Приложение 1 к РПД
Информационная безопасность
39.03.01 Социология
Направленность (профиль)
Цифровая и экспертно-аналитическая социология
Форма обучения – очная
Год набора – 2022

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.	Кафедра	Экономики и управления
2.	Направление подготовки	39.03.01 Социология
3.	Направленность (профиль)	Цифровая и экспертно-аналитическая социология
4.	Дисциплина (модуль)	Информационная безопасность
5.	Форма обучения	очная
6.	Год набора	2022

1. Методические рекомендации

1.1. Методические рекомендации по организации работы обучающихся во время проведения лекционных занятий

Изучение курса предполагает владение обучающимися информацией о текущих исследованиях в сфере системного анализа и управления, а также общей теории систем, проводимых как на территории нашей страны, так и за рубежом.

В ходе лекций преподаватель излагает и разъясняет основные, наиболее сложные понятия темы, а также связанные с ней теоретические и практические проблемы, дает рекомендации для практического занятия и указания для выполнения самостоятельной работы.

В ходе лекционных занятий обучающемуся необходимо вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание изучаемой дисциплины, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве.

Желательно оставить в рабочих конспектах поля, на которых делать пометки, подчеркивающие особую важность тех или иных теоретических положений. Рекомендуется активно задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

1.2 Методические рекомендации по подготовке к семинарским (практическим) занятиям

На практических занятиях обучающиеся должны закреплять теоретические знания, полученные на лекциях и в ходе самостоятельной работы с источниками, развивать навыки научного анализа текстов, умение дискутировать, отстаивать свою точку зрения на проблемы системного анализа в различных предметных областях, что способствует выработке мировоззрения будущего бакалавра.

Практическое занятие так же предполагает выполнение индивидуальных заданий на ПК и работу в группах. Оно начинается со вступительного слова преподавателя, формулирующего цель занятия и характеризующего его основную проблематику. Затем, как правило, выполняется задание по заданной теме. В целях контроля подготовленности обучающихся преподаватель в ходе практического занятия может осуществлять текущий

контроль знаний в виде тестовых заданий и устного опроса по результатам проделанной работы.

1.3. Методические рекомендации по подготовке доклада

Алгоритм создания доклада:

1 этап – определение темы доклада

2 этап – определение цели доклада

3 этап − подробное раскрытие информации

4 этап − формулирование основных тезисов и выводов.

1.4. Методические рекомендации по составлению глоссария

1. Внимательно прочитайте и ознакомьтесь с текстом. Вы встретите в нем много различных терминов, которые имеются по данной теме.

2. После того, как вы определили наиболее часто встречающиеся термины, вы должны составить из них список. Слова в этом списке должны быть расположены в строго алфавитном порядке, так как глоссарий представляет собой не что иное, как словарь специализированных терминов.

3. После этого начинается работа по составлению статей глоссария. Статья глоссария - это определение термина. Она состоит из двух частей: 1. заочная формулировка термина в именительном падеже; 2. содержательная часть, объемно раскрывающая смысл данного термина.

При составлении глоссария важно придерживаться следующих правил:

- стремитесь к максимальной точности и достоверности информации;
- старайтесь указывать корректные научные термины и избегать всякого рода жаргонизмов. В случае употребления такового, давайте ему краткое и понятное пояснение;
- излагая несколько точек зрения в статье по поводу спорного вопроса, не принимайте ни одну из указанных позиций. Глоссария - это всего лишь констатация имеющихся фактов;
- также не забывайте приводить в пример контекст, в котором может употреблять данный термин;
- при желании в глоссарий можно включить не только отельные слова и термины, но и целые фразы.

1.5. Методические рекомендации по проведению занятий в интерактивной форме (выполнение кейс-стади)

Интерактивное обучение представляет собой способ познания, осуществляемый в формах совместной деятельности обучающихся, т.е. все участники образовательного процесса взаимодействуют друг с другом, совместно решают поставленные проблемы, моделируют ситуации, обмениваются информацией, оценивают действие коллег и свое собственное поведение, погружаются в реальную атмосферу делового сотрудничества по разрешению проблем.

