Автономная некоммерческая организация высшего образования
«МОСКОВСКИЙ МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ»

Рабочая программа дисциплины

Информационная безопасность и защита персональных данных сотрудников

Направление подготовки	Управление персоналом
Код	38.03.03
Направленность (профиль)	Управление персоналом организации и государственной службы
Квалификация (степень) выпускника	бакалавр

Москва
2026

1. Перечень кодов компетенций, формируемых дисциплиной в процессе освоения образовательной программы

Группа компетенций	Категория компетенций	Код
Профессиональные		**ПК-7**

2. Компетенции и индикаторы их достижения

Код компетенции	Формулировка компетенции	Индикаторы достижения компетенции
ПК-7	Способен вести кадровое делопроизводство и организовывать архивное хранение кадровых документов в соответствии с действующими нормативно-правовыми актами, составлять кадровую отчетность, обеспечить защиту персональных данных сотрудников, оптимизировать оптимизации документооборот и схемы функциональных взаимосвязей между подразделениями	**ПК-7.1** ведет кадровое делопроизводство и организовывает архивное хранение кадровых документов в соответствии с действующими нормативно-правовыми актами **ПК-7.2** участвует в составлении кадровой отчетности, обеспечивает защиту персональных данных сотрудников, оптимизирует документооборот и схемы функциональных взаимосвязей между подразделениями **ПК-7.3** выполняет администрирование процессов и документооборота по вопросам обеспечения персоналом

3. Описание планируемых результатов обучения по дисциплине

3.1. Описание планируемых результатов обучения по дисциплине

Планируемые результаты обучения по дисциплине представлены дескрипторами (знания, умения, навыки).

Дескрипторы по дисциплине	Знать	Уметь	Владеть
Код компетенции	**ПК-7**		

	– функции документа, классификацию документов, современные требования к документационному обеспечению управления; – способы документирования; – основы разработки кадровой политики; – технологии управления развитием персонала (управление социальным развитием; организации обучения персонала; организации текущей деловой оценки, в т.ч. аттестации персонала; управления деловой карьерой и служебно-профессиональным продвижением персонала); – основы кадрового планирования в организации; – основные положения занятости и трудоустройства; – особенности организации и применения наемного труда; – особенности организационного проектирования систем управления персоналом; – этапы организационного проектирования;	– применять полученные знания в организациях; – выполнять ключевые технологические операции при работе с документами; – принимать участие в разработке корпоративных, конкурентных и функциональных стратегий развития организации в части управления персоналом; – прогнозировать и планировать потребность организации в персонале в соответствии со стратегическими планами организации и определять эффективные пути ее удовлетворения; – оперировать понятиями и категориями трудового законодательства; – толковать и правильно применять нормы трудового законодательства; – осуществлять анализ систем управления персоналом с помощью различных методов;	– основными методами и приемами исследовательской, аналитической и практической работы в области документационного обслуживания; – методами разработки и реализации стратегий управления персоналом; – методами планирования численности и профессионального состава персонала в соответствии со стратегическими планами организации; – современными технологиями управления персоналом организации (найма, отбора, приема и расстановки персонала; социализации, профориентации и трудовой адаптации персонала; организации труда персонала, высвобождения персонала); – навыками работы с

			нормативными правовыми актами; – навыками разрешения правовых проблем в сфере труда; – методами проаектирования систем управления; – технологией организационного проаектирования.

4. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Информационная безопасность и защита персональных данных сотрудников» относится к части, формируемой участниками образовательных отношений учебного плана ОПОП.

Данная дисциплина взаимосвязана с другими дисциплинами: «Организация кадровой службы и кадровый учет», «Противодействие коррупции в органах законодательной и исполнительной власти», «Кадровое обеспечение организации», «Основы кадровой политики и кадрового планирования».

В рамках освоения программы бакалавриата выпускники готовятся к решению задач профессиональной деятельности следующих типов: организационно-управленческой.

Профиль (направленность) программы установлена путем ее ориентации на сферу профессиональной деятельности выпускников: Управление персоналом организации и государственной службы.

5. Объем дисциплины

Виды учебной работы	***Формы обучения***	
	Очно-заочная	***Очно-заочная с применением ДОТ***
Общая трудоемкость: зачетные единицы/часы	3/108	3/108
Контактная работа:		
Занятия лекционного типа	12	2
Занятия семинарского типа	24	8
Промежуточная аттестация: **зачет**	0,1	0,1
Самостоятельная работа (СРС)	71,9	97,9

6. Содержание дисциплины (модуля), структурированное по темам / разделам с указанием отведенного на них количества академических часов и видов учебных занятий

6.1. Распределение часов по разделам/темам и видам работы

6.1.1 Очно-заочная форма обучения

№ п/п	Раздел/тема	Виды учебной работы (в часах)						
		Контактная работа						Самостоятельная работа
		Занятия лекционного типа		Занятия семинарского типа				
		Лекции	*Иные учебные занятия*	*Практические занятия*	*Семинары*	*Лабораторные работы*	*Иные*	
1	Введение в безопасность информационных систем.	4		6				14
2	Угрозы безопасности информационных систем и их реализация.	2		4				14
3	Защита персональных данных.	2		6				14
4	Криптографические системы защиты информации.	2		4				14
5	Программно-технические средства защиты информации.	2		4				15,9
	Промежуточная аттестация	**0,1**						
	Всего	**12**		**24**				**71,9**
	Итого	**108**						

6.1.1 Очно-заочная форма обучения с применением ДОТ

№ п/п	Раздел/тема	Виды учебной работы (в часах)						
		Контактная работа						Самостоятельная работа
		Занятия лекционного типа		Занятия семинарского типа				
		Лекции	*Иные учебные занятия*	*Практические занятия*	*Семинары*	*Лабораторные работы*	*Иные*	
1	Введение в безопасность информационных систем.	1		1				19
2	Угрозы безопасности информационных систем и их			1				21,9

