МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сибирский государственный университет геосистем и технологий»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

НАПРАВЛЕНИЕ ПОДГОТОВКИ
10.04.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Профиль подготовки/Специализация
«Управление информационной безопасностью»

УРОВЕНЬ ВЫСШЕГО ОБРАЗОВАНИЯ
МАГИСТРАТУРА

Новосибирск – 2026

Оглавление

1 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ» 3
2 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «МЕТОДОЛОГИЯ НАУЧНЫХ ИССЛЕДОВАНИЙ» 9
3 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «ПРОЕКТНЫЙ МЕНЕДЖМЕНТ» 15
4 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «ПРОФЕССИОНАЛЬНЫЙ ИНОСТРАННЫЙ ЯЗЫК» 22
5 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «СИСТЕМЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА» 35
6 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» 38
7 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ» 43
8 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «ФИЛОСОФСКИЕ ПРОБЛЕМЫ НАУКИ И ОБЩЕСТВА» 50
9 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «МЕТОДЫ И СРЕДСТВА ПРОТИВОДЕЙСТВИЯ ТЕХНИЧЕСКИМ КАНАЛАМ С ИСПОЛЬЗОВАНИЕМ БПЛА» 61
10 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «НАУЧНО-ТЕХНИЧЕСКИЙ СЕМИНАР» 69
11 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «НОРМАТИВНАЯ ПРАВОВАЯ И МЕТОДИЧЕСКАЯ ДОКУМЕНТАЦИЯ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ» 75
12 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ» 81
13 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «ОРГАНИЗАЦИЯ И ТЕХНОЛОГИИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ» 87
14 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «ТЕОРИЯ СИСТЕМ И СИСТЕМНЫЙ АНАЛИЗ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» 90
15 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» 95
16 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «КОНТРОЛЬ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА» 101
17 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «КОНТРОЛЬ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ» 110
18 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «ПРОЦЕССНЫЙ ПОДХОД В УПРАВЛЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ» 118
19 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «ТЕОРИЯ ПРИНЯТИЯ РЕШЕНИЙ В ВОПРОСАХ ЗАЩИТЫ ИНФОРМАЦИИ» 121
20 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «ТЕХНИЧЕСКИЕ, ОРГАНИЗАЦИОННЫЕ И КАДРОВЫЕ АСПЕКТЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ» 126
21 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «МОДЕЛИРОВАНИЕ И УПРАВЛЕНИЕ ЖИЗНЕННЫМ ЦИКЛОМ ИНФОРМАЦИОННЫХ СИСТЕМ» 134

1 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ»

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ

1. Что такое контентная категоризация?
2. Как классифицируется информация по уровню конфиденциальности? Что такое метки документов? Каковы основные способы хранения информации?
3. Каковы основные способы хранения конфиденциальной информации? Что такое сводная информация? Что такое интеллектуальная собственность? Что такое неструктурированная информация? Что такое локальные копии?
4. Каковы основные направления защиты информации? В чем особенности защиты документов и защиты каналов утечки?
5. В чем суть мониторинга (аудита) действий пользователей?
6. Как классифицируются внутренние нарушители? В чем особенности следующих типов: неосторожные, манипулируемые, саботажники, нелояльные? Чем отличаются нарушители, мотивированные извне. Знаете ли Вы другие типы нарушителей?
7. В чем суть нетехнических мер защиты от внутренних угроз: психологических мер, организационных мер?
8. Как определяются права локальных пользователей? В чем суть стандартизации ПО? Какие бывают специфические решения?
9. Как выглядит классификация файрволов?
10. Что такое пакетные фильтры? Что такое пограничные роутеры?
11. Что такое персональные файрволы и персональные устройства файрвола?
12. Что такое прокси-сервер прикладного уровня, выделенные прокси-серверы?
13. В чем особенности гибридных технологий файрвола? Как осуществляется трансляция сетевых адресов (NAT)? Что такое статическая трансляция сетевых адресов, скрытая трансляция сетевых адресов?
14. Каковы основные принципы построения окружения файрвола? Что такое DMZ-сети? Что такое конфигурация с одной сетью? ServiceLeg конфигурация? Конфигурация с двумя DMZ? Что такое виртуальные частные сети?
15. Каково расположение VPN-серверов? Что такое Интранет, Экстранет? Охарактеризуйте компоненты инфраструктуры: концентраторы и коммутаторы. Каково расположение серверов в DMZ?
16. Что такое внешне доступные серверы? Чем отличаются VPN и Dial-in серверы? Что такое внутренние серверы? Что такое DNS-серверы?
17. Что такое политика безопасности файрвола. Что такое политика файрвола? Как осуществляется реализация набора правил? Как происходит тестирование политики файрвола? Каковы возможные подходы к эксплуатации файрвола?
18. В чем суть сопровождения файрвола и управления файрволом? Как поддерживается физическая безопасность окружения файрвола? Как происходит администрирование файрвола?
19. В чем особенности встраивания файрволов в ОС? Каковы основные стратегии восстановления после сбоев файрвола? Каковы возможности создания логов файрвола?
20. Что такое инциденты безопасности? В чем главная цель создании ябackup'ов файрволов?
21. Каковы основные характеристики пакетных фильтров в ОС FreeBSD?
22. В чем особенности ПО пакетных фильтров Open BSD Packet Filter (PF) и ALTO?
23. Указание необходимости использования PF. Каковы основные опции ядра, опции rc conf? Указание необходимости использования ALTO.
24. Как происходит создание правил фильтрации? IPFILTER (IPF) файрвол. Указание необходимости использования IPF.

25. Как осуществляется трансляция сетевых адресов NAT? В чем особенности NATдля очень больших LAN? Как осуществляется использование пула публичных адресов? Что такое PortRedirection?

26. Что такое система обнаружения атак? Почему следует использовать IDS? Каковы основные типы IDS?

27. Каковы основные типы базовой архитектуры IDS? В чем преимущества и недостатки совместного расположения Host и Target и их разделения?

28. Каковы основные способы управления IDS? Что такое централизованное управление, частично распределенное управление, полностью распределенное управление?

29. Что такое скорость реакции? В чем отличия Network-Based lDS, Host-BasedIDS, Application-Based IDS?

30. В чем суть анализа, выполняемого IDS? Как происходит определение злоупотреблений? Как происходит определение аномалий? Каковы возможные ответные действия IDS? Каковы возможные активные действия? Как осуществляется сбор дополнительной информации?

31. Что такое изменение окружения? Как осуществляется выполнение действия против атакующего? Что такое пассивные действия? В чем суть тревоги и оповещения? Как используются SNMP Traps? Каковы возможности отчетов и архивирования?

32. Какие бывают системы анализа и оценки уязвимостей? В чем состоит процесс анализа уязвимостей? На чем основана классификация инструментальных средств анализа уязвимостей?

33. В чем суть Host-Based анализа уязвимостей?

34. В чем суть Network-Based анализа уязвимостей? Каковы преимущества и недостатки систем анализа уязвимостей?

35. В чём смысл Zero Trust подхода в ИБ?

36. Понятие социальной инженерии, определения, примеры?

37. Определение SIEM системы, область применения, функционал?

38. Модель нарушителя Howard – Longstaff?

39. Определение и принципы работы VLAN?

40. Стандарт PCI DSS?

ТИПОВЫЕ ПРАКТИЧЕСКИЕ ЗАДАНИЯ ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ

1. Проанализировать трафик при копировании текстовых файлов без использования криптозащиты.

2. Откройте окно управления межсетевым экраном. Опишите действующие настройки. Создайте новое разрешающее правило.

3. Найдите правило, разрешающее отсылку ICMP-пакетов echorequest. Проверьте его работу для какого-нибудь узла из локальной или внешней сети, используя его ip-адрес (например, командой ping 192.168.0.10 можно проверить доступность компьютера с указанным адресом).

4. Активируйте ведение журнала. Выполните команду ping для узла, для которого создавалось блокирующее правило.

5. Определите: какой протокол установлен по умолчанию на вашем компьютере.

ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

Министерство науки и высшего образования РФ Федеральное государственное бюджетное образовательное учреждение высшего образования	10.04.01 Информационная безопасность (код и направление подготовки) Организация и управление информационной безопасностью

«Сибирский государственный университет геосистем и технологий» Кафедра: информационной безопасности	(профиль подготовки) Защищенные информационные системы (дисциплина)

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Что такое контентная категоризация?
2. Каковы основные принципы построения окружения файрвола? Что такое DMZ-сети? Что такое конфигурация с одной сетью, ServiceLeg конфигурация, конфигурация с двумя DMZ? Что такое виртуальные частные сети?
3. Активируйте ведение журнала. Выполните команду ping для узла, для которого создавалось блокирующее правило.

Составитель _____ И.О.Ф.
(подпись)

Заведующий кафедрой _____ И.О.Ф.
(подпись)

ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ

Раздел 1

1. Что такое объект защиты информации?
2. Каковы основные составляющие КЗИ?
3. Как осуществляется структурирование защищаемой информации?
4. Каков порядок структурирования информации? Как происходит оформление результата?
5. Что такое грифы конфиденциальности? Приведите примеры.

Раздел 2

1. Как определяется цена информации? Каков порядок расчета?
2. В чем экономический смысл расчета цены информации?
3. Каковы основные угрозы информации на объекте защиты?
4. В чем суть моделирования объекта информации. Каков порядок моделирования?
5. Какие исходные данные необходимы для моделирования объекта защиты?
6. Как происходит оформление результатов моделирования объекта защиты?
7. Как происходит моделирование угроз безопасности информации?

Раздел 3

1. Что такое модель злоумышленника?
2. Как происходит моделирование физического проникновения? Каковы исходные данные?
3. Каков порядок моделирования физического проникновения?
4. Как осуществляется оценка угрозы физического проникновения?
5. Как осуществляется определение рангов угрозы физического проникновения?
6. Как происходит оформление результата моделирования физического проникновения?
7. Что такое реальность угрозы проникновения? Каков порядок расчета? Приведите примеры.

Раздел 4

1. Каковы организационные меры по улучшению защиты информации от физического доступа?

2. Каковы технические меры по улучшению защиты информации от физического доступа?

3. Как происходит численное моделирование каналов утечки информации? Приведите пример канала утечки.

4. Что такое радиоэлектронный канал утечки? Каковы индикаторы?

5. Что такое акустический канал утечки? Каковы индикаторы?

Раздел 5

1. Что такое материально-вещественный канал утечки? Каковы индикаторы.
2. Что такое оптический канал утечки? Каковы индикаторы.
3. Как происходит оценка реальности канала утечки, расчет?
4. В чем суть экономической модели угроз (каналов утечки)?
5. Какие группы защищаемой информации по степени обновляемости Вы знаете?
6. Как происходит оценка пропускной способности акустического канала?

Раздел 6

1. Как происходит оценка пропускной способности визуального канала?
2. Как происходит оценка пропускной способности канала химического контроля?
3. Как происходит оформление расчета пропускной способности каналов утечки и определение ранга угрозы?
4. Какие Вы знаете современные стандарты при найме персонала?
5. В чем суть резервирования персонала?

ВОПРОСЫ ДЛЯ КОНТРОЛЬНЫХ РАБОТ

1) Перечислите сетевые атаки на канальном уровне семиуровневой модели OSI.
2) Каким образом обеспечивается безопасность протоколов RIP, OSPF&?
3) Дайте определение политики безопасности. Перечислите виды политик безопасности.
4) Атакам какого вида подвержена дискреционная политика безопасности?
5) Перечислите особенности ролевого управления доступом.
6) Основные правила модели Белла-ЛаПадула.
7) Приведите перечень основных механизмов обеспечения информационной безопасности.
8) Перечислите методы активного аудита.
9) Опишите методику ранжирования интерфейсов по степени уязвимости.
10) Приведите классификацию атак по методике STRIDE.

ТЕМЫ РЕФЕРАТОВ

1. Базовые принципы обеспечения безопасности локальной вычислительной сети
2. Информационная безопасность и защита информации
3. Методы обеспечения информационной безопасности
4. Комплексная защита информации на предприятии
5. Программно-аппаратные средства защиты информации от НСД
6. Использование межсетевых экранов для защиты локальных сетей
7. Сравнительный анализ операционных систем семейств Windows и Linux
8. Персональный сетевой экран;
9. Интеллектуальная защита в режиме реального времени;
10. Режим безопасного запуска программ;
11. Предотвращение угроз, атак;
12. Проверка веб-страниц, файлов и сообщений;
13. Самозащита антивируса от попыток выключения со стороны вредоносного ПО;

14. Защита конфиденциальных данных;
15. Защита от кражи паролей, логинов и личных данных;

Реферат – краткая запись идей, содержащихся в одном или нескольких источниках, которая требует умения сопоставлять и анализировать различные точки зрения. Реферат – одна из форм интерпретации исходного текста или нескольких источников. Поэтому реферат, в отличие от конспекта, является новым, авторским текстом. Новизна в данном случае подразумевает новое изложение, систематизацию материала, особую авторскую позицию при сопоставлении различных точек зрения.

Реферирование предполагает изложение какого-либо вопроса на основе классификации, обобщения, анализа и синтеза одного или нескольких источников.

Виды рефератов

По полноте изложения	Информативные (рефераты-конспекты)
	Индикативные (рефераты-резюме)
По количеству реферируемых источников	Монографические
	Обзорные

Реферат должен отвечать ряду требований.

Требования по оформлению:

– объем реферата от 10 до 15 страниц формата А4, шрифт Times New Roman, кегль 14 пт, полуторный междустрочный интервал, выравнивание текста – по ширине, нумерация страниц в верхнем колонтитуле по центру, автоматические переносы слов (кроме титульного листа), поля: снизу и сверху – 20 мм, слева – 25 мм, справа – 10 мм;

– на титульном листе указывается: название реферата, Фамилия И.О. обучающегося, номер группы;

– список использованных источников – современная, актуальная литература, не менее трех источников, полное указание выходных данных для книжных и периодических изданий, адреса сайтов с которых заимствован материал, по тексту реферата должны быть ссылки на источники.

Требования по структуре:

– реферат включает титульный лист, оглавление, введение, основной текст, заключение, список литературы, приложения (при необходимости);

– основной текст должен содержать несколько разделов.

Требования по содержанию:

– реферат должен содержать достоверные и актуальные сведения на достаточном научном уровне;

– реферат, кроме текста (формат .doc или .docx), может дополнительно содержать: качественные цветные иллюстрации, фрагменты программного кода и другие материалы, качественно дополняющие основную часть реферата.

ФОНД ТЕСТОВЫХ ЗАДАНИЙ

1 Какие права необходимо иметь для переименования файла?

А) Необходимо быть владельцем файла.

Б) Необходимо иметь право на чтение файла.

В) Необходимо иметь право на запись в файл.

Г) Необходимо иметь право на вход и запись в каталог (так как изменяется только имя файла в соответствующей записи каталога).

2 Укажите правильный вариант ответа

Какому из процессов планировщик задач выделит больше процессорного времени?

А) Процессу, запущенному от имени администратора.

Б) Процессу, запущенному от имени пользователя.

В) Сервису (демону), запущенному системой на этапе загрузки.

Г) Процессу, имеющему более высокий приоритет.

Д) Процессу, занимающему больше виртуальной памяти.

3 Укажите правильный вариант ответа

А) Что означает опция nosuid, установленная для сменного машинного носителя в файле /etc/fstab?

Б) Предупреждение пользователям, чтобы они не запускали файлов с установленным битом setuid с этого носителя.

В) Игнорирование ядром системы битов setuid в исполняемых файлах, размещенных на сменном носителе.

Г) Запрет на копирование специальных файлов типа su, passwd, mount, umount с жесткого диска на сменный носитель.

Д) Предупреждение пользователям об ограничении использования утилиты chmod.

2 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «МЕТОДОЛОГИЯ НАУЧНЫХ ИССЛЕДОВАНИЙ»

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ЗАЧЕТУ

1 Философские основания методологии научного исследования.
2 Понятие о методе и методологии научного исследования.
3 Теория, метод и методика, их взаимосвязь.
4 Научный понятийный аппарат.
5 Типология методов научного исследования.
6 Взаимосвязь предмета и метода исследования.
7 Научные факты и их роль в научном исследовании.
8 Исследование и диагностика.
9 Способы поиска научно-технической, управленческой и экономической информации.
10 Вероятностно-статистические методы, применяемые при проведении исследований.
11 Сущность математического подобия и моделирования.
12 Требования надежности, валидности и чувствительности применяемых методик.
13 Способы представления результатов эксперимента.
14 Сущность математического планирования эксперимента. Критерии оптимальности применяемых параметров.
15 Сравнительная характеристика однофакторного и многофакторного планирования эксперимента. Их достоинства и недостатки.
16 Регрессионный и корреляционный анализы. Условия применения метода наименьших квадратов.
17 Порядок применения процедуры проверки адекватности модели.
18 Методы статистической обработки результатов эксперимента.
19 Статистические критерии, применяемые для обработки результатов исследований. Нулевая гипотеза. Условия применения критериев.

ТИПОВЫЕ ПРАКТИЧЕСКИЕ ЗАДАНИЯ ДЛЯ ПОДГОТОВКИ К ЗАЧЕТУ

Задание 1

Выявите факторы, оказывающие влияние на реализацию угрозы внедрения вредоносного кода внутренним нарушителем. Установите значения уровней для каждого фактора. Составьте матрицу планирования.

Задание 2

На основании результатов оценки реализации угроз внедрения вредоносного кода внутренним нарушителем выведите математическую модель полнофакторного эксперимента, рассчитайте коэффициент корреляции и параметры регрессии.

Задание 3

Для результатов исследования по оценке рисков возникновения угроз проведите их статистическую обработку – рассчитайте математическое ожидание, дисперсию и СКО случайной величины.

Задание 4

Закончите предложение

1.1 Вопрос, задача, требующие разрешения, исследования…
1.2 Лаконичная формулировка проблемы исследования…
1.3 Процесс или явление, порождающие проблемную ситуацию...
1.4 Отдельный аспект объекта, точка зрения, с которой рассматривается объект -…
1.5 Научное предположение, выдвигаемое для объяснения каких-либо явлений…
1.6 Способ решения проблемы исследования...
1.7 Представление о результатах исследования…

Задание 5

Установите правильную последовательность этапов научного исследования:

a. Анализ, интерпретация и оформление результатов.

b. Выбор методологии: исходной концепции, опорных теоретических положений, идеи, исследовательского подхода. Выбор методов исследования.

c. Общее ознакомление с проблемой исследования, обоснование ее актуальности, уровня разработанности; определение объекта и предмета, темы исследования. Формулирование общей цели исследования и соотнесенных с ней задач.

d. Организация и проведение преобразующего (формирующего) эксперимента.

e. Построение гипотезы исследования.

f. Проведение констатирующего эксперимента (диагностики) с целью установления исходного состояния предмета исследования.

g. Апробация исследования и выработка практических рекомендаций.

Задание 6

Напротив каждого метода в таблице поставьте букву, соответствующую определенной группе методов: методы работы с информацией – и; методы научного познания –п; методы творческого решения проблемы исследования – т.

Методы исследования

a. методы поиска информации

b. наблюдение

c. моделирование

d. методы обработки полученной информации

e. эксперимент

f. метод структурного анализа проблемы исследования

g. методы хранение научной информации

ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ

Тема 1 «Методологические основы научного знания. Направления и этапы проведения научных исследований»

1. Что такое методология?
2. В чем заключается репродуктивная и продуктивная деятельность человека?
3. Что означает понятие «организация»?
4. Что такое наука, и какими признаками она характеризуется?
5. Перечислите функции науки.
6. Расскажите об этапах развития науки.
7. Что такое знание? Виды знаний.
8. В чем отличие чувственного и рационального познания?
9. Перечислить основные структурные элементы познания.
10. Перечислите виды научных исследований?

Тема 2 «Принципы этики научного исследования»

1. Что поднимают под этикой научного исследования?
2. Какова роль научного руководителя в проведении исследований?
3. Как обеспечивается научная добросовестность исследователя и в чем заключается проблема плагиата?
4. Каковы основные принципы работы с научной литературой? Как оценить соответствие используемой литературы избранному ракурсу работы?
5. Какие подходы применяют в процессе реферирования научной литературы? В чем заключается основное отличие авторской позиции от реферативного изложения работы?
6. Каковы принципы научного цитирования. Приведите основные положения культуры

цитирования.

7. Каков порядок работы с научной литературой на иностранных языках?

Тема 3 «Планирование и организация проведения научных исследований»

1. Что называют откликом системы на внешнее воздействие? Назовите основные факторы, оказывающие влияние на возникновение угроз информационной безопасности. Какие уровни этих фактором можно выделить?

2. В чем заключается сущность дисперсионного анализа? Приведите алгоритм его применения. В чем заключается разница между однофакторным и многофакторным дисперсионным анализом? Каков алгоритм составления плана двухфакторного дисперсионного анализа?

3. В чем заключаются особенности планирования эксперимента в условиях неоднородности? Как осуществлять трех- и четырехфакторное планирование эксперимента?

4. Порядок составления математической модели на основании результатов дисперсионного анализа? Каков алгоритм проведения полного факторного эксперимента?

5. Что называют дробным факторным экспериментом? Каков алгоритм его применения?

6. Каков алгоритм применения регрессионного анализа? Как оценить коэффициенты регрессии?

Тема 4 «Обработка результатов научных исследований»

1. Какие законы распределения случайных величин применяют при проведении исследований в области информационной безопасности? Что называют случайными величинами, как их оценивают методами математической статистики?

2. Каков алгоритм процесса шкалирования данных? Что понимают под вариационным рядом по исходным и сгруппированным данным?

3. Каков порядок построения гистограммы? Приведите алгоритм применения метода моментов, порядок оценки математического ожидания, коэффициента ассиметрии, доверительного интервала.

4. Что называют гипотез, какие виды гипотез можно применить для исследований в области информационной безопасности? Каков алгоритм применения распределения Фишера, Стьюдента?

5. Каков порядок распространения результатов выборочного обследования на генеральную совокупность? Что называют малой выборкой? Приведите особенности расчета средней и предельной ошибки в малых выборках. Каков алгоритм применения методов сводки и группировки экспериментальных данных для выборочных наблюдений?

ФОНД ТЕСТОВЫХ ЗАДАНИЙ

1 _____ - это совокупность приемов, операций и способов теоретического познания и практического преобразования действительности при достижении определенных результатов.

a) метод *
b) принцип
c) эксперимент
d) разработка

2 _____ - это учение о принципах, формах, методах познания и преобразования действительности, применении принципов мировоззрения к процессу познания, духовному творчеству и практике.

a) методология *
b) идеология
c) аналогия
d) морфология

3 Исходя из результатов деятельности, наука может быть:

a) фундаментальная

b) прикладная
c) в виде разработок
d) фундаментальная, прикладная и в виде разработок *

4 Методика научного исследования представляет собой:
a) систему и последовательность действий по исследованию явлений и процессов
b) совокупность теоретических принципов и методов исследования реальности
c) способ познания объективного мира при помощи последовательных действий и наблюдений
d) все перечисленные определения *

5 Наука или комплекс наук, в области которых ведутся исследования, это …
a) научное направление *
b) научная теория
c) научная концепция
d) научный эксперимент

6 Метод научного познания, в основу которого положена процедура соединения различных элементов предмета в единое целое, систему, без чего невозможно действительно научное познание этого предмета:
a) Анализ
b) Синтез *
c) Индукция
d) Дедукция

7 Метод познания, при котором происходит перенос значения, полученного в ходе рассмотрения какого-либо одного объекта, на другой, менее изученный и в данный момент изучаемый:
a) Наблюдение
b) Эксперимент
c) Аналогия *
d) Синтез

8 Метод научного познания, основанный на изучении каких-либо объектов посредством их моделей:
a) Моделирование *
b) Аналогия
c) Эксперимент
d) Синтез

9 Науки, занимающиеся решением технологических, инженерных, экономических и иных проблем, называются…
a) общественные науки
b) философские науки
c) технические науки*
d) естественные науки

10 Физика, механика, химия, биология относятся к…
a) общественным наукам
b) философским наукам
c) техническим наукам
d) естественным наукам *

11 Метод научного исследования – это…
a) система последовательных действий, модель исследования
b) предварительные обобщения и выводы
c) временное предположение для систематизации имеющегося фактического материала
d) способ исследования, способ деятельности *

12 Методика научного исследования – это…
a) система последовательных действий, модель исследования *
b) предварительные обобщения и выводы

c) временное предположение для систематизации имеющегося фактического материала
d) способ исследования, способ деятельности

13 Наблюдение, эксперимент и сравнение относятся к основным _____ методам исследования.

a) общекультурным
b) общелогическим
c) эмпирическим *
d) теоретическим

14 Целенаправленное изучение предметов, которое опирается в основном на данные органов чувств (ощущение, восприятие, представление) – это…

a) наблюдение *
b) эксперимент
c) сравнение
d) теоретизация

15 Активное и целенаправленное вмешательство в протекание изучаемого процесса – это…

a) наблюдение
b) эксперимент *
c) сравнение
d) теоретизация

16 Познавательная операция, лежащая в основе суждений о сходстве или различии объектов – это…

a) наблюдение
b) эксперимент
c) сравнение *
d) теоретизация

17 Анализ как общелогический метод исследования – это…

a) разделение объекта на составные части с целью их самостоятельного изучения *
b) мысленное отвлечение от несущественных свойств, связей и одновременное выделение одной или нескольких интересующих исследователя сторон изучаемого объекта
c) прием познания, в результате которого устанавливаются общие свойства и признаки объектов
d) метод познания, содержанием которого является совокупность приемов соединения отдельных частей предмета в единое целое

18 Синтез как общелогический метод исследования – это…

a) разделение объекта на составные части с целью их самостоятельного изучения
b) мысленное отвлечение от несущественных свойств, связей и одновременное выделение одной или нескольких интересующих исследователя сторон изучаемого объекта
c) прием познания, в результате которого устанавливаются общие свойства и признаки объектов
d) метод познания, содержанием которого является совокупность приемов соединения отдельных частей предмета в единое целое *

19 Индукция как общелогический метод исследования – это…

a) совокупность познавательных операций, в результате которых осуществляется движение мысли от менее общих положений к более общим *
b) использование общих научных положений при исследовании конкретных явлений
c) разделение объекта на составные части с целью их самостоятельного изучения
d) метод познания, содержанием которого является совокупность приемов соединения отдельных частей предмета в единое целое

20 Дедукция как общелогический метод исследования – это…

a) совокупность познавательных операций, в результате которых осуществляется движение мысли от менее общих положений к более общим
b) использование общих научных положений при исследовании конкретных явлений *

c) разделение объекта на составные части с целью их самостоятельного изучения
d) метод познания, содержанием которого является совокупность приемов соединения отдельных частей предмета в единое целое.

