ. ред. М. О. Буяновой. – Ростов-на-Дону : Феникс, 2017. – 572 с. – (Высшее образование). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=562838. – Библиогр.: с. 555-565. – ISBN 978-5-222-27709-6. – Текст : электронный.

2. Петренко, В. И. Защита персональных данных в информационных системах : учебное пособие / В. И. Петренко ; Северо-Кавказский федеральный университет. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2016. – 201 с. : схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=459205. – Текст : электронный.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1.https://www.garant.ru – Информационно-правовая система «Гарант [Электронный ресурс] / Режим доступа: https://www.garant.ru.

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

11. Методические указания обучающимся по освоению дисциплины (модуля)

При освоении материала дисциплины необходимо:

– спланировать и распределить время, необходимое для изучения дисциплины;
– конкретизировать для себя план изучения материала;
– ознакомиться с объемом и характером внеаудиторной самостоятельной работы для полноценного освоения каждой из тем дисциплины.

Сценарий изучения курса:
– проработайте каждую тему по предлагаемому ниже алгоритму действий;
– регулярно выполняйте задания для самостоятельной работы, своевременно отчитывайтесь преподавателю об их выполнении;
– изучив весь материал, проверьте свой уровень усвоения содержания дисциплины и готовность к сдаче зачета/экзамена, выполнив задания и ответив самостоятельно на примерные вопросы для промежуточной аттестации.

Алгоритм работы над каждой темой:
– изучите содержание темы вначале по лекционному материалу, а затем по другим источникам;
– прочитайте дополнительную литературу из списка, предложенного преподавателем;
– выпишите в тетрадь основные понятия и категории по теме, используя лекционный материал или словари, что поможет быстро повторить материал при подготовке к промежуточной аттестации;
– составьте краткий план ответа по каждому вопросу, выносимому на обсуждение на аудиторном занятии;
– повторите определения терминов, относящихся к теме;
– продумайте примеры и иллюстрации к обсуждению вопросов по изучаемой теме;
– подберите цитаты ученых, общественных деятелей, публицистов, уместные с точки зрения обсуждаемой проблемы;
– продумывайте высказывания по темам, предложенным к аудиторным занятиям.

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, что поможет при подготовке рефератов, текстов речей, при подготовке к промежуточной аттестации;
– выберите те источники, которые наиболее подходят для изучения конкретной темы;
– проработайте содержание источника, сформулируйте собственную точку зрения на проблему с опорой на полученную информацию.

12. Перечень информационных технологий

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

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

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

12.2 Перечень информационных справочных систем (обновление выполняется еженедельно)

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

12.3 Перечень современных профессиональных баз данных

1. Электронная библиотечная система Znanium. com (http://znanium.com/)
2. Единое окно доступа к образовательным ресурсам (http://window.edu.ru)

3. Профессиональная база данных «Открытые данные Министерства образования и науки РФ» (http://xn--- 8sblcdzzacvuc0jbg.xn--80abucjiibhv9a.xn--p1ai/ope

13. Материально-техническое обеспечение дисциплины(модуля)

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

Учебная аудитория для проведения учебных занятий.
Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.
Лаборатория вычислительной техники.
Помещение оснащено оборудованием и техническими средствами обучения.
Основное оборудование:
Автоматизированное рабочее место в составе (системный блок, монитор, клавиатура, мышь, гарнитура, проектор, интерактивная доска), магнитно-маркерная доска.
Лабораторное оборудование: автоматизированное рабочее место (компьютеры – 24 шт.).

Помещение для самостоятельной работы.
Помещение оснащено оборудованием и техническими средствами обучения.
Основное оборудование:
Компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду университета (персональный компьютер 10 шт.).
Учебно-наглядные пособия:
Презентации.

Помещение для самостоятельной работы.
Читальный зал.
Основное оборудование:
Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета (компьютер 10 шт., проектор с экраном 1 шт., многофункциональное устройство 1 шт., принтер 1 шт.)
Учебно-наглядные пособия:
Учебники и учебно-методические пособия, периодические издания, справочная литература.
Стенды с тематическими выставками.