	реализация.							
3	Защита персональных данных.	1		2				19
4	Криптографические системы защиты информации.			2				19
5	Программно-технические средства защиты информации.			2				19
	Промежуточная аттестация	**0,1**						
	Всего	**2**		**8**				**97,9**
	Итого	**108**						

6.1. Программа дисциплины, структурированная по темам / разделам

6.2.1. Содержание лекционного курса

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1.	Введение в безопасность информационных систем.	Понятие информационной безопасности и защищенной системы. Необходимость защиты информационных систем и телекоммуникаций. Технические предпосылки кризиса информационной безопасности. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Особенности сертификации и стандартизации криптографических услуг. Законодательная база информационной безопасности. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности. Роль стандартов информационной безопасности. Квалификационный анализ уровня безопасности.
2.	Угрозы безопасности информационных систем и их реализация.	Виды возможных нарушений информационной системы. Анализ угроз информационной безопасности. Классификация видов угроз информационной безопасности по различным признакам (по природе возникновения, степени преднамеренности и т.п.). Свойства информации: конфиденциальность, доступность, целостность.
3.	Защита персональных данных.	Правовые основы защиты персональных данных. Правовые документы основных органов, регулирующие процесс обработки персональных данных. Требование к документации предприятия по

		защите персональных данных. Требование к документации юридических лиц по защите персональных данных. Требования к документации по обработке персональных данных работников. Типовые документы, регламентирующие получение, обработку, хранение и передачу персональных данных. Планирование мероприятий по защите персональных данных. Угрозы безопасности персональных данных. Классификация информационных систем персональных данных (ИСПДн).
4.	Криптографические системы защиты информации.	Криптографические преобразования. Шифрование и дешифрование информации. Причины нарушения безопасности информации при ее обработке СКЗИ (утечки информации по техническому каналу, неисправности в элементах СКЗИ, работа совместно с другими программами).
5.	Программно-технические средства защиты информации.	Особенности современных информационных систем, факторы, влияющие на безопасность информационной системы. Понятие информационного сервиса безопасности. Виды сервисов безопасности. Парольные схемы аутентификации. Симметричные схемы аутентификации субъекта. Несимметричные схемы аутентификации (с открытым ключом). Аутентификация с третьей доверенной стороной (схема Kerberos). Токены, смарт-карты, их применение. Использование биометрических данных при аутентификации пользователей.

6.2.2. Содержание практических занятий

№ п/п	Наименование раздела дисциплины	Содержание практических занятий
1.	Введение в безопасность информационных систем.	№ 1. Информационная безопасность и безопасность информации. № 2. Нормативно-правовые основы информационной безопасности. № 3. Организационное обеспечение информационной безопасности.
2.	Угрозы безопасности информационных систем и их реализация.	№ 1. Понятие угрозы. Виды противников или «нарушителей». № 2. Защита информации.
3.	Защита персональных данных.	№ 1. Изучение ФЗ № 152-ФЗ «О персональных данных» № 2. Порядок работы с персональными данными работника. № 3. Планирование мероприятий по защите персональных данных.

		№ 4. Изучение методов обезличивания персональных данных.
4.	Криптографические системы защиты информации.	№ 1. Методы криптографии. Средства криптографической защиты информации (СКЗИ). № 2. Использование криптографических средств для решения задач идентификация и аутентификация. № 3. Программно-технические средства защиты информации
5.	Программно-технические средства защиты информации.	№ 1. Общее представление о структуре защищенной информационной системы. № 2. Идентификация и аутентификация. № 3. Сервисы управления доступом. № 4. Защита данных и сервисов от воздействия вредоносных программ.

6.2.3. Содержание самостоятельной работы

№ п/п	Наименование раздела дисциплины	Содержание самостоятельной работы
1.	Введение в безопасность информационных систем.	Использование защищенных компьютерных систем. Общие принципы построения защищенных систем. Иерархический метод разработки защищенных систем. Структурный принцип. Принцип модульного программирования. Исследование корректности реализации и верификации автоматизированных систем. Спецификация требований, предъявляемых к системе. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.
2.	Угрозы безопасности информационных систем и их реализация.	Угроза раскрытия параметров системы, угроза нарушения конфиденциальности, угроза нарушения целостности, угроза отказа служб. Примеры реализации угроз информационной безопасности. Основные принципы обеспечения информационной безопасности в автоматизированных системах. Причины, виды и каналы утечки информации.
3.	Защита персональных данных.	Основы организации и обеспечения комплексной защиты персональных данных при их обработке в ИСПДн. Порядок создания и эксплуатации ИСПДн. Методы работы с постоянными сотрудниками. Административно-правовые нарушения в области связи и информации. Ответственность за нарушение требований по защите персональных данных. Система государственного надзора и контроля в области персональных данных. Проверка персонала при приеме на работу.
4.	Криптографические	Контроль за целостностью информации. Хэш-

	системы защиты информации.	функции, принципы использования. Современные симметричные криптосистемы. Двухключевые криптографические системы хэш-функций для обеспечения целостности данных.
5.	Программно-технические средства защиты информации.	Механизмы доступа данных в операционных системах, системах управления базами данных. Ролевая модель управления доступом. Протоколирование и аудит. Задачи и функции аудита. Структура журналов аудита. Активный аудит, методы активного аудита. Обеспечение защиты корпоративной информационной среды от атак на информационные сервисы. Защита Интернет-подключений, функции и назначение межсетевых экранов. Понятие демилитаризованной зоны. Виртуальные частные сети (VPN), их назначение и использование в корпоративных информационных системах. Вирусы, троянские программы. Антивирусное программное обеспечение. Защита системы электронной почты. Спам, борьба со спамом.