3 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «ПРОЕКТНЫЙ МЕНЕДЖМЕНТ»

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ

1. Понятие «проект» и его определение
2. Ключевые международные стандарты управления проектами. На решение каких задач направлено создание каждого стандарта?
3. Чем различается базовый подход, заложенный в стандарт PMBOK, от подходов, на котором основан стандарт ICB?
4. Каковы основные виды деятельности в ходе управления проектом?
5. Сравнение функций традиционного и проектного менеджмента.
6. Кто является участниками и заинтересованными сторонами проекта? В чем выражаются их интересы?
7. Каковы точки соприкосновения и точки конфликтов интересов участников проекта?
8. В чем заключается важность правильной постановки целей проекта? Каким критериям эти цели должны отвечать?
9. Исходя из каких критериев можно выделять фазы жизненного цикла проекта?
10. Какими преимуществами обладают разные типы организационных структур, в рамках которых может быть реализован конкретный проект?
11. Подсистемы управления проектами.
12. Что необходимо сделать, начиная новый проект?
13. Каковы типичные ошибки реализации начального этапа проекта?
14. Зачем необходимо совещание по определению проекта? Каковы его участники? Какие вопросы выносятся на обсуждение? Что будет результатом совещания?
15. Разработка концепции проекта: формирование идеи проекта, предварительная целей и задач проекта, предварительный анализ осуществляемости проекта, ходатайство о намерениях.
16. Прединвестиционная фаза проекта: прединвестиционные исследования, проектный анализ, оценка жизнеспособности и финансовой реализуемости проекта, технико-экономическое обоснование проекта, бизнес-план.
17. Организационные структуры управления проектами.
18. Понятие офиса проекта, основные принципы проектирования и состав офиса проекта.
19. Зачем нужен центр управления проектом? Какова его типовая модель? Как он функционирует?
20. Какова методология распределения обязанностей, определения уровней отчетности и взаимодействия.
21. Источники и организация проектного финансирования
22. Маркетинг проекта
23. Разработка проектной документации
24. Экспертиза проекта
25. Процессы управления ресурсами проекта. Основные принципы планирования ресурсов проекта.
26. Основные методы планирования проекта.
27. Как составляется план контрольных точек, каковы его преимущества и недостатки
28. Какова основная идея графиков Ганта, каковы их преимущества и недостатки?
29. Что такое сетевые графики, каков их способ построения? Каковы дополнительные возможности сетевых графиков?
30. Управление командой проекта
31. Оценка эффективности проекта. Методы оценки.
32. Влияние риска и неопределенности при оценке эффективности проекта
33. Управление стоимостью проекта

34. Контроль и регулирование проекта. Объясните, какую роль играет контроль и мониторинг в реализации проекта? Перечислите какими методами можно осуществить контроль реализации проекта. Кто должен осуществлять мониторинг реализации проекта?

35. Какие разделы включает в себя план коммуникаций проекта?

36. Какие действия необходимы при завершении проекта? Каковы задачи руководителя проекта при завершении проекта?

37. Использование пакетов прикладных программ в проектном менеджменте.

ТИПОВЫЕ ЗАДАЧИ ДЛЯ ЭКЗАМЕНА

1. Определить минимальную цену новой технологии, если пришлось приобрести оборудования на 20 млн.руб., дополнительная прибыль от применения технологии в течение 5 лет составляет 4 млн. руб. Стоимость капитала составляет 20%.
2. Проведите статические сравнительные расчеты издержек. Учитывайте полную загрузку оборудования и проверьте следует ли делать замену некоторого объекта на новый.

Данные	Инвестиционный объект	
	Старый	Новый
Расходы на приобретение, ₽	50000	100000
Средний связанный капитал, ₽	27500	55000
Технический срок службы	10 лет	10 лет
Производственная мощность	10000 ед.	10000 ед.
Остаточный срок службы оборудования	3 года	
Остаточная стоимость оборудования, ₽	15000	
Ликвидационный доход в настоящее время, ₽	10000	
Прогнозируемый ликвидационный доход, ₽	2000	
Условно-постоянные издержки производства, ₽	5000	6000
Условно-переменные издержки на единицу продукции, ₽	1,5	0,5
Ставка процента	10%	10%

При каких условиях старое оборудование будет выгоднее нового и на сколько?

ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

МИНОБРНАУКИ РОССИИ Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет геосистем и технологий» Кафедра: информационной безопасности	10.04.01 «Информационная безопасность» (код и направление подготовки) Организация и управление информационной безопасностью (профиль подготовки) Проектный менеджмент (дисциплина)

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Понятие «проект» и его определение

2. Прединвестиционная фаза проекта: прединвестиционные исследования, проектный анализ, оценка жизнеспособности и финансовой реализуемости проекта, технико-экономическое обоснование проекта, бизнес-план.

3. Задача. Предприятие обладает технологией, позволяющей ему продавать продукцию по цене, превышающей цены конкурентов на 1200 руб./шт. По прогнозам преимущество в прибыли сохранится в течение четырех лет. Объем выпуска продукции по годам, тыс. шт.: 1-й год -

25, 2-й – 28, 3-й – 28, 4-й год – 26. Оценить стоимость технологии исходя их ставки дисконтирования 12%.

Составитель _____ Ф.И.О.
(подпись)

Заведующий кафедрой _____ Ф.И.О.
(подпись)

ФОНД ТЕСТОВЫХ ЗАДАНИЙ

Примеры тестовых заданий (формирование УК-1):

Понятие «проект» объединяет разнообразные виды деятельности, характеризуемые рядом следующих признаков:

А) неограниченная протяженность во времени

Б) направленность на достижение конкретных целей

В) обособленное выполнение многочисленных, взаимосвязанных действий

Г) все перечисленные признаки

Основное отличие проекта от производственной системы заключается в том, что:

А) проект является неоднократной, циклической деятельностью

Б) проект является однократной, не циклической деятельностью

В) принципиальных отличий нет

С точки зрения системного подхода проект – это:

А) документально оформленный план сооружения или конструкции

Б) группа элементов, организованных таким образом, что они в состоянии действовать как единое целое в целях достижения поставленных перед ними целей

В) некоторая задача без определённых данных и результатов, которая должна быть решена в максимально возможный короткий срок времени

Г) процесс перехода из исходного состояния в конечное – результат при участии ряда ограничений и механизмов

Какие существуют ограничения при реализации проекта?

А) культурологические

Б) логистические

В) время

Г) нормативно-правовые

Д) финансовые

Е) исследование ситуации и развития компании

Ж) финансовые

З) все перечисленные ограничения

Примеры заданий (формирование УК -2)

Описание ситуации: небольшое кафе в парке отдыха, одно из многих, имеет 9 столиков. Посетители, увидев свободный столик, садятся и их обслуживают. Время пребывания клиентов за столиком распределено экспоненциально и в среднем составляет 24 минуты. Если свободных мест нет, люди проходят мимо в расположенные неподалеку практически такие же кафе. Поток потенциальных клиентов можно считать пуассоновским, его интенсивность – 1 (пара или группа) за 2 минуты.

Контрольный вопрос. Хозяин подумывает немного расширить кафе и довести количество столиков до дюжины. Принесет ли ему выгоду этот шаг, если занятый столик приносит ему 750 рублей в час, из которых остается оплатить содержание одного столика – 300 руб в час. Какое

количество столиков принесет ему наибольшую прибыль?

Описание ситуации: Автоматическая телефонная система фирмы «Такси по телефону» может поставить в очередь максимум трех клиентов. Каждый оператор, работающий в системе тратит на прием заказа в среднем 2 минуты. Звонки же поступают в среднем 1 раз в минуту. Распределение времени обслуживания и интервала времени между звонками – экспоненциальное. Один клиент в среднем приносит прибыль 5 долларов. Если клиент не дозванивается он вызывает такси другой компании. Если в настоящее время нет свободных такси, то клиент также будет потерян. Данная компания имеет парк из 22 такси, среднее время обслуживания клиента 20 минут (распределено экспоненциально). Водитель получает 6 долларов в час, а оператор 4 доллара. В настоящее время фирма имеет 4 операторов.

Контрольный вопрос: какова упущенная выгода фирмы от потери не дозвонившихся или неудовлетворенных клиентов?

Каково оптимальное количество операторов?

Пример контрольного задания (формирование УК-3 и УК-6)

Администрация района рассматривает возможность переустройства рынка. После сноса старых палаток проектом предусмотрено строительство павильона с последующей сдачей его площадей в аренду. Работы, которые необходимо выполнить при реализации проекта, их взаимосвязь и время выполнения каждой из работ указаны в следующей таблице

Работа	Содержание работы	Непосредственно предшествующая работа	Время выполнения (недель)
A	Подготовить архитектурный проект	-	2
B	Определить будущих арендаторов	-	10
C	Подготовить проспект для арендаторов	A	3
D	Выбрать подрядчика	A	3
E	Подготовить документы для получения разрешения	A	1
F	Получить разрешение на строительство	E	4
G	Осуществить строительство	D, F	10
H	Заключить контракты с арендаторами	B, C	10
i	Вселить арендаторов в павильон	G, H	2

Вопросы:

1. постройте сетевой график выполнения всех работ проекта
2. Какие работы находятся на критическом пути и какова его длительность?
3. На сколько недель можно отложить начало выполнения работы E, чтобы это не повлияло на срок выполнения проекта?
4. Чему равен свободный резерв времени выполнения работы B?
5. Постройте календарный график проекта, если его начало датируется сегодняшним числом, а работать вы планируете без выходных.

ПРИМЕРЫ КЕЙСОВ

Пример кейса по «Проектному менеджменту»

Наименование проекта: **Постановка системы управления проектами**

Спонсор проекта: отсутствует

Руководитель проекта: недавно нанятый кандидат на должность начальника отдела проектов

Другие участники: все функциональные руководители, директор направления

Предпосылки проекта: необходимость сохранить жизнеспособность компании и выйти на

конкурентоспособный уровень

Границы: пилотные маркетинговые проблемы, затем тиражирование

Цель: постановка системы управления проектами для увеличения прибыльности основной деятельности и снижение рисков

Задачи:

Диагностика существующей проектной деятельности и разработка концепции системы УП

Проектирование системы управления проектами

Разработка документов, регламентирующих систему правления проектами

Организация разработки и реализации выбранных проектов

Внедрение информационной системы управления проектов (ИСУП)

Результаты:

1) создана структура проектного офиса
2) внедрена методология управления проектами
3) создана система мотивации
4) обучен персонал
5) используется единое программное обеспечение
6) создана эффективная система коммуникаций
7) создана система управления качеством
8) наличие актуального архива проектов

Предположения: будет найден спонсор проекта, возможно выделят бюджет для всеобщего обучения

Этапы проекта:

Этап 1. Диагностика существующей проектной деятельности и разработка системы управления проектами (СУП)

Этап 2. Проектирование системы управления проектами

Этап 3. Разработка документов, регламентирующих систему управления проектами

Этап 4. Организация разработки и реализация выбранных проектов

Этап 5. Внедрение информационной системы управления проектами (ИСУП)

Описание ситуации:

Недавно нанятый сотрудник на должность начальника отдела проектов Никифор назначен руководитель проекта по внедрению системы управления проектами. Ранее он работал в маленькой компании, где управление проектами было конкурентным преимуществом. Проекты под его руководством завершались успешно. Имеет сертификат PMP и является горячим приверженцем системного управления проектами.

За первый месяц работы по результатам проведенного этапа диагностики состояния СУП Никифор выявил определенные факты.

Описание ситуации (выявленные факторы): предыдущие проекты имеют очень слабую репутацию в компании так же, как и руководители, которые ими управляли. В компании существуют зачатки перехода от структуры иерархического типа (функциональной) к структуре адаптивного (органического) типа (слабой матричной).

В рамках функциональной структуры выполнением проекта часто пренебрегают в пользу выполнения основных функциональных обязанностей. Эта проблема усугубляется, когда проект ставит разные приоритеты для разных отделов. Например, для отдела рекламы проект может быть важным и срочным, в то время как отдел продаж считает его второстепенным. При этом отдельных функциональных специалистов интересует только свой сегмент работы, но не проект в целом, что приводит к разрыву в достижении целей проекта и они не достигаются (например, отдел рекламы обеспечивает рекламные мероприятия по акциям, а в торговых точках персонал нивелирует полностью эффективность рекламы своим поведением).

Мотивация ответственных за проект слабая, проект рассматривается многими как лишняя работа, напрямую не связанная со своим профессиональным и служебным ростом. Проекты не определяются заранее в виде оформленного списка, что свидетельствует, с одной стороны, о

том, что в компании либо часто меняется или пере утверждается стратегия, либо неэффективно поставлены коммуникация между высшим руководством и руководителями среднего звена.

Персонал негативно воспринимает все изменения и саботирует новые процессы и указания. Большинство сотрудников не знают, где можно получить документальную информацию о предыдущих проектах, и строят предположения о том, что такая информация есть на компьютере одного из менеджеров проекта. Сами же менеджеры проектов отвечают, что задокументированной информации нигде нет.

Эффективность в проектах не оценивается, критерии эффективности отсутствуют, также, как и отсутствует формально назначенный сотрудник, который несет ответственность за проведение и результаты оценки.

Координация взаимодействия между подразделениями не регламентирована формально, поэтому основная часть взаимодействий осуществляется на уровне личных неформальных связей, что влечет за собой не всегда желаемый результат, возникновение личных конфликтов и конфликтов, связанных с распределением человеческих ресурсов на те или иные работы в проектах.

Большинство сотрудников убеждены в том, что сотрудники всей компании стремятся обезопасить себя от любого риска при выполнении работы в проектах. Обучение управлению проектами никто не проходил. Отсутствует единое понимание термина «проект». Осознание необходимости внесения изменений для реализации управления проектами находится на низком уровне, так как высшее руководство сомневается, что управление проектами – это специальность, а не временные назначения людей. Методология управления проектами отсутствует.

Задачи кейса:

Список существующих факторов показал, что существующая ситуация неблагоприятна для последующего внедрения системы управления проектами и несет в себе угрозу.

На основе полученных фактов по результатам диагностики необходимо:

Сформулировать отражает ли список приведенных фактов вероятность наступления событий риска или влияние этих событий на дальнейшее внедрение системы управления проектами?

Выявить и записать риски, которые могут помешать дальнейшему внедрению.

Определить собственников (ответственность) за данные риски.

Определить подход к ранжированию рисков.

Проранжировать риски.

Определить, как какой-либо свершившийся риск может создать дополнительные риски.

Разработать мероприятия устранения/минимизации рисков и время (срок) относительно этапов проекта их устранения (до или после какого-либо этапа).

Отобразить все данные в формате плана управления рисками.

Насколько будет эффективным план управления рисками, разработанный руководителем проекта в одиночку?

ТЕМЫ РЕФЕРАТОВ/ ЭССЭ

1. Опыт выполнения проектов на базе школ в Сколково
2. Опыт выполнения проектов в новосибирском Технопарке
3. Серийное предпринимательство

Реферат – краткая запись идей, содержащихся в одном или нескольких источниках, которая требует умения сопоставлять и анализировать различные точки зрения. Реферат – одна из форм интерпретации исходного текста или нескольких источников. Поэтому реферат, в отличие от конспекта, является новым, авторским текстом. Новизна в данном случае подразумевает новое изложение, систематизацию материала, особую авторскую позицию при сопоставлении различных точек зрения.

Реферирование предполагает изложение какого-либо вопроса на основе классификации, обобщения, анализа и синтеза одного или нескольких источников.

Виды рефератов

По полноте изложения	Информативные (рефераты-конспекты)
	Индикативные (рефераты-резюме)
По количеству реферируемых источников	Монографические
	Обзорные

Реферат должен отвечать ряду требований.

Требования по оформлению:

– объем реферата от 10 до 15 страниц формата А4, шрифт Times New Roman, кегль 14 пт, полуторный междустрочный интервал, выравнивание текста – по ширине, нумерация страниц в верхнем колонтитуле по центру, автоматические переносы слов (кроме титульного листа), поля: снизу и сверху – 20 мм, слева – 25 мм, справа – 10 мм;

– на титульном листе указывается: название реферата, Фамилия И.О. обучающегося, номер группы;

– список использованных источников – современная, актуальная литература, не менее трех источников, полное указание выходных данных для книжных и периодических изданий, адреса сайтов с которых заимствован материал, по тексту реферата должны быть ссылки на источники.

Требования по структуре:

– реферат включает титульный лист, оглавление, введение, основной текст, заключение, список литературы, приложения (при необходимости);

– основной текст должен содержать несколько разделов.

Требования по содержанию:

– реферат должен содержать достоверные и актуальные сведения на достаточном научном уровне;

– реферат, кроме текста (формат .doc или .docx), может дополнительно содержать: качественные цветные иллюстрации, фрагменты программного кода и другие материалы, качественно дополняющие основную часть реферата.

4 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «ПРОФЕССИОНАЛЬНЫЙ ИНОСТРАННЫЙ ЯЗЫК»

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ЗАЧЕТУ

1. В чем заключаются основные моменты Вашей специальности?
2. Каковы специфика Вашей научной работы, цели, актуальность исследования?
3. Какова специальная терминология на иностранном языке, используемая в научных текстах.
4. Каковы основные приемы перевода специального текста?

ТИПОВЫЕ ПРАКТИЧЕСКИЕ ЗАДАНИЯ ДЛЯ ПОДГОТОВКИ К ЗАЧЕТУ

1. Письменный перевод текста по специальности. Объем – 500 п.зн., время – 15 мин.
2. Ознакомительное чтение текста по специальности. Объем – 2000 п.зн., время – 30 мин. Беседа по содержанию текста.
3. Собеседование на одну из предложенных тем: «Моя специальность», «Инновации», «Магистерская диссертация».

ФОНД ТЕСТОВЫХ ЗАДАНИЙ

Вводный тест по английскому языку

Выберите правильный вариант:

1. I _____ dinner with my client tomorrow.
a) am having; b) have been having; c) have; d) will have;

2. I_____ Ted last night. He was ok.
a) have seen; b) will see; c) had seen; **d)saw**;
3. Mary is a good girl. She_____her mother with the housework.
a) is always helping; b) had always helped; **c) always helps;** d) always helped;
4. Look! The garden is all white. It _____all night .
a) snows; b) **has been snowing;** c) was snowing; d) had snowed;

5. He’s a famous singer. He _____ 200 concerts since 1991.
a) is giving; b) has been giving; **c) has given;** d) had been giving;

6. Don’t phone me tonight. I _____ for my French exam.
a) will study; b) study; **c) will be studying;** d) will have studied;

7. Those cakes _____ delicious! Can I have one more, please?
a) tastes; b) are tasting; c) tasting; **d) taste;**

8. Three young children _____ from their burning house yesterday.
a) was rescued; b) rescued; **c) were rescued;** d) are rescued;

9. They look so much alike. They _____twins.
a) must be; b) can be; c) might be; d) should be;

10. This is an official meeting. I think you _____wear a business suit.
a) should; b) may; c) can; d) shouldn’t;

11. - Mum, I have done my homework. _____ I go for a walk with my friends?
- Yes, of course.
a) Can; b) May; c) Should; d) Must;

12. The boss is well-pleased with my work and I hope I _____ a promotion soon.
a) will be given; b) am given; c) will give; d) will have given;

13.Yesterday I arrived at the town and my friend met me at the station so I _____ take a taxi.
a) don't have to; b) couldn't c) don't need to; d) **didn't have to;**

14. These words are very rude! You _____ speak to your mother like that!
a) don't have to; b) needn't; c) shouldn't; **d) mustn't;**

15. The students _____ to talk during the exam.
a) is not allowed; b) do not allow; **c) are not allowed;** d) was not allowed;

Вводный тест по немецкому языку

I. Укажите номер правильного перевода выделенных слов:
1. Der Junge antwortet in der Prüfung ausgezeichnet.
(1. ответил; 2. отвечал; **3. отвечает**; 4. ответит)

2. Die Studenten nahmen an der wissenschaftlichen Konferenz teil.
(1. участвуют; 2. участвовал; **3. участвовали**; 4. будут участвовать)

3. In unserem Werk wird man bald vollautomatische Werkzeugmaschinen erzeugen.
(1. выпускают; **2. будут выпускать;** 3. выпустили; 4. будет выпускать)

II. Укажите номера эквивалентов русскому слову, данному в скобках.
1. Der Gelehrte (создал) seine besten Arbeiten nach dem Krieg.
(1. schafft; 2. ist... geschaffen; **3. hat... geschaffen;** 4. wird ... schaffen)

2. Die Volkswirtschaft des Landes (будет развиваться) im schnellen Tempo.
(1. entwickelte sich; 2. hat sich ... entwickelt; 3. hatte sich ... entwickelt; **4. wird sich ... entwickeln**).

3. Die Zahl der Atomkraftwerke (растет) von Jahr zu Jahr.
(1. wuchs; **2. wächst;** 3. ist... gewachsen; 4. wird ... wachsen).

4. Die Wissenschaftler (продолжали) ihre Arbeit.
(**l. setzten ... fort;** 2. setzen ... fort; 3. setze ... fort; 4. werden ... fortsetzen)

III. Укажите номер русского слова, соответствующего правильному переводу выделенных слов.
1. Er sollte ausländische Ausstellung unbedingt besuchen.
(**1. должен был;** 2. мог; 3. должен; 4. может)

2. Auf diese Prüfung musste man sich gut vorbereiten.
(1. нужно; **2. нужно было;** 3. можно; 4. можно было)

3. Er soll eine komplizierte Arbeit erfüllen.

(**1. должен;** 2. должен был; 3. мог; 4. может)

4. Der Student will diese Arbeit fortsetzen.
(1. хотел; 2. должен был; 3. должен; **4. хочет**)

IV. Укажите номер русского слова, соответствующего правильному переводу выделенных определений.

1. Heute bekam ich eine ***kompliziertere*** Aufgabe als damals.
(1. сложное; 2. самое сложное; **3. более сложное;** 4. наисложнейшее)

2. Das ***schönste*** Theater befindet sich in unserer Stadt.
(**1. самый красивый**; 2. красивый; 3. более красивый; 4 очень красивый)

V. Укажите номер слова, подходящего к данному существительному как определение.

1. Die ... Studenten sassen im Horsaal.
(1. gelesenen; **2. lesenden;** 3. lesen; 4. lesend)

2. Das ... Experiment ist für mich sehr interessant.
(1. durchführende; 2. durchführen; **3. durchgeführte;** 4. durchführend)

VI. Укажите номер русского слова, соответствующего правильному переводу выделенных слов.

1. An unserer Hochschule studiert man Deutsch und Englisch.
(1. изучается; **2. изучают;** 3. изучали; 4. изучает)

Тест по английскому языку

Задание 1
Заполните пропуск:
Information becomes _____ when it enters an information technology system.
Варианты ответа:
a. data b. day c. datum d. dale

Задание 2
Заполните пропуск:
The purposes of _____ systems are to process input, maintain files of data and produce information, reports and other output.
Варианты ответа:
a. information b. communication c. connection d.inflection

Задание 3
Заполните пропуск:
Many information systems are implemented with generic “off-the-shelf” software rather than with _____ programs.
Варианты ответа:
a. hand-made b. well-done c. custom-built d. build-up

Задание 4
Заполните пропуск:
GIS is _____ .
Варианты ответа:
a. Geological Information System b. Geometrical Information System
c. Geographic Information System d. Geodetic Information System

Задание 5

Заполните пропуск:

Geographical data describes objects from the real world in terms of the object's position with respect to a known _____ system.

Варианты ответа:

a. subordinate b. coordinate c. superior d. point

Задание 6

Заполните пропуск:

The most important aspects of data quality are: accuracy, _____ and completeness.

Варианты ответа:

a. actuality b. currency c. frequency d. adequacy

Задание 7

Заполните пропуск:

The ability to perform complex special analysis rapidly provides a quantitative as well as _____ advantage.

Варианты ответа:

a. quality b. question c. qualitative d. qualified

Задание 8

Заполните пропуск:

In the context of GIS technology, spatial data are landscape features which can be represented on a _____.

Варианты ответа:

a. chart b. card c. cart d. screen

Задание 9

Заполните пропуск:

Geographic spatial data occur on, in, or above the planet _____.

Варианты ответа:

a. surface b. floor c. soil d. bottom

Задание 10

Заполните пропуск:

An _____ is a thing in the real world with an independent existence.