По дисциплине «Информационная безопасность» предусмотрено в качестве интерактивной формы обучение – выполнение кейс-стади.

Необходимо разбиться на группы по 3-4 человека. Каждая группа выбирает сферу деятельности из представленного ниже списка:

- производство высокотехнологичных товаров,
- рекламное агентство,
- разработка программного обеспечения,
- банк,
- университет
- иная по согласованию с преподавателем.

Реализуемые действия:

- придумать название выбранной организации, ее миссию, положение на рынке, основные задачи;
- описать особенности выбранной организации в трех-четырех абзацах;
- распределить между собой роли, соответствующие организационной структуре выбранной организации (директор предприятия, начальник ИТ-отдела, директор охраны, администратор сети и т.д.);
- составить политику безопасности выбранной организации (каждый участник группы отвечает за раздел политики безопасности, соответствующий своей роли);

Результаты работы предоставить в виде отчета с кратким представление организации и документа Концепция информационной безопасности.

Структура документа Концепция информационной безопасности

ВВЕДЕНИЕ

1.ОБЩИЕ ПОЛОЖЕНИЯ

Назначение документа.

Правовая основа документа.

2.ОЪЕКТЫ ЗАЩИТЫ

Назначение, цель создания и эксплуатации КИС как объекта информатизации.

Структура, состав и размещение основных компонентов КИС и информационные связи с другими объектами.

Категории пользователей, режимы использования и уровни доступа к информации.

Уязвимость основных компонентов КИС.

3.ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Интересы субъектов информационных отношений.

Цели защиты.

Основные задачи системы обеспечения безопасности информации КИС.

Основные пути достижения целей защиты.

4.ОСНОВНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ КИС

Угрозы безопасности информации и их источники.

Умышленные действия сторонних лиц, зарегистрированных пользователей и обслуживающего персонала.

Утечка информации по техническим каналам.

Неформальная модель возможных нарушителей.

5.ОСНОВНЫЕ ПОЛОЖЕНИЯ ТЕХНИЧЕСКОЙ ПОЛИТИКИ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ КИС

Техническая политика в области обеспечения безопасности информации.

Формирование режима безопасности информации.

6.ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

7.МЕРЫ,МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ТРЕБУЕМОГО УРОВНЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Меры обеспечения безопасности

Правовые меры

Организационно-административные меры

Физические средства защиты

Программно-аппаратные средства защиты

Средства идентификации и аутентификации пользователей

Средства разграничения доступа зарегистрированных пользователей

Средства обеспечения контроля целостности программных и информационных ресурсов

Средства оперативного контроля и регистрации событий безопасности

1.6. Методические рекомендации по решению теста

Тестовая система предусматривает вопросы/задания, на которые обучающийся должен дать один или несколько вариантов правильного ответа из предложенного списка ответов. При поиске ответа необходимо проявлять внимательность.

При отсутствии какого–либо одного ответа на вопрос, предусматривающий множественный выбор, весь ответ считается неправильным.

Ответы правильные выделяются в тесте подчеркиванием или любым другим допустимым символом.

1.7. Методические рекомендации по подготовке к сдаче зачета

Зачет является формой итогового контроля знаний и умений обучающихся по данной дисциплине, полученных на лекциях, практических занятиях и в процессе самостоятельной работы.

В период подготовки к зачету обучающиеся вновь обращаются к учебно-методическому материалу и закрепляют промежуточные знания.

Подготовка студента к зачету включает в себя три этапа:

- самостоятельная работа в течение семестра;
- непосредственная подготовка в дни, предшествующие зачету по темам курса;
- подготовка к ответу на вопросы.

При подготовке к зачету обучающимся целесообразно использовать материалы лекций, основную и дополнительную литературу.

На зачет выносится материал в объеме, предусмотренном рабочей программой учебной дисциплины за семестр. Зачет проводится в форме итогового теста в электронной оболочке.