7. Текущий контроль по дисциплине (модулю) в рамках учебных занятий

В рамках текущего контроля преподаватель самостоятельно может проводить следующие мероприятия:

№ п/п	Контролируемые разделы (темы)	Наименование оценочного средства
1.	Введение в безопасность информационных систем.	Опрос, проблемно-аналитическое задание, тестирование. Реализация программы с применением ДОТ: Тестирование, ситуационные задачи, проблемные задачи.
2.	Угрозы безопасности информационных систем и их реализация.	Опрос, проблемно-аналитическое задание, исследовательский проект, творческий проект, тестирование. Реализация программы с применением ДОТ: Тестирование, ситуационные задачи, проблемные задачи
3.	Защита персональных данных.	Опрос, исследовательский проект, проблемно-аналитическое задание, тестирование. Реализация программы с применением ДОТ: Тестирование, ситуационные задачи, проблемные задачи
4.	Криптографические системы защиты информации.	Опрос, проблемно-аналитическое задание, тестирование. Реализация программы с применением ДОТ: Тестирование, ситуационные задачи, проблемные задачи.
5.	Программно-технические	Опрос, проблемно-аналитическое задание, тестирование.

	средства защиты информации.	Реализация программы с применением ДОТ: Тестирование, ситуационные задачи, проблемные задачи.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

8.2. Основная литература:

1. Информационная безопасность и правовые основы защиты персональных данных: учебное пособие / А. В. Терехов, В. Н. Чернышов, А. В. Платенкин, А. В. Селезнев. — Тамбов: Тамбовский государственный технический университет, ЭБС АСВ, 2023. — 80 с. — ISBN 978-5-8265-2648-4. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/141049.html
2. Киренберг, А. Г. Информационная безопасность современных операционных систем: учебное пособие / А. Г. Киренберг. — Кемерово: Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2022. — 138 с. — ISBN 978-5-00137-320-9. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/128393.html
3. Киренберг, А. Г. Системное администрирование и информационная безопасность сетей ЭВМ: учебное пособие / А. Г. Киренберг. — Кемерово: Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2022. — 119 с. — ISBN 978-5-00137-292-9. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/128406.html
4. Фомин, Д. В. Информационная безопасность: учебник / Д. В. Фомин. — Москва: Ай Пи Ар Медиа, 2022. — 222 с. — ISBN 978-5-4497-1548-7. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/118876.html

8.2 Дополнительная литература:

1. Басыня, Е. А. Сетевая информационная безопасность: учебник / Е. А. Басыня. — Москва: Национальный исследовательский ядерный университет «МИФИ», 2023. — 224 с. — ISBN 978-5-7262-2949-2. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/132693.html
2. Багамаева, З. З. Делопроизводство и режим секретности : электронное учебное пособие / З. З. Багамаева. — Махачкала : Северо-Кавказский институт (филиал) Всероссийского государственного университета юстиции (РПА Минюста России), 2014. — 202 с. — ISBN 978-5-89172-668-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/49984.html

8.3. Периодические издания:

1. Воронежский государственный технический университет. Информационные технологии в строительных, социальных и экономических системах. https://www.iprbookshop.ru/64279.html
2. «Информационные технологии» ISSN 1684-640 http://novtex.ru/IT/

9. Перечень ресурсов информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), необходимых для освоения дисциплины (модуля)

1. Федеральный портал «Российское образование» http://www.edu.ru
2. Электронно-библиотечная система «Научная электронная библиотека eLIBRARY.RU» https://www.elibrary.ru
3. Электронно-библиотечная система IPR BOOKS https://www.iprbookshop.ru
4. Электронно-библиотечная система ЛАНЬ https://e.lanbook.com
5. Электронная библиотечная система https://biblioclub.ru

10. Методические указания для обучающихся по освоению дисциплины (модуля)

Успешное освоение данного курса базируется на рациональном сочетании нескольких видов учебной деятельности – лекций, семинарских занятий, самостоятельной работы. При этом самостоятельную работу следует рассматривать одним из главных звеньев полноценного высшего образования, на которую отводится значительная часть учебного времени.

Самостоятельная работа студентов складывается из следующих составляющих:

1. Работа с основной и дополнительной литературой, с материалами интернета и конспектами лекций;

2. Внеаудиторная подготовка к контрольным работам, выполнение докладов, рефератов и курсовых работ;

3. Выполнение самостоятельных практических работ;

4. Подготовка к экзаменам (зачетам) непосредственно перед ними.

Для правильной организации работы необходимо учитывать порядок изучения разделов курса, находящихся в строгой логической последовательности. Поэтому хорошее усвоение одной части дисциплины является предпосылкой для успешного перехода к следующей. Задания, проблемные вопросы, предложенные для изучения дисциплины, в том числе и для самостоятельного выполнения, носят междисциплинарный характер и базируются, прежде всего, на причинно-следственных связях между компонентами окружающего нас мира. Важным составляющим в изучении данного курса является решение ситуационных задач и работа над проблемно-аналитическими заданиями, что предполагает знание соответствующей научной терминологии и т.д.

Для лучшего запоминания материала целесообразно использовать индивидуальные особенности и разные виды памяти: зрительную, слуховую, ассоциативную. Успешному запоминанию также способствует приведение ярких свидетельств и наглядных примеров. Учебный материал должен постоянно повторяться и закрепляться.

При выполнении докладов, творческих, информационных, исследовательских проектов особое внимание следует обращать на подбор источников информации и методику работы с ними.

