МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Заведующий кафедрой
информационной безопасности
(наименование ф-та полностью)
М.О. Таныгин
(подпись, инициалы, фамилия)
« *29* » *августа* 2022 г.

ОЦЕНОЧНЫЕ СРЕДСТВА
для текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Введение в специальность и планирование профессиональной карьеры
(наименование учебной дисциплины)

10.05.02 Информационная безопасность телекоммуникационных систем, направленность (профиль) «Управление безопасностью телекоммуникационных систем и сетей»
(код и наименование ОПОП ВО)

2022

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ

Тема 1. Основы информационной безопасности

1. Определение информационной безопасности.
2. Определение защиты информации.
3. Угрозы информационной безопасности.
4. Информационное оружие.
5. Направления национальной безопасности.
6. Меры для защиты субъектов информационных отношений.

Тема 2. Основные понятия информационной безопасности. Стандартизация

1. Определение информации.
2. Характеристики защиты информации.
3. Системный подход.
4. Параметры системы защиты информации.
5. Свойства информации.
6. Права доступа.
7. Стандарт, стандартизация.
8. Группы стандартов и спецификаций в области ИБ.

Тема 3. Показатели информации. Комплексность системы защиты информации

1. Показатели качества информации.
2. Перечислите виды защиты информации.
3. Принцип комплексности.
4. Целевая комплексность.
5. Требования к КСИБ.

Тема 4. Технические средства защиты информации

1. Задача технических средств защиты информации.
2. Определение показателя качества речевой информации.
3. Назовите способы защиты информации.
4. Пассивное техническое средство защиты
5. Назначение экранирования

6. Активное техническое средство защиты

Тема 5. Роль специалиста в области информационной безопасности.

1. Роль специалиста в области информационной безопасности.
2. Самые оцениваемые тематики.

Тема 6. Стратегия и практика развития компетенций

1. Виды практик развития компетенций.
2. Отраслевой подход
3. Подход специализации

Тема 7. Введение в планирование карьеры

1. Определение карьеры.
2. Типы карьеры.
3. Планирование карьеры.
4. Перечислите этапы карьеры.

Тема 8. Модели успешного профессионального поведения

1. Определение компетенции и компетентности.
2. Базовые профессиональные навыки.
3. Базовые профессиональные компетенции.
4. Уровень эффективности работы.

Тема 9. Технология целеполагания

1. Первоначальная стадия.
2. Перечислите принципы постановки карьерных целей.
3. Назовите принципы карьерной стратегии.
4. Правила карьерной стратегии.

Критерии оценки:

- 2 балла по шкале БРС выставляется обучающемуся, если даны точные ответы, демонстрируется знание дополнительной литературы и материала, не раскрытого на лекции;

- 1 балла по шкале БРС выставляется обучающемуся, если имеется знание терминов и понятий, понимаются основные взаимосвязи процессов и явлений;

- 0 балла по шкале БРС выставляется обучающемуся, отсутствует знание базовых терминов и понятий, отсутствие понимания взаимосвязи понятий.

1.2 ЗАДАНИЯ К ПРАКТИЧЕСКОМУ ЗАНЯТИЮ

Тема 1

Задание №1

Какие меры должен в себя включать комплексный подход к обеспечению информационной безопасности?

1) законодательные

2) социальные

3) административные

4) процедурные

5) научно-технические

6) моральные

Задание№2

К какому уровню обеспечения ИБ относится «Доктрина информационной безопасности Российской Федерации»?

1) законодательный

2) административный

3) процедурный

4) научно-технический

Задание№3

В организации проводятся проверки «чистый стол», целью которых является выявление нарушений требований по хранению ключевых носителей и конфиденциальных документов. К какому уровню обеспечения ИБ они относятся?

1) законодательный

2) административный

3) процедурный

4) научно-технический

Задание№4

Какой термин определяет защищенность информации, ресурсов и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений — производителям, владельцам пользователям информации и поддерживающей инфраструктуре?

1) стратегическая безопасность

2) информационная безопасность

3) экономическая безопасность

4) корпоративная безопасность

Тема 2

Задание№1

Как называется подтверждение соответствия объектов требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров?

1) аттестация

2) аккредитация

3) сертификация

4) лицензирование

Задание№2

Какие участники системы сертификации должны проходить обязательную аккредитацию на право проведения работ по сертификации?

1) федеральный орган по сертификации

2) центральный орган системы сертификации

3) органы по сертификации средств защиты информации

4) испытательные лаборатории

5) изготовители

Задание№3

Какой участник системы сертификации ведет государственный реестр участников сертификации и сертифицированных средств защиты информации?

1) федеральный орган по сертификации

2) центральный орган системы сертификации

3) орган по сертификации средств защиты информации

4) испытательная лаборатория

5) изготовитель

Задание№4

Какой участник системы сертификации проводит сертификационные испытания средств защиты информации и по их результатам оформляют заключения и протоколы?

1) федеральный орган по сертификации

2) центральный орган системы сертификации

3) орган по сертификации средств защиты информации

4) испытательная лаборатория

5) изготовитель

Тема 3

Задание№1

До начала обработки персональных данных оператор обязан:

1) получить письменное согласие субъекта персональных данных

2) получить устное согласие субъекта персональных данных

3) уведомить регулятора о своем намерении в письменной форме

4) уведомить регулятора о своем намерении в устной форме

Задание№2

Если в результате несанкционированного доступа персональные данные были уничтожены, оператор обязан:

1) уведомить об этом регулятора

2) уведомить об этом субъекта персональных данных

3) немедленно восстановить персональные данные

4) произвести перенастройку средств защиты информации

Задание№3

Обязанность по обеспечению безопасности персональных данных при их обработке полностью возлагается на:

1) субъекта персональных данных

2) оператора персональных данных

3) доверенное лицо

4) администратора безопасности информационной системы персональных данных

Тема 4

Задание№1

К составляющим компетенции не относится:
1) руководство
2) управление человеческими ресурсами
3) лидерство
4) обязанности

Задание№2
Профессиональная компетенция не включает в себя:
1) функциональную компетентность
2) интеллектуальную компетентность
3) сознательную компетентность
4) социальную компетентность