На выполнение теста отводится 30 минут.

Результат зачета выражается оценками «зачтено», «н зачтено»

Для прохождения зачета обучающемуся необходимо иметь при себе зачетную книжку и письменные принадлежности.

За нарушение дисциплины и порядка обучающиеся могут быть удалены с зачета.

2. Планы практических занятий

Тема 1. Информационная безопасность и уровни ее обеспечения

Цель: работа с базовыми понятиями информационной безопасности и уровнями и уровнями ее обеспечения.

План

Информационные активы ИС предприятия.

Основные понятия дисциплины.

Составляющие информационной безопасности.

Субъекты информационных отношений.

Классификация данных по степени конфиденциальности.

Уровни обеспечения ИБ.

Классификация угроз ИБ.

Литература [1 с.7-30, 2 с.22-129]

Вопросы для самопроверки

1. Дайте понятие и классифицируйте угрозы информационной безопасности.
2. Дайте понятие и классифицируйте уязвимости информационных систем и технологий.
3. Каковы особенности обеспечения информационной безопасности в условиях функционирования в России глобальных сетей?

4. Перечислить цели и задачи обеспечения информационной безопасности в рамках конкретной предметной области.

5. Перечислить виды противников или «нарушителей» информационной безопасности. Приведите их классификацию.

6. Дайте понятие вирусов (разрушающих программных воздействий) и приведите их классификацию.

7. Какие существуют виды возможных нарушений безопасности информационной системы? Приведите примеры в рамках конкретной предметной области.

8. Перечислите базовые методы и средства противодействия и локализации угроз и уязвимостей. Каковы основные критерии выбора?

Задания для самостоятельной работы

Задание 1 Подготовить доклад по теме

Задание 2 Составить глоссарий по базовым понятиям

Тема 2. Основные нормативные документы в сфере обеспечения информационной безопасности.

Цель: ознакомиться с законодательными и нормативно-правовыми актами, регламентирующие вопросы информационной безопасности и защиты информации.

План

Стандартизация ИБ

Стандарт «Оранжевая книга»

Стандарт «ОК»

Рекомендации X.800

Отечественные организации, занимающиеся разработкой стандартов

Отечественные оценочные стандарты

Нормативная законодательная база.

Литература [1 с.12-30]

Задание для самостоятельной работы

Ознакомиться с представленными ниже законодательными документами и нормативно-правовыми актами: Провести краткое конспектирование основных статей документов, регламентирующих вопросы информационной безопасности и защиты информации. Сформировать словарь понятий данных в указанных документах.

Текст документов представлен в папке «Законодательство».

Конституция РФ

-статья 23

-статья 24

-статья 29

-статья 41

-статья 44

Доктрина информационной безопасности РФ

Гражданский Кодекс РФ

-глава 71.

Трудовой кодекс РФ.

-глава 14.

Уголовный Кодекс РФ

-статья 283.

-другие статьи, касающиеся правонарушений в информационной сфере

6.ФЗ «Об информации, информационных технологиях и защите информации»

7.ФЗ «О государственной тайне»

8.Указ Президента РФ от 30 ноября 1995 г. N 1203 "Об утверждении перечня сведений, отнесенных к государственной тайне" (с изменениями и дополнениями)

9.ФЗ «О коммерческой тайне»

Постановление Правительства РСФСР от 5 декабря 1991 г. N 35 "О перечне сведений, которые не могут составлять коммерческую тайну" (с изменениями и дополнениями)

10.ФЗ «О персональных данных»

11." Федеральный закон от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи" (с изменениями и дополнениями)

12. Указ Президента РФ от 17 марта 2008 г. N 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена" (с изменениями и дополнениями)

13.Указ Президента РФ от 22 мая 2015 г. N 260 "О некоторых вопросах информационной безопасности Российской Федерации"

14.Постановление Правительства РФ от 2 июня 2008 г. N 418 "О Министерстве связи и массовых коммуникаций Российской Федерации"

15.Указ Президента РФ от 16 августа 2004 г. N 1085 "Вопросы Федеральной службы по техническому и экспортному контролю"

16. Окинавская хартия глобального информационного общества (http://www.iis.ru/library/okinawa/charter.ru.html).