Для успешной сдачи экзамена (зачета) рекомендуется соблюдать следующие правила:

1. Подготовка к экзамену (зачету) должна проводиться систематически, в течение всего семестра.

2. Интенсивная подготовка должна начаться не позднее, чем за месяц до экзамена.

3. Время непосредственно перед экзаменом (зачетом) лучше использовать таким образом, чтобы оставить последний день свободным для повторения курса в целом, для систематизации материала и доработки отдельных вопросов.

На экзамене высокую оценку получают студенты, использующие данные, полученные в процессе выполнения самостоятельных работ, а также использующие собственные выводы на основе изученного материала.

Учитывая значительный объем теоретического материала, студентам рекомендуется регулярное посещение и подробное конспектирование лекций.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

1. Microsoft Windows Server;

2.Семейство ОС Microsoft Windows;

3. Libre Office свободно распространяемый офисный пакет с открытым исходным кодом;

4. Информационно-справочная система: Система КонсультантПлюс (КонсультантПлюс);

5. Информационно-правовое обеспечение Гарант: Электронный периодический справочник «Система ГАРАНТ» (Система ГАРАНТ);

Перечень используемого программного обеспечения указан в п.12 данной рабочей программы дисциплины.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

12.1. Учебная аудитория для проведения учебных занятий, предусмотренных образовательной программой, оснащенная оборудованием и техническими средствами обучения.

Специализированная мебель:

Комплект учебной мебели (стол, стул) по количеству обучающихся; комплект мебели для преподавателя; доска (маркерная).

Технические средства обучения:

Компьютер в сборе для преподавателя, проектор, экран, колонки

Перечень лицензионного программного обеспечения, в том числе отечественного производства:

Windows 10, КонсультантПлюс, Kaspersky Endpoint Security.

Перечень свободно распространяемого программного обеспечения:

Яндекс Браузер, LibreOffice, МТС Линк.

Подключение к сети «Интернет» и обеспечение доступа в электронную информационно-образовательную среду ММУ.

12.2. Помещение для самостоятельной работы обучающихся.

Специализированная мебель:

Комплект учебной мебели (стол, стул) по количеству обучающихся; комплект мебели для преподавателя; доска (маркерная).

Технические средства обучения:

Компьютер в сборе для преподавателя; компьютеры в сборе для обучающихся; колонки; проектор, экран.

Перечень лицензионного программного обеспечения, в том числе отечественного производства:

Windows Server 2016, Windows 10, Microsoft Office, КонсультантПлюс, Kaspersky Endpoint Security.

Перечень свободно распространяемого программного обеспечения:

Яндекс Браузер, LibreOffice, МТС Линк, Gimp, Paint.net, AnyLogic, Inkscape.

Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду ММУ.

13.Образовательные технологии, используемые при освоении дисциплины

Для освоения дисциплины используются как традиционные формы занятий – лекции (типы лекций – установочная, вводная, текущая, заключительная, обзорная; виды лекций – проблемная, визуальная, лекция конференция, лекция консультация); и семинарские (практические) занятия, так и активные и интерактивные формы занятий - деловые и ролевые игры, решение ситуационных задач и разбор конкретных ситуаций.

На учебных занятиях используются технические средства обучения мультимедийной аудитории: компьютер, монитор, колонки, настенный экран, проектор, микрофон, пакет программ Microsoft Office для демонстрации презентаций и медиафайлов, видеопроектор для демонстрации слайдов, видеосюжетов и др. Тестирование обучаемых может осуществляться с использованием компьютерного оборудования университета.

13.1. В освоении учебной дисциплины используются следующие традиционные образовательные технологии:

- чтение проблемно-информационных лекций с использованием доски и видеоматериалов;
- семинарские занятия для обсуждения, дискуссий и обмена мнениями;
- контрольные опросы;
- консультации;
- самостоятельная работа студентов с учебной литературой и первоисточниками;
- подготовка и обсуждение рефератов (проектов), презентаций (научно-исследовательская работа);
- тестирование по основным темам дисциплины.

13.2. Активные и интерактивные методы и формы обучения

Из перечня видов: («*мозговой штурм», анализ НПА, анализ проблемных ситуаций, анализ конкретных ситуаций, инциденты, имитация коллективной профессиональной деятельности, разыгрывание ролей, творческая работа, связанная с освоением дисциплины, ролевая игра, круглый стол, диспут, беседа, дискуссия, мини-конференция и др.*) используются следующие:

- *диспут;*
- *анализ проблемных, творческих заданий, ситуационных задач;*
- *ролевая игра;*
- *круглый стол;*
- *мини-конференция;*
- *дискуссия;*
- *беседа.*

13.3. Особенности обучения инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ)

При организации обучения по дисциплине учитываются особенности организации взаимодействия с инвалидами и лицами с ограниченными возможностями здоровья (далее – инвалиды и лица с ОВЗ) с целью обеспечения их прав. При обучении учитываются особенности их психофизического развития, индивидуальные возможности и при необходимости обеспечивается коррекция нарушений развития и социальная адаптация указанных лиц.

Выбор методов обучения определяется содержанием обучения, уровнем методического и материально-технического обеспечения, особенностями восприятия учебной информации студентов с инвалидностью и студентов с ограниченными возможностями здоровья и т.д. В образовательном процессе используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с

целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе.

При обучении лиц с ограниченными возможностями здоровья электронное обучение и дистанционные образовательные технологии предусматривают возможность приема-передачи информации в доступных для них формах.