Варианты ответа:

a. entity b. entry c. attribute d. attachment

Задание 11

Заполните пропуск:

The purposes of information systems _____ to process input, maintain files of data and produce information, reports and other output.

Варианты ответа:

a. is b. were c. was d. are

Задание 12

Заполните пропуск:

To be of any use, a computer-based information system _____ function properly.

Варианты ответа:

a. can b. would c.must d.shall

Задание 13

Заполните пропуск:

The GIS is operated _____ the staff who report to a management.

Варианты ответа:

a. on b. at c. by d. behind

Задание 14

Заполните пропуск:

The information is _____ to develop alternative designs that meet the organization's criteria.

Варианты ответа:

a. use b. to use c. using d. used

Задание 15

Заполните пропуск:

Complex information systems _____nowadays.

Варианты ответа:

a. are widely using b. are widely used c. have widely used d. is widely used

Прочитайте текст и выполните задания:

Information as a Resource and Commodity

In the late 20th century, information has acquired two major utilitarian connotations. On the one hand, it is considered an economic resource, somewhat on part with other resources such as labour, material, and capital. This view stems from evidence that the possession, manipulation, and use of information can increase the cost-effectiveness of many physical and cognitive processes. The rise in information-processing activities in industrial manufacturing as well as in human problem solving has been remarkable. Analysis of one of the three traditional divisions of economy, the service sector, shows a sharp increase in information-intensive activities since the beginning of the 20th century. By 1975 these activities accounted for half of the labour force of the United States, giving rise to the so-called information society.

As an individual and societal resource, information has some interesting characteristics that separate it from the traditional notions of economic resources. Unlike other resources, information is expansive, with limits apparently imposed only by time and human cognitive capabilities. Its expansiveness is attributable to the following:

(1) it is naturally diffusive;

(2) it reproduces rather than being consumed through use; and

(3) it can be shared only, not exchanged in transactions.

At the same time, information is compressive, both syntactically and semantically. Coupled with its ability to be substituted for other economic resources, its transportability at very high speeds, and its ability to impart advantages to the holder of information, these characteristics, are at the base of such societalindustries as research, education, publishing, marketing, and even politics. Societal concern with the husbanding of information resources has extended from the traditional domain of libraries and archives to encompass organizational, institutional, and governmental information under the umbrella of information resource management.

The second perception of information is that it is an economic commodity, which helps to stimulate the world wide growth of a new segment of national economies – the information sector. Taking advantage of the properties of information and building on the perception of its individual and societal utility and value, this sector provides a broad range of information products and services.

Задание 16

Определите, является ли утверждение:

In the late 20th century, information has acquired two major utilitarian connotations.

Варианты ответа: а) ложным б) истинным с) в тексте нет информации

Задание 17
Определите, является ли утверждение:
Unlike other resources, information is unlimited.
Варианты ответа: а) ложным б) истинным с) в тексте нет информации

Задание 18
Определите, является ли утверждение:
By 1992 the market share of the U.S. information service sector had grown to about $25 billion.
Варианты ответа: а) ложным б) истинным с) в тексте нет информации

Задание 19
Определите, является ли утверждение:
By 1975 information activities accounted for half of the labour force of the United States.
Варианты ответа: а) ложным б) истинным с) в тексте нет информации

Задание 20
Определите, является ли утверждение:
The information sector provides a broad range of information products and services.
Варианты ответа: а) ложным б) истинным с) в тексте нет информации

Тест по немецкому языку

I. Из данных предложений определите то, в котором глагол „haben" выражает долженствование:
1. Das Auge hat die Bestandteile des Spektrums mit entsprechenden Hilfsmitteln zu sehen.
2. Fraunhofer hat dunkle Linien in dem Spektrum des Sonnenlichtes festgestellt.
3. Das Licht hat Wellencharakter.

II. Из данных предложений определите то, в котором глагол „sein" выражает долженствование:
1. Der Charakter eines Strahlenbündels ist z. B. bei der Bilderzeugung durch optische Instrumente zu verändern.
2. Einfach zu übersehen ist die sogenannte reguläre Reflexion, bei der der beleuchtete Gegenstand eine versilberte Glasplatte, ein poliertes Metallstück, eine Flüssigkeitsoberfläche oder ein Körper mit ähnlich geglätteter Oberfläche ist.
3. Das Wort Medium ist der lateinischen Sprache entnommen

III. Укажите номера эквивалентов русскому слову, данному в скобках.
Der Gelehrte (создал) seine besten Arbeiten nach dem Krieg.
1. schafft;
2. ist... geschaffen;
3. hat... geschaffen;
4. wird ... schaffen

IV. Укажите номер русского слова, соответствующего правильному переводу выделенных слов.
Auf diese Prüfung **musste** man sich gut vorbereiten.
(1. нужно; 2. нужно было; 3. можно; 4. можно было)

V. Укажите номер русского слова, соответствующего правильному переводу выделенных определений.
Heute bekam ich eine **kompliziertere** Aufgabe als damals.
1. сложное;

2. самое сложное;
3. более сложное;
4. наисложнейшее.

VI. Укажите номер слова, подходящего к данному существительному как определение.
Das ... Experiment ist für mich sehr interessant.
1. durchführende;
2. durchführen;
3. durchgeführte;
4. durchführend.

VII. Укажите номер предложения, в котором причастие переводится словом «спрашивая».
1. Der gefragte Student antwortete richtig.
2. Der fragende Student stand von seinem Platz auf.
3. Fragend zeigte er dem Lektor seine Zeichnung.

VIII. Укажите номер русского слова, соответствующего правильному переводу выделенных слов.
Man **zeigte** uns modeme Apparatur.
1. показывают;
2. показали;
3. показывает;
4. показывается

IX. Выберите правильный перевод сказуемого в страдательном залоге (Passiv):
1. Das Gerätwirdgeprüft.
1. прибор проверили;
2. прибор проверяют;
3, прибор будут проверять;

X. В каком предложении сказуемое выражает результат действия (Stativ):
1. Der Text ist übersetzt worden.
2. Der Text wurde übersetzt.
3. Der Text ist übersetzt.

XI. Укажите правильный перевод выделенных:
Von der Richtigkeit seiner Idee überzeugt, setzte der Ingenieur die Arbeit fort.
a) Инженер, продолжая работу, убеждал в правильности своей идеи.
b) Убежденный в правильности своей идеи, инженер продолжал работу.
c) Убеждая в правильности своей идеи, инженер продолжал работу.

XII. Укажите правильный перевод выделенных:
Der Kollege, dessen Buch ich lese, hat eine grosse Bibliothek.
a) Коллега, книгу которого я читаю, имеет большую библиотеку.
b) Коллега читает книгу, которую он взял в библиотеке.
c) Коллега читает книги, которые он берет в библиотеке.

XIII. Укажите правильный перевод выделенных:
Der Wissenschaftler, an den Problemen der Mikroelektronik intensiv arbeitend, hielt einen interessanten Vortrag.
a) Ученый сделал интересный доклад о проблемах микроэлектроники.
b) Проблемы микроэлектроники, над которыми работал ученый, освещены в его докладе.

c) Ученый интенсивно работающий над проблемами микроэлектроники, сделал интересный доклад.

XIV. Укажите правильный перевод выделенных:
Der neue Stoff, in unserem Labor entwickelt, wird im Maschinenbau verwendet.
a) Новый материал, разработанный в машиностроении, применяют в нашей лаборатории.
b) Новый материал, разработанный в нашей лаборатории, применяют в машиностроении.
c) Разрабатываемый в нашей лаборатории новый материал будет применяться в машиностроении.

XV. Выберите правильный ответ на вопрос:
Zu welchem Zweck lesen wir die Fachzeitschriften? Wir lesen die Fachzeitschriften,...
a) ohne neue Information zu bekommen;
b) statt neue Information zu bekommen;
c) um neue Information zu bekommen.

КОМПЛЕКТ КОНТРОЛЬНЫХ ЗАДАНИЙ ПО АНГЛИЙСКОМУ ЯЗЫКУ

I. *Перепишите и переведите следующие предложения. Определите по грамматическим признакам, какую функцию выполняет окончание –* ‘*ed*’, *т. е. служит ли оно:*

а) показателем стандартного глагола в *Past Indefinite*;

б) показателем *Participle II* от стандартного глагола в функции определения к существительному;

в) частью сказуемого от стандартного глагола в *Passive Voice* or *Perfect Tense*;

г) устоявшимся *прилагательным*.

1. B. Franklin is acknowledged to have invented a means of protecting against the disastrous effects of lightning – the lightning rod. 2. After many difficulties he at last managed to enter the university. 3. This design was to be worked out by a highly qualified engineer. 4. The American Constitution was finally adopted in 1788. 5. The loosely organized colonies needed a single military commander to unify their forces. 6. An organization’s information management requirements are determined by some factors: two general factors are the environment and size of the organization, and two specific factors are the area and level of the organization. 7. He was a very talented mathematician.

II. *Перепишите и переведите сложные предложения, обращая внимание на многофункциональность глагола* “*to be*”:

а)словарное значение – ‘*быть чем-то (кем-то)*’;‘*находиться*’ *где-то*;

б) вспомогательн. гл. *для* образования PassiveVoice и ContinuousTense*;*

в) модальное значение *долженствования;*

г) *глагол-связка* в именном составном сказуемом.

1. Because the beam (луч, пучок света) is so small, it is very important in delicate surgery and is used in eye operations. 2. Students are to be at the lecture in time. 3. Potential laser application in medicine is also being studied at the centre. 4. His task was to prepare everything for the experiment. 5. The journalist has been to his business trip in Siberia. 6. Today’s generation is the best-informed than ever. 7. To be beneficial, a cadastral system should be combined with a reliable land registration system.

III. *Перепишите и переведите следующие предложения, обращая внимание на многофункциональность глагола* “*to have*”:

а) *словарное (смысловое*) значение – ‘*иметь*’, ‘*обладать*’;

б) вспомогательный глагол для образования –*Perfect Tense*;

в) в качестве *модального* глагола – ‘*должен*’;

г) выражение *действия* сочетанием – ‘*to have’* + существительное.

1. Human societies *have* become increasingly dependent for their well-being on the ability to collect and analyze geographic information. 2. Public administration, for example, *has to* know exactly where pipes and cables are located in the ground if it wants to build new houses or renovate the sewer system. 3. They *have* some interesting information concerning this event. 4. I'*ve* just *had* my hair done. 5. Marriage is a matter of learning to live with one particular person with whom you *have* chosen to blend your life. 6. He *has* a degree in information technologies (IT).

IV. *Перепишите и переведите следующие предложения, обращая внимание на многофункциональность глагола* '*to do*':

а)словарное (смысловое) значение – 'делать', 'выполнять';

б) вспомогательный глагол формы: (*do, does, did*) для *образования вопросительной* и отрицательной форм в *Present*и *Past Indefinite*;

в) для *замены* смыслового глагола во избежание повторения;

г) *усилительный* глагол формы (*do, does, did)* перед инфинитивом смыслового глагола.

1. They always do their work well. 2. Love *does* much, money *does* everything. 3. Who saw him yesterday? Ann *did.* 4. I *didn't* watch this film. 5. I *do* help you. 6. They *did not* have the time *to do* this work themselves. 7. In fact, not only d*oes* a computer store the data electronically, it can also retrieve, sort, analyze, process, and then it can store the information again for use in the future. 8. Do you do any sports?

V. *Перепишите и переведите следующие предложения, содержащие разные формы сравнения прилагательных*; *подчеркните в предложениях*

1. The simple ideas are always the best. 2. This method of work is the most efficient compared with all the other methods. 3. The greater the knowledge of the land, the better the possibilities will be to guide the development. 4. The next fifteen years were the happiest of G. Washington's life. 5. A major role of computer science has been to alleviate such problems, mainly by making computer systems cheaper, faster, more reliable, and easier to use. 6. The problems that afflict the nation's public facilities are much wider and costlier and difficult to tackle because local authorities and city boards, with some help from the national government, often have to depend on local property taxes to finance such projects. 7. The problem is even worse in industrial cities.

VI. *Перепишите и переведите следующие предложения, обращая внимание на перевод личных, неопределённых и отрицательных местоимений*

1. Nobody knows anything about the origin of this strange phenomenon. 2. He had some interesting information about the achievements in his field. 3. They had no relatives in this town. 4. He needs someone who is an expert in this field. 5. Something was unusual in his behavior. 6. None of us is immune to geologic hazards. 7. Nothing was interesting at the party.

VII. *Перепишите и переведите предложения, обращая внимание на особенности определений, выраженных именем существительным; подчеркните их:*

This research centre is famous not only in our country but throughout (all over) the world. 2. Some of our university teachers do a lot of research concerning this problem. 3. He is on his business trip at the moment. 4. The city transport system is not very well organized. 5. The laboratory equipment is not of the latest generation. 6. Management skills may be acquired through education or experience. 7. Land resource management is concerned with the inventory, allocation, development, and conservation of a community's resources.

VIII. *Перепишите и переведите следующие предложения; подчеркните в каждом из них глагол-сказуемое и определите его видо-временную форму и залог*:

1. Most of the people, who have access to the Internet, use the network only for sending and receiving e-messages. 2. British geodesist, George Everest, completed the topographic survey of India, on which depended the accurate mapping of the subcontinent. 3. Computers are now an important part

of everything; without them, the modern world will stop. 4. She was sitting there doing nothing. 5. The group of researchers has been analyzing the results of the experiment for a week. 6. They have set up a laboratory that designs laser systems for environmental control. 7. A lot of effort has been made to develop standards for data acquisition and processing.

IX. *Переведите текст; выполните задания к нему.*

One of the prominent features of 20th – century technology has been the development and exploitation of new communications media. Concurrent with the growth of devices for transmitting and processing information, a unifying theory known as information theory was developed. It was initiated by the U.S. electrical engineer Claude E. Shannon. In its broadest sense, information is interpreted to include the messages occurring in any of the standard communications media, such as telegraph, radio, or television, and the signals involved in electronic computers, servomechanisms systems, and other data-processing devices. The chief concern of information theory is to discover mathematical laws governing systems designed to communicate or manipulate information. A basic idea in information theory is that information can be treated very much like a physical quantity, such as mass or energy, that's why it sets up quantitative measures of information and of the capacity of various systems to transmit, store and otherwise process information. Some of the problems treated are related to finding the best methods of using various available communication systems and the best methods for separating the wanted information, or signal, from the extraneous information, or noise. Another problem is the setting of upper bounds on what it is possible to achieve with a given information carrying medium (often called an information channel). While the central results are chiefly of interest to communication engineers, some of the concepts have been adopted and found useful in such fields as psychology and linguistics. The information theory overlaps heavily with communication theory, but is more oriented toward the fundamental limitations on the processing and communication of information and less oriented toward the detailed operation of the devices employed.

1. Выполните лексико-грамматический анализ текста
2. Выполните реферирование текста

КОМПЛЕКТ КОНТРОЛЬНЫХ ЗАДАНИЙ ПО НЕМЕЦКОМУ ЯЗЫКУ

I. Перепишите предложения, раскройте скобки, поставьте глагол в форму причастия I или II, чтобы получилось распространенное определение, переведите предложения на русский язык:

Образец: Die an unserer Hochschule (ausbilden) Fachleute arbeiten in verschiedenen Gebieten unseres Landes. – Die an unserer Hochschule ausgebildeten Fachleute arbeiten in verschiedenen Gebieten unseres Landes (Специалисты, подготовленные в нашем вузе, работают в различных областях нашей страны).

1. Ein Strahlenverlauf, der für eine (bestimmen) Richtung festgelegt wurde, ist auch in umgekehrter Richtung möglich. 2. Die Versuche zeigen, daß (einfallen, reflektieren und brechen) Strahl in einer Ebene liegen. 3. Das Verhältnis des Sinus des Einfallswinkels zu dem Sinus des Brechungswinkels ist eine Konstante, die den (benutzen) Stoff kennzeichnet. Sie heißt Brechungsquotient oder Brechzahl.

II. Из данных слов составьте сложные слова и переведите их на русский язык:

Das Licht – die Energie, glühen – die Lampe, das Haupt – das Licht – die Quelle, fix – der Stern, die Sonne – der Strahl, die Beleuchtung – die Technik, die Wärme – die Energie.

III. Раскройте скобки, поставьте глагол в указанную форму пассива, переведите предложения на русский язык:

1. Von Lichttechniker … neue Arten von Kaltlichtstrahlern … … (schaffen – Futurum Passiv). 2. Für das Vakuum … die Lichtgeschwindigkeit heute mit 299 793 km/s … (angeben – Präsens Passiv). 3. Die Lichtgeschwindigkeit … zuerst mit astronomischer Methode … (messen – Imperfekt Passiv), die von Olaf Römer stammt. 4. Das Verfahren der Bestimmung der Lichtgeschwindigkeit, das auf

der Aberration der Fixsterne beruht, … von Bradley … (entwickeln - worden Perfekt Passiv).

IV. Перепишите предложения, подчеркните в придаточном предложении относительное местоимение (союз) и сказуемое, переведите предложения на русский язык:

1. Körper, die von dem auffallenden Licht einen großen Teil reflektieren, haben ein hohes Reflexionsvermögen. 2. Einfach zu übersehen ist die sogenannte reguläre Reflexion, bei der der beleuchtete Gegenstand eine versilberte Glasplatte, ein poliertes Metallstück, eine Flüssigkeitsoberfläche oder ein Körper mit ähnlich geglätteter Oberfläche ist. 3. Vergrößert man den Einfallswinkel, erhält man einen größeren Brechungswinkel. 4. Tritt ein Lichtstrahl von einem optisch dünneren in ein optisch dichteres Medium über, wird er zum Einfallslot hin gebrochen, tritt er vom optisch dichteren in das optisch dünnere Medium über, wird er vom Einfallslot weg gebrochen.

V. Поставьте, где необходимо частицу zu:

l. Dem Kind macht es Spaß, der Mutter verschiedene Geschichten (erzählen). 2. Es ist nicht leicht, in einem fremden Land (leben). 3. Der Mann hilft seiner Frau aus dem Auto (aussteigen). 4. Ich kann heute Abend zu dir nicht (kommen), ich habe noch viel (tun). 5. Die Mutter lehrt die Tochter das Zimmer in Ordnung (bringen). 6. Er hat keine Lust, Schularbeiten (machen). 7. Die Frau verspricht ihrem Kind ein neues Spielzeug (bringen). 8. Nach dem Spiel laufen die Kinder (essen). 9. Soll ich die frage noch einmal (wiederholen)? 10. Wir hören im Saal die Kinder (singen).

VI. Поставьте в следующих предложениях прилагательные в Komparativ, переведите предложения:

1. Ihre Übersetzung ist (schwierig), als die Übersetzung von Michael. 2. Das Wetter ist heute viel (kalt) als gestern. 3. Dieser Schüler ist (schwach) als die anderen in der Klasse. 4. Ich gehe heute nicht spazieren und sehe (gern) fern. 5. Unsere neue Wohnung ist bedeutend (groß) als die alte. 6. In der Turnstunde läuft Peter (schnell) als Olaf. 7. Die Luft wird langsam (warm). 8. Die Großmutter fühlt sich schon (gut). 9. Sportliche Leistungen Werners sind (hoch) als im vorigen Jahr. 10. Moskau ist (alt) als St. Petersburg, und Berlin ist (jung) als Moskau.

VIII. Употребите стоящие в скобках прилагательные или наречия в Superlativ, переведите предложения:

1. In dieser Woche war es nicht besonders warm, (kühl) Tag war Dienstag. 2. (Bekannt) Werk von Johann Wolfgang von Goethe heißt "Faust". 3. Durch Russland fließen viele Flüsse, die Wolga ist davon (groß und breit). 4. Der Februar ist (kurz) Monat des Jahres. 5. Ninas Aufsatz war (gut und interessant) in der Gruppe. 6. In diesem blauen Kleid bist du schön, aber in dem roten siehst du (gut) aus. 7. (Viel) Gemälde der Dresdener Gemäldegalerie wurden nach dem Weltkrieg restauriert. 8. Der 22. Dezember ist (kurz) Tag im Jahr. 9. Ich gehe gewöhnlich nicht viel spazieren, (viel) sitze ich zu Hause und lese etwas. 10. Im Mai singen vor unseren Fenstern viele Vögel, (schön) singt aber die Nachtigall.

ТЕМЫ ДОКЛАДОВ

Целью проекта является научить обучающегося самостоятельному поиску информации на английском языке по заданной тематике:

1. "Моя специальность"

Требования к докладу: подготовка доклада связана с отбором лексико-грамматических средств, необходимых для построения содержательного доклада, посвященного профессиональной деятельности специалиста, а также организацией отдельных структурных элементов презентации (графических и вербальных) в единое целое.

1. Презентация не должна быть меньше 10 слайдов.

2. Первый лист – это титульный лист, на котором обязательно должны быть представлены: название проекта, фамилия, имя, отчество автора, наименование учебного заведения, факультет и номер группы учащегося.

3. Следующим слайдом должно быть содержание, где представлены основные этапы (моменты) презентации. Желательно, чтобы из содержания по гиперссылке можно перейти на необходимую страницу и вернуться вновь на содержание.

4. Дизайн - эргономические требования: сочетаемость цветов, ограниченное количество объектов на слайде, цвет текста.

5. Последними слайдами презентации должны быть глоссарий и список литературы.

Требования к оформлению презентации

В оформлении презентаций выделяют два блока: оформление слайдов и представление информации на них. Для создания качественной презентации необходимо соблюдать ряд требований, предъявляемых к оформлению данных блоков.

Оформление слайдов. Стиль

1. Соблюдайте единый стиль оформления.

2. Избегайте стилей, которые будут отвлекать от самой презентации.

3. Вспомогательная информация (управляющие кнопки) не должны преобладать над основной информацией (текстом, иллюстрациями).

Фон

1. Для фона предпочтительны холодные тона.

2. Использование цвета.

3. На одном слайде рекомендуется использовать не более трех цветов: один для фона, один для заголовка, один для текста.

4. Для фона и текста используйте контрастные цвета.

5. Обратите внимание на цвет гиперссылок (до и после использования).

Анимационные эффекты.

1. Используйте возможности компьютерной анимации для представления информации на слайде.

2. Не стоит злоупотреблять различными анимационными эффектами, они не должны отвлекать внимание от содержания информации на слайде.

Представление информации

1. Содержание информации.

2. Используйте короткие слова и предложения.

3. Заголовки должны привлекать внимание аудитории.

Расположение информации на странице

1. Предпочтительно горизонтальное расположение информации.

2. Наиболее важная информация должна располагаться в центре экрана.

3. Если на слайде располагается картинка, надпись должна располагаться под ней.

Шрифты

1. Для заголовков – не менее 24.

2. Для информации не менее 18.

3. Шрифты без засечек легче читать с большого расстояния.

4. Нельзя смешивать разные типы шрифтов в одной презентации.

5. Для выделения информации следует использовать жирный шрифт, курсив или подчеркивание.

6. Нельзя злоупотреблять прописными буквами (они читаются хуже строчных).

Способы выделения информации

Следует использовать:

-рамки; границы, заливку;

-штриховку, стрелки;

- рисунки, диаграммы, схемы для иллюстрации наиболее важных фактов.

- лучше не располагать на одном слайде более 2 рисунков, так как иначе внимание слушателей будет рассеиваться.

- не стоит вставлять в презентации большие таблицы: они трудны для восприятия - лучше заменять их графиками, построенными на основе этих таблиц.

Объем информации

1. Не стоит заполнять один слайд слишком большим объемом информации.

2. Наибольшая эффективность достигается тогда, когда ключевые пункты отображаются по одному на каждом отдельном слайде.

Виды слайдов

Для обеспечения разнообразия следует использовать разные виды слайдов: с текстом; с таблицами; с диаграммами.

- на последнем слайде презентации размещение ссылок на использованные источники и иллюстрации является обязательным.

- все иллюстрации и фотографии, используемые в презентации, должны быть оптимизированы (сжаты).

5 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «СИСТЕМЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА»

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ЗАЧЕТУ

1. Искусственный интеллект как направление знаний. Основные направления. «Сильный» и «слабый» ИИ. Критерий интеллектуальности. Тест Тьюринга. Критика теста Тьюринга.

2. Философские аспекты ИИ. Теория симуляции реальности Н.Бострома. Цифровая философия. Э.Фредкина. Эволюционная кибернетики В.Ф.Турчина.

3. Понятие сингулярности. Трансгуманистическая философия: основные постулаты.

4. Модели памяти и мышления человека. Чанки. Структуры и процессы.

5. Восходящий, нисходящий, эволюционный и эмерджентный подходы к реализации ИИ. Понятие о нейронных сетях.

6. Знания и информация. Понятие о представлении знаний. Статические и динамические знания. Модели явного и неявного представления знаний.

7. Процедурное представление знаний. Продукции. Деревья «И-ИЛИ». Деревья вывода.

8. Сетевое представление знаний. Семантические сети. Концептуальные графы. Представление знаний тройками объект-атрибут-значение. Представление семантической сети на Прологе.

9. Фреймовое представление знаний. Основные операции логического вывода во фреймовом представлении. Реализация фреймового подхода на языке Пролог.

10. Представление знаний на основе формальной логики. Пролог как возможный язык логического представления знаний.

11. Представление графов. Задача поиска пути в графе. Решение задач методом поиска в пространстве состояний.

12. Поиск в нагруженном графе. Алгоритм поиска с весовой функцией и его реализация на Прологе.

13. Понятие об эвристическом поиске. Допустимость, монотонность, информированность. Критерий допустимости А-алгоритма поиска. Примеры.