Задание№3
В структуре профессиональной компетенции к элементам квалификации не относят:
1) поведение
2) знания
3) умения
4) навыки

Заданиее№4
Не существует вида компетенции
1) индивидуальна;
2) корпоративная
3) ключевая
4) смешанная

Тема 5

Задание№1

Какой этап не включается в управление планированием карьеры -:

1) обучение нового сотрудника

2) разработка плана развития карьеры

3) увольнение работника

4) реализация плана развития карьеры

Задание№2

От чего не зависит реализация плана развития карьеры:

1) профессионального и индивидуального развития

2) эффективного партнерства с руководителем

3) заметного положения в организации

4) погодных условий

Задание№3

От 25 до 30 лет длится какой этап карьеры:

1) предварительный

2) этап продвижения

3) этап становления

4) этап сохранения

Тема 6

Задание№1

Планируя работу по профессиональному развитию молодых специалистов, следует отдать предпочтение …

1) групповым методам обучения
2) индивидуальным методам обучения
3) самообучению

Задание№2

Изменение должностного статуса человека, его социальной роли, увеличение степени и пространства должностного авторитета называется …

1) деловой карьерой
2) должностным ростом
3) профессиональным ростом
4) повышением

Задание№3
… карьера предполагает чередование вертикального и горизонтального роста
1) Вертикальная
2) Горизонтальная
3) Ступенчатая
4) Скрытая
Задание№4
… карьера, предполагает переход в другую функциональную область, расширение полномочий в рамках того же уровня структурной иерархии
1) Вертикальная
2) Горизонтальная
3) Ступенчатая
4) Скрытая

Тема 7
Задание№1
В число основных понятий ролевого управления доступом входит:
1) объект
2) субъект
3) метод

Задание№2
В число направлений повседневной деятельности на процедурном уровне входят:
1) ситуационное управление;
2) конфигурационное управление
3) оптимальное управление

Задание№3
В число универсальных сервисов безопасности входят:
1) средства построения виртуальных локальных сетей;
2) экранирование;
3) протоколирование и аудит

Тема 8

Задание№1

Планируя работу по профессиональному развитию молодых специалистов, следует отдать предпочтение …
1) групповым методам обучения
2) индивидуальным методам обучения
3) самообучению

Задание№2
Изменение должностного статуса человека, его социальной роли, увеличение степени и пространства должностного авторитета называется …
1) деловой карьерой
2) должностным ростом
3) профессиональным ростом
4) повышением

Задание№3
… карьера предполагает чередование вертикального и горизонтального роста
1) Вертикальная
2) Горизонтальная
3) Ступенчатая
4) Скрытая
Задание№4
… карьера, предполагает переход в другую функциональную область, расширение полномочий в рамках того же уровня структурной иерархии
1) Вертикальная
2) Горизонтальная
3) Ступенчатая
4) Скрытая

Тема 9

Задание№1

До начала обработки персональных данных оператор обязан:

1) получить письменное согласие субъекта персональных данных

2) получить устное согласие субъекта персональных данных

3) уведомить регулятора о своем намерении в письменной форме

4) уведомить регулятора о своем намерении в устной форме

Задание№2

Если в результате несанкционированного доступа персональные данные были уничтожены, оператор обязан:

1) уведомить об этом регулятора

2) уведомить об этом субъекта персональных данных

3) немедленно восстановить персональные данные

4) произвести перенастройку средств защиты информации

Задание№3

Обязанность по обеспечению безопасности персональных данных при их обработке полностью возлагается на:

1) субъекта персональных данных

2) оператора персональных данных

3) доверенное лицо

4) администратора безопасности информационной системы персональных данных

Критерии оценки:

3 балла (или оценка «отлично») выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

2 балла (или оценка «хорошо») выставляется обучающемуся, если он владеет содержанием вопроса, но допускает некоторые недочеты при ответе; допускает незначительные неточности при определении основных понятий; недостаточно аргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свой ответ типовыми примерами.

1 балл (или оценка «удовлетворительно») выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов (или оценка «неудовлетворительно») выставляется обучающемуся, если он не владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основные определения; не может привести или приводит неправильные примеры; не отвечает на уточняющие

и (или) дополнительные вопросы преподавателя или допускает при ответе на них грубые ошибки

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

2.1 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ

Задания в закрытой форме

1. Информационное оружие – это:
1) комплекс мероприятий, направленных на обеспечение важнейших аспектов информационной безопасности: целостности, доступности и, если нужно, конфиденциальности информации, используемых для ввода, хранения, обработки и передачи данных
2) процесс сбора, накопления, обработки, хранения, распределения и поиска информации
преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа

2.Под информационной безопасностью понимается:
1) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуре
2) охрана персональных данных, государственной служебной и других видов информации ограниченного доступа
3) набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных

3.К направлениям национальной безопасности не относится:
1) экономическая
2) оборонная
3) юридическая

4.Законы, нормативные акты, стандарты относятся к мерам защиты субъектов информационных отношений:
1) административным
2) законодательным
процедурным

5.Качество передачи сигналов передачи данных оцениваются
1) искажениями формы сигналов

2) отсутствием искажения в принятой информации
3) числом ошибок в принятой информации, т.е. верностью передачи.

6. Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления - это
1) данные
2) информация
3) знания

7. Угроза безопасности – это:
1) совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации
2) нарушение целостности информации
комплекс мероприятий, проводимых для взлома информации

8. К параметрам системы защиты информации не относится:
1) входы и выходы системы
2) процессы внутри системы, занимающиеся преобразованием информации
цели и задачи

9.К важным свойствам информации относится:
1) полезность
2) доступность
новизна

10.Конфиденциальность информации – это:
1) действия, проводимые с целью закрытия доступа к информации субъектов, не имеющих на это право
2) состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право
состояние информации, при котором доступ к ней субъектами, не имеющими на это права, осуществляется лишь в некоторых случаях

11. Состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно?
1) допустимость
2) доступность
3) целостность

12.К этапам карьеры не относится:
1) становление
2) начальный
3) пенсионный

13. Тип карьеры, характеризующийся пожизненной занятостью на единственной работе?
1) регулярная карьера
2) постоянная карьера
устойчивая карьера

14. К траектории движения человека в организации относится:
1) диагональная карьера.
2) центростремительная карьера;
3) восходящая карьера;

15.Какой возраст относится к этапу «сохранения» карьеры:
1) до 60 лет;
2) до 40 лет;
до 70 лет.

16. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
1. а) Сотрудники
2. б) Хакеры
3. в) Атакующие
4. г) Контрагенты (лица, работающие по договору)

17. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
1) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
2) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
3) Улучшить контроль за безопасностью этой информации
4) Снизить уровень классификации этой информации

18. Что самое главное должно продумать руководство при классификации данных?
1) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
2) Необходимый уровень доступности, целостности и конфиденциальности
3) Оценить уровень риска и отменить контрмеры
4) Управление доступом, которое должно защищать данных

19. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
1) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски

2) Когда риски не могут быть приняты во внимание по политическим соображениям
3) Когда необходимые защитные меры слишком сложны
4) Когда стоимость контрмер превышает ценность актива и потенциальные потери

20. Эффективная программа безопасности требует сбалансированного
1) Технических и нетехнических методов
2) Контрмер и защитных механизмов
3) Физической безопасности и технических средств защиты
4) Процедур безопасности и шифрования

21. Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?
1) Много информации нужно собрать и ввести в программу
2) Руководство должно одобрить создание группы
3) Анализ рисков не может быть автоматизирован, что связано с самой природой оценки
4) Множество людей должно одобрить данные

22. Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?
Варианты ответа:
1) Много информации нужно собрать и ввести в программу
2) Руководство должно одобрить создание группы
3) Анализ рисков не может быть автоматизирован, что связано с самой природой оценки
4) Множество людей должно одобрить данные

23. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?
1) Список стандартов, процедур и политик для разработки программы безопасности
2) Текущая версия ISO 17799
3) Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
4) Открытый стандарт, определяющий цели контроля

24. Из каких четырех доменов состоит CobiT?
1) Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
2) Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

3) Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка
4) Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

25. Что представляет собой стандарт ISO/IEC 27799?
1) Стандарт по защите персональных данных о здоровье
2) Новая версия BS 17799
3) Определения для новой серии ISO 27000
4) Новая версия NIST 800-60

26. CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO?
1) COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам
2) COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень
3) COSO учитывает корпоративную культуру и разработку политик
4) COSO – это система отказоустойчивости

27.Что лучше всего описывает цель расчета ALE:
1)количественно оценить уровень безопасности среды
2)оценить потенциальные потери от угрозы в год
3) количественно оценить уровень безопасности среды

28. К конфиденциальной информации относятся документы, содержащие
1) государственную тайну
2) законодательные акты
3) "ноу-хау"
4) сведения о золотом запасе страны

29. Запрещено относить к информации ограниченного доступа
1) информацию о чрезвычайных ситуациях
2) информацию о деятельности органов государственной власти
3) документы открытых архивов и библиотек
4) все, перечисленное в остальных пунктах

30. К конфиденциальной информации не относится
1) коммерческая тайна
2) персональные данные о гражданах
3) государственная тайна
4) "ноу-хау"

31. Для успешной реализации концепции комплексной защиты при построении автоматизированной системы ...

1) необходимо создать нескольких последовательных зон безопасности, чтобы наиболее важная зона безопасности объекта находилась внутри других зон
2) следует установить некоторый приемлемый уровень безопасности без попыток создать абсолютную защиту
3) должны быть разработаны и регулярно использоваться все необходимые механизмы гарантированного обеспечения требуемого уровня защищенности информации
4) требуется предварительное ранжирование угроз по степени их важности с точки зрения влияния на технико-экономические показатели

32. Исходным пунктом проектирования систем защиты информации является ...
1) формирование требований к защите информации
2) определение значений важнейших параметров защищаемой информации
3) построение математической модели системы защиты
4) разработка процедур оперативного реагирования на непредвиденные ситуации

33. Для долгосрочного управления комплексной системой защиты характерно ...
1) использование только средств защиты, которые включены в состав системы защиты информации и находятся в работоспособном состоянии
2) большое внимание развитию и совершенствованию концепции защиты
3) преобладание процедур оперативного реагирования в случае возникновения непредвиденных ситуаций над иными процедурами управления
4) отсутствие изменений в архитектуре средств защиты и автоматизированной системы

34. Непрерывное слежение за функционированием механизмов защиты относится к показателям
1) планирования управлением защиты
2) календарно-планового руководства защитой информации
3) обеспечения повседневной деятельности средств защиты
4) оперативно-диспетчерского управления

35. Имеет целью организацию и обеспечение выполнения плановых мероприятий по защите информации
1) планирование управлением защиты
2) календарно-плановое руководство защитой информации
3) обеспечение повседневной деятельности средств защиты
4) оперативно-диспетчерское управление

36. Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?
1) Анализ связующего дерева
2) AS/NZS
3) NIST
4) Анализ сбоев и дефектов

37. Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?
1) Безопасная OECD
2) ISOIEC
3) OECD

38. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:
1) гаммирования
2) подстановки
3) кодирования
4) перестановки
5) аналитических преобразований

39. Защита информации от утечки- это деятельность по предотвращению:
1) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации
2) воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации
3) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений
4) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа
5) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации

40. Икусственные угрозы безопасности информации вызваны:
1) деятельностью человека
2) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения
3) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека

4) корыстными устремлениями злоумышленников
5) ошибками при действиях персонала

41. К основным непреднамеренным искусственным угрозам АСОИ относится:
1) физическое разрушение системы путем взрыва, поджога и т.п.
2) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи
3) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.
4) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств
5) неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы

42. Антивирус запоминает исходное состояние программ, каталогов и системных областей диска когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным:
1) детектор
2) доктор
3) сканер
4) ревизор
5) сторож

43. Антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов:
1) детектор
2) доктор
3) сканер
4) ревизор
5) сторож

44. Активный перехват информации - это перехват, который:
1) заключается в установке подслушивающего устройства в аппаратуру средств обработки информации
2) основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций
3) неправомерно использует технологические отходы информационного процесса
4) осуществляется путем использования оптической техники
5) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера

45. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:
1) активный перехват
2) пассивный перехват
3) аудиоперехват
4) видеоперехват
5) просмотр мусора.

46. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:
1) активный перехват
2) пассивный перехват
3) аудиоперехват
4) видеоперехват

47. Перехват, который осуществляется путем использования оптической техники называется:
1) активный перехват
2) пассивный перехват
3) аудиоперехват
4) видеоперехват
5) просмотр мусора.

48. К внутренним нарушителям информационной безопасности относится:
1) клиенты
2) пользователи системы
3) посетители
4) любые лица, находящиеся внутри контролируемой территории
5) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации
6) персонал, обслуживающий технические средства
7) сотрудники отделов разработки и сопровождения ПО
8) технический персонал, обслуживающий здание

Задания в открытой форме

1. Защита информации – это…
2. Информационное оружие – это…
3. Планирование карьеры- это…
4. Базовые профессиональные компетенции включают в себя…
5. Принципами карьерной стратегии являются…
6. Информация- это…
7. Защита информации характеризуется…
8. Угрозами информационной безопасности являются…

9. Параметрами системы защиты информации являются…
10. Конфиденциальность информации-это…
11. Показателями качества информации являются…
12. Устойчивость информации отражает…
13. Задачей технических средств защиты является…
14. Пассивное техническое средство защиты- это…
15. К активным техническим средствам защиты относятся…
16. Вакансии для молодых специалистов постоянно открывают…
17. Карьера-это…
18. Устойчивая карьера-это…
19. К этапам карьеры можно отнести…
20. Компетенции-это…

Задания на установление соответствия

1. Между основами информационной безопасности и понятиями

	Информационная безопасность-это	А	комплекс мероприятий, направленных на обеспечение важнейших аспектов информационной безопасности: целостности, доступности и, если нужно, конфиденциальности информации, используемых для ввода, хранения, обработки и передачи данных.
2	Защита информации-это	Б	это оборотная сторона использования информационных технологий.
3	Угрозы информационной безопасности-это…	В	средства уничтожения, искажения или хищения информационных массивов, добывание из них необходимой информации после

			преодоления системы защиты, ограничения или воспрещения доступа к ним законных пользователей, дезорганизации работы технических средств, вывода из строя телекоммуникационных сетей, компьютерных систем, всех средств высокотехнологического обеспечения жизни общества и функционирования государства.
4	Информационное оружие-это…	Г	защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуре.

2. Между формами адекватности информации и понятиями

1	Синтаксическая адекватность	А	Эта форма определяет степень соответствия образа объекта и самого объекта
2	Семантическая (смысловая) адекватность	Б	отражает отношение информации и ее потребителя, соответствие информации цели

			управления, которая на ее основе реализуется.
3	Прагматическая (потребительская) адекватность	В	отображает формально-структурные характеристики информации и не затрагивает ее смыслового содержания.

3. Показателями информации и понятиями

1.	Достаточность информации	А	определяется степенью близости получаемой информации к реальному состоянию объекта, процесса, явления и т.п.
2.	Актуальность информации	Б	содержит минимальный, но достаточный для принятия правильного решения состав (набор показателей)
3.	Точность информации	В	определяется ее свойством отражать реально существующие объекты с необходимой точностью
4.	Достоверность информации	Г	определяется степенью сохранения ценности информации для управления в момент ее использования и зависит от динамики изменения ее характеристик и от интервала времени, прошедшего с момента возникновения данной информации.

4.Между принципами комплексности и понятиями

1.	Структурная комплексность	А	подразумевает интеграцию всех видов и направлений информационной безопасности для достижения поставленных целей.
1.	Функциональная комплексность	Б	предполагает обеспечение требуемого уровня защиты во всех элементах системы обработки информации.
3.	Временная комплексность	В	означает, что защита информации должна быть направлена на все выполняемые информационной системой функции.
4.	Инструментальная комплексность	Г	предполагает непрерывность осуществления мероприятий защиты информации на всех этапах жизненного цикла информационной системы.

5. Между практиками развития компетенция и понятиями

1	Производственная практика –это	А	добровольная безвозмездная деятельность на благо общества и отдельных граждан.
2.	Волонтерство -это	Б.	это способ заработка, который позволяет сотрудничать с разными работодателями (даже одновременно!) без постоянного

			трудоустройства в какой-либо организации
3.	Фриланс-это	В.	важная составляющего учебного процесса, позволяющая сориентироваться на рынке труда и найти себя в будущей профессии

6. Между типами карьеры и понятиями

1.	Профессиональная карьера- это	А	тип карьеры, при котором люди остаются в определенной отрасли и прокладывают путь с более низких на более высокие должности в одной или нескольких организациях
2.	Линейная карьера-это	Б	тип карьеры, при котором люди проходят через ряд профессий, каждая из которых строится на уже приобретенных навыках и умениях, но требует и новых навыков
3.	Спиральная карьера-это	В	тип карьеры, для которого характерно смена многих видов профессиональной деятельности, не связанных друг с другом.
4.	Переменчивая карьера-это	Г	рост знаний, умений, навыков.

7. Между этапами карьеры и понятиями

1.	Предварительный 9 до 25 лет) -	А	пик совершенствования квалификации
2.	«Становления» (до 30 лет) -	Б	Смена деятельности
3.	«Сохранения» (до 60 лет)-	В	обучение и поиск сферы деятельности
4.	«Пенсионный» (после 65 лет) -	Г	освоение выбранной профессии и приобретение специфических навыков и знаний

8. Между определениями методов успешного профессионального поведения и понятиями

1.	Компетенция - это	А	профессиональные навыки человека
2.	Компетентность- это	Б	особенности поведения, которые определяют результативность работы.
3.	Базовые профессиональные навыки-это	В	устойчивые формы поведения, которые помогают человеку на занимаемой им позиции качественно и эффективно достигать поставленных перед ним целей.

9. Между индивидуальными качествами человека и понятиями

1.	Коммуникативные навыки- это	А	совокупность сведений и познаний, а также осведомленность в определенной сфере деятельности, необходимые для качественного исполнения должностных обязанностей с целью достижения результатов в профессиональной служебной деятельности
2.	Психофизические особенности - это	Б	основания идеологического, морального, политического или эстетического характера, которые нужны человеку для того, чтобы оценить социальные события или объекты.
3.	Ценностные ориентации- это	В	способность общения, взаимодействие людей друг с другом.
4.	Теоретические и профессиональные знания -	Г	это особенности его психики, развитие, строение организма, состояние здоровья.