Обучающиеся из числа лиц с ограниченными возможностями здоровья обеспечены печатными и электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

Приложение

Автономная некоммерческая организация высшего образования
«МОСКОВСКИЙ МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

Информационная безопасность и защита персональных данных сотрудников

Направление подготовки	Управление персоналом
Код	38.03.03
Направленность (профиль)	Управление персоналом организации и государственной службы
Квалификация (степень) выпускника	бакалавр

Москва
2026 г.

1. Перечень кодов компетенций, формируемых дисциплиной в процессе освоения образовательной программы

Группа компетенций	Категория компетенций	Код
Профессиональные		ПК-7

2. Компетенции и индикаторы их достижения

Код компетенции	Формулировка компетенции	Индикаторы достижения компетенции
ПК-7	Способен вести кадровое делопроизводство и организовывать архивное хранение кадровых документов в соответствии с действующими нормативно-правовыми актами, составлять кадровую отчетность, обеспечить защиту персональных данных сотрудников, оптимизировать оптимизации документооборот и схемы функциональных взаимосвязей между подразделениями	ПК-7.1 ведет кадровое делопроизводство и организовывает архивное хранение кадровых документов в соответствии с действующими нормативно-правовыми актами ПК-7.2 участвует в составлении кадровой отчетности, обеспечивает защиту персональных данных сотрудников, оптимизирует документооборот и схемы функциональных взаимосвязей между подразделениями ПК-7.3 участвует в составлении и реализации планов (программ) социального развития с учетом фактического состояния социальной сферы, экономического состояния и общих целей развития организации

3. Описание планируемых результатов обучения по дисциплине

3.1. Описание планируемых результатов обучения по дисциплине

Планируемые результаты обучения по дисциплине представлены дескрипторами (знания, умения, навыки).

Дескрипторы по дисциплине	Знать	Уметь	Владеть
Код компетенции	**ПК-7**		

	– функции документа, классификацию документов, современные требования к документационному обеспечению управления; – способы документирования; – основы разработки кадровой политики; – технологии управления развитием персонала (управление социальным развитием; организации обучения персонала; организации текущей деловой оценки, в т.ч. аттестации персонала; управления деловой карьерой и служебно-профессиональным продвижением персонала); – основы кадрового планирования в организации; – основные положения занятости и трудоустройства; – особенности организации и применения наемного труда; – особенности организационного проектирования систем управления персоналом; – этапы организационного проектирования;	– применять полученные знания в организациях; – выполнять ключевые технологические операции при работе с документами; – принимать участие в разработке корпоративных, конкурентных и функциональных стратегий развития организации в части управления персоналом; – прогнозировать и планировать потребность организации в персонале в соответствии со стратегическими планами организации и определять эффективные пути ее удовлетворения; – оперировать понятиями и категориями трудового законодательства; – толковать и правильно применять нормы трудового законодательства; – осуществлять анализ	– основными методами и приемами исследовательской, аналитической и практической работы в области документационного обслуживания; – методами разработки и реализации стратегий управления персоналом; – методами планирования численности и профессионального состава персонала в соответствии со стратегическими планами организации; – современными технологиями управления персоналом организации (найма, отбора, приема и расстановки персонала; социализации, профориентации и трудовой адаптации персонала; организации труда персонала, высвобождения персонала); – навыками работы с нормативными правовыми актами; – навыками разрешения правовых проблем в сфере труда; – методами проаектирования систем управления; – технологией организационного

		систем управления персоналом с помощью различных методов;	проаектирования.

3.2. Критерии оценки знаний студентов

Шкала оценивания	Индикаторы достижения	Показатели оценивания результатов обучения
ОТЛИЧНО/Зачтено	Знает:	- студент глубоко и всесторонне усвоил материал, уверенно, логично, последовательно и грамотно его излагает, опираясь на знания основной и дополнительной литературы, - на основе системных научных знаний делает квалифицированные выводы и обобщения, свободно оперирует категориями и понятиями.
	Умеет:	- студент умеет самостоятельно и правильно решать учебно-профессиональные задачи или задания, уверенно, логично, последовательно и аргументировано излагать свое решение, используя научные понятия, ссылаясь на нормативную базу.
	Владеет:	- студент владеет рациональными методами (с использованием рациональных методик) решения сложных профессиональных задач, представленных деловыми играми, кейсами и т.д.; При решении продемонстрировал навыки - выделения главного, - связкой теоретических положений с требованиями руководящих документов, - изложения мыслей в логической последовательности, - самостоятельного анализа факты, событий, явлений, процессов в их взаимосвязи и диалектическом развитии.
ХОРОШО/Зачтено	Знает:	- студент твердо усвоил материал, достаточно грамотно его излагает, опираясь на знания основной и дополнительной литературы, - затрудняется в формулировании квалифицированных выводов и обобщений, оперирует категориями и понятиями, но не всегда правильно их верифицирует.
	Умеет:	- студент умеет самостоятельно и в основном правильно решать учебно-профессиональные задачи или задания, уверенно, логично, последовательно и аргументировано излагать свое решение, не в полной мере используя научные понятия и ссылки на нормативную базу.