14. Поиск по принципу первый-лучший (жадный алгоритм поиска) и его реализация на Прологе.

15. Реализация алгоритма A* на Прологе.

16. Поиск с итерационным погружением (ID).

17. Различные способы повышения эффективности алгоритмов поиска: поиск с использованием списка пар пройденных вершин, представление путей деревьями.

18. Экспертные системы. Продукционные экспертные системы. Структура экспертной системы. База знаний. Машина вывода.

19. Основные подходы к построению экспертных систем. Оболочки экспертных систем. Роль инженера по знаниям. Основные методы, испольуемые инженером по знаниям. Жизненный цикл экспертной системы.

20. Прямой логический вывод. Иллюстрация прямого вывода на деревьях И-ИЛИ. Конфликтное множество. Связь с поиском в пространстве состояний. Применение различных алгоритмов поиска.

21. Обратный логический вывод. Иллюстрация обратного логического вывода на деревьях И-ИЛИ. Конфликтное множество. Связь с поиском в пространстве состояний. Применение различных алгоритмов поиска.

22. Принципы построения баз знаний с продукционным представлением и прямым логическим выводом на языке Пролог.

23. Принципы построения баз знаний с продукционным представлением и обратным логическим выводом на языке Пролог.

24. Понятие онтологии. Примеры онтологий. Таксономия и тезаурус. Языки представления онтологий и инструментарии для создания онтологий (Protege, Ontolingua).

25. Распределенный искусственный интеллект. Многоагентные системы. Коммуникации в многоагентных системах. Использование онтологий для семантического согласования агентов.

26. Использование многоагентных систем для моделирования коллективного поведения. Среда агентного моделирования NetLogo. Примеры.

27. Онтологии в глобальном масштабе. База знаний CyC. Семантическая паутина Symantic Web. Языки RDF, RDF-S, OWL. Способы записи RDF Graph, RDF-triplets, RDF-XML.

28. Дескриптивные логики. Синтаксис и семантика дескриптивных логик. Дескриптивные логики как основа построения семантической паутины.

ТИПОВЫЕ ПРАКТИЧЕСКИЕ ЗАДАНИЯ ДЛЯ ПОДГОТОВКИ К ЗАЧЕТУ

1. Естественный язык и формализация предметных знаний.
2. Модель языка как преобразователя «Смысл-Текст».
3. Информационный поиск и семантический анализ корпуса текстов.
4. Текстовые процессоры.
5. Машинный перевод.
6. Применение методов машинного обучения для борьбы с плагиатом.
7. Вопросно-ответные системы.
8. Системы автоматического реферирования.
9. Морфология и синтаксис в задаче семантической кластеризации.
10. Семантические отношения как основа формирования классов смысловой эквивалентности.
11. Кластеризация семантических знаний в задаче распознавания ситуаций смысловой эквивалентности.
12. Сортовая классификация лексики русского языка и ее использование при формировании семантических классов слов.
13. Автоматизация накопления знаний о синонимии и семантическая схожесть текстов предметного языка.
14. Методы анализа формальных понятий в задаче автоматизированного пополнения лингвистических ресурсов.
15. Машинное понимание текстов в общей задаче распознавания образов.

ТЕМЫ ДОКЛАДОВ

1. Автоматизация пополнения словаря словоформ для морфологического анализа слов русского языка.
2. Автоматизация пополнения словаря основ для морфологического анализа слов русского языка.
3. Применение методов анализа формальных понятий для автоматизации формирования стратегий синтаксического анализа текстов.
4. Применение методов анализа формальных понятий для автоматизации формирования тезауруса предметной области.

ВОПРОСЫ К КОНТРОЛЬНОЙ РАБОТЕ

1) Искусственный интеллект как научная область. Основные направления исследований. Классификация интеллектуальных систем.

2) Проблемная область интеллектуальной системы. Характеристики предметной области и решаемых задач.

3) Понятие поля знаний. Предметный язык. Семиотическая модель поля знаний. Стратегии получения знаний. Лингвистический аспект извлечения знаний: понятийная структура и словарь пользователя. Структурирование знаний.

4) Представление задач в пространстве состояний. Состояния и операторы. Представление операторов системой продукций.

5) Методы поиска в пространстве состояний. Поиск на графе. Слепой перебор.

6) Методы поиска в пространстве состояний: метод полного перебора.

7) Методы поиска в пространстве состояний: метод равных цен.

8) Методы поиска в пространстве состояний: метод перебора в глубину.

9) Перебор на произвольных графах.

10) Методы поиска в пространстве состояний: использование эвристической информации.

11) Оценочная функция и ее свойства. Алгоритм упорядоченного поиска.

12) Оптимальный алгоритм перебора. Выбор эвристической функции. Эвристическая сила алгоритма упорядоченного поиска.

13) Критерии качества работы методов перебора.

14) Представления, допускающие сведение задач к подзадачам. «И/ИЛИ» графы.

15) Разрешимость вершин в «И/ИЛИ» графе.

16) Использование механизмов планирования при сведении задачи к совокупности подзадач.

17) Ключевые операторы и вычисляемые различия.

18) Этапы перебора на «И/ИЛИ» графах при сведении задач к совокупностям подзадач.

19) Взаимные различия методов перебора на «И/ИЛИ» графах. Основные трудности организации перебора на «И/ИЛИ» графе.

20) «И/ИЛИ» дерево. Стоимости деревьев решений.

21) Оптимальное дерево: использование оценок стоимости для прямого перебора.

22) Потенциальное дерево решения. Алгоритм упорядоченного перебора для деревьев «И/ИЛИ».

23) Представление знаний как направление исследований по искусственному интеллекту.

24) Данные и знания. Отличительные особенности знаний.

25) Экстенсиональные и интенсиональные представления в моделях данных. Языки описания и манипулирования данными.

26) Модели представления знаний в интеллектуальных системах: сравнительная характеристика.

27) Представление знаний правилами. Структура продукционной системы.

28) Прямой и обратный вывод. Разрешение конфликтов. Анализ контекста применения правила.

29) Представление системы продукций «И/ИЛИ» графом. Вывод при наличии нечеткой информации.

30) Управление выводом в продукционной системе. Установка ограничений на генерацию конфликтного набора. Вывод по приоритету глубины. Проблемы реализации стратегий поиска вывода.

31) Пути повышения эффективности функционирования продукционной системы.

32) Основные требования к языку представления знаний интеллектуальной системы.

33) Модель семантической сети Куиллиана. Формализация семантической сети. Описание иерархической структуры понятия и диаграмма представления.

34) Процедурные семантические сети. Разделение семантической сети. Вывод с помощью семантической сети.

35) Понятие фрейма. Особенности фреймового представления знаний.

36) Основные свойства фреймов. Слоты. Фреймовые системы.

37) Структура данных фрейма. Демоны и присоединенные процедуры. Способы управления выводом.

6 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ЗАЧЕТУ

1. Дать базовые определения информационной безопасности в широком смысле?
2. Что представляет из себя “Оранжевая книга”?
3. Законодательная база РФ в сфере информационной безопасности?
4. Дать определение SIEM, цели, состав, назначение?
5. Дать определение криптографическим примитивам, назначение, применение?
6. Каковы особенности, этапы внешнего аудита ИБ предприятия?
7. Промышленные протоколы Profibus, Modbus?
8. Методы защиты информации в системах СКУД?
9. Технические каналы утечки информации?
10. Этапы и методы определения актуальных угроз на АС?
11. Методы разграничения доступа к информации?
12. Дать определение DLP систем?
13. Дать определение, назначение систем IDS/IPS?
14. Назначение протокола IPsec, режимы работы?
15. Назначение протоколов защищённой передачи SSH, SSL, TLS?

ТИПОВЫЕ ПРАКТИЧЕСКИЕ ЗАДАНИЯ ДЛЯ ПОДГОТОВКИ К ЗАЧЕТУ

1. Приведите примеры использования средств обеспечения информационной безопасности в реальной жизни?
2. Провести качественный анализ среди указанных антивирусных систем.

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ

1. Дать определение IDS/IPS системам?
2. Методы разграничения доступа?
3. Связка этапов AAA, определение, назначение?
4. Протоколы IoT?
5. Цели и назначения систем автоматизированного управления производственными процессами?
6. Определение КИИ, характеристики, признаки, список по отраслям?
7. Методы определения рисков для АС?
8. Модели нарушителя ИБ?
9. Модели угроз ИБ, разновидности?
10. ISO 31010, ISO 27001?
11. МСЭ – Т Х.805, назначение, состав, основное применение рекомендации?
12. Типы удалённых атак на АС?
13. Стандарт безопасности 3D Secure?
14. Дать характеристику, таксономию программно-аппаратных закладок?
15. Назначение стандарта PCI DSS?
16. Что такое ГосСОПКА, назначение, определение?
17. Дать определение объекту КИИ?
18. SQL – Injection, как вид атаки, определение, характеристики?
19. Понятие Tempest атак?
20. Определение Pentest в широком смысле, назначение, виды?

ТИПОВЫЕ ПРАКТИЧЕСКИЕ ЗАДАНИЯ ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ

1. В ОС MS Windows с помощью утилиты My Simple Desktop 2.0 организовать запрет на изменения рабочего стола, панели задач и меню «Пуск», сделать невозможным внесение изменений в настройки дисплея и контекстного меню проводника. Организовать доступ к панели управления, свойствам папок и системному реестру и заблокировать использование горячих клавиш MS Windows.

ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

Министерство науки и высшего образования РФ Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет геосистем и технологий» Кафедра: информационной безопасности	10.04.01 Информационная безопасность (код и направление подготовки) Организация и управление информационной безопасностью (профиль подготовки) Технологии обеспечения информационной безопасности (дисциплина)

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Методы разграничения доступа?
2. В ОС MS Windows с помощью утилиты My Simple Desktop 2.0 организовать запрет на изменения рабочего стола, панели задач и меню «Пуск», сделать невозможным внесение изменений в настройки дисплея и контекстного меню проводника. Организовать доступ к панели управления, свойствам папок и системному реестру и заблокировать использование горячих клавиш MS Windows?

Составитель _____ И.О.Ф.
(подпись)

Заведующий кафедрой _____ И.О.Ф.
(подпись)

ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ
1 семестр

Раздел 1 - Базовые определения предметной области информационной безопасности (ИБ)

1) Приведите основные определения, применимые к технологиям обеспечения информационной безопасности.
2) Опишите сущность политики безопасности и порядок ее разработки.
3) Что называют обобщенной моделью угроз и что включает в себя это понятие?
4) Приведите характеристику моделей нарушителя информационной безопасности.

Раздел 2 - Методики обеспечения ИБ автоматизированных систем (АС)

1) Приведите характеристику организационных методов, обеспечивающих информационную безопасность автоматизированных систем.
2) Приведите характеристику технических методов, обеспечивающих информационную безопасность автоматизированных систем.
3) Приведите сравнительную характеристику содержательной части стандартов, регламентирующих применение технологий обеспечения информационной безопасности.

Раздел 3 – Сетевая безопасность согласно модели OSI

1) Приведите типы атак на автоматизированные системы.
2) Приведите характеристику каждого вида атак на автоматизированные системы.
3) Какие уязвимости характерны для автоматизированных систем согласно OSI.

Раздел 4 - Методы и средства обеспечения сетевой безопасности согласно модели OSI

1) Приведите характеристику методов разграничения доступа.
2) Опишите сущность протоколов аутентификации.
3) Приведите виды DLP-систем и их сравнительную характеристику.
4) Приведите сравнительную характеристику антивирусных систем.
5) Приведите характеристику систем блокирования нежелательного трафика.

2 семестр

Раздел 5 – Мониторинг, техническая эксплуатация автоматизированных систем

1) Приведите типы сетевого мониторинга и их сравнительную характеристику.
2) Как осуществляется техническая эксплуатация защищенных автоматизированных систем.
3) Какие применяют методы технической эксплуатации.

Раздел 6 - Проектирование защищённых АС. ГОСТЫ, рекомендации

1) Перечислите этапы проектирования защищенных автоматизированных систем, приведите их характеристику с точки зрения применяемых технологий обеспечения информационной безопасности.
2) Опишите жизненный цикл защищенных автоматизированных систем.
3) Как осуществляется минимизация рисков информационной безопасности в проектируемых автоматизированных системах.

Раздел 7 – Криптография в автоматизированных системах

1) Какие криптографические алгоритмы применяют для защиты информации в автоматизированных систем.
2) Приведите сравнительную характеристику криптографических алгоритмов.

Раздел 8 – Методы защиты WEB-приложений

1) В чем заключается применений веб-технологий.
2) Приведите характеристику протоколов. Какие методы применяют в протоколе HTTP.
3) Какие способы реализации сеансов можно применять.

Опрос оценивается по пятибалльной шкале:

Балл	*Критерии оценки (содержательная характеристика)*
1 (неудовлетворительно) Повторная подготовка	Обучающийся не владеет теоретическим материалом, допуская грубые ошибки, испытывает затруднения в формулировке собственных суждений, неспособен ответить на дополнительные вопросы
2 (неудовлетворительно) Повторная подготовка	Обучающийся практически не владеет теоретическим материалом, допуская ошибки по сущности рассматриваемых (обсуждаемых) вопросов, испытывает затруднения в формулировке собственных обоснованных и аргументированных суждений, допускает ошибки при ответе на дополнительные вопросы
3 (удовлетворительно)	Обучающийся владеет теоретическим материалом на минимально допустимом уровне, отсутствуют ошибки при описании теории, испытывает затруднения в формулировке собственных обоснованных

	и аргументированных суждений, допуская незначительные ошибки на дополнительные вопросы
4 (хорошо)	Обучающийся владеет теоретическим материалом, отсутствуют ошибки при описании теории, формулирует собственные, самостоятельные, обоснованные, аргументированные суждения, допуская незначительные ошибки на дополнительные вопросы
5 (отлично)	Обучающийся владеет теоретическим материалом, отсутствуют ошибки при описании теории, формулирует собственные, самостоятельные, обоснованные, аргументированные суждения, представляет полные и развернутые ответы на дополнительные вопросы

ФОНД ТЕСТОВЫХ ЗАДАНИЙ

В каждом вопросе только один правильный ответ.

Вариант 1

1. Автоматизированные системы (АС) это…

А) Системы работающие автономно;

Б) Системы, работающие в режиме удалённого управления человеком;

В) Система собирающая, обрабатывающая информацию от управляемого объекта автоматизации;

Г) Часть производственной системы выполняющей функции в автоматическом режиме.

2. Информационная безопасность в АС:

А) политика безопасности производственных процессов;

Б) информационная безопасность технологических сетей;

В) защита информации в протоколах типа Modbus;

Г) все в совокупности.

3. Методы защиты информации - это...

А) процесс выстраивания политики безопасности в АС;

Б) технологии защиты информации в информационных системах;

В) совокупность законодательных, организационных, технических решений в области ИБ;

Г) подходы к поддержке измерений информационной безопасности.

4. Антивирусное программное обеспечение это…

А) прикладное ПО необходимое для оптимизации работы вычислительной системы;

Б) ПО необходимое для реализации разграничения доступа к информационным средам;

В) система фильтрации входящего трафика на вычислительную систему;

Г) специализированное ПО, применяемое в вычислительных системах для анализа, обработки информации, являющейся паразитной для информационных систем.

5. SIEM это...

А) антивирусное ПО;

Б) программный Firewall;

В) система DLP;

Г) система IDS/IPS;

Д) все выше перечисленное.

6. Sniffing это…

А) атака, направленная на понижение работоспособности вычислительной системы;

Б) вид атаки, использующий системы радио подавления;

В) атака, связанная с получением парольного доступа к доверенной системе;

Г) вид атаки, направленный на снятие информации с сети связи используя специализиро-

ванный программно – аппаратные средства.

7. Надёжность АС это...
А) время наработки на отказ АС;
Б) время восстановления АС;
В) ремонтопригодность элементов АС;
Г) наличие систем резервирования элементов АС;
Д) всё вышеперечисленное.

8. DDos атака это…
А) атака с использованием протоколов обмена информации направленная на переполнение буфера приёма сетевого устройства;
Б) атака связанная с уязвимостями баз данных, типа SQL;
В) атака, связанная с подбором паролей к доверенной системе;
Г) ничего из вышеперечисленного.

9. Инцидент информационной безопасности это:
А) атака на информационную систему, завершившаяся успехом;
Б) попытки совершения нерегламентированных действий в доверенной системе;
В) нарушение измерений информационной безопасности, таких как, доступность, целостность, конфиденциальность информации;
Г) всё вышеперечисленное.

10. Пентест это…
А) тестирование систем электропитания АС;
Б) тест на выявление уязвимостей ПО АС;
В) тестирование систем мониторинга АС;
Г) комплекс тестов, обеспечивающих повышение защищённости от информационных атак систем АС.

11. SCADA системы это…
А) системы спецсвязи;
Б) системы управления производством;
В) системы учёта рабочего времени и доступа на объект;
Г) системы, связанные с производством.

7 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ

1. Понятие СУИБ.
2. Цели обеспечения информационной безопасности.
3. Методы реализации программы информационной безопасности.
4. Информационная безопасность с точки зрения бизнеса.
5. Цена информации.
6. Меры обеспечения информационной безопасности.
7. Управление информационной безопасностью.
8. Процесс ITIL: Управление информационной безопасностью.
9. Процессный подход к управлению информационной безопасностью.
10. Проблемы безопасности, Аспекты безопасности.
11. Технические средства, Недостатки технических средств.
12. Суть процессного подхода.
13. Классификация и атрибуты процессов.
14. Процессы управления и обеспечения информационной безопасности.
15. Сервис-ориентированный подход к информационной инфраструктуре предприятия.
16. Стандарт 9001–рекомендуемая база-ИСО/МЭК 27001.
17. История 27001. Выгоды внедрения стандарта.
18. Активы – основные объекты стандарта.
19. Идентификация активов, реестр активов, интегрированные активы.
20. Структура стандарта.
21. требования к СУИБ.
22. Ключевые процессы СУИБ.
23. Требования стандарта (с точки зрения реализации на практике).
24. Взаимосвязь стандартов.
25. Система управление рисками по требованию стандарта ISO 27001:2005.
26. Алгоритм определения рисков.
27. Идентификация и оценка активов.
28. Идентификация уязвимостей.
29. Реестр рисков.
30. Управление рисками.
31. Общая структура управленческой работы по обеспечению информационной безопасности на уровне предприятия.
32. Методика управления рисками ИБ.
33. Структура организационной деятельности в сфере информационной безопасности на предприятии.
34. Определение целей управления информационной безопасностью.
35. Политика в области безопасности.
36. Структура политики информационной безопасности и процесс ее разработки.
37. Проведение предварительного исследования состояния информационной безопасности.
38. Собственно разработка политики безопасности.
39. Внедрение разработанных политик безопасности.
40. Анализ соблюдения требований внедренной политики безопасности и формулирование требований по ее дальнейшему совершенствованию (возврат к первому этапу, на новый цикл совершенствования).
41. Организация системы безопасности.

42. Классификация активов и управление.
43. Основные принципы управления рисками информационной безопасности.
44. Практический подход к построению системы управления ИБ.

ТИПОВЫЕ ПРАКТИЧЕСКИЕ ЗАДАНИЯ ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ

Задача 1. Рассчитать итоговую стоимость всех элементов информации и долю бюджета, выделенного на их охрану, если весь бюджет на информационную безопасность всех элементов составляет 1 млн. рублей.

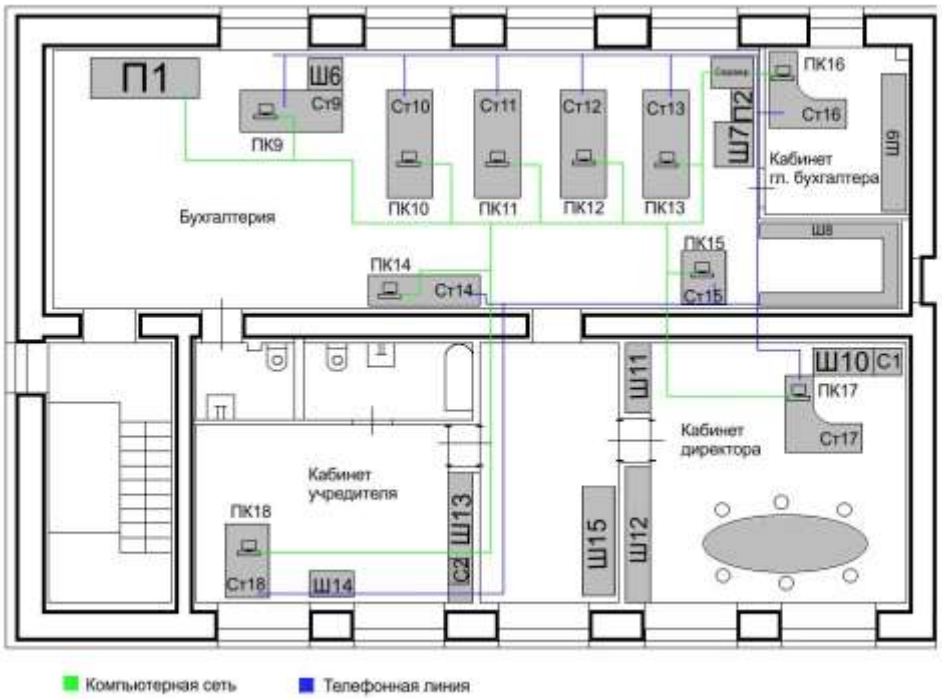
Наименование	Гриф секретности	Объем, стр.	Цена за стр., у.е
Технологические карты производства	К	210	100
Бизнес-план и стратегия развития	К	150	100
Договоры и контракты	ДСП	600	10
Архив документов	ДСП	500	10

Задача 2. Структурировать элементы информации в организации и присвоить гриф секретности

№	Наименование	Источник	Местонахождение источника
1	Технологические карты производства	технолог финансовый директор	бухгалтерия зал опт. продаж
		бум. документы	Ш6, С2
		эл. документы	ПК9, ПК18
2	Бизнес-план и стратегии развития	учредитель, директор	каб. учредителя каб. директора
		бум. документы,	Ш10, Ш14
		эл. документы	ПК17, ПК18
3	Договоры и контракты	бум. документы	Ст6
4	Архивы документов	бум. документы	Ш8
5	Состав и размер имущества компании	учредитель, директор, финансовый директор	каб. учредителя каб. директора зал опт. продаж
		бум. документы	С1,С2
6	Сведения о безопасности	начальник СБ	бухгалтерия
		бум. документы	Ст11
		эл. документы	ПК11
7	Бухгалтерская информация	главный бухгалтер	каб. гл. бухгалтера
		бум. документы	Ст10, Ст12, Ст16, Ш9
		эл. документы	ПК10, ПК12, ПК16
8	Доходы, объемы продаж	финансовый директор, главный бухгалтер	зал опт. продаж каб. гл. бухгалтера
		бум. документы	Ст5, Ст16, Ш9
		эл. документы	ПК5, ПК16
9	Себестоимость товаров	финансовый директор	зал опт. продаж
		бум. документы	Ст5
		эл. документы	ПК5
10	Анализ спроса и предложения	финансовый директор	зал опт. продаж
		эл. документы	ПК5
11	Сведения о конкурентах	начальник опт. продаж	зал опт. продаж

		бум. документы	Ст6
		эл. документы	ПК6
12	База данных клиентов фирмы	эл. документы	ПК6
13	База данных сотрудников	бум. документы	Ст14, Ш15
		эл. документы	ПК14
14	Записи телефонных перегово-ров с клиентами	эл. документы	Сервер, ПК11

Задача 3. Оценить относительную сложность преодоления препятствий для злоумышленника и оценить величину угрозы информации (из задачи 2) для различных путей проникновения в кабинет директора.



Способ проникновения	*Относительная сложность*
Окна в кабинетах	
Окна в кабинете директора	
Внутренние двери	
Внешние двери	
Видеокамеры	
ДРС	
Пролом стены	
Проход (спуск) через крышу	
ИК-датчик	
МК-датчик	
Отключение ПКП	
Отключение видеорегистратора	

ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

Министерство науки и высшего образования РФ Федеральное государственное бюджетное	10.04.01 Информационная безопасность (код и направление подготовки)

образовательное учреждение высшего образования «Сибирский государственный университет геосистем и технологий» Кафедра: информационной безопасности	Организация и управление информационной безопасностью (профиль подготовки) Управление информационной безопасностью (дисциплина)

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Что такое контентная категоризация?
2. Каковы основные принципы построения окружения файрвола? Что такое DMZ-сети? Что такое конфигурация с одной сетью, ServiceLeg конфигурация, конфигурация с двумя DMZ? Что такое виртуальные частные сети?
3. Провести пример реальной атаки и проанализировать сообщения от IDSSnort.

Составитель _____ И.О.Ф.
(подпись)

Заведующий кафедрой _____ И.О.Ф.
(подпись)

ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ

Раздел 1 «Предмет и содержание курса»

1. Совет по управлению информационной безопасностью.
2. Инфраструктура информационной безопасности.
3. Проектирование СУИБ.
4. Управление конфигурациями.
5. Управление инцидентами.
6. Управление проблемами.
7. Управление изменениями.
8. Управление релизами.
9. Процессы управления СУИБ.
10. Преимущества использования процесса.
11. Аудит информационной безопасности: виды аудита, принципы и процедура проведения.
12. Аудит информационной безопасности КИС.