10. Между принципами постановки карьеры и целей

1	Привлекательность	А	цель должна быть формализована и предполагать критерии оценки ее достижения
2	Реальность	Б	цель должна соответствовать личным интересам, ценностям,

			установкам, представ-лениям.
3	Прогрессивность	В	цели должны касаться профессионального продвижения и развития способностей к исполнению ближайшей профессиональной роли или функции.
4	Возможность оценки результативности	Г	каждая из последующих подцелей должна предполагать наращивание способностей и возможностей

11. Между принципами карьерной стратегии и характеристиками

1.	Принцип осмысленности	А	Гибкость в построении линии карьерного движения.
2.	Принцип маневренности	Б	Любое карьерное действие должно быть целесообразным, осуществляться сообразно целям, индивидуальным и общим.
3.	Принцип соразмерности	В	Необходима презентация ваших успехов. Они должны быть замечены и оценены по достоинству.
4.	Принцип заметности	Г	Нужно двигаться в группе, не отставая, но и не вырываясь далеко вперед.

12. Между свойствами информации и понятиями

1	Целостность информации- это	А	состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право
2	Конфиденциальность информации- это	Б	состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно
3	Доступность информации- это	В	состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право

13. Между принципами информационной безопасности и понятиями

1.	Оператор системы информации - это	А	автор информации или тот, кому ее передали на законных основаниях.
2.	Обладающий информацией - это	Б	действие, которое подготовил, спланировал и осуществил злоумышленник, чтобы найти уязвимое место в сети. Завершиться атака может угрозой безопасности информации
3.	Атака на компьютеры, объединенные в одну систему - это	В	физическое или юридическое лицо, обеспечивающее применение данных, их обработку, но только если

			сведения указаны в базах данных.

14. Между спецификой ИБ и понятием

1.	Пентестеры —	А	они ищут возможные потенциальные и известные уязвимости в аппаратных и сетевых комплексах. Проще говоря, знают, как с помощью Windows, Linux или других систем злоумышленник может попасть в ваш компьютер и установить нужное ПО. Могут как найти возможность взлома, так и создать систему, в которую будет сложно попасть.
2.	Специалисты по разработке-	Б	называемые «белые», или «этичные» хакеры. Они не взламывают ресурсы бизнеса незаконно. Вместо этого они работают на компании и ищут уязвимости, которые потом исправляют разработчики. Бывает, такие люди трудятся на окладе, или участвуют в программах Bug Bounty — когда бизнес просит проверить их защиту, обещая за найденные баги премию
3.	Специалисты по сетям-	В	такие специалисты участвуют создании приложений и программ. Проще говоря, изучают архитектуру и готовый код и подсказывают, что здесь может быть ошибка или «форточка» для взлома. Банальный пример — оставить в форме ввода сайта

			возможность отправить SQL-инъекцию

15. Между видами карьерного роста и понятиями

1.	Вертикальный карьерный рост	А	Человек получает профессиональные и «мягкие» навыки, которые нужны разработчику, и детально разберётся во всех нюансах веб-разработки.
2.	Горизонтальный карьерный рост	Б	Человек приходит на работу стажёром, а через несколько лет становится руководителем отдела. В этом варианте развития специалист проходит несколько ступеней. В корпоративном мире их называют грейдами.
3.	Смешанный карьерный рост-	В	более гибкий вариант развития карьеры. Он не означает, что специалист обязательно станет руководителем или останется в той же профессии, где начинал карьеру.

16. Между основными подходами изучения компетенций и понятиями

1	Ресурсный подход-	А	это подход, акцентирующий внимание на результате

			образования, причем в качестве результата рассматривается не сумма усвоенной информации, а способность человека действовать в различных проблемных ситуациях. Набор этих ситуаций зависит от типа (специфики) образовательного учреждения: общего или профессионального образования, начального, среднего или высшего, какого именно профессионального образования
2	Компетентностный подход-	Б	подход, где в центре внимания психолога находится человеческое поведение, действия и результаты наших действий, все внешнее, видимое и объективное
3	Поведенческий подход-	В	это новая парадигма корпоративной стратегии, который возник как помощь компаниям в достижении большей конкурентоспособности в постоянно меняющейся, глобализирующейся в деловой среде XXI века. Этот подход рассматривает компетенцию управленческого персонала (знания, навыки, способности) как источник конкурентного преимущества компании. Взаимосвязь между

			компетенциями управленческого персонала как стратегического ресурса и самой стратегией может быть выявлена на различных уровнях.

17. Видами угроз ИБ и понятиями

1	Техногенные-	А	так называемый «человеческий фактор». Пользователь может допустить непреднамеренные действия (например, случайно отключить антивирус) и специальные (совершить информационное преступление — например, взломать систему доступа).
2	Антропогенные-	Б	Эти проблемы трудно предвидеть и почти невозможно предотвратить. К ним относятся стихийные бедствия и сопутствующие им явления (землетрясения, пожары, подтопления).
3	Стихийные-	В	это угрозы, вызванные уязвимостями в техническом обеспечении и защитных инструментах. Их сложно спрогнозировать

18. Между средствами защиты и понятиями

1	Физические средства защиты-	А	это простые и системные, комплексные программы, предназначенные для решения частных и комплексных задач, связанных с обеспечением ИБ. Примером комплексных решений служат DLP-системы и SIEM-системы: первые служат для предотвращения утечки, переформатирования информации и перенаправления информационных потоков, вторые – обеспечивают защиту от инцидентов в сфере информационной безопасности.
2	Аппаратные средства защиты-	Б	это механические, электрические, электронные механизмы, которые функционируют независимо от информационных систем и создают препятствия для доступа к ним. Замки, в том числе электронные, экраны, жалюзи призваны создавать препятствия для контакта дестабилизирующих факторов с системами.
3	Программные средства-	В	это электрические, электронные, оптические, лазерные и другие устройства, которые встраиваются в

			информационные и телекоммуникационные системы.