	Владеет:	- студент в целом владеет рациональными методами решения сложных профессиональных задач, представленных деловыми играми, кейсами и т.д.; При решении смог продемонстрировать достаточность, но не глубинность навыков - выделения главного, - изложения мыслей в логической последовательности. - связки теоретических положений с требованиями руководящих документов, - самостоятельного анализа факты, событий, явлений, процессов в их взаимосвязи и диалектическом развитии.
УДОВЛЕТВОРИТЕЛЬНО/Зачтено	Знает:	- студент ориентируется в материале, однако затрудняется в его изложении; - показывает недостаточность знаний основной и дополнительной литературы; - слабо аргументирует научные положения; - практически не способен сформулировать выводы и обобщения; - частично владеет системой понятий.
	Умеет:	- студент в основном умеет решить учебно-профессиональную задачу или задание, но допускает ошибки, слабо аргументирует свое решение, недостаточно использует научные понятия и руководящие документы.
	Владеет:	- студент владеет некоторыми рациональными методами решения сложных профессиональных задач, представленных деловыми играми, кейсами и т.д.; При решении продемонстрировал недостаточность навыков - выделения главного, - изложения мыслей в логической последовательности. - связки теоретических положений с требованиями руководящих документов, - самостоятельного анализа факты, событий, явлений, процессов в их взаимосвязи и диалектическом развитии.
НЕУДОВЛЕТВОРИТЕЛЬНО/ Не зачтено	Знает:	- студент не усвоил значительной части материала; - не может аргументировать научные положения; - не формулирует квалифицированных выводов и обобщений; - не владеет системой понятий.
	Умеет:	студент не показал умение решать учебно-профессиональную задачу или задание.
	Владеет:	не выполнены требования, предъявляемые к навыкам, оцениваемым «удовлетворительно».

При ответе на вопросы в рамках прохождения промежуточной аттестации (зачет/ зачет с оценкой/ экзамен) допускается вольная формулировка ответа, по смыслу раскрывающая содержание ответа, указанного в фонде оценочных средств, в качестве верного ответа.

4. Типовые контрольные задания (закрытого, открытого и иного типа) для проведения промежуточной аттестации, необходимые для оценки достижения компетенции, соотнесенной с результатами обучения по дисциплине

ТЕСТИРОВАНИЕ

ПК-7

1. Что из перечисленного относится к основным принципам обеспечения защиты персональных данных сотрудников? Выберите несколько вариантов ответов.

а) Обработка персональных данных должна осуществляться на законной и справедливой основе

б) Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей

в) При обработке персональных данных должны быть обеспечены точность, достаточность и актуальность персональных данных

г) Персональные данные могут храниться неограниченно долго без определения срока

Ответ: а) Обработка персональных данных должна осуществляться на законной и справедливой основе; б) Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей; в) При обработке персональных данных должны быть обеспечены точность, достаточность и актуальность персональных данных

2. Какой федеральный закон является основным в области регулирования обработки персональных данных в Российской Федерации?

а) ФЗ № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

б) ФЗ № 152-ФЗ «О персональных данных»

в) ФЗ № 63-ФЗ «Об электронной подписи»

г) ФЗ № 5485-1 «О государственной тайне»

Ответ: б) ФЗ № 152-ФЗ «О персональных данных»

3. Какие категории персональных данных выделяет Федеральный закон «О персональных данных»?

а) Служебные и коммерческие

б) Общедоступные, специальные, биометрические

в) Личные и корпоративные

г) Стратегические и тактические

Ответ: б) Общедоступные, специальные, биометрические

4. Что из перечисленного относится к специальным категориям персональных данных?

а) Раса, национальная принадлежность, политические взгляды

б) Фамилия, имя, отчество

в) Место работы и должность

г) Номер телефона и адрес электронной почты

Ответ: а) Раса, национальная принадлежность, политические взгляды

5. Какие документы должны быть разработаны в организации для обеспечения защиты персональных данных сотрудников? Выберите несколько вариантов ответов.

а) Политика в отношении обработки персональных данных

б) Перечень мер по обеспечению безопасности персональных данных

в) Договор аренды офисного помещения

г) Согласие на обработку персональных данных

Ответ: а) Политика в отношении обработки персональных данных; б) Перечень мер по обеспечению безопасности персональных данных; г) Согласие на обработку персональных данных

6. Что понимается под конфиденциальностью информации?

а) Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя

б) Возможность за приемлемое время получить требуемую информационную услугу

в) Актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения

г) Свободное распространение информации без ограничений

Ответ: а) Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя

7. Кто является оператором персональных данных согласно ФЗ № 152-ФЗ?

а) Физическое лицо, чьи персональные данные обрабатываются

б) Государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных

в) Суд, рассматривающий дела о нарушении прав субъектов персональных данных

г) Общественная организация, контролирующая соблюдение законодательства о персональных данных

Ответ: б) Государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных

8. Какие действия относятся к обработке персональных данных? Выберите несколько вариантов ответов.

а) Сбор персональных данных

б) Хранение персональных данных

в) Уничтожение персональных данных

г) Создание резюме сотрудника другим лицом без согласия

Ответ: а) Сбор персональных данных; б) Хранение персональных данных; в) Уничтожение персональных данных

9. Что такое обезличивание персональных данных?

а) Действия, в результате которых персональные данные становятся доступными неограниченному кругу лиц

б) Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных

в) Полное удаление всех персональных данных из информационной системы

г) Передача персональных данных третьим лицам с согласия субъекта

Ответ: б) Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных

10. В каком случае допускается обработка персональных данных без согласия субъекта персональных данных?

а) Для маркетинговых исследований без указания цели

б) Когда обработка персональных данных необходима для исполнения договора, стороной которого является субъект персональных данных

в) Для создания базы данных потенциальных клиентов

г) Для передачи данных родственникам без уведомления субъекта

Ответ: б) Когда обработка персональных данных необходима для исполнения договора, стороной которого является субъект персональных данных

11. Назовите основной федеральный закон, регулирующий отношения, связанные с обработкой персональных данных в Российской Федерации. Запишите ответ в виде названия закона с указанием номера.

Ответ: Федеральный закон № 152-ФЗ «О персональных данных»

12. Запишите термин, который обозначает действия, в результате которых становится невозможным определить принадлежность персональных данных конкретному лицу без использования дополнительной информации.