Раздел 2 «Стандартизация в области управления ИБ»

1. Процесс утверждения средств обработки информации.
2. Распределение обязанностей, связанных с информационной безопасностью.
3. Разработка плана и механизмов внедрения требований СУИБ в реальную КИС.
4. Способы оценки информационной безопасности. Метрики информационной безопасности (ISO 27004, NIST 800-55).
5. Оценка информационной безопасности на основе моделей зрелости процессов (ISO 21827, ISO 15504, Cobit, стандарт ЦБ РФ СТО ИББС).

Раздел 3 «Процессный подход. Область деятельности СУИБ. Ролевая структура СУИБ. Политика СУИБ»

1. Построение СУИБ, консультации и сопровождение процесса внедрения.
2. Разработка процесса обучения сотрудников вопросам осведомленности их в области ИБ.
3. Предупреждения, определение новых угроз.
4. Взаимоотношения с другими процессами.

Раздел 4 «Управление рисками ИБ. Анализ рисков ИБ. Основные процессы СУИБ»

1. Сотрудничество между организациями.
2. Координация в области информационной безопасности.
3. Углубленный анализ информационных рисков с учетом их влияния на различные критерии ИБ (доступность, конфиденциальность, целостность).
4. Внутренние правила работы Политики Безопасности.

Раздел 5 «Внедрение мер (контрольных процедур) по обеспечению ИБ»

1. Контроль – политика и организация информационной безопасности.
2. Независимая оценка информационной безопасности.
3. Консультации специалистов по информационной безопасности.
4. Проверка соответствия политике безопасности и реализация Планов по безопасности;
5. Проведение аудита безопасности ИТ-систем.
6. Определение и принятие мер несоответствующего использования ИТ-ресурсов.
7. Проверка аспектов безопасности в других видах ИТ-аудита.
8. Отчеты об эффективности подпроцессов.
9. Результаты аудиторских проверок, анализа и внутренних оценок.

ФОНД ТЕСТОВЫХ ЗАДАНИЙ

1. Аудит информационной безопасности – это:

1) экспертное обследование различных аспектов защищенности информационных ресурсов

2) проверка правильности оформления и учета расходов на средства защиты информации

3) проверка уровня защищенности информационных ресурсов

2. Аудит информационной безопасности представляет собой:

1) проверку выполнения требований законодательства по защите сведений, составляющих коммерческую тайну

2) оценку мер по защите информационных ресурсов

3) проверку выполнения требований государственных стандартов в сфере информационной безопасности

3. Проведение комплексного внешнего аудита предприятия с последующей сертификацией демонстрирует его контрагентам:

1) способность предприятия выступать в качестве надежного партнера, которому можно доверить конфиденциальные сведения

2) полное отсутствие уязвимостей в сетях, серверах и базах данных

3) достаточную страховую защиту от информационных рисков

4. Сертификация системы безопасности на соответствие требованиям стандарта ISO 17799 может быть осуществлена по результатам:

1) внешнего аудита

2) внутреннего аудита

3) инструментальной проверки защищенности

5. Аудит информационной безопасности подразделяется на:

1) текущий и итоговый

2) внешний и внутренний

3) объективный и субъективный

6. Услуги внешних аудиторов используются для:

1) снижения затрат на аудит
2) повышения объективности аудита
3) получения сертификатов на соответствие определенным стандартам

7. Инициирование аудита информационной безопасности на предприятии производится:
1) аудиторскими организациями
2) руководством предприятия
3) пользователями информационной системы предприятия

8. Инициаторами аудита информационной безопасности могут выступать:
1) государственные структуры
2) органы стандартизации
3) руководители предприятия

9. Цели аудита информационной безопасности могут включать в себя:
1) выявление лиц, нарушающих требования информационной безопасности
(2) сертификацию на соответствие общепризнанным требованиям и стандартам
3) установление степени защищенности информационных ресурсов

10. К целям аудита информационной безопасности относятся:
1) проверка достижения поставленных целей в сфере информационной безопасности
2) выявление фактов нарушения информационной безопасности
3) привлечение к ответственности лиц, виновных в краже и утрате конфиденциальных данных

11. Заключительной стадией аудита является:
1) внесение изменений в действующие политики безопасности
2) проведение аттестации сотрудников департамента информационной безопасности
3) формирование аудиторского заключения

12. Для поддержки разработки политик безопасности используются:
1) автоматизированные сканеры уязвимостей
2) электронные справочные системы
3) средства управления паролями

13. Электронные справочные системы по информационной безопасности содержат:
1) образцы заключений по результатам аудиторских проверок политики безопасности
2) образцы политик безопасности
3) образцы шаблонов и бланков документов, используемых для управления безопасностью

14. В электронных справочных системах, используемых для управления информационной безопасностью, содержатся:
1) типовые регламенты аудита информационной безопасности
2) типовая документация на системы защиты информации
3) типовые политики безопасности

15. В системах автоматизированного интерактивного анализа политик безопасности заключения о состоянии политики безопасности формируются на основе:
1) результатов аудита информационной безопасности
2) ответов на вопросы, задаваемые программой
3) семантического анализа текстов политик безопасности

16. Перечень систем, процессов и действий, которые могут подвергаться мониторингу, включает в себя, но не ограничивается следующим:

1) реализация процессов СМИБ

2) менеджмент инцидентов

3) менеджмент уязвимостей

4) анализ уязвимостей

17. Потенциальными кандидатами для оценки защищенности являются следующие процессы и действия СМИБ:

1) планирование

2) руководство

3) анализ управления

4) анализ уязвимостей

18. Мониторинг, оценка защищенности, анализ и оценивание, показанные на рисунке 2 состоят из следующих процессов:

1) выявление информационных потребностей

2) спецификация и поддержка показателей

3) установка процедур

4) анализ базовой конфигурации

19. Независимо от того, выполняется ли оценка защищенности вручную или автоматизировано, организации могут определить следующие роли и обязанности, связанные с оценкой защищенности:

1) потребитель оценки защищенности

2) планировщик оценки защищенности

3) рецензент оценки

4) эксперт органа по аттестации

20. В зависимости от целей для количественной оценки могут использоваться показатели эффективности, такие, как:

1) экономия средств, связанная с использованием СМИБ или за счет сокращения затрат на устранение последствий инцидентов ИБ

2) повышение степени доверия клиентов из-за использования СМИБ

3) достижение других целей ИБ

4) снижение категории/класса защиты объекта информатизации

8 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «ФИЛОСОФСКИЕ ПРОБЛЕМЫ НАУКИ И ОБЩЕСТВА»

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ЗАЧЕТУ

1. Предмет и задачи философии науки.
2. Наука и философия.
3. Наука как социальный институт.
4. Роль науки в истории общества.
5. Научные революции в истории науки.
6. Современная научная картина мира.
7. Научное и вненаучное познание. Паранаука.
8. Научная проблема.
9. Научная гипотеза.
10. Понятие научного факта.
11. Эмпирический уровень научного познания.
12. Теоретический уровень научного познания.
13. Метод и методология. Классификация методов.
14. Критерии научного исследования.
15. Знание и научная истина.
16. Идеалы и нормы научного исследования.
17. Системный подход в науке.
18. Синергетика как новая научная парадигма.
19. Компьютеризация науки и ее последствия.
20. Сущность техники. Техническое и техническое.
21. Философия техники как раздел философского знания.
22. Взаимоотношение науки и техники в истории общества.
23. Технические науки как область философии техники.
24. Специфика технических наук и особенности технической теории.
25. Особенности современных неклассических научно-технических дисциплин.
26. Естествознание и технические науки.
27. Технологический детерминизм и технократия.
28. Инженерная этика и ответственность ученого.
29. Социальная оценка техники и социально-экологическая экспертиза.
30. Научно-технический прогресс и концепция устойчивого развития.

ТИПОВЫЕ ПРАКТИЧЕСКИЕ ЗАДАНИЯ ДЛЯ ПОДГОТОВКИ К ЗАЧЕТУ

1. По таблице распределите объекты и предметы изучения:

	Объект	Предмет
Технология	а) Техника, техническое действие и техническое знание	I) Техническое действие
Технические науки	б) Техника и техническое действие	II) Развитие технического сознания
Философия техники	в) Техника (артефакт)	III) Техническое знание

2. Как соотносятся между собой философия и наука?

а) философия является частью науки,
б) наука является частью философии,
в) философия и наука частично включаются друг в друга,
г) философия и наука исключают друг друга.

4. Установите соответствие между естественнонаучной картиной мира и принятыми в ней представлениями о пространстве и времени: 1) механистическая картина мира, 2) классическая картина мира, 3) современная научная картина мира:

а) пустого пространства не существует; физический вакуум – материальный, активный элемент устройства вселенной, наличие у которого энергии заставляет её расширяться с ускорением.

б) пространство и время представляют собой некоторые субстанции, существующие сами по себе, вне какой-либо связи с материальными телами.

в) пространство изотропно, но неоднородно: у вселенной существует центр, от которого разбегаются галактики.

г) пространство и время представляют собой систему отношений между материальными телами, которая зависит от выбора системы отсчёта.

5. Установите соответствие между естественнонаучной картиной мира и принятыми в ней представлениями о движении: 1) механистическая картина мира 2) электромагнитная картина мира 3) синергетическая научная картина мира:

а) всё происходящее в мире сводится к перемещению заряженных частиц и изменению создаваемых ими полей.

б) существуют качественно различные, несводимые друг к другу формы движения; вселенная существует не просто в движении, а в развитии.

в) всё происходящее в мире сводится к перемещению тел и частиц; принципиальных различий между разными формами движения не существует.

г) движение – это любое изменение вообще; источником движения материи является перводвигатель, расположенный за пределами вселенной.

6. Установите соответствие между естественнонаучной картиной мира и принятыми в ней представлениями о детерминированности событий в мире: 1) механическая картина мира, 2) электромагнитная картина мира, 3) современная научная картина мира:

а) можно однозначно определить состояние материальной точки для любого прошлого и будущего момента времени, зная координаты и скорость в начальный момент и действующие на неё силы.

б) точное предсказание будущего состояния любого материального объекта невозможно, поскольку требует знания «скрытых параметров», измерить которые существующие приборы не могут.

в) точный прогноз будущего невозможен; можно предсказать лишь возможные варианты будущего и вероятности их осуществления.

г) можно точно рассчитать будущее вселенной, зная, как в ней распределены физические поля и порождающие их заряженные частицы.

7. Установите соответствие между структурным уровнем материи и объектами, относящимися к нему: 1) мегамир, 2) макромир, 3) микромир:

а) кучевое облако и электронное облако,

б) газопылевая туманность и нейтронная звезда,

в) кучевое облако и туман,

г) электронное облако и кварк.

8. Установите соответствие между структурными единицами вещества и их характерными размерами: 1) ядра атомов, 2) атомы, 3) бактерии:

а) несколько микрометров (10^{-6} м),

б) доли миллиметра (10^{-3} м),

в) несколько фемтометров (10^{-15} м),

г) доли нанометра (10^{-9} м).

9. Установите соответствие между свойством системы и примером проявления этого свойства: 1) проявление интегративных свойств, 2) проявление аддитивных свойств, 3) проявление иерархичности систем:

а) молекула белка обладает свойствами, которые не присущи свойствам аминокислот, из которых она построена,

б) в химических расчётах масса молекулы является суммой масс атомов, из которых она состоит,

в) молекулы состоят из атомов, а атомы – из элементарных частиц,

г) свойства молекулы белка полностью определяются свойствами аминокислот, из которых белок построен,

10. Теория истолкования, имеющая целью выявить смысл текста, исходя из его объективных (значение слов и их исторически обусловленные вариации) и субъективных (намерения авторов) оснований, называется: а) методология, б) гносеология, в) герменевтика, г) пропедевтика.

11. Назовите основные три значения понятия науки (выберите три правильных варианта):

а) форма духовной деятельности;

б) система дисциплинарных знаний;

в) социальный институт;

г) единственный способ получения объективной истины;

д) строго математизированное знание;

отчасти систематизированное знание.

12. Расположите перечисленные формы научного познания в соответствии с последовательностью, которая имеет место в реальном процессе научного познания:

1) теория; 2) факт; 3) гипотеза; 4) проблема.

а) 1, 3, 2, 4;

б) 4, 2, 3, 1;

в) 2, 4, 1, 3;

г) 2, 4, 3, 1.

13. Перечислить методы и средства, которые используются на эмпирическом и теоретическом уровне исследования:

а) наблюдение, эксперимент, сравнение, измерение, описание, приборы и приборные установки;

б) мысленный эксперимент, идеализация, аксиоматический метод, гипотетико- дедуктивный метод.

14. Расположите феномены в порядке от наиболее общих (абстрактных) к конкретным:

а) научно-техническая революция

б) информатизация

в) прогресс

г) развитие

д) изменение

15. Распределите отрасти техники на пассивные и активные:

а) военные машины,

б) производственные машины,

в) железнодорожные пути,

г) телефон, телеграф,

д) средства умственного труда,

е) мосты, тоннели.

ВОПРОСЫ ДЛЯ ЗАЩИТЫ ПРАКТИЧЕСКИХ РАБОТ

Практическая работа 1. Специфика философского знания

1. Определите понятие мировоззрения.
2. Какой способ существования присущ природе?
3. Какой способ существования присущ обществу?
4. Какой способ существования присущ Богу?

5. Какой способ существования присущ человеку?
6. Что стало причиной смены мифологии новыми формами идеологии?
7. В чем заключается специфика религии?
8. В чем заключается специфика науки?
9. В чем заключается специфика искусства?
10. В чем заключается специфика философии?
11. Какова последовательность этапов эволюции философского знания?
12. С чем связано изменение предмета философии в истории мировоззрения?
13. Что такое метод?
14. Какие методы эффективны?
15. Какой метод оптимален?
16. Какие методы использует теоретик?
17. Что характерно для метафизического метода мышления?
18. Каковы принципы формальной логики?
19. Что характерно для диалектического метода мышления?
20. Каковы принципы диалектической логики?
21. Проиллюстрируйте целостный характер мифа.
22. Найдите примеры современной мифологии.
23. Покажите общность и различие философии и религии.
24. Покажите общность и различие философии и науки.
25. Покажите общность и различие философии и искусства.
26. Определите специфику философского знания как рефлексию.
27. Покажите, что определяет эпоху в развитии духовной культуры общества.
28. Покажите на примере разные способы решения одной и той же задачи.
29. Подберите примеры формально-логического мышления.
30. Подберите примеры диалектического мышления.

Практическая работа 2. Философия культуры

1. Чем искусственное отличается от естественного?
2. Каков первоначальный смысл слова «культура»?
3. Чем общество людей отличается от животных «сообществ»?
4. Как проявляет себя разум на поверхности планеты Земля?
5. Зачем и когда появляются города?
6. Что изучает аксиология?
7. Как и почему дифференцируется социум?
8. В чем специфика людей, вещей, институтов и знаков как типов ценностей?
9. Как соотносятся язык и речь, языки «живые» и «мертвые»?
10. Когда и зачем изобретается письменность?
11. Почему зависимость ценности людей и вещей от затрат прямая?
12. Почему зависимость ценности социальных ролей и знаков от затрат обратная?
13. Обоснуйте отличие культуры от натуры.
14. Рассудите, есть ли граница у ноосферы.
15. Дайте определение ценности и разверните его содержание.
16. Проиллюстрируйте принцип социального эгоцентризма.
17. Постройте иерархию ценности вещей: «дом», «автомобиль», «дача», «зажигалка», «мобильник», «планшетник».
18. Ранжируйте ценности: «любовь», «образование», «здоровье», «богатство», «власть».

Практическая работа 3. Философская антропология

1. Какие стороны существа раскрывают определения человека?
2. Что определяет сущность человека?
3. Какие стадии проходит процесс социализации индивида?
4. Что определяет человека как ценность?
5. Каковы главные факторы антропогенеза?

6. Что является источником индивидуального сознания?
7. Какие элементы сознания являются природными по происхождению?
8. Какие элементы сознания формируются культурой?
9. Что является решающим фактором свободы воли?
10. В чем полнее всего проявляется свобода человека?
11. Что придает жизни человека смысл?
12. В чем выражается достоинство смерти?
13. Перечислите свойства человека как индивида.
14. Перечислите качества человека как личности.
15. Проиллюстрируйте принцип комбинаторности в формировании индивидуальности человека.
16. Покажите, как орудийная деятельность животных превращается в человеческий труд.
17. Охарактеризуйте системообразующую роль мышления в структуре индивидуального сознания.
18. Перечислите возможные цели, придающие жизни смысл.

Практическая работа 4. Философия науки

1. Что отличает науку от религии и искусства?
2. Какой характер имела наука в эпоху Античности?
3. Какой характер приобрела наука в Средние века?
4. Чем занималась наука в эпоху Возрождения?
5. Каковы характерные черты эмпирической науки Нового времени?
6. Каковы признаки классицизма применительно к науке?
7. Какой характер имела наука в XIX веке?
8. В чем проявляется неклассический характер науки в XX веке?
9. Что такое парадигма по версии Томаса Куна?
10. Что предполагает исследовательская программа у Пола Фейерабенда?
11. Сравните признаки науки и религии.
12. Сравните признаки науки и искусства.
13. Покажите общее и особенное в науке и философии.
14. Выведите зависимость характера науки от доминант культуры в разные эпохи.
15. Сопоставьте специфику предмета философии и характер науки в разные эпохи.

Практическая работа 5. Философия техники

1. Каково происхождение слова «техника»?
2. В чем состоит различие техники и технологии?
3. Что означают понятия: артефакт, инструмент, механизм, машина, автомат, робот?
4. К какому виду техники относится компьютер?
5. Какое общество называют информационным?
6. Какой смысл вкладывает Мартин Хайдеггер в понятие «постав»?
7. Что такое компьютерный вирус?
8. Была ли техника у древнего человека?
9. Оцените техническую базу патриархального общества.
10. Охарактеризуйте промышленную революцию Нового времени.
11. Покажите важнейшие черты индустрии.
12. Перечислите ступени развития орудий, двигателей и элементов управления в технических устройствах.
13. Оцените отличия станка от машины, машины от автомата, автомата от робота.
14. Оцените перспективы дальнейшей эволюции техники в обозримом будущем человечества.

ФОНД ТЕСТОВЫХ ЗАДАНИЙ

1. В какой картине мира «естественное» и «сверхъестественное» не отличаются друг от друга?
а) в научной,
б) в религиозной,
в) в мифологической,
г) в философской.
2. Как соотносятся между собой философия и наука?
а) философия является частью науки,
б) наука является частью философии,
в) философия и наука частично включаются друг в друга,
г) философия и наука исключают друг друга.
3. Что отражает в себе предмет философии?
а) уникальность мира,
б) всеобщность мира,
в) полезность мира,
г) упорядоченность мира.
4. В отличие от науки, философия …
а) является систематизированным знанием,
б) внутренне непротиворечива,
в) опирается на факты,
г) постигает мир в его универсальной целостности.
5. Как называется функция философии, связанная с разработкой и осмыслением способов познания мира?
а) гуманистическая,
б) критическая,
в) методологическая,
г) мировоззренческая.
6. Для развития философии не характерно:
а) преемственность,
б) влияние научных достижений,
в) ценностная составляющая,
г) догматизм.
7. Основной вопрос философии – это:
а) учение о бессмертии индивидуальной души,
б) вопрос о соотношении сознания и бытия,
в) учение о гармоничном развитии личности,
г) проблема происхождения жизни и разума.
8. Что Арнольд Тойнби считал основным объектом философского изучения истории?
а) общественно-экономические формации,
б) национально-исторические системы,
в) духовно-исторические основы общества,
г) культурно-исторические типы общества.
9. Основанием общественной жизни в марксизме считается…
а) наука,
б) рост населения,
в) нормативные установления,
г) способ производства.
10. Нормы, в которых зафиксировано формальное равенство людей,
а) право,
б) политика,
в) мораль,
г) религия.

11. Какое учение имеет своим предметом систему ценностей?
а) аксиология,
б) квиетизм,
в) герменевтика,
г) фидеизм.
12. Что является определяющим признаком для понятия «ценности»?
а) справедливость и добропорядочность,
б) драгоценности и богатство.
в) то, что значимо в жизни,
г) то, что является необходимым в жизни.
13. В философии «агностицизм» - это…
а) рассмотрение процесса познания,
б) рассмотрение объектов познания,
в) отрицание принципиальной возможности познания мира,
г) сомнение в возможности познания мира.
14. Поскольку истина не зависит от познающего субъекта, она…
а) абстрактна,
б) объективна,
в) субъективна,
г) абсолютна.
15. Какой ответ на вопрос о том, что является источником познания, дает рационализм?
а) единственным источником познания является интуиция,
б) источником познания является опыт,
в) источником познания является разум,
г) источником познания являются ощущения.
16. Получение знания без осознания процесса логических рассуждений, ведущих к нему есть:
а) интроспекция,
б) интуиция,
в) интенция,
г) дефиниция.
17. Форма научного знания, содержащая предположения и нуждающаяся в доказательстве, есть:
а) теория,
б) принцип,
в) закон,
г) гипотеза,
18. Совокупность каких признаков обязательна для научной теории?
а) системность, непротиворечивость, объективность, проверяемость, универсальность;
б) непротиворечивость, проверяемость, принципиальная опровержимость, объективность, системность;
в) объективность, непротиворечивость, очевидность, системность, проверяемость;
г) проверяемость, непротиворечивость, объективность, системность, неизменность.
19. К эмпирическому уровню научного познания относится …
а) выдвижение гипотез,
б) построение картины мира,
в) построение теории,
г) анализ фактов.
20. Расположите перечисленные формы научного познания в соответствии с последовательностью, которая имеет место в реальном процессе научного познания: 1) теория; 2) факт; 3) гипотеза; 4) проблема.
д) 1, 3, 2, 4;
е) 4, 2, 3, 1;

ж) 2, 4, 1, 3;
з) 2, 4, 3, 1.

21. Начало научно-технической революции приходится на период …
а) начала XIX в.,
б) середины XX в.,
в) конца XIX в.,
г) начала XX в.

22. Какое положение верно отражает соотношение науки и этики в реальном процессе научного познания?
а) Все, что объективно истинно, то нравственно;
б) Достижения науки не могут быть безнравственными;
в) Научные теории могут быть как нравственными, так и безнравственными;
г) Нравственная оценка относится только к использованию научных положений.

23. Этот философ считал, что техника убийственно действует на душу
а) Э. Тоффлер,
б) Н. Бердяев,
в) Д. Белл,
г) У. Ростоу.

24. Наука как специфический тип духовного производства и социальный институт возникла в эпоху…
а) античности,
б) средних веков,
в) Возрождения,
г) Нового времени.

25. Второй период научно-технической революции приходится на …
а) начала XIX в.,
б) середины XX в.,
в) конца XIX в.,
г) 70-ые гг. XX в.

26. Техническая революция сопровождается….
а) созданием атомной энергетики,
б) машинизацией производства,
в) возникновением генной инженерии,
г) применением нанотехнологий.

27. Укажите, в каком из суждений нашла отражение точка зрения антисциентизма:
а) наука - источник прогресса человеческого общества;
б) научные достижения могут быть использованы как на благо, так и во зло;
в) объективная истина представляет собой абсолютную ценность, которая стоит вне всякой этической оценки;
г) наука есть институт, который в современных условиях стал враждебен человеку, он ведет к дегуманизации природы и общества.

ТЕМЫ РЕФЕРАТОВ

1. Философия науки: предмет, метод, функции.
2. Методы философского анализа науки.
3. Философия техники: предмет, метод, функции.
4. Основные постулаты классической социологии знания.
5. Диахронное и синхронное разнообразие науки.
6. Свобода научных исследований и социальная ответственность ученого.
7. Особенности научной политики на рубеже третьего тысячелетия.
8. Основные концепции взаимоотношения науки и философии.

9. Проблема преемственности в развитии научных теорий. Кумулятивизм и парадигматизм.
10. Основные философские парадигмы в исследовании науки.
11. Философские проблемы науки и методы их исследования.
12. Социально-психологические основания научной деятельности.
13. Философские основания и проблемы социального познания.
14. Человек как предмет комплексного философско-научного исследования.
15. Философские проблемы управления научным коллективом
16. Основные проблемы современной философии науки.
17. Типология представлений о природе философии науки.
18. Философия науки как историческое социокультурное знание.
19. Философия науки и близкие ей области науковедения.
20. Социологический подход к исследованию развития науки.
21. Место науки в культуре техногенной цивилизации.
22. Особенности науки как особой сферы познавательной деятельности.
23. Наука и культура: механизм взаимодействия.
24. Наука как особая сфера культуры.
25. Изменение базисных ценностей науки в традиционалистской и техногенной традиции;
26. Функции науки в жизни общества.
27. Особенности науки как социального института;
28. Наука и экономика.
29. Наука и власть.
30. Наука и общество: формы взаимодействия.
31. Эволюция способов трансляции научного знания.
32. Проблемы государственного регулирования науки.
33. Научное и вненаучное знание.
34. Роль науки в современном образовании и формировании личности.
35. Соотношение науки и философии.
36. Наука и искусство как формы познания мира.
37. Наука и игра, их роль в познании мира.
38. Наука и обыденное познание.
39. Научная деятельность и ее структура.
40. Научная рациональность, ее основные характеристики.
41. Философские основания науки, их виды и функции.
42. Механизм и формы взаимосвязи конкретно-научного и философского знания.
43. Наука и глобальные проблемы человечества.
44. Естественно-научная и гуманитарная культура.
45. Проблемы развития современной российской науки.
46. Возникновение античной науки: атомистическая научная программа.
47. Математическая программа в античной науке.
48. Судьба античных научных программ в Средние века.
49. Формирование науки Нового времени в трудах Галилея.
50. Научная программа Ньютона.
51. Теория относительности А. Эйнштейна и становление неклассической науки.
52. Арабская наука и ее роль в развитии европейской культуры.
53. Социально-исторические предпосылки и специфические черты средневековой науки.
54. Исследование феномена науки и ее соотношения с философией в «Метафизике» и «Физике» Аристотеля.
55. Учение Ф. Бэкона о науке и ее роли в прогрессе человеческого общества. («Новый Органон»). 56. Р. Декарт о науке и методе научного исследования («Рассуждение о методе»).
57. Учение Г. Лейбница о методе.
58. И. Кант об основаниях научного анализа и методологической функции метафизики («Критика чистого разума»).