19. Между основными видами конфиденциальной информации и понятиями

1	Персональные данные-	А	внутренняя информация о работе компании: технологиях, методах управления, клиентской базе. Если эти данные станут известны посторонним, компания может потерять прибыль.
2	Коммерческая тайна-	Б	сюда относят военные сведения, данные разведки, информацию о состоянии экономики, науки и техники государства, его внешней политики. Эти данные самые конфиденциальные — к безопасности информационных систем, в которых хранится такая информация, предъявляют самые строгие требования.
3	Государственная тайна-	В	информация о конкретном человеке: ФИО, паспортные данные, номер телефона, физиологические особенности, семейное положение и другие данные
4	Служебная тайна-	Г	информация, которая известна отдельным службам, например,

			налоговой или ЗАГСу. Эти данные обычно хранят государственные органы, они отвечают за их защиту и предоставляют только по запросу.

20. Между видами информационной технологии и понятиями

1	Объект информатизации-	А	улучшение качества жизни людей за счет увеличения производительности и облегчения условий их труда.
2	Цель информатизации-	Б	это идеи человечества и указания по их реализации, накопленные в форме, позволяющей их воспроизводство.
3	Информационная технология-	В	средства и системы информатизации, технические средства приема, передачи и обработки информации, помещения, в которых они установлены, а также помещения, предназначенные для проведения служебных совещаний, заседаний и переговоров.
4	Информационные ресурсы-	Г	это совокупность методов и устройств, используемых людьми для обработки информации.

Задания на установление правильной последовательности

1. Расположить этапы КСЗИ:

1. Разработка «Технического задания на создание КСЗИ»
2. Подготовка организационно-распорядительной документации
3. Разработка «Плана защиты информации».
4. Обследование информационной инфраструктуры Заказчика.

2. Расположить этапы стадии создания системы защиты информации:

1. Внедрение системы защиты информации (этап установки, настройки, испытаний).
2. Формирование требований к системе защиты информации (предпроектный этап)
3. Подтверждение соответствия системы защиты информации (этап оценки).
4. Разработка системы защиты информации (этап проектирования).

3. Установить порядок проведения аттестации информационных систем по требованиям безопасности информации:

1. Оформление, регистрация и выдача аттестата соответствия

2. Разработка программы и методики аттестационных испытаний
3. Подача и рассмотрение заявки на аттестацию
4. Проведение аттестационных испытаний объекта
5. Предварительное ознакомление с аттестуемым объектом (при необходимости)

4. Установить порядок уровня развития компетенций:

1. Разработка программы обучения
2. Составление модели компетенций
3. Оценка уровня навыков

5. Установить этапы процесса технологии целеполагания:

1. Выбор методик целеполагания
2. Переход к составлению пошагового плана достижения цели и его
3. Определение потребностей и мотивов

6. Расположить этапы планирования развития карьеры:

1. Постановка целей в личной и профессиональной жизни
2. Периодическая оценка эффективности
3. Оценка себя и выявление областей силы и способностей

4. Планирование действий по достижению целей.
5. Найти карьерные возможности, которые соответствуют вашим сильным сторонам

7. Установить этапы формирования требований к системе защиты информации:

1. Классификация объекта по требованиям защиты информации (установление уровня защищенности обрабатываемой информации)
2. Классификация объекта по требованиям защиты информации (установление уровня защищенности обрабатываемой информации)
3. Принятие решения о необходимости защиты обрабатываемой информации
4. Определение требований к системе защиты информации

8. Расположить план реализации (внедрение и функционирование) системы обеспечения информационной безопасности:

1. Внедрить выбранные меры управления
2. Реализовать план обработки рисков
3. Реализовать программы по обучению и повышению квалификации сотрудников
4. Разработать план обработки рисков
5. Определить способ измерения результативности

9. Расположить стадии идентификации:

1. Сравнительное исследование
2. Формулирование вывода о тождестве или различии объектов
3. Раздельное исследование
4. Оценка результатов сравнения

10. Расположить стадии профессионального личного роста:

1. Стадия выяснения
2. Стадия профессиональной адаптации
3. Стадия роста
4. Стадия развития профессионализма
5. Стадия профессиональной стабилизации

11. Установить процесс грамотной защиты от несанкционированного доступа:

1. Оценить возможности передачи информации между пользователями
2. Отсортировать и разбить информацию на классы
3. Определить уровни допуска к данным для пользователей

12. Расположите опции защиты программы от несанкционированного доступа:

1. контроль допуска к информации для пользователей разных уровней
2. обнаружение и регистрация попыток НСД
3. аутентификация и идентификация при входе в систему
4. обеспечение безопасности во время профилактических или ремонтных работ

13. Установите порядок защиты беспроводных сетей:

1. Создание сложного пароля
2. Использование протокола WPA/WPA2
3. Отключение показа наименования подключения

14. Установите последовательность процесса анализа угроз информации:

1. Зону риска;
2. Степень ущерба от его реализации
3. Гипотетическую фигуру злоумышленника
4. Источник риска;
5. Вероятность реализации риска

15. Указать процесс удаления вредоносного файла способом перехода в безопасный режим:

1. После перезагрузки компьютера выберите «Поиск и устранение неисправностей», затем «Дополнительные параметры», а затем на экране «Выбор действия» нажмите «Параметры загрузки».
2. При отображении меню с нумерованными параметрами запуска, выберите номер 4 или F4, чтобы запустить компьютер в безопасном режиме.
3. При появлении экрана входа в систему, удерживайте нажатой клавишу Shift и выберите «Питание», а затем «Перезагрузить
4. В следующем окне нажмите на кнопку «Перезагрузить» и дождитесь появления следующего экрана.
5. Перезагрузите компьютер

16. Установить этапы идентификации пользователя:

1. Маркер доступа
2. Запуск программы
3. Прохождение процессов потока
4. Вход пользователя в систему

17. Расположить общую схему подготовки электронного письма:

1. Проверка HTML-контентов
2. Реальная рассылка
3. Сборка письма
4. Тестовая рассылка;
5. Подготовка контентов

18. Указать последовательно защиты персональных данных:

1. Разработка технического задания
2. Реализация технической части системы защиты
3. Обследование
4. Проектирование системы защиты
5. Моделирование угроз

19. Указать Этапы построения системы информационной безопасности предприятия:

1. Определяется политика безопасности, допустимый степень риска, набор процедур и методов исключения несанкционированного доступа к информационным ресурсам
2. Проведение предварительного обследования состояния объекта и уровня организации защиты информации
3. Обосновывается структура и технология функционирования комплексной системы защиты информации
4.Обосновываются задачи защиты информации, их классификации и определяются необходимые меры защиты.