Ответ: Обезличивание персональных данных

13. Назовите лицо, которое самостоятельно создало информацию либо получило на основании закона или договора право разрешать или ограничивать доступ к информации.

Ответ: Обладатель информации

14. Запишите термин, обозначающий совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Ответ: Угроза

15. Назовите категорию персональных данных, к которой относятся сведения о физиологических особенностях человека, на основании которых можно установить его личность.

Ответ: Биометрические персональные данные

16. Запишите термин, который в соответствии с ФЗ № 152-ФЗ означает любое действие или совокупность действий, совершаемых с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу, обезличивание, блокирование, удаление, уничтожение персональных данных.

Ответ: Обработка персональных данных

17. Назовите государственный орган, осуществляющий контроль и надзор за обработкой персональных данных в Российской Федерации. Запишите полное наименование в именительном падеже.

Ответ: Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)

18. Запишите термин, который в контексте защиты информации означает возможность за приемлемое время получить требуемую информационную услугу.

Ответ: Доступность информации

19. Назовите срок, в течение которого оператор персональных данных обязан сообщить субъекту персональных данных о наличии персональных данных, относящихся к соответствующему субъекту. Запишите ответ в виде количества рабочих дней.

Ответ: 30 дней

20. Запишите термин, обозначающий совокупность законодательных актов, нормативно-правовых документов и требований, которые обязательны в системе защиты информации.

Ответ: Правовое обеспечение безопасности информации

21. Установите соответствие между категориями персональных данных и их характеристиками:

№	Категория персональных данных	Буква	Характеристика
1	Общедоступные персональные данные	А	Физиологические особенности человека, позволяющие установить его личность
2	Специальные категории персональных данных	Б	Данные, ставшие известными неограниченному кругу лиц с согласия субъекта
3	Биометрические персональные данные	В	Раса, национальность, политические взгляды, религиозные и философские убеждения

Заполните соответствующие буквы под цифрами:

1	2	3

Ответ: 1Б, 2В, 3А

22. Установите соответствие между основными составляющими информационной безопасности и их определениями:

№	Составляющая ИБ	Буква	Определение
1	Конфиденциальность	А	Актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения
2	Целостность	Б	Защита от несанкционированного доступа к

№	Составляющая ИБ	Буква	Определение
			информации
3	Доступность	В	Возможность за приемлемое время получить требуемую информационную услугу

Заполните соответствующие буквы под цифрами:

1	2	3

Ответ: 1Б, 2А, 3В

Примерный список вопросов

1. Понятие информационной безопасности. Основные составляющие. Важность проблемы.
2. Распространение объектно-ориентированного подхода на информационную безопасность.
3. Понятие угрозы. Наиболее распространенные угрозы. Классификация угроз. Защита информации от случайных угроз.
4. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы в РФ.
5. Законодательный уровень информационной безопасности. Обзор зарубежного законодательства в области ИБ.
6. Назначение и задачи в сфере обеспечения информационной безопасности.
7. Международные стандарты информационного обмена. Стандарт ISO/IEC15408.
8. Российские стандарты защищенности автоматизированных систем.
9. Основные положения теории информационной безопасности. Модели безопасности и их применение.
10. Информационная безопасность в условиях функционирования в России глобальных сетей.
11. Виды противников или «нарушителей».
12. Классификация компьютерных вирусов. Методы и средства борьбы с вирусами. Виды возможных нарушений информационной системы. Виды защиты.
13. Шпионское ПО. Рекламное ПО.
14. Система охраны объектов компьютерных систем.
15. Организация работы с конфиденциальными информационными ресурсами.
16. Защита от злоумышленных действий обслуживающего персонала и пользователей. Защита от несанкционированного копирования программного обеспечения.
17. Средства защиты компьютеров. Программно-аппаратные методы и средства ограничения доступа к компонентам компьютера.
18. Типы несанкционированного доступа и условия работы средств защиты.
19. Методы криптографии.
20. Основные понятия шифрования. Стандарты шифрования.
21. Методы шифрования с симметричным ключом. Системы шифрования с открытым ключом.

22. Методы и средства хранения ключевой информации. Анализ программных реализаций.
23. Защита от разрушающих программных воздействий.
24. Основные технологии построения защищенных ЭИС.
25. Системные вопросы защиты программ и данных.
26. Защита вычислительной сети. Классификация вторжений.
27. Системы архивирования и дублирования информации.
28. Защита информации в операционных системах. Защита информации в прикладном ПО.
29. Проблема защиты информации в распределенных сетях.
30. Межсетевой экран. Классификация межсетевых экранов. Брандмауеры. Основные понятия.

Примерный перечень вопросов к промежуточной аттестации:

1. Какая информация является объектом права собственности, и какие особенности для нее характерны.
2. Охарактеризуйте избыточное кодирование в целом с точки зрения обнаружения и исправления случайных ошибок.
3. Что определяет при таком кодировании минимальное кодовое расстояние.
4. Дайте общую характеристику кода Хэмминга и равновесного кода.
5. Рассмотрите на примере шифрование аналитическими методами с использованием преобразований матричной алгебры.
6. Что представляют собой односторонние функции?
7. Как используется в алгоритме RSA с открытым ключом разложение больших чисел на простые множители?
8. Приведите классификацию методов шифрования в зависимости от способа преобразования информации.
9. Проанализируйте основные технологические этапы, реализуемые в процессе разработки КСЗИ.
10. Как реализуются резидентные функции загрузочного вируса с точки зрения его распространения.
11. Поясните сущность эвристического анализа, применяемого для удаления вирусов
12. Каковы основные принципы и условия обработки персональных данных согласно Федеральному закону № 152-ФЗ «О персональных данных»?
13. Опишите права субъекта персональных данных на доступ к своим данным и порядок их реализации в организации.
14. Какие меры организационного характера необходимо реализовать для обеспечения безопасности персональных данных при их обработке в кадровой службе?
15. Что такое политика оператора в отношении обработки персональных данных, и какие разделы она должна включать?
16. Как классифицируются угрозы безопасности персональных данных при их обработке в информационных системах?
17. Перечислите основные способы защиты персональных данных от несанкционированного доступа (НСД) в локальной сети организации.
18. Что представляет собой система защиты персональных данных (СЗПД) и какие требования предъявляются к ее уровням защищенности?
19. Охарактеризуйте порядок действий работодателя при утечке персональных данных сотрудников, включая уведомление уполномоченных органов.
20. Какие требования предъявляются к уничтожению персональных данных при достижении целей обработки или отзыве согласия субъекта?
21. В чем заключается сущность криптографической защиты персональных данных при передаче по открытым каналам связи?