Тема 3. Информационная безопасность вычислительных сетей.

Цель: рассмотреть основные виды вирусов, дать анализ современных антивирусных программ, познакомиться с особенностями реализации аспектов информационной безопасности в компьютерных сетях.

План

Основы ИБ в компьютерных сетях

Удаленные атаки

Виды вирусов

Антивирусные программы

Литература [3 С14-28]

Задания для самостоятельной работы

Задние 1: Дать краткую характеристику основным видам вирусов.

Задание 2: Проанализировать возможности программ антивирусной защиты (5 программ). Результаты представить в виде таблицы:

Название	**Разработчик**	**Способ распространения**	**Режимы работы, функциональные возможности**	**Виды вирусов и ПО, с которыми антивирус борется**	**Примечание**

Задание 3: Дать краткую характеристику таким видам спама, как: вредоносные вложения и ссылки, фишинг. Проанализировать тематический состав спама. Привести примеры.

Задание 4: Дать краткие рекомендации по безопасной работе с электронной почтой по схеме:

порталы, предоставляющие услуги электронной почты,

требования к логину и паролю для создания и использования электронной почты,

предотвращение заражения компьютерными вирусами и проникновения на компьютер активного содержимого,

отказ в обслуживании или переполнение почтового ящика,

утечка конфиденциальной информации.

Задание 5: Дать краткие рекомендации по работе с электронными платежными терминалами и системами.

Тема 4. Криптографические методы защиты информации.

Цель: познакомиться с историй шифрования, освоить некоторые методы шифрования.

План

1. Основы криптографии
2.Основы шифрования
3. Метод Плейфера
4. Метод Цезаря
5. Кодирование информации по принципу «телефона»
6. Кодирование по методу Полибия

Литература [1 с.31-65]

Задание 1

Подобрать мультимедийный материал для оформления презентации по теме «История шифрования».

Задание 2

Закодировать понятие «информационная безопасность» по методу Плейфера. *Примечание*: определение термина взять из Интернета в любой трактовке с указанием источника данных.

Шифр Плейфера использует матрицу 5x5 (для латинского алфавита, для русского алфавита необходимо увеличить размер матрицы до 6x6), содержащую ключевое слово или фразу. Для создания матрицы и использования шифра достаточно запомнить ключевое слово и четыре простых правила. Чтобы составить ключевую матрицу, в первую очередь нужно заполнить пустые ячейки матрицы буквами ключевого слова (не записывая повторяющиеся символы), потом заполнить оставшиеся ячейки матрицы символами алфавита, не встречающимися в ключевом слове, по порядку (в английских текстах обычно опускается символ «Q», чтобы уменьшить алфавит, в других версиях «I» и «J» объединяются в одну ячейку). Ключевое слово может быть записано в верхней строке матрицы слева направо, либо по спирали из левого верхнего угла к центру. Ключевое слово, дополненное алфавитом составляет матрицу 5x5 и является ключом шифра.

Для того, чтобы зашифровать сообщение необходимо разбить его на биграммы (группы из двух символов), например «Hello World» становится «HE LL OW OR LD», и отыскать эти биграммы в таблице. Два символа биграммы соответствуют углам прямоугольника в ключевой матрице. Определяем положения углов этого прямоугольника относительно друг друга. Затем руководствуясь следующими 4 правилами зашифровываем пары символов исходного текста:

Если два символа биграммы совпадают, добавляем после первого символа «X», зашифровываем новую пару символов и продолжаем. В некоторых вариантах шифра Плейфера вместо «X» используется «Q».

Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки.

Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящимися непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца.

Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника.

Для расшифровки необходимо использовать инверсию этих четырёх правил, откидывая символы «X» (или «Q»), если они не несут смысла в исходном сообщении.