59. Г. Гегель о философии как «науке наук» и роли диалектического метода в конструировании научного знания («Энциклопедия философских наук», т. 1).
60. С. Булгаков о науке и прогрессе («Философия хозяйства»: природа науки; основные проблемы теории прогресса).
61. В. Вернадский о науке и ее роли в становлении ноосферы («О науке», «Научная мысль как планетное явление»).
62. Г. Риккерт о науке («Науки о природе и науки о культуре»).
63. М. Хайдеггер о науке нового времени и технике как судьбе европейского человечества («Наука и осмысление»).
64. Учение Х. Ортеги-и-Гассета о науке и технике («Положение науки и исторический разум»).
65. М. Вебер о науке и «рационализации» мира («Наука как призвание и профессия»).
66. Г. Гадамер о научном познании («Истина и метод»).
67. А. Уайтхед о науке и современной цивилизации («Избранные работы по философии»).
68. Д. Бернал о роли науки в жизни общества («Наука в истории общества»).
69. Б. Рассел о научном познании («Человеческое познание», «Философия логического атомизма»).
70. Неопозитивизм Л. Витгенштейна («Логико-философский трактат»).
71. Р. Карнап о философии и науке («Философские основания физики»).
72. Роль конструирования в математическом познании (Г.Б. Лейбниц).
73. Скептицизм и наука (Д. Юм).
74. Рождение культа науки в эпоху просвещения (А. Тюрго, Ж. Кондорсе).
75. История науки в философии Ж.Ж. Руссо.
76. Первый позитивизм как философия науки. (О. Конт, Г. Спенсер).
77. Критика науки в «философии жизни» Ф. Ницше, А. Бергсона.
78. Проблема науки в неокантианстве.
79. Образ науки в русской философии.
80. Философия русского космизма.
81. Философские проблемы теории относительности.
82. Взаимодействие науки и философии в русской культуре.
83. Взаимодействие эксперимента и теории в их развитии.
84. Научное предвидение, его формы и возможности.
85. Виды научных гипотез и их эвристическая роль.
86. Гносеологические проблемы научного прогнозирования.
87. Научная идея, ее социокультурная и гносеологическая обусловленность.
88. Структура и функции научной теории.
89. Проблема истины в научном познании.
90. Идеалы и нормы научного познания.
91. Научная картина мира и стиль научного мышления.
92. Научные законы и их классификация
93. Основные философские парадигмы в исследовании науки.
94. Проблема преемственности в развитии научных теорий
95. Философские основания науки и их виды.
96. Проблемы и перспективы современной герменевтики.
97. Структурализм как междисциплинарная научная парадигма.
98. Эволюционная эпистемология К. Поппера.
99. Развитие науки как смена парадигм (Т. Кун).
100. Структура научно-исследовательских программ (И. Лакатос).
101. Методологический анархизм П. Фейерабенда.
102. Эпистемология неявного знания М. Полани.
106. Понятие научной революции и ее виды.
107. Наука и глобальные проблемы современного человечества.
108. Роль и функции науки в инновационной экономике.

109. Неклассическая наука и ее особенности.
110. Главные характеристики современной постнеклассической науки.
111. Философско-социологические проблемы развития техники.
112. Традиции и революции в истории науки.
113. Основные проблемы современной философии техники.
114. Наука и техника, эволюция взаимоотношений.
115. Техника как специфическая форма культуры.
116. Техногенная цивилизация и философское осмысление ее судеб.
119. Синергетика и становление постнеклассической науки
120. Коэволюционная стратегия в современной науке.
121. Информационные технологии в современной науке.
122. Экологическая проблематика в современном научном мировоззрении.
123. Синергетика как новое миропонимание.
124. Идея универсального эволюционизма в науке XX–XXI вв.
125. Особенности стиля мышления науки XX–XXI вв.
126. Экологическая проблема, ее научные, социально-философские и этико- гуманистические аспекты.
127. Человек и ноосфера.
128. Понятие самоорганизации в современной науке.
129. Научное познание и ценности техногенной цивилизации.
130. Проблема рациональности на рубеже XX–XXI вв.
131. Свобода научного поиска и социальная ответственность ученого.
132. Этические проблемы науки
133. Концепции постиндустриального общества.
134. Синергетическая парадигма в современной науке.

9 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «МЕТОДЫ И СРЕДСТВА ПРОТИВОДЕЙСТВИЯ ТЕХНИЧЕСКИМ КАНАЛАМ С ИСПОЛЬЗОВАНИЕМ БПЛА»

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ

1. Что такое технические каналы утечки информации. Классификация?
2. Каковы цели и задачи инженерно-технической защиты информации?
1. Что такое коммерческая разведка. Промышленный шпионаж?
2. Что такое ТСПИ и ВТСС?
3. Что такое акустические речевые сигналы. Особенности их восприятия?
4. Что такое фонемы, октавы и форманты в акустическом речевом сигнале?
5. Что такое разборчивость речи?
6. Что такое словесная, слоговая и другие виды разборчивости речи?
7. Каковы характеристики речевого сигнала?
8. Каковы обстоятельства, влияющие на разборчивость речи?
9. Каков порядок расчёта словесной разборчивости?
10. Каковы наиболее опасные объекты с точки зрения акустической разведки?
11. Что такое средства скрытого видеонаблюдения?
12. Что такое угрозы безопасности информации?
13. Что такое электромагнитный канал утечки информации?
14. Что такое электрический канал утечки информации?
15. Что такое параметрический канал утечки информации?
16. Что такое акустический канал утечки информации?
17. Что такое вибрационный канал утечки информации?
18. Что такое визуальный канал утечки информации?
19. Каковы средства перехвата акустической информации?
20. Что такое направленные микрофоны. Виды?
21. Каковы характеристики направленных микрофонов?
22. Что такое трубчатый, щелевой направленный микрофон?
23. Что такое направленный микрофон органного типа?
24. Что такое параболический направленный микрофон?
25. Каково применение направленных микрофонов на открытой местности и в помещниях?
26. Каковы способы защиты информации от утечки через канал ПЭМИН?
27. Что такое активная радиотехническая маскировка?
28. Какова эффективность экранирования от ПЭМИН?
29. Каковы физические процессы при электромагнитном экранировании?
30. Каковы материалы, применяемые при экранировании от ПЭМИН?
31. Каковы способы экранирования от ПЭМИН?
32. Что такое звукопоглощающие материалы и конструкции?
33. Что такое звукопоглощающие конструкции?
34. Что такое резонансные звукопоглотители?
35. Что такое виброизоляция?
36. Каковы цели и задачи инженерно-технической защиты информации?
37. Что такое коммерческая разведка. Промышленный шпионаж?

.

ТИПОВЫЕ ПРАКТИЧЕСКИЕ ЗАДАНИЯ ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ

Задача № 1.

На открытом участке местности, в идеальных условиях слова команд начальника службы безопасности, подаваемые голосом, воспринимаются его сотрудниками, находящимися на рас-

стоянии 0,4 м., как 68 дБ по уровню громкости звука. Определить предельную дальность регистрации этих команд подслушивающим аудиооператором, воспринимающим эту информацию на слух. Аудиооператор воспринимает информацию вплоть до порога чувствительности человеческого уха.

Задача №2.

Трубчатый щелевой направленный микрофон при всех закрытых отверстиях на боковой поверхности трубки выделяет звук с частотой f1=280Гц в качестве основной звуковой частоты. Определить на каком расстоянии d от входа в эту трубку должно быть открыто отверстие, чтобы работающий при 0° С такой микрофон кроме звука с частотой 280 Гц, выделял бы звук с основной частотой f2=600Гц.

Задача №3

Конструкция направленного микрофона органного типа предполагает наличие семи трубок разной длины, равномерно уменьшающихся от наибольшей к наименьшей. Рассчитать, какой длины должны быть эти трубки, если необходимо выделить спектр частот человеческой речи от 200 до 4000 Гц.

Задача №4

Определить дальность распознавания лица человека (20 см), при условии, что камера наблюдает его массивом элементов матрицы ПЗС размером 40х40. Разрешение матрицы 1024х768.

Вариант	1	2	3	4	5	6	7	8	9
Формат, дюйм	1/4	1/3	1/2	1/5	1/4	1/3	1/2	1/5	1/4
Фокусное расст., мм	8,5	8	6,4	5,8	4,3	3,8	8,5	8	6,4

Вариант	10	11	12	13	14	15	16	17	18
Формат, дюйм	1/3	1/2	1/5	1/4	1/3	1/2	1/5	1/4	1/3
Фокусное расст., мм	5,8	4,3	3,8	7,5	5,2	6,0	2,8	4,3	3,2

ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

Министерство науки и высшего образования РФ Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет геосистем и технологий»	10.04.01 Информационная безопасность (код и направление подготовки) Организация и управление информационной безопасностью (профиль подготовки) Методы противодействия техническим

Кафедра: информационной безопасности	каналам с использованием БПЛА (дисциплина)

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Что такое технические каналы утечки информации, классификация?
2. Что такое звукопоглощающие материалы и конструкции?
3. Трубчатый щелевой направленный микрофон при всех закрытых отверстиях на боковой поверхности трубки выделяет звук с частотой f1=280Гц в качестве основной звуковой частоты. Определить на каком расстоянии d от входа в эту трубку должно быть открыто отверстие, чтобы работающий при 0° С такой микрофон кроме звука с частотой 280 Гц, выделял бы звук с основной частотой f2=600Гц.

Составитель _____ И.О.Ф.
(подпись)

Заведующий кафедрой _____ И.О.Ф.
(подпись)

Шкала и критерии оценивания

Ответ обучающегося на экзамене оценивается по пятибалльной шкале:

– *оценка «отлично»* – ответы обучающегося на вопросы экзаменационного билета и дополнительные вопросы экзаменатора полные, аргументированные, обстоятельные; высказываемые предположения подтверждены конкретными примерами; практические задания выполнены по стандартной или самостоятельно разработанной методике, в полном объеме, без ошибок в расчетах, с подробными пояснениями, сделаны полные аргументированные выводы;

– *оценка «хорошо»* – обучающийся ответил на все вопросы задания, дал точные определения и понятия; однако затрудняется подтвердить теоретические положения практическими примерами; практические задания выполнены по стандартной методике без ошибок в расчетах, однако даны недостаточно полные пояснения по анализу показателей;

– *оценка «удовлетворительно»* – обучающийся правильно ответил на все вопросы, но с недостаточно полной аргументацией; выполнил не менее 50 % практических заданий;

– *оценка «неудовлетворительно»* – обучающийся не смог ответить на 2/3 вопросов билета; не справился с практическим заданием или выполнил менее 50 % практических заданий.

ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ

Раздел 1

1. Что такое технические каналы утечки информации. Классификация?
2. Что такое объект защиты информации?
3. Виды угроз объектам защиты?
4. Каковы цели и задачи инженерно-технической защиты информации?
5. Основные этапы построения модели объекта защиты?
6. Основные этапы модели угроз?
7. Привести примеры организационных и технических мер защиты информации.
8. Что такое акустические речевые сигналы. Особенности их восприятия?
9. Что такое фонемы, октавы и форманты в акустическом речевом сигнале?
10. Что такое разборчивость речи?
11. Что такое словесная, слоговая и другие виды разборчивости речи?
12. Каковы характеристики речевого сигнала?
13. Каковы обстоятельства, влияющие на разборчивость речи?
14. Каков порядок расчёта словесной разборчивости?

Раздел 2

1. Что такое угрозы безопасности информации?
2. Что такое электромагнитный канал утечки информации?
3. Что такое электрический канал утечки информации?
4. Что такое параметрический канал утечки информации?
5. Что такое акустический канал утечки информации?
6. Что такое вибрационный канал утечки информации?
7. Что такое визуальный канал утечки информации?
8. Каковы цели канала утечки ПЭМИН?
9. Каковы источники и особенности ПЭМИН?
10. Каковы средства перехвата акустической информации?
11. Каковы особенности использования виброакустического канала?
12. Что такое направленные микрофоны. Виды?
13. Каковы характеристики направленных микрофонов?
14. Что такое трубчатый, щелевой направленный микрофон?
15. Что такое направленный микрофон органного типа?
16. Что такое параболический направленный микрофон?
17. Каково применение направленных микрофонов на открытой местности и в помещниях?
18. Каковы наиболее опасные объекты с точки зрения акустической разведки?
19. Что такое средства скрытого видеонаблюдения?

ПРИМЕРНЫЕ ТЕМЫ РЕФЕРАТОВ

1) Современные системы БПЛА
2) Оптические средства разведки на беспилотных аппаратах
3) Сравнительный анализ систем оптической и акустической разведки БПЛА

Шкала и критерии оценивания

Опрос оценивается по пятибалльной шкале:

Балл	*Критерии оценки (содержательная характеристика)*
1 (неудовлетворительно) Повторная подготовка	Обучающийся не владеет теоретическим материалом, допуская грубые ошибки, испытывает затруднения в формулировке собственных суждений, неспособен ответить на дополнительные вопросы
2 (неудовлетворительно) Повторная подготовка	Обучающийся практически не владеет теоретическим материалом, допуская ошибки по сущности рассматриваемых (обсуждаемых) вопросов, испытывает затруднения в формулировке собственных обоснованных и аргументированных суждений, допускает ошибки при ответе на дополнительные вопросы
3 (удовлетворительно)	Обучающийся владеет теоретическим материалом на минимально допустимом уровне, отсутствуют ошибки при описании теории, испытывает затруднения в формулировке собственных обоснованных и аргументированных суждений, допуская незначительные ошибки на дополнительные вопросы
4 (хорошо)	Обучающийся владеет теоретическим материалом, отсутствуют ошибки при описании теории, формулирует собственные, самостоятельные, обоснованные, аргументированные суждения, допуская незначительные ошибки на дополнительные вопросы

5 (отлично)	Обучающийся владеет теоретическим материалом, отсутствуют ошибки при описании теории, формулирует собственные, самостоятельные, обоснованные, аргументированные суждения, представляет полные и развернутые ответы на дополнительные вопросы

ФОНД ТЕСТОВЫХ ЗАДАНИЙ

1. Технические каналы утечки информации. Уберите лишний.

a) Акустический;
b) Визуальный;
c) Фотографический;
d) Электромагнитный

2. Промышленный шпионаж это:
a) Кража деталей из промышленного цеха;
b) Кража конфиденциальной информации;
c) Разведка на поле боя.

3. Направленный микрофон относится к каналу утечки информации
a) Акустический;
b) Визуальный;
c) Материальный;
d) Электромагнитный.

4. Радиозакладка относится к каналу утечки информации
a) Акустический;
b) Визуальный;
c) Материальный;

5. Скрытая видеокамера относится к каналу утечки информации
a) Акустический;
b) Визуальный;
c) Материальный;
d) Электромагнитный.

6. Средства прослушивания телефонной линии относятся к каналу утечки информации:
a) Акустический;
b) Визуальный;
c) Материальный;
d) Электромагнитный.

7. Кража документов относится к каналу утечки информации
a) Акустический;
b) Визуальный;
c) Материальный;
d) Электромагнитный.

8. Кража образцов химических веществ относится к каналу утечки информации
a) Акустический;
b) Визуальный;
c) Материальный;
d) Электромагнитный.

9. Явление отражения звуковых волн используется в
a) Линейной группе микрофонов;
b) В параболическом микрофоне;
c) В трубчатом микрофоне;
d) В фазированной решетке.

10. Трубки разной длины используются в
a) Линейной группе микрофонов;
b) В параболическом микрофоне;
c) Органном микрофоне;
d) В трубчатом микрофоне;
e) В фазированной решетке.

11. Плоскость с точечными микрофонами используется
a) Линейной группе микрофонов;
b) В параболическом микрофоне;
c) В трубчатом микрофоне;
d) В фазированной решетке.

12. Типичная дальность применения направленного микрофона в условиях городской шумной улицы
a) До 100 м;
b) До 25 – 50 м
c) До 15 – 25 м

14. Типичная дальность применения направленного микрофона в условиях тихой городской улицы
a) До 100 м;
b) До 25 – 50 м
c) До 15 – 25 м

15. Типичная дальность применения направленного микрофона в условиях загородной местности
a) До 100 м;
b) До 25 – 50 м
c) До 15 – 25 м

16. Что больше всего оказывает влияние на дальность действия микрофона
a) Осадки;
b) Давление воздуха;
c) Температура воздуха;
d) Турбулентность воздуха.

17. Что больше всего оказывает влияние на дальность действия микрофона
a) Посторонние шумы;
b) Давление воздуха;
c) Температура воздуха;
d) Турбулентность воздуха.

18. Скорость звука в воздухе. Выберите наиболее близкое значение
a) 784 м/с

b) 153 м/с
c) 343 м/с
d) 1100 м/с

19. Скорость звука в воде. Выберите наиболее близкое значение
a) 1000 м/с
b) 1310 м/с
c) 1440 м/с
d) 5000 м/с

20. Скорость звука в стали. Выберите наиболее близкое значение
a) 1000 м/с
b) 1500 м/с
c) 4000 м/с
d) 5000 м/с

21. Диапазоны слышимости звука для человека
a) 100 – 500 Гц
b) 16 – 20000 Гц
c) 51 – 14400 Гц
d) 163 – 9900 Гц

22. Явление убывания интенсивности звуковой волны с расстоянием описывается
a) Законом Планка;
b) Законом обратных квадратов;
c) Теоремой Котельникова;
d) Законом Кирхгофа;

23. Интенсивность звука измеряется в
a) Децибелах
b) Кг/м^3
c) вт/м^2
d) Гц

24. Уровень интенсивность (громкость) измеряется в
a) Децибелах
b) Кг/м^3
c) вт/м^2
d) Гц

25. Порог слышимости человеческого уха в вт/м^2
a) 1
b) 10^{-5}
c) 10^{-12}
d) 10^{-1}

26. Порог слышимости человеческого уха в децибелах
a) 10
b) 120
c) 0
d) 1

27. Болевой порог человеческого уха в вт/м^2

a) 1
b) 10^{-5}
c) 10^{-12}
d) 10^{-1}

28. Болевой порог человеческого уха в децибелах

a) 1000
b) 120
c) 0
d) 1

29. На дальность перехвата звука на открытой местности влияет (вычеркните лишнее):

a) Температура и влажность воздуха;
b) Направление и сила ветра;
c) Турбулентность;
d) Ревербации;
e) Осадки.

30. Амплитуда белого шума

a) Одинакова на всех частотах;
b) Высокая на низких частотах и далее снижается;
c) Повышается с ростом частоты;
d) Снижается на средних частотах.

10 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «НАУЧНО-ТЕХНИЧЕСКИЙ СЕМИНАР»

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ЗАЧЕТУ

1 В чем заключается цель проведения научно-технического семинара и каков порядок его организации и проведения?

2 Научно-технические проблемы и приоритеты обеспечения информационной безопасности (физико-математические, технические).

3 Проблемы кадрового обеспечения информационной безопасности

4 Этапы научно-исследовательской работы. Понятийный аппарат научного исследования.

5 Опишите структуру магистерской диссертации? Какие требования предъявляются к цели и задачам исследования, основным положениям, выносимым на защиту?

6 Какие условия обеспечивают патентоспособность промышленного образца? Каков порядок проведения патентного поиска?

7 Что называют научной новизной? Как формулировать актуальность исследования? Порядок установления степени научной разработанности проблемы?

8 Порядок формулировки теоретической и прикладной значимости результатов проведенных исследований.

9 Формы представления результатов научных исследований – доклад научной конференции, статья, магистерская диссертации. Особенности стилистики, оформление работ.

10 Каковы принципы составления плана магистерской диссертации и ее содержания. Порядок проведения защиты магистерской диссертации.

ТИПОВЫЕ ПРАКТИЧЕСКИЕ ЗАДАНИЯ ДЛЯ ПОДГОТОВКИ К ЗАЧЕТУ

1 Сформулируйте основные положения доктрины информационной безопасности РФ. Назовите приоритеты развития информационной безопасности.

2 Сформулируйте цель и задачи научного исследования в рамках решения конкретной проблемы в области информационной безопасности.

3 Разработайте план проведения научных исследований в рамках решения конкретной проблемы в области информационной безопасности.

4 Проведите патентный поиск для решения поставленной задачи в области информационной безопасности.

ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ

Раздел 1 «Понятие о научно-техническом семинаре»

1 Что называют критериями научности? Какие основополагающие критерии научности можно выделить в области информационной безопасности?

2 Какие требования предъявляют к научно-исследовательской работе магистрантов? Этапы выполнения НИР.

3 Какова роль магистранта и научного руководителя, а также модератора в организации и проведении научно-технического семинара?

4 Какие проблемы обеспечения информационной безопасности относятся к научно-технической области?

Раздел 2 «Основные этапы планирования и выполнения магистерской диссертации»

1 Что такое диссертация и магистерская диссертация?

2 Как происходит построение гипотезы?

3 Какие требования предъявляются к определению темы?

4 Какова структура магистерской диссертации?

5 Что такое объект и предмет научного исследования?
6 Как оценить научную новизну исследования?
7 Что входит в основную часть диссертации?
8 Чем характеризуются научные положения?
9 Какие основные характерные черты аргументации вам известны?
10 Сколько глав включает диссертация? Какова их структура?
11 Над какими объектами промышленной собственности осуществляется охрана в РФ?
12 Что такое патент?
13 Что может являться объектом изобретения?
14 Что можно отнести к веществам как объектам изобретения?
15 Какие изобретения не могут быть признаны патентоспособными?
16 Какие условия патентоспособности полезной модели вам известны?
17 Что такое патентный поиск?
18 Как осуществлять патентный поиск?
19 Каковы цели патентного поиска?
20 Какие виды патентного поиска вам известны?

Раздел 3 «Методика написания исследовательской работы»

1 Каков порядок оценки перспективности темы исследования с учетом скорости старения информации? Количественная оценка показателя перспективности. Варианты оценочной системы.

2 Порядок формулировки теоретической и прикладной значимости результатов научного исследования.

3 Порядок установления степени разработанности проблемы и поиск нерешенных проблем и вопросов в рамках выбранного направления исследований в сфере информационной безопасности

Раздел 4 «Представление результатов научных исследований»

1 Порядок постановки проблемы исследования, особенности проектирования научных исследований.

2 Какие требования предъявляют к публикациям? Каков порядок рецензирования статей и тезисов докладов конференций?

3 Каковы этапы процесса публикации статей в зарубежных журналах? Порядок поиска необходимого журнала.

4 Классификация статей в РФ. Журналы, входящие в базу данных ВАК.

ПРИМЕРНЫЕ ТЕМЫ РЕФЕРАТОВ

1 Виды и уровни научных исследований в сфере информационной безопасности.

2 Философские методы научных исследований в сфере информационной безопасности.

3 Частные и специальные методы исследования в сфере информационной безопасности.

4 Методика разработки программы научно-исследовательской работы.

5 Системный подход к научным исследованиям в сфере информационной безопасности.

6 Доказательство и аргументация при проведении исследований в сфере информационной безопасности.

7 Основные источники научной информации в сфере информационной безопасности.

8 Сбор эмпирических данных путем изучения документов в сфере информационной безопасности.

9 Методы обработки эмпирических данных в сфере информационной безопасности.

10 Электронные формы информационных ресурсов.

11 Графические способы изложения иллюстративного материала в магистерской диссертации по информационной безопасности.

12 Составление библиографических списков применительно к сфере информационной безопасности. Правила оформления библиографических ссылок.

Реферат – краткая запись идей, содержащихся в одном или нескольких источниках, которая требует умения сопоставлять и анализировать различные точки зрения. Реферат – одна из форм интерпретации исходного текста или нескольких источников. Поэтому реферат, в отличие от конспекта, является новым, авторским текстом. Новизна в данном случае подразумевает новое изложение, систематизацию материала, особую авторскую позицию при сопоставлении различных точек зрения.

Реферирование предполагает изложение какого-либо вопроса на основе классификации, обобщения, анализа и синтеза одного или нескольких источников.

Виды рефератов

По полноте изложения	Информативные (рефераты-конспекты)
	Индикативные (рефераты-резюме)
По количеству реферируемых источников	Монографические
	Обзорные

Реферат должен отвечать ряду требований.

Требования по оформлению:

– объем реферата от 10 до 15 страниц формата А4, шрифт Times New Roman, кегль 14 пт, полуторный междустрочный интервал, выравнивание текста – по ширине, нумерация страниц в верхнем колонтитуле по центру, автоматические переносы слов (кроме титульного листа), поля: снизу и сверху – 20 мм, слева – 25 мм, справа – 10 мм;

– на титульном листе указывается: название реферата, Фамилия И.О. обучающегося, номер группы;

– список использованных источников – современная, актуальная литература, не менее трех источников, полное указание выходных данных для книжных и периодических изданий, адреса сайтов с которых заимствован материал, по тексту реферата должны быть ссылки на источники.