22. Каковы особенности обработки специальных категорий персональных данных (биометрических, о состоянии здоровья) в управлении персоналом?
23. Опишите роль и ответственность лица, ответственного за обработку персональных данных в организации.
24. Что такое трансграничная передача персональных данных и какие ограничения на нее установлены российским законодательством?
25. Как проводится оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения требований их защиты?
26. Какие организационно-распорядительные документы должны быть разработаны оператором для обеспечения защиты персональных данных?
27. Проанализируйте типовые ошибки сотрудников отдела кадров, приводящие к утечке персональных данных, и методы их предотвращения.
28. Что такое модель угроз безопасности персональных данных и модель нарушителя? Какие сведения они включают?
29. Каков порядок проведения внутреннего контроля соответствия обработки персональных данных установленным требованиям?
30. Охарактеризуйте ответственность (дисциплинарную, административную, уголовную) за нарушение законодательства о персональных данных в Российской Федерации.

Типовые проблемные задачи

№1 Оцените время раскрытия пароля, если число символов в сообщении, передаваемом в систему при попытке получить доступ к ней, равно 20, 600 симв/мин – скорость передачи символов, длина пароля равна 6, число символов в алфавите – 26. Ответ дать в месяцах.

Типовые ситуационные задачи

№ 1 Выберите необходимую длину пароля, чтобы вероятность его отгадывания не превышала 0.001 за 3 месяца. На одну попытку посылается 20 символов, скорость передачи данных равна 600 символов в минуту.

№2 Зашифровать с помощью алгоритма RSA сообщение на русском языке «РИМ».

Примерные варианты контрольных работ

Вариант 1.

1. Методы оценки рисков информационной безопасности на предприятии.
2. Генерирование множества альтернатив с применением экспертных методов при разработке СЗИ.
3. Основные этапы принятия управленческих решений в области построения защищенных систем обработки информации.

Вариант 2.

1. Этапы построения защищенных систем обработки информации.
2. «Куб безопасности» в координатах ОСНОВА, НАПРАВЛЕНИЯ, ЭТАПЫ. Обработка трехмерных матриц для оценки эффективности СЗИ.
3. Пример использования метода строчных сумм для составления матрицы альтернативных проектов СЗИ.

Вариант 3.

1. Управление рисками. Модель безопасности с полным перекрытием.
2. Модель элементарной защиты объекта информатизации. Пример расчета прочности защиты.
3. Парное сравнение альтернатив (метод парных сравнений).

Вариант 4.

1. Пример использования сетей Петри для построения сценария действий нарушителя и сигнатур атак.
2. Оценка альтернативных проектов организации СЗИ с использованием критериального

метода.
3. Обзор современных программных продуктов для оценки рисков.
Вариант 5.
1. Модель многозвенной защиты объекта информатизации. Пример расчета прочности защиты.
2. Альтернативы и критерии. Требования к набору критериев. Оценка важности критериев.
3. Пример исследования эффективности СЗИ с использованием морфологической матрицы.

Темы исследовательских, творческих проектов

1. Этапы и общие принципы разработки защищенных информационных систем.
2. Предпосылки отнесения информации к категории конфиденциальной и выявление конфиденциальных сведений.
3. Сценарии последовательности действий нарушителя системы защиты информации. Пример построения сценария действий нарушителя с использованием графов.
4. Международные стандарты в области защиты информационных систем.
5. Цели, задачи и стадии проведения аудита информационной безопасности.
6. Оценка ущерба от нарушений информационной безопасности на различных этапах жизненного цикла объекта информатизации.
7. Методы оценки рисков информационной безопасности.
8. Шкалы оценки ущерба при нарушении информационной безопасности на объекте оценки.
9. Управление рисками. Модель безопасности с полным перекрытием.
10. Концепция управление рисками согласно ISO-15408.
11. Lifecycle Security – обобщенная схема построения комплексной защиты компьютерной сети предприятия.
12. Методика управления рисками, предлагаемая Microsoft (MSAT).
13. Обзор современных программных продуктов для оценки рисков.
14. Особенности моделирования сложных организационно-технических систем.
15. Моделирование процесса защиты информации в информационной системе с использованием графовых структур.
16. Пример использования графов для расчета защищенности от физического проникновения.
17. Генерирование множества альтернатив с применением экспертных методов при построении защищенной системы обработки информации.
18. Модель процесса защиты информации в виде трёхдольного графа.
19. Оценка альтернативных проектов организации системы защиты информации с использованием критериального метода.
20. Оценка альтернативных проектов организации системы защиты информации с использованием метода парных сравнений.
21. Информационные технологии, используемые в системах поддержки управленческих решений в области построения защищенных систем обработки информации.
22. Перспективные направления в организации и управлении системой защиты информации на предприятии.