Используем ключ «playfair example», тогда матрица примет вид:

P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
J	K	N	O	S
T	U	V	W	Z

Зашифруем сообщение «Hide the gold in the tree stump»:
HI DE TH EG OL DI NT HE TR EX ES TU MP
Биграмма HI формирует прямоугольник, заменяем её на BM.
Биграмма DE расположена в одном столбце, заменяем её на ND.
Биграмма TH формирует прямоугольник, заменяем её на ZB.
Биграмма EG формирует прямоугольник, заменяем её на XD.
Биграмма OL формирует прямоугольник, заменяем её на KY.
Биграмма DI формирует прямоугольник, заменяем её на BE.
Биграмма NT формирует прямоугольник, заменяем её на JV.
Биграмма HE формирует прямоугольник, заменяем её на DM.
Биграмма TR формирует прямоугольник, заменяем её на UI.
Биграмма EX находится в одной строке, заменяем её на XM.
Биграмма ES формирует прямоугольник, заменяем её на MN.
Биграмма TU находится в одной строке, заменяем её на UV.
Биграмма MP формирует прямоугольник, заменяем её на IF.
Получаем зашифрованный текст «BM ND ZB XD KY BE JV DM UI XM MN UV IF».
Таким образом сообщение «Hide the gold in the tree stump» преобразуется в «BMNDZBXDKYBEJVDMUIXMMNUVIF»

Задание 3

Выполнить кодирование информацию по принципу «телефона». Простейшая система этого шифра заключается в том, что азбука разбивается на группы с равным числом букв и каждая из них обозначается двумя цифрами. Первая цифра обозначает группу, а вторая – порядковый номер буквы в этой группе.

АБВГ	ДЕЖЗ	ИКЛМ	НОПР	СТУФ	ХЦЧШ	ЩЫЮЯ
1	2	3	4	5	6	7

Зашифрованные слова, например «документ», будут выглядеть следующим образом:
21 42 32 53 34 22 41 52

Задание 4

Выполнить кодирование информации по принципу шифра Цезаря (шифр замены со смещением алфавита на n символов).

Шифр Цезаря, также известный, как шифр сдвига, код Цезаря или сдвиг Цезаря — один из самых простых и наиболее широко известных методов шифрования.

Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций

левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.

Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами.

Шаг шифрования, выполняемый шифром Цезаря, часто включается как часть более сложных схем, таких как шифр Виженера.

Тема 5. Технологии и методы построения защищенных информационных систем

Цель: коллективно разработать концепцию информационной безопасности для выбранной предметной области.

План

Защита информации: определение, классификация и характеристика основных методов и средств; практика применения, специфика использования (по областям применения).

Основные технологии построения защищенных ИС.

Использование защищенных компьютерных систем.

Гарантированно защищенные информационные системы.

Политика информационной безопасности.

Профиль защиты.

Задание по безопасности.

Риски информационной безопасности

Литература[3 с.28-42]

Задание для самостоятельной работы

Задание 1

Необходимо разбиться на группы по 3-4 человека. Каждая группа выбирает сферу деятельности из представленного ниже списка:

- производство высокотехнологичных товаров,
- рекламное агентство,
- разработка программного обеспечения,
- банк,
- университет
- предметная область по согласованию с преподавателем.

Необходимо:

- придумать название выбранной организации, ее миссию, положение на рынке, основные задачи;
- описать особенности выбранной организации в трех-четырех абзацах;
- распределить между собой роли, соответствующие организационной структуре выбранной организации (директор предприятия, начальник ИТ-отдела, директор охраны, администратор сети и т.д.);
- сформировать документ "Концепция информационной безопасности" выбранной организации (каждый участник группы отвечает за раздел политики безопасности, соответствующий своей роли);

Результаты работы предоставить в виде отчета. Оценка задания будет включать как индивидуальную оценку каждого участника, так и групповую (полнота и согласованность).

Задание 2

Сравнить методики оценки рисков информационной безопасности.