Требования по структуре:

– реферат включает титульный лист, оглавление, введение, основной текст, заключение, список литературы, приложения (при необходимости);

– основной текст должен содержать несколько разделов.

Требования по содержанию:

– реферат должен содержать достоверные и актуальные сведения на достаточном научном уровне;

– реферат, кроме текста (формат .doc или .docx), может дополнительно содержать: качественные цветные иллюстрации, фрагменты программного кода и другие материалы, качественно дополняющие основную часть реферата.

ФОНД ТЕСТОВЫХ ЗАДАНИЙ

1 _____ – определяющее положение в системе взглядов, теорий и т.п.

1. Дедукция
2. Идея *
3. Индукция
4. Аспект

2 _____ функция социологического исследования указывает на наличие программы, построенной в соответствии с установленной структурой, как основополагающего требования и признака научности социологического исследования.

1. Организационная
2. Эвристическая
3. Нормативная *
4. Программирующая

3 _____ – это противоречие между имеющимся знанием и назревшей общественной потребностью, а иногда и просто столкновение качества нового знания с количеством знания старого, что типично для научных исследований.

1. Типология
2. Проблема *
3. Выборка
4. Научная этика

4 _____ – процедура упорядочения любых объектов по возрастанию или убыванию некоторого их свойства при условии, что они этим свойством обладают.

1. Ранг
2. Эмпирическая типологизация
3. Ранжирование *
4. Эмперическое исследование

5 Верны ли определения?

А) Гипотеза должна подвергаться логическому анализу, устанавливающему её непротиворечивость.

В) Гипотеза не должна подвергаться логическому анализу, устанавливающему её непротиворечивость.

Подберите правильный ответ

1. А – да, В – да
2. А – нет, В - да
3. А – да, В – нет *
4. А – нет, В – нет

6 _____ – метод, предполагающий не менее четырёх признаков, по которым определяются респонденты.

1. Квотная выборная совокупность *
2. Гипотеза в социологическом исследовании
3. Генеральная совокупность
4. Сплошной метод

7 ______ гипотеза – это обоснованное предположение о происхождении и свойствах единичных фактов, конкретных событий и явлений.

1. Рабочая

2. Общая
3. Единичная
4. Частная *

8 Закон ___ – выражаемое в формальной логике важное условие истинности проблемы, являющееся свойством ее доказательности.

1. достаточного основания *
2. дифференциации
3. социализации
4. социальной мобильности

9 Верны ли определения?

А) При коллективизме результаты исследования должны быть открыты для научного сообщества.

В) При универсализме, результаты исследования должны быть открыты для научного сообщества.

Подберите правильный ответ

1. А – да, В – да *
2. А – нет, В - да
3. А – да, В - нет
4. А – нет, В – нет

10 _____ – основной способ сбора, обработки и анализа данных.

1. Метод *
2. Методология
3. Принцип
4. Выборка

11 Верны ли определения?

А) Общенаучную методологию научных исследований следует трактовать как систему общих условий и ориентиров в познавательной (исследовательской) деятельности.

В) Индукция – это вид умозаключения от общего к частному, когда из массы частных случаев делается обобщенный вывод о всей совокупности таких случаев.

Подберите правильный ответ

1. А – да, В – да
2. А – нет, В - да
3. А – да, В – нет *
4. А – нет, В – нет

12 ___ – задача научного характера, требующая проведения научного исследования, является основным планово-отчетным показателем научно-исследовательской работы.

1. Наука
2. Научная теория
3. Научная тема *
4. Научная дисциплина

13 _____ – форма логического мышления, в которой раскрываются внутренние, существенные стороны и отношения исследуемых предметов.

1. Категория *
2. Гипотеза
3. Концепция
4. Принцип

14 _____ – раздел науки, который на данном уровне ее развития, в данное время освоен и внедрен в учебный процесс высшей школы.

1. Научная теория
2. Научная дисциплина *
3. Научная тема

4. Наука

15 Особое место среди описательных гипотез занимают гипотезы о существовании какого-либо объекта, которые называют ___ гипотезами.

1. Описательными
2. Объяснительными
3. Экзистенциальными *
4. Функциональными

16 _____ - научно-исследовательская работа, подготовленная для публичной защиты на соискание ученой степени

1. Диссертация *
2. Аннотация
3. Статья
4. Очерк

17 ___ исследование по своему характеру носит комплексный характер, в нем применяются самые различные формы сбора и анализа информации.

1. Аналитическое *
2. Когортное
3. Выборочное
4. Описательное

18 Во ___ соискатель презентирует свою программу и стратегии исследования, здесь дается обоснование актуальности темы диссертации, изложение целевой установки, определяются задачи, дается общее представление о работе, а также все концепты исследовательской программы.

1. Заключении
2. Введении *
3. Оглавлении
4. Основной части

19 _____ – слово или словосочетание, наиболее полно и специфично характеризующее содержание научного документа или его части.

1. Аспект
2. Ключевое слово *
3. Индукция
4. Аналогия

20 _____ – совокупность специальных приемов для эффективного использования того или иного метода.

1. Техника *
2. Принцип
3. Метод
4. методология

11 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «НОРМАТИВНАЯ ПРАВОВАЯ И МЕТОДИЧЕСКАЯ ДОКУМЕНТАЦИЯ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ»

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ

1. Каковы основные отечественные и зарубежные стандарты в области информационной безопасности?

2. Какая система называется безопасной и какая надежной?

3. Что такое политика безопасности?

4. Каковы основные предметные направления ЗИ?

5. Что такое государственная тайна?

6. Что называется коммерческой тайной?

7. Что такое служебная тайна?

8. Что представляет профессиональная тайна?

9. Какие мероприятий защиты информации относятся к инженерно-техническим?

10. Каковы источники права на доступ к информации?

11. Каковы уровни доступа к информации с точки зрения законодательства?

12. Что такое информация ограниченного распространения?

13. Каковы виды доступа к информации?

14. В чем может заключаться ответственность за нарушение законодательства в информационной сфере?

15. Что такое Доктрина ИБ РФ?

16. Перечислите основные составляющие национальных интересов РФ в информационной сфере.

17. Дайте определение ИБ.

18. Сформулируйте интересы государства, общества и личности в информационной сфере.

19. Что такое доступность информации?

20. Что такое конфиденциальная информация, государственная и коммерческая тайна?

21. Назовите три степени секретности.

22. Назовите три категории ценности коммерческой информации.

23. Назовите основные методы определения количества информации.

24. Перечислите основные виды угроз ИБ.

25. Перечислите основные принципы обеспечения ИБ.

26. Сформулируйте основные направления международного сотрудничества Российской Федерации в области ИБ.

27. В чем заключаются национальные интересы и безопасность РФ.

28. В чём заключаются основные задачи государства в сфере обеспечения информационной безопасности?

29. Назовите основные отечественные и зарубежные стандарты в области информацион ной безопасности.

30. Раскройте содержание основных принципов Доктрины ИБ РФ.

31. Перечислите основные направления обеспечения ИБ в мировой практике.

32. Сформулируйте основные задачи обеспечения ИБ.

33. Приведите основные функции государственной системы обеспечения ИБ РФ.

34. Сформулируйте задачи обеспечения безопасности функционирования информации в КС.

35. Назовите основные критерии, предъявляемые международными и отечественными стандартами к информационной безопасности и защите информации.

36. Понятие и виды информации, защищаемой законодательством Российской Федерации. Основные концептуальные положения системы защиты информации.

37. Концептуальная модель информационной безопасности. Действия, приводящие к неправомерному овладению конфиденциальной информацией.

38. Правовая защита – направление защиты информации. Государственное регулирование информационной безопасности. Доктрина информационной безопасности РФ.

39. Организационная защита – направление защиты информации. Содержание основных организационных мероприятий. Функционал службы защиты информации.

40. Инженерно-техническая защита – направление защиты информации. Классификация средств инженерно-технической защиты. Краткая характеристика основных классов.

41. Способы защиты информации. Классификация способов защиты (мероприятий по защите информации).

42. Характеристика основных защитных действий. Способы пресечения разглашения конфиденциальной информации.

43. Правовое регулирование технологического обмена. Защита интеллектуальной собственности. Критерии ценности документов.

44. Предпосылки к разглашению сведений, составляющих коммерческую тайну. Экспертиза ценности документов.

45. Алгоритм создания системы информационной безопасности на предприятии. Содержание этапов создания (реконструкции) системы информационной безопасности предприятия.

46. Кому принадлежит право разрешать или ограничивать доступ к информации и определять условия такого доступа?

47. Чем определен перечень сведений конфиденциального характера?

48. Какие мероприятия защиты информации относятся к правовым?

49. Какие мероприятий защиты информации относятся к организационным?

ТИПОВЫЕ ПРАКТИЧЕСКИЕ ЗАДАНИЯ ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ

1. Составить аналитическую записку - обзор по предложенному перечню правовых актов;

2. Найти определения информационно-аналитических систем в соответствии с классификацией, принятой в действующей системе правовых актов и нормативно-методических документов. Отметить нормативные документы, регламентирующие функционирование конкретной ИАС в предлагаемом перечне нормативных документов.

3. Разработать частную модель угроз безопасности для организации, имеющей информационную систему обработки персональных данных. Заполнить шаблон частной модели угроз по исходным условиям информационной систем обработки персональным данным.

4. Прочитать задачу, найти правовое обоснование и разрешить противоречивую правовую ситуацию. 2. Обсудить найденное решение, обосновать свою позицию аргументами и положениям правовых актов. Задача: Общественная организация «За здоровье нации» обратилась к администрации Аргаяшской птицефабрики с заявлением о предоставлении информации о технике безопасности на предприятии: уровне ПДК в воздухе производственных помещений, уровне травматизма на производстве и выплате компенсаций по здоровьесбережению. Руководство предприятия отказалось удовлетворить просьбу общественной организации, мотивируя свое отказное решение тем, что указанные данные являются конфиденциальной информацией. Дайте разъяснения по существу сложившейся ситуации, приведите правовые нормы в обоснование своих доводов.

5. Найдите Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Скопируйте реквизиты и преамбулу закона, вставьте эти данные в отчет по лабораторной работе. Найдите статью, посвященную ограниченному доступу к информации, скопируйте ее сохраните её в отчет.

ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

Министерство науки и высшего образования РФ Федеральное государственное бюджетное	10.04.01 Информационная безопасность (код и направление подготовки)

образовательное учреждение высшего образования «Сибирский государственный университет геосистем и технологий» Кафедра: информационной безопасности	Организация и управление информационной безопасностью (профиль подготовки) Нормативно-правовая и методическая документация в сфере защиты информации (дисциплина)

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Основные отечественные и зарубежные стандарты в области информационной безопасности.

2. Основные составляющие национальных интересов РФ в информационной сфере.

3. Разработать программу и методику опытной эксплуатации системы защиты информации значимого объекта критической информационной инфраструктуры 3 категории (состав три рабочих станции, один сервер, один коммутатор, сетевой принтер, подключения к сети интернет)

Составитель _____ И.О.Ф.
(подпись)

Заведующий кафедрой _____ И.О.Ф.
(подпись)

ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ

Раздел 1

1. ГОСТ 28147–89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

2. ГОСТ Р 34. 10–94 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма».

3. ГОСТ Р 34. 11–94 «Информационная технология. Криптографическая защита информации. Функция хэширования».

4. ГОСТ Р 50739–95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования».

5. При создании систем защиты информации государственных информационных систем должны быть учтены и другие нормативные документы. Какие?

Раздел 2

1. На этапе формирования требований к защите информации ГИС решаются следующие задачи. Какие?

2. Разработка системы защиты информации ГИС включает следующие шаги. Какие?

3. Перечень разрабатываемых документов.

4. Основные документы по внедрению системы защиты информации информационной системы.

5. Порядок проведения аттестации ГИС.

Раздел 3

1. Как отличить ГИС от не ГИС?
2. Понятие ИСПДн.
3. Какие нормативные акты регулируют вопросы защиты персональных данных?
4. Как определить категорию персональных данных, обрабатываемых на предприятии?

5. Как классифицировать ИСПДн? Какие относятся к типовым, а какие к специальным?
6. В каких случаях предприятие обязано уведомлять Роскомнадзор об обработке ПД, а в каких нет?

Раздел 4

1. Какие организационные меры по обеспечению безопасности ПД надо предпринять?
2. Что надо сделать в первую очередь, что можно сделать позже?
3. Где найти перечень сертифицированных средств защиты информации?
4. Когда проводят аттестацию ИСПДн и каким образом?
5. Понятие КВО и КИИ.

ТЕМЫ РЕФЕРАТОВ

1 Информационные отношения как объект правового регулирования
2 Правовой режим защиты государственной и служебной тайны. Организация режима секретности
3 Нормативные и организационно-распорядительные документы, регламентирующие работу по защите информации
4 Организационно-правовые механизмы защиты коммерческой тайны
5 Институт правовой защиты персональных данных
6 Организационно-правовые механизмы защиты персональных данных
7 Государственное регулирование деятельности в области защиты информации (ПЗ)
8 Организация процедур лицензирования и сертификации по защите информации
9 Пресечение нарушений в сфере компьютерной информации (ПЗ)
10 Правовая защита информационных систем (ПЗ)
11 Организация многорубежной системы охраны и физической защиты информации(ПЗ)
12 Порядок организации режимных мероприятий (ПЗ)
13 Порядок организации работы с персоналом в системе защиты информации (ПЗ)
14 Организация служебного расследования по фактам утраты информации (ПЗ)
15 Порядок организации конфиденциального делопроизводства и документооборота
16 Организация защиты информации при организации конфиденциальных переговоров, приеме посетителей и командированных лиц (ПЗ)
17 Организация работы службы безопасности предприятия (ПЗ)

Реферат – краткая запись идей, содержащихся в одном или нескольких источниках, которая требует умения сопоставлять и анализировать различные точки зрения. Реферат – одна из форм интерпретации исходного текста или нескольких источников. Поэтому реферат, в отличие от конспекта, является новым, авторским текстом. Новизна в данном случае подразумевает новое изложение, систематизацию материала, особую авторскую позицию при сопоставлении различных точек зрения.

Реферирование предполагает изложение какого-либо вопроса на основе классификации, обобщения, анализа и синтеза одного или нескольких источников.

Виды рефератов

По полноте изложения	Информативные (рефераты-конспекты)
	Индикативные (рефераты-резюме)
По количеству реферируемых источников	Монографические
	Обзорные

Реферат должен отвечать ряду требований.

Требования по оформлению:

– объем реферата от 10 до 15 страниц формата А4, шрифт Times New Roman, кегль 14 пт, полуторный междустрочный интервал, выравнивание текста – по ширине, нумерация страниц в

верхнем колонтитуле по центру, автоматические переносы слов (кроме титульного листа), поля: снизу и сверху – 20 мм, слева – 25 мм, справа – 10 мм;

– на титульном листе указывается: название реферата, Фамилия И.О. обучающегося, номер группы;

– список использованных источников – современная, актуальная литература, не менее трех источников, полное указание выходных данных для книжных и периодических изданий, адреса сайтов с которых заимствован материал, по тексту реферата должны быть ссылки на источники.

Требования по структуре:

– реферат включает титульный лист, оглавление, введение, основной текст, заключение, список литературы, приложения (при необходимости);

– основной текст должен содержать несколько разделов.

Требования по содержанию:

– реферат должен содержать достоверные и актуальные сведения на достаточном научном уровне;

– реферат, кроме текста (формат .doc или .docx), может дополнительно содержать: качественные цветные иллюстрации, фрагменты программного кода и другие материалы, качественно дополняющие основную часть реферата.

ПРИМЕРЫ ПРОЕКТНЫХ ЗАДАНИЙ

В соответствии с действующим законодательством по защите информации в ГИС оператор информационной системы должен принимать технические и организационные меры. Для выполнения организационных мероприятий разрабатывается комплект внутренних документов, в соответствии с которыми оператор ГИС в дальнейшем осуществляет обработку и защиту защищаемой информации.

С целью выполнения требований нормативных документов по защите информации в ГИС, а также с целью регламентации дальнейших действий оператора ГИС по защите таких данных необходимо с учетом реальных условий обработки информации разработать внутренние документы регламентирующие:

— правила и процедуры идентификации и аутентификации пользователей ГИС;

— правила разграничения доступа к ресурсам ГИС;

— правила и процедуры управления информационными потоками;

— правила и процедуры управления установкой (инсталляцией) компонентов программного обеспечения в ГИС;

— правила защиты машинных носителей информации;

— правила и процедуры контроля интерфейсов ввода-вывода;

— правила и процедуры гарантированного уничтожения информации;

— использование и контроль технологий беспроводного доступа и правила защиты беспроводных соединений;

— правила взаимодействия информационных систем с внешними информационными системами;

— правила и процедуры обеспечения доверенной загрузки средств вычислительной техники;

— правила и процедуры применения удаленного доступа к ГИС;

— правила и процедуры обнаружения (предотвращения) вторжений;

— правила и процедуры выявления, анализа и устранения уязвимостей;

— правила и процедуры контроля установки обновлений программного обеспечения;

— правила и процедуры контроля состава технических средств, программного обеспечения и средств защиты информации ГИС;

— правила и процедуры контроля целостности программного обеспечения;

— правила и процедуры резервирования технических средств, программного обеспечения, баз данных, средств защиты информации и их восстановления при возникновении нештатных ситуаций;

— правила использования электронной почты и защиты от спама;

— правила и процедуры контроля использования технологий мобильного кода;

— ролевую систему доступа к ресурсам ГИС;

— перечень лиц, должностей, служб и процессов, допущенных к работе с ресурсами ГИС;

— перечень лиц, допущенных в помещения, в которых производится обработка персональных данных;

— перечень разрешенного в ГИС программного обеспечения;

— правила реагирования на инциденты информационной безопасности;

— другие правила и процедуры.

Помимо указанных правил и процедур дополнительно должны разрабатываться инструкции пользователей ГИС, лиц, ответственных за защиту информации в ГИС (администраторов безопасности), формы: актов, соглашений о неразглашении, уничтожения документов, журналов учета и т. д.

В зависимости от условий функционирования ГИС, некоторые правила и процедуры из представленного выше списка могут исключаться, а некоторые – добавляться (например, в списке нет правил и процедур защиты виртуальной инфраструктуры). Исходя из этого, разработка комплекта документов по защите информации в ГИС достаточно индивидуализирована для каждой системы.

Разработанная инструкция должен отвечать ряду требований.

Требования по оформлению:

– объем инструкции от 10 до 15 страниц формата А4, шрифт Times New Roman, кегль 14 пт, полуторный междустрочный интервал, выравнивание текста – по ширине, нумерация страниц в верхнем колонтитуле по центру, автоматические переносы слов (кроме титульного листа), поля: снизу и сверху – 20 мм, слева – 25 мм, справа – 10 мм;

– на титульном листе указывается: название инструкции, Фамилия И.О. обучающегося, номер группы;

– список использованных источников – современная, актуальная литература, не менее трех источников, полное указание выходных данных для книжных и периодических изданий, адреса сайтов с которых заимствован материал, по тексту реферата должны быть ссылки на источники.

Требования по структуре:

– инструкция включает титульный лист, оглавление, введение, основной текст, заключение, список литературы, приложения (при необходимости);

– основной текст должен содержать несколько разделов.

Требования по содержанию:

– инструкция должен содержать достоверные и актуальные сведения на достаточном правовом уровне.

12 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ»

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ЗАЧЕТУ

1. Меры обеспечения безопасности АС. Раскройте понятие идентификация.
2. Меры обеспечения безопасности АС. Раскройте понятие аутентификация.
3. Меры обеспечения безопасности АС. Какие основные методы разграничения доступа вам известны?
4. Общая классификация мер обеспечения безопасности АС.
5. Для чего нужны общие критерии оценки безопасности IT?
6. Раскройте понятие объект оценки общих критериев оценки безопасности IT
7. По каким критериям относить автоматизированную систему к гис?
8. Раскройте понятие «аудит информационной безопасности».
9. Раскройте термин «событие информационной безопасности».
10. Основные угрозы безопасности информации ас и их классификация.
11. Примеры уязвимостей информационно-технологических ресурсов ас.
12. Классификация каналов проникновения в систему и утечки информации.
13. Опишите спиральную модель (эволюционную) модель жизненного цикла разработки АС.
14. Опишите процессную модель жизненного цикла разработки ас.
15. Какие методы проектирования АС вам известны?
16. Что является целью защиты информации в АС в защищенном исполнении?
17. Какие стороны принимают участие в работах по созданию АСЗИ?
18. Основные этапы развития ИС и АС.
19. Администрирование АС. Каковы функции и службы администрирования?
20. Администрирование АС. Назовите категории административного персонала.
21. Меры обеспечения безопасности АС. Что такое криптографическое преобразование информации в АС?
22. Меры обеспечения безопасности АС. Что такое межсетевое экранирование?
23. Раскройте понятия функциональные требования и требования доверия общих критериев оценки безопасности IT.
24. Раскройте понятие профиль защиты общих критериев оценки безопасности IT.
25. Чем опытная эксплуатация АС отличается от промышленной?

ТИПОВЫЕ ПРАКТИЧЕСКИЕ ЗАДАНИЯ ДЛЯ ПОДГОТОВКИ К ЗАЧЕТУ

1. Определить виды информации ограниченного доступа и состав носителей информации обрабатываемые в автоматизированной системе.
2. Изучить порядок формирования и структуру Банк данных уязвимостей информационных систем.
3. Классифицировать состав угроз информационной безопасности. Определить состав актуальных угроз безопасности информации для автоматизированной системы на основе БДУ.
4. Разработать модель угроз безопасности информации ИС ПДн.
5. Разработать макет технического задания (ТЗ) на автоматизированную систему в защищенном исполнении в составе основных разделов.
6. Определить состав применяемых сервисов безопасности программно-технического уровня для варианта автоматизированной системы, с учетом особенностей объекта информатизации.
7. Представить вариант модели данных, систем и процессов защиты информации в автоматизированной системе.

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ

1. Понятие автоматизированной системы (АС), ее основное предназначение.

2. Разновидности классификации и варианты реализации АС.

3. Понятие автоматизированной системы обработки данных и ее особенности.

4. Исторические этапы развития информационных систем.

5. Модели данных, систем и процессов защиты информации в АС.

6. Стандарты в области информационной безопасности. Оценочные стандарты и спецификации.

7. Международные стандарты оценки защищенности АС.

8. Отечественные стандарты и руководящие документы о защите информации в АС.

9. Критерии оценки безопасности информационных технологий. Среда безопасности объекта оценки.

10. Особенности современных АС как объектов защиты.

11. Актуальные угрозы безопасности информации АС и их классификация.

12. Разработка модели угроз безопасности информации в АС. Модель нарушителя.

13. Базовая модель угроз ИС ПДн, содержание и порядок использования.

14. Цель, задачи и этапы оценки угроз безопасности информации.

Разработка частной модели угроз ИС ПДн.

15. Общая характеристика стадий, этапов и задач разработки АС.

16. Содержание предпроектной группы стадий и этапов разработки АС.

17. Содержание группы стадий и этапов работ по проектированию АС.

18. Содержание группы стадий и этапов работ по вводу в эксплуатацию АС.

19. Особенности и основные понятия автоматизированного проектирования.

20. Структура системы автоматизированного проектирования (САПР). Классификация САПР.

21. Автоматизированное проектирование систем (подсистем) безопасности и защиты информации.

22. Понятие системы защиты АС в защищенном исполнении и требования к ней.

23. Участники работ по созданию (модернизации) АС в защищенном исполнении.

24. Общие требования по разработке АС в защищенном исполнении.

25. Состав комплекса работ по созданию системы ЗИ АС в защищенном исполнении.

ТИПОВЫЕ ПРАКТИЧЕСКИЕ ЗАДАНИЯ ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ

1. Разработать модель многоуровневой защиты автоматизированной системы с учетом рубежей безопасности на уровнях:

- административном;
- процедурном;
- программно-техническом.

2. В составе программно-технического уровня защиты автоматизированной системы применить:

- уровень защиты периметра (firewall, СОВ);
- уровень защиты внутренней сети (VLAN: IPSec, персональные МЭ);
- уровень защиты узлов (серверов и АРМ, конфигурация, ПО НСД);
- уровень защиты приложений (настройки, обновления, АЗ);
- уровень защиты данных (файловая система, шифрование).

3. Разработать модель разрешительной системы доступа к ресурсам автоматизированной системы одним из способов представления информации о правах доступа в информационной системе:

- по спискам полномочий субъектов доступа;
- по спискам управления доступом к объекту.

4. Сформировать матрицу полномочий доступа для варианта информационной системы.

ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

Министерство науки и высшего образования РФ Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет геосистем и технологий» Кафедра: информационной безопасности	10.04.01 Информационная безопасность (код и направление подготовки) Организация и управление информационной безопасностью (профиль подготовки) Обеспечение безопасности автоматизированных систем (дисциплина)

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Международные стандарты оценки защищенности АС.
2. Цель, задачи и этапы оценки угроз безопасности информации.
3. Понятие системы защиты АС в защищенном исполнении и требования к ней.