20. Указать этапы работы антивирусной программы:

1. Попытаться вылечить, удалив вредоносный код
2. Монитор. Отслеживает все манипуляции с файлами в режиме реального времени
3. Сканер. Ищет вредоносное ПО в оперативной памяти, загрузочных записях при включении, на локальных и внешних дисках, а также в системных файлах ОС
4. Удалить, если вылечить не удалось
5. Поместить в карантин, чтобы вылечить позже или удалить

Шкала оценивания результатов тестирования: в соответствии с действующей в университете балльно-рейтинговой системой оценивание результатов промежуточной аттестации обучающихся осуществляется в рамках 100-балльной шкалы, при этом максимальный балл по

промежуточной аттестации обучающихся по очной форме обучения составляет 36 баллов, по очно-заочной и заочной формам обучения – 60 баллов (установлено положением П 02.016).

Максимальный балл за тестирование представляет собой разность двух чисел: максимального балла по промежуточной аттестации для данной формы обучения (36) и максимального балла за решение компетентностно-ориентированной задачи (6).

Балл, полученный обучающимся за тестирование, суммируется с баллом, выставленным ему за решение компетентностно-ориентированной задачи.

Общий балл по промежуточной аттестации суммируется с баллами, полученными обучающимся по результатам текущего контроля успеваемости в течение семестра; сумма баллов переводится в оценку по 5-балльной шкале следующим образом:

Соответствие 100-балльной и 5-балльной шкал

Сумма баллов по 100-балльной шкале	Оценка по 5-балльной шкале
100-85	Отлично
84-70	Хорошо
69-50	Удовлетворительно
49 и менее	Неудовлетворительно

2 .2 КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ЗАДАЧИ

Задача№1

Выбрать известный Вам официальный карьерный портал, представленный в сети Интернет и выполнить с его помощью поиск вакансии «Системный администратор». Результаты исследования представить табличной форме:

Наименование и электронный адрес карьерного портала	Количество вакансий, в г. Курск	Количество вакансий, всего (по России)	Заработная плата (минимальная и максимальная)	Основные квалификационные требования, предъявляемые работодателем
1	2	3	4	5

Задача№2

Используя следующие интернет – ресурсы, заполните таблицу:

1. Работа в России. Общероссийская база вакансий. https://trudvsem.ru/

2. Superjob. https://kursk.superjob.ru/
3. Росработа. http://kursk.rosrabota.ru/
4. HeadHunter https://kursk.hh.ru/
5. Работавгороде. http://kursk.rabotavgorode.ru/
6. Карьера https://career.ru/

Предприятие, адрес	Источник информации (ссылка)	Без опыта работы		Опыт до 3 лет		Опыт свыше 3 лет	
		Должность	з/п, руб.	должность	з/п, руб.	должность	з/п, руб.
1.							
2.							
3.							

Задача№3

Проведите классификацию видов карьеры, заполнив соответствующие графы таблице:

Классификационные признаки	Виды карьеры по соответствующему признаку
1. По отношению к организации:	
2. По отношению к месту	
3. По признаку профессии, специальности:	
4. По признаку времени пребывания на каждой ступени:	

Задача№4

Опишите, заполнив соответствующие графы таблицы, период и основные характеристики каждого из этапов карьеры:

Этап	Основные характеристики этапа
1.Предварительный	
2. Становление	
3.Продвижения	
4. Сохранения	

Задача№5

Изобразите в таблице конфигурацию видов карьеры и напишите комментарии:

Наименование конфигурации карьеры	Рисунок, комментарии и примеры к нему
Целевая карьера	
Монотонная карьера	
Спиральная карьера	

Стабилизационная карьера	
Затухающая карьера	

Задача№6

Представьте, что вы устраиваетесь на должность программиста в управление информатизации ЮЗГУ. Используя данную информацию, заполните таблицу:

№	Наименование	Справочник классификатора	Код	Содержание
1	Вид деятельности	Общероссийский классификатор видов экономической деятельности		
2	Специальность по образованию	Общероссийский классификатор специальностей по образованию		
3	Занятие	Общероссийский классификатор занятий		
4	Профессия, олжность	Общероссийский классификатор профессий рабочих, должностей служащих и тарифных разрядов		
5	Квалификация	Единый квалификационный справочник должностей руководителей, специалистов и других служащих		

Задача№7

Представьте, что вы устраиваетесь на должность разработчика программного обеспечения на предприятие ООО «ВТИ-Сервис» - поставщика всего спектра торгового оборудования и онлайн-касс, систем безопасности и мониторинга, специализированного торгового ПО и IT услуг в городе Курске. Используя данную информацию, заполните таблицу:

№	Наименование	Справочник классификатора	Код	Содержание
1	Вид деятельности	Общероссийский классификатор видов экономической деятельности		
2	Специальность по образованию	Общероссийский классификатор специальностей по образованию		
3	Занятие	Общероссийский		

		классификатор занятий		
4	Профессия, олжность	Общероссийский классификатор профессий рабочих, должностей служащих и тарифных разрядов		
5	Квалификация	Единый квалификационный справочник должностей руководителей, специалистов и других служащих		

Задача№8

Представьте, что вы устраиваетесь на должность инженера - электроника в АО «Авиаавтоматика им. В.В. Тарасова», которое является разработчиком и производителем радиоэлектронной продукции. Предприятие разрабатывает и производит системы управления оружием, интерфейсные блоки, системы регистрации полетной информации, органы оперативного управления для перспективных и модернизируемых летательных аппаратов (ЛА), бронетанковой техники, электрические и электромагнитные приводы. Используя данную информацию, заполните таблицу:

№	Наименование	Справочник классификатора	Код	Содержание
1	Вид деятельности	Общероссийский классификатор видов экономической деятельности		
2	Специальность по образованию	Общероссийский классификатор специальностей по образованию		
3	Занятие	Общероссийский классификатор занятий		
4	Профессия, олжность	Общероссийский классификатор профессий рабочих, должностей служащих и тарифных разрядов		
5	Квалификация	Единый квалификационный справочник должностей руководителей, специалистов и других служащих		

Задача№9

Представьте, что вы устраиваетесь на должность инженера – схемотехника в Курский завод «Маяк» - филиал АО «ННПО имени М.В. Фрунзе». Вот уже более 50 лет завод занимается разработкой и производством приборов дозиметрического и радиационного контроля. Для обеспечения развивающейся отечественной ядерной энергетики специальными средствами измерений. Параллельно с дозиметрией, с 1962 года завод осваивает производство радиоизмерительной техники: генераторов импульсов прямоугольной и специальной формы, измерителей амплитудно-частотных характеристик (АЧХ), усилителей измерительных, вакуумметров. Используя данную информацию, заполните таблицу:

№	Наименование	Справочник классификатора	Код	Содержание
1	Вид деятельности	Общероссийский классификатор видов экономической деятельности		
2	Специальность по образованию	Общероссийский классификатор специальностей по образованию		
3	Занятие	Общероссийский классификатор занятий		
4	Профессия, олжность	Общероссийский классификатор профессий рабочих, должностей служащих и тарифных разрядов		
5	Квалификация	Единый квалификационный справочник должностей руководителей, специалистов и других служащих		

Задача№10

Представьте, что вы устраиваетесь на должность специалиста по информационной безопасности в АО «Совтест АТЕ». Инжиниринговое предприятие «Совтест АТЕ» 27 лет занимается оснащением предприятий России и СНГ современным оборудованием для производства и тестирования радиоэлектроники и электротехнических изделий. Предприятие осуществляет передачу заказчикам технологий разработки и производства высокотехнологичной продукции. Предприятие разрабатывает и внедряет на собственном заводе информационные системы управления производством, основанные на концепции «Индустрия 4.0». Используя данную информацию, заполните таблицу:

№	Наименование	Справочник классификатора	Код	Содержание
1	Вид	Общероссийский		

	деятельности	классификатор видов экономической деятельности		
2	Специальность по образованию	Общероссийский классификатор специальностей по образованию		
3	Занятие	Общероссийский классификатор занятий		
4	Профессия, олжность	Общероссийский классификатор профессий рабочих, должностей служащих и тарифных разрядов		
5	Квалификация	Единый квалификационный справочник должностей руководителей, специалистов и других служащих		

Задача№11

Представьте, что вы устраиваетесь на должность инженера- биотехнолога на предприятие ОАО "Фармстандарт-Лексредства", который занимается разработкой и производством современных, качественных, доступных лекарственных препаратов, удовлетворяющих требованиям здравоохранения и ожиданиям пациентов, является крупнейшим производителем готовых лекарственных средств в Центрально-Черноземном регионе и входит в десятку крупнейших производителей медикаментов в России. Используя данную информацию, заполните таблицу:

№	Наименование	Справочник классификатора	Код	Содержание
1	Вид деятельности	Общероссийский классификатор видов экономической деятельности		
2	Специальность по образованию	Общероссийский классификатор специальностей по образованию		
3	Занятие	Общероссийский классификатор занятий		
4	Профессия, олжность	Общероссийский классификатор профессий рабочих, должностей служащих и тарифных разрядов		

5	Квалификация	Единый квалификационный справочник должностей руководителей, специалистов и других служащих		

Шкала оценивания решения компетентностно-ориентированной задачи: в соответствии с действующей в университете балльно-рейтинговой системой оценивание результатов промежуточной аттестации обучающихся осуществляется в рамках 100-балльной шкалы, при этом максимальный балл по промежуточной аттестации обучающихся по очной форме обучения составляет 36 баллов, по очно-заочной и заочной формам обучения – 60 (установлено положением П 02.016).

Максимальное количество баллов за решение компетентностно-ориентированной задачи – 6 баллов.

Балл, полученный обучающимся за решение компетентностно-ориентированной задачи, суммируется с баллом, выставленным ему по результатам тестирования. Общий балл промежуточной аттестации суммируется с баллами, полученными обучающимся по результатам текущего контроля успеваемости в течение семестра; сумма баллов переводится в оценку по 5-балльной шкале следующим образом:

Соответствие 100-балльной и 5-балльной шкал

Сумма баллов по 100-балльной шкале	Оценка по 5-балльной шкале
100-85	Отлично
84-70	Хорошо
69-50	Удовлетворительно
49 и менее	Неудовлетворительно

Критерии оценивания решения компетентностно-ориентированной задачи (нижеследующие критерии оценки являются примерными и могут корректироваться):

6-5 баллов выставляется обучающемуся, если решение задачи демонстрирует глубокое понимание обучающимся предложенной проблемы и разностороннее ее рассмотрение; свободно конструируемая работа представляет собой логичное, ясное и при этом краткое, точное описание хода решения задачи (последовательности (или выполнения) необходимых трудовых действий) и формулировку доказанного, правильного вывода (ответа); при этом обучающимся предложено несколько вариантов решения или оригинальное, нестандартное решение (или наиболее эффективное, или наиболее рациональное, или оптимальное, или единственно правильное решение); задача решена в установленное преподавателем время или с опережением времени.

4-3 балла выставляется обучающемуся, если решение задачи демонстрирует понимание обучающимся предложенной проблемы; задача решена типовым способом в установленное преподавателем время; имеют место общие фразы и (или) несущественные недочеты в описании хода решения и (или) вывода (ответа).

2-1 балла выставляется обучающемуся, если решение задачи демонстрирует поверхностное понимание обучающимся предложенной проблемы; осуществлена попытка шаблонного решения задачи, но при ее решении допущены ошибки и (или) превышено установленное преподавателем время.

0 баллов выставляется обучающемуся, если решение задачи демонстрирует непонимание обучающимся предложенной проблемы, и (или) значительное место занимают общие фразы и голословные рассуждения, и (или) задача не решена.