Составитель _____ И.О.Ф.
(подпись)

Заведующий кафедрой _____ И.О.Ф.
(подпись)

Шкала и критерии оценивания

Ответ обучающегося на экзамене оценивается по пятибалльной шкале:

– *оценка «отлично»* – ответы обучающегося на вопросы экзаменационного билета и дополнительные вопросы экзаменатора полные, аргументированные, обстоятельные; высказываемые предположения подтверждены конкретными примерами; практические задания выполнены по стандартной или самостоятельно разработанной методике, в полном объеме, без ошибок в расчетах, с подробными пояснениями, сделаны полные аргументированные выводы;

– *оценка «хорошо»* – обучающийся ответил на все вопросы задания, дал точные определения и понятия; однако затрудняется подтвердить теоретические положения практическими примерами; практические задания выполнены по стандартной методике без ошибок в расчетах, однако даны недостаточно полные пояснения по анализу показателей;

– *оценка «удовлетворительно»* – обучающийся правильно ответил на все вопросы, но с недостаточно полной аргументацией; выполнил не менее 50 % практических заданий;

– *оценка «неудовлетворительно»* – обучающийся не смог ответить на 2/3 вопросов билета; не справился с практическим заданием или выполнил менее 50 % практических заданий.

ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ
2 СЕМЕСТР

Раздел 1

1. Типы обеспечивающих подсистем.
2. Информационное обеспечение ЗИС.
3. Техническое обеспечение ЗИС.
4. Математическое и программное обеспечение ЗИС.
5. Организационное обеспечение ЗИС.
6. Правовое обеспечение ЗИС.
7. Классификация ИС по признаку структурированности задач. Понятие структурированности задач.
8. Типы ИС, используемые для решения частично-структурированных задач.
9. Классификация ЗИС по функциональному признаку и уровням управления. Функциональный признак.

10. Типы ИС оперативного (операционного) уровня. Классификация ИС по функциональному признаку и уровням управления.

Раздел 2

1. Введение в экспертные системы. Роли эксперта, инженера знаний и пользователя.
2. База знаний, правила, машина вывода, интерфейс пользователя, средства работы с файлами.
3. Технология разработки защищенных систем.
4. Логическое программирование и защищенных системы.
5. Языки искусственного интеллекта.
6. Подсистема анализа и синтеза входных и выходных сообщений.
7. Диалоговая подсистема.
8. Объяснительные способности защищенных систем.

3 СЕМЕСТР

Раздел 1

1. Общие требования по безопасности информации в автоматизированной системе.
2. Последовательность формирования требований по безопасности информации.
3. Разработка частной модели угроз безопасности информации.
4. Оценка угроз безопасности информации в автоматизированной системе.
5. Организация работ по созданию автоматизированной системы.
6. Автоматизация проектирования автоматизированной системы.
7. Техническое задание на создание автоматизированной системы в защищенном исполнении.
8. Требования к автоматизированной системе по защите от НСД.
9 Средства обеспечения отказоустойчивости автоматизированной системы.
10. Порядок выполнения обязанностей администратора информационной безопасности автоматизированной системы.
11. Эксплуатационная документация защищенной автоматизированной системы.

Раздел 2

1. Работы по защите информации на стадии разработки АС: «Формирование требований».
2. Работы по защите информации на стадии разработки АС: «Разработка концепции АС».
3. Работы по защите информации на стадии разработки АС: «Техническое задание».
4. Работы по защите информации на стадии разработки АС: «Эскизный проект».
5. Работы по защите информации на стадии разработки АС: «Технический проект».
6. Работы по защите информации на стадии разработки АС: «Рабочая документация».
7. Работы по защите информации на стадии разработки АС: «Ввод в действие».
8. Работы по защите информации на стадии разработки АС: «Сопровождение АС».

ПРИМЕРНЫЕ ТЕМЫ РЕФЕРАТОВ

2 семестр

4) Методики проектирования защищенных баз данных для информационно-аналитических систем.

5) Обзор международных стандартов по вопросам построения защищенных систем.

6) Сравнительный анализ современных технологий и сервисов, применяемых при разработке и развертывании защищенных систем.

3 семестр

1) Графические средства представления проектных решений.

2) Методы и инструментальные средства организации проектной деятельности.
3) Автоматизация создания модели угроз безопасности объектов.
4) Применение нелинейного локатора для обнаружение полупроводниковых элементов.
5) Уязвимости в программном обеспечении и возможные меры по их устранению.

ФОНД ТЕСТОВЫХ ЗАДАНИЙ

1. Как называется мера доверия, которая может быть оказана архитектуре, инфраструктуре, программно-аппаратной реализации системы и методам управления её конфигурацией и целостностью?

Ответ:
1) эффективность безопасности;
2) гарантированность безопасности;
3) непрерывность безопасности;
4) надежность безопасности.

2. Каким термином обозначается анализ регистрационной информации системы защиты?
Ответ:
1) мониторинг;
2) аудит;
3) аккредитация;
3) сертификация.

3. Что означает система защиты с полным перекрытием?
Ответ:
1) для половины (и более) уязвимостей есть устраняющие барьеры;
2) для любой уязвимости есть устраняющий ее барьер;
3) у любой уязвимости есть риск ее реализации;
4) количество уязвимостей меньше, чем количество препятствующих им барьеров.

4. Чем характеризуется степень сопротивляемости механизма защиты?
Ответ:
1) вероятностью его преодоления;
2) количеством угроз, которым этот механизм препятствует;
3) величиной потерь в случае успешного прохождения;
4) стоимостью механизма защиты.

5. Защищенность системы защиты определяется как величина…
Ответ:
1) обратная суммарному количеству рисков;
2) обратная остаточному риску;
3) обратная уязвимости;
4) равная сумме всех уязвимостей.

6. В чем заключается идеология открытых систем информационной безопасности?
Ответ:
1) в строгом соответствии систем информационной безопасности законодательству страны, котором они созданы;
2) в строгом соблюдении совокупности профилей, протоколов и стандартов де-факто и де-юре;
3) в открытости информации о стоимости реализации конкретной системы защиты;
4) в открытости программных кодов средств защиты от производителей разных стран.

7. В чем заключается принцип минимизации привилегий?

Ответ:

1) выделение полных прав доступа только администраторам системы;

2) выделение только тех прав, которые необходимы для реализации своих должностных обязанностей;

3) выделение прав доступа в зависимости от величины возможного ущерба;

4) в минимизации рисков от реализации угроз.

8. В чем заключается принцип эшелонирования обороны?

Ответ:

1) в том, чтобы использовать максимально возможное количество защитных средств;

2) в простоте и управляемости информационной системы;

3) в усилении самого надежного защитного рубежа;

4) в том, чтобы не полагаться на один защитный рубеж.

9. Что из нижеперечисленного относится к оперативным методам повышения безопасности?

Ответ:

1) систематическое тестирование;

2) предотвращение ошибок в CASE-технологиях

3) обязательная сертификация;

4) программная избыточность.

На каких принципах должна строиться архитектура ЗИС?

Ответ:

1) проектирование на принципе закрытых систем;

2) проектирование на принципе открытых систем

4) усиление самого слабого звена;

5) эшелонирование обороны.

13 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «ОРГАНИЗАЦИЯ И ТЕХНОЛОГИИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ»

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ

1. Охарактеризовать условия обработки персональных данных: согласие субъекта на обработку, обрабатываемые без уведомленияперсональных данных?
2. Каковы особенности обработки персональных данных в государственных или муниципальных информационныхсистемах персональных данных?
3. Какие Федеральные органы, уполномоченные в области обеспечения безопасности персональных данных?
4. Охарактеризовать сферу деятельности регуляторов?
5. Описать функции Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций?
6. Описать функции Федеральной службы технического и экспортного контроля?
7. Описать функции Федеральной службы безопасности в области защиты персональных данных?
8. Привести пример методических документов регуляторов? Типы, основание, порядок, сроки и содержание поверок?
9. Каковы обязанности операторов персональных данных?
10. Какова ответственность оператора в области защиты персональныхданных: гражданская, уголовная, административная, дисциплинарная?
11. Классификация угроз безопасности персональных данных?
12. Понятие информационной системы персональных данных?
13. Каковы типовые и специальные информационные системы персональных данных?
14. Какова структура информационной системы персональных данных?
15. Назвать критерии классификации типовых информационных систем персональных данных?
16. Перечислить правовые меры защиты?
17. Перечислить организационно-административные меры защиты?
18. Как происходит регистрация фактов несанкционированной повторной и дополнительной записи информации?
19. Применение средств электронной цифровой подписи для сохранения целостности и неизменности персональных данных?
20. Описать процедуру уничтожения персональных данных?
21. Локальные акты, регламентирующие работу с персональнымиданными в организации?
22. Описать процесс проектирования локальных актов регламентирующих персональных данных без использования средств автоматизации?

ТИПОВЫЕ ПРАКТИЧЕСКИЕ ЗАДАНИЯ ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ

6. Дать пример разработки документов регулирующих защиту персональныхданных в автоматизированных информационных системах.
7. Дать пример проектирования локальных актов регламентирующих персональныхданных без использования средств автоматизации.
8. Дать пример локального акта, регламентирующего работу с персональными данными в организации
9. Рассчитать расстояние возможного использования оптического средства несанкционированного доступа к конфиденциальной информации по заданным параметрам.

ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

Министерство науки и высшего образования РФ Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет геосистем и технологий» Кафедра: информационной безопасности	10.04.01 Информационная безопасность (код и направление подготовки) Организация и управление информационной безопасностью (профиль подготовки) Организация и технологии защиты персональных данных (дисциплина)

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Охарактеризовать условия обработки персональных данных: согласие субъекта на обработку, обрабатываемые без уведомленияперсональных данных?
2. Каковы обязанности операторов персональных данных?
3. Дать пример проектирования локальных актов регламентирующих персональныхданных без использования средств автоматизации?

Составитель _____ И.О.Ф.
(подпись)

Заведующий кафедрой _____ И.О.Ф.
(подпись)

ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ

Раздел 1

6. Перечислить основные нормативно-правовые акты в области защиты персональных данных?
7. Каковы требования обеспечения конфиденциальности персональных данных?
8. Перечислить специальные категории персональных данных?
9. Каковы права субъекта персональных данных на доступ к своим персональным данным? Перечислить принципы обработки и хранения персональных данных?

Раздел 2

1. Дать анализ ихарактеристики угроз возможной утечки персональных данных по техническим каналам?
2. Дать анализ и характеристик угроз несанкционированного доступа к информации в информационной системе персональных данных?
3. Каковы типовые модели угроз безопасностиперсональных данных, обрабатываемых в информационных системах?
4. Привести пример формирования перечня актуальных угроз безопасности персональным данным?

Раздел 3

1. Перечислить технические меры защитыот НСД в информационных системах персональных данных различного класса?
2. Описать процедуру присвоения материальному носителю идентификационного номера?
3. Описать процедуру учета экземпляров материальных носителей?
4. Средства идентификации информационной системы персональных данных и оператора персональных данных?

14 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «ТЕОРИЯ СИСТЕМ И СИСТЕМНЫЙ АНАЛИЗ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ЗАЧЕТУ

1) Понятие и классификация систем.
2) Методы принятия управленческих решений
3) Структура систем.
4) Функции систем.
5) Модель системного анализа: модель «черного ящика».
6) Модель системного анализа: модель состава систем
7) Модель системного анализа: модель структуры системы
8) Основные принципы системного анализа
9) Основные методы системного анализа.
10) Генерирование множества альтернатив.
11) Сценарный подход к принятию решений.
12) Экспертные методы принятия решений.
13) Сущность метода Делфи.
14) Сущность морфологического анализа.
15) Сущность критериального метода.
16) Принятие решения на основе выбора на базе бинарных отношений.
17) метод принятия решений на основании функции выбора.
18) Принятие решений методом парных сравнений.
19) Этапы системного проектирования.
20) Оценка качества и эффективности информационных систем.
21) Практическое применение структурного анализа систем.
22) Средства структурного анализа и их взаимоотношения
23) Средства и методы управления проектами
24) Информационные системы управления проектами
25) Подход CPI/TQM к управлению проектами
26) Характеристика стандарта ISO 9000
27) Сущность реинжиниринга бизнес-процессов
28) Применение системных принципов при проектировании.
29) Применение моделей при проектировании системы защиты информации.

ТИПОВЫЕ ПРАКТИЧЕСКИЕ ЗАДАНИЯ ДЛЯ ПОДГОТОВКИ К ЗАЧЕТУ

1. Классифицируйте предложенную систему по следующим признакам:

- происхождение (естественные, искусственные, смешанные);
- сложность (простые, сложные);
- изолированность (открытые, закрытые);
- характер функционирования (стабильные, самостабилизирующиеся, самоорганизующиеся);
- способ задания целей (цели задаются извне, цели формируются внутри);
- способ управления (самоуправляемые, управляемые извне, с комбинированным управлением).

2. Выделите основные подсистемы исследуемой системы. В рамках каждой их них выделите более мелкие подсистемы и элементы. Представьте компоненты системы в виде иерархии

3. Опишите сущностное свойство системы и его внешнее проявление (явление). Определите, является ли данное свойство эмерджентным. Ответ обоснуйте

ВОПРОСЫ ПО ТЕМАМ / РАЗДЕЛАМ ДИСЦИПЛИНЫ

Раздел 1. Основы системного анализа

1. Определение и свойства систем
2. Классификация и функции систем.
3. Сущность и содержание структурного прогнозирования.
4. Сущность математических методов прогнозирования.
5. Сущность прогнозирования по аналогии.
6. Анализ внешней среды и ее влияния на реализацию альтернатив.
7. Алгоритм разработки управленческих решений в вопросах информационной безопасности.

Раздел 2. Прикладные модели и методы системного анализа в области информационных систем

1. Особенности системного подхода к проектированию информационных систем.
2. Основные этапы системного проектирования. оценка качества и эффективности информационных систем.
3. Средства структурного анализа и их взаимоотношения.
4. Построение диаграммы потоков данных (Data Flow Diagram).
5. Построение диаграммы «сущность-связь» (Entity-Relation diagram).
6. Построение диаграммы переходов систояний (State-Transition Diagram).
7. Сущность методологии SADT.
8. Сущность стандартов и модели IDEF: стандарт IDEF0, стандарт IDEF1X, стандарт IDEF3.
9. Сущности методологии SSADM.
10. Сущность методологии Мартина.

Раздел 3. Практическое применение системного анализа в управлении организационно-экономическими системами

1. Определение и особенности управление проектами.
2. Средства и методы управления проектами.
3. Информационные системы управления проектами.
4. Особенности реорганизация деятельности по методике Business systems planning.
5. Подход CPI/TQM.
6. Сущность стандарта ISO 9000.
7. Реинжиниринг бизнес-процессов.

Раздел 4. Системный подход к информационной безопасности

1. Основные цели защиты информации.
2. Основные задачи систем защиты информации.
3. Основы проектирования систем защиты информации.
4. Применение системных принципов при проектировании.
5. Обоснование выбора средств и методов при проектировании систем защиты информации.
6. Основные принципы проектирования систем защиты информации.
7. Основные средства системы защиты информации.
8. Стратегии применения средств защиты информации.
9. Анализ информационных рисков, угрозы и уязвимости системы.
10. Оценка рисков.
11. Учет угроз и рисков при проектировании информационных систем.
12. Оценивание эффективности защиты информации.
13. Применение моделей при проектировании системы защиты информации.

ТЕМЫ РЕФЕРАТОВ

1. Модели и методы системного анализа.
2. Информационная поддержка принятия решений.
3. Практическое применение структурного анализа систем в информационной безопасности.
4. Управление проектами в сфере информационной безопасности.
5. Информационные системы управления проектами.
6. Применение методики Business system planning.
7. Применение подхода CPI/TQM в управлении проектами в сфере информационной безопасности.
8. Международные стандарты по управлению проектами.
9. ISO 9000 стандарты по управлению проектами.
10. Системный подход к информационной безопасности.

Реферат – краткая запись идей, содержащихся в одном или нескольких источниках, которая требует умения сопоставлять и анализировать различные точки зрения. Реферат – одна из форм интерпретации исходного текста или нескольких источников. Поэтому реферат, в отличие от конспекта, является новым, авторским текстом. Новизна в данном случае подразумевает новое изложение, систематизацию материала, особую авторскую позицию при сопоставлении различных точек зрения.

Реферирование предполагает изложение какого-либо вопроса на основе классификации, обобщения, анализа и синтеза одного или нескольких источников.

Виды рефератов

По полноте изложения	Информативные (рефераты-конспекты)
	Индикативные (рефераты-резюме)
По количеству реферируемых источников	Монографические
	Обзорные

Реферат должен отвечать ряду требований.

Требования по оформлению:

– объем реферата от 10 до 15 страниц формата А4, шрифт Times New Roman, кегль 14 пт, полуторный междустрочный интервал, выравнивание текста – по ширине, нумерация страниц в верхнем колонтитуле по центру, автоматические переносы слов (кроме титульного листа), поля: снизу и сверху – 20 мм, слева – 25 мм, справа – 10 мм;

– на титульном листе указывается: название реферата, Фамилия И.О. обучающегося, номер группы;

– список использованных источников – современная, актуальная литература, не менее трех источников, полное указание выходных данных для книжных и периодических изданий, адреса сайтов с которых заимствован материал, по тексту реферата должны быть ссылки на источники.

Требования по структуре:

– реферат включает титульный лист, оглавление, введение, основной текст, заключение, список литературы, приложения (при необходимости);

– основной текст должен содержать несколько разделов.

Требования по содержанию:

– реферат должен содержать достоверные и актуальные сведения на достаточном научном уровне;

– реферат, кроме текста (формат .doc или .docx), может дополнительно содержать: качественные цветные иллюстрации, фрагменты программного кода и другие материалы, качественно дополняющие основную часть реферата.

КОМПЛЕКТ КЕЙС-ЗАДАЧ

Кейс 1.

В коммерческой организации, которая занимается поставками компьютерной техники для государственных и муниципальных органов. При сумме потенциального контракта (поставки) более 100 тысяч рублей данная компания должна участвовать в тендере, соответственно сталкиваться с конкурентной борьбой во время проведения торгов. Компания не имеет никаких внутренних документов, касающихся информационной безопасности, в том числе политики безопасности. В процессе участия в одной из процедур торгов ответственный менеджер по торгам получает на корпоративную почту письмо с заголовком "Срочно. Документы" с неизвестного адреса. Данное письмо содержит единственный архивный файл без текста самого письма. Менеджер открывает архив, после чего автоматически запускается вирус, который не только блокирует рабочий компьютер с установленным программным обеспечением для торгов и авторизированной электронной подписью организации, но и пытается распространяться по внутренней сети компании.

Сотрудники ИТ-отдела реагируют достаточно оперативно, локализуют распространение вируса, устраняют сам вирус и последствия его действия на всех зараженных компьютерах в течение 3-х часов. Но за это время торги закрываются, и компания упускает крупный контракт (порядка миллиона рублей)

Кто, по Вашему мнению, виноват в данной ситуации (менеджер, который открывал неизвестное письмо; сотрудники ИТ-отдела, которые не предприняли превентивных мер)? Кого следует наказать?

Правильный ответ В данном случае: виноват первый руководитель организации (например, генеральный директор), который не инициировал создание и внедрение политики безопасности. В политике безопасности могли быть описаны правила работы с электронной почтой, отдельно могли быть представлены правила организации работы во время проведения торгов, а также правила проведения инструктажа сотрудников. Также в политике безопасности расписываются правила передачи ответственности при проведении определенных действий. Если политика внедрена, инструктаж проведен, менеджер расписался о проведении инструктажа, то он не только 10 раз задумается, стоит ли открывать неизвестные письма, но и будет понимать, что наказание будет грозить непосредственно ему, так как на время торгов на него будет полностью возложена ответственность за их проведение.

Кейс 2.

«Расчет рисков информационной безопасности»

Описание ситуации: Например, информационная система Компании состоит из двух ресурсов: сервера и рабочей станции, которые находятся в одной сетевой группе, т.е. физически связанны между собой.

На сервере хранятся виды информации: бухгалтерский отчет и база клиентов Компании. На рабочей станции расположена база данных наименований товаров Компании с описанием.

К серверу локальный доступ имеет группа пользователей (к первой информации – бухгалтерский отчет): – главный бухгалтер. К серверу удаленный доступ имеют группы пользователей (ко второй информации – база клиентов Компании): – бухгалтер (с рабочей станции); – финансовый директор (через глобальную сеть Интернет).

К рабочей станции локальный доступ имеет группа пользователей (к базе данных наименований товаров Компании с описанием): – бухгалтер.

По правилам работы модели бухгалтер при удаленном доступе к серверу является группой обычных пользователей, а финансовый директор – группой авторизованных пользователей. Причем, бухгалтер имеет удаленный доступ к серверу через коммутатор.

Задание: Рассчитать риски информационной безопасности на основе модели информационных потоков.

Кейс 3.

Описание ситуации

В одной из компаний был зафиксирован следующий инцидент: при увольнении с работы системный администратор украл разрабатываемый в компании программный продукт и передал его конкурентам, которые выпустили программу на рынок под своим товарным знаком. Кроме этого, он внес изменения в информационную систему, в результате которых после его ухода функционирование определенных ее компонентов было нарушено. Привлечь администратора к ответственности в данном случае оказалось невозможно, так как, во-первых, не выполнялась регистрация его действий, во-вторых, администратор мог удалить все доказательства своих неправомерных действий и, в-третьих, не была налажена процедура сбора улик об инциденте.

Задание. 1. Определите возможные причины инцидента и степень ответственности сотрудника. 2. Определите меры, направленные на предотвращение повторных инцидентов. 3. Подготовьте проекты соответствующих документов.

Кейс 4.

Описание ситуации

В одной из компаний сотрудник хранил на мобильном компьютере конфиденциальные сведения компании без применения средств шифрования. После работы он забрал компьютер домой и забыл его в машине, которую оставил под окнами дома, а ночью машину взломали, и компьютер был украден. Злоумышленники получили доступ к конфиденциальной информации компании и могли продать ее конкурентам. Кроме этого, на компьютере хранилась ценная информация, которая не была зарезервирована на другом носителе.

Задание. 1. Определите возможные причины инцидента и степень ответственности сотрудника. 2. Определите меры, направленные на предотвращение повторных инцидентов. 3. Подготовьте проекты соответствующих документов.

Кейс 5.

Описание ситуации.

В Белозерске Вологодской области врач центральной районной больницы выписал список медицинских препаратов на «черновике». за разглашение персональных данных. Черновиком оказался талон амбулаторного больного, где были указаны персональные данные другого пациенты: ФИО, год рождения, номер паспорта, домашний адрес и диагноз.

Задание. 1. Определите возможные причины инцидента и степень ответственности сотрудника. 2. Определите меры, направленные на предотвращение повторных инцидентов. 3. Подготовьте проекты соответствующих документов.

Кейс 5.

Описание ситуации.

В больнице поселка Всеволодо-Вильва Пермского края пациентке вместе с результатами ЭКГ выдали список других пациентов. На черновике, к которому приклеили расшифровку кардиограммы, указаны фамилии, имена, даты рождения, домашние адреса и паспортные данные.

Задание. 1. Определите возможные причины инцидента и степень ответственности сотрудника. 2. Определите меры, направленные на предотвращение повторных инцидентов. 3. Подготовьте проекты соответствующих документов.

15 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ

21. Каково назначение СУИБ?
22. Что представляет собой жизненный цикл СУИБ?
23. Какие нормы, рекомендации определяют понятие информационного риска?
24. Определение бизнес процессов как они связаны с теорией риска?
25. Процесс управления инцидентами безопасности?
26. Методики определения актуальных рисков для бизнес-процессов?
27. Аудит информационной безопасности?
28. Этапы борьбы с рисковыми ситуациями?
29. Оценка рисков ИБ. Планирование мер по обработке выявленных рисков ИБ?
30. Внедрение специализированного программного обеспечения в области управления рисками?
31. Этапы внедрения СУИБ на реальных объектах КИИ?
32. Определение объекта КИИ?
33. Стандарт BS 7799-3?
34. Концепция управления рисками в ISO 19011:2011?
35. Что представляет собой федеральная концепция управления рисками (ФСУР)?
36. Что такое концепция управления рисками ИБ по стандарту COSO ERM?
37. Стратегия моделирования рисков информационной безопасности?
38. Модель нарушителя ИБ?
39. Типы моделей угроз ИБ?
40. Стратегии минимизации рисков, связанных с социальной инженерией?
41. Стратегии эффективного управления кадрами на предприятиях?
42. Роли высшего менеджмента предприятия в определении политики формирования стратегий минимизации рисков ИБ?

ТИПОВЫЕ ПРАКТИЧЕСКИЕ ЗАДАНИЯ ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ

1. Подготовьте в программе MSAT исходные данные для расчёта рисков.
2. Подготовьте в программе MSAT отчёт о проведённых исследованиях.
3. Настройте политику распространения обновлений. Проверьте ее работу. Сформируйте отчет о распространении обновлений.

ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

Министерство науки и высшего образования РФ Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет геосистем и технологий» Кафедра: информационной безопасности	10.04.01 Информационная безопасность (код и направление подготовки) Организация и управление информационной безопасности (профиль подготовки) Управление рисками информационной безопасности (дисциплина)

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Определение бизнес процессов как они связаны с теорией риска.
2. Определение объекта КИИ.

3. Стандарт BS 7799-3.

Составитель _____ И.О.Ф.
(подпись)

Заведующий кафедрой _____ И.О.Ф.
(подпись)

ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ

Раздел 1 «Введение. Основная тематика направления ИБ. Процессный подход»

1. Актуальность проблемы управления информационной безопасностью организации. Место и роль процессов по управлению рисками в общей системе обеспечения информационной безопасности и защиты информационных ресурсов.

2. Актуальность реализации процессов управления рисками информационной безопасности. Термины и определения.

Раздел 2 «Область деятельности СУИБ. Ролевая структура СУИБ. Политика СУИБ. Стандартизация в области управления ИБ»

1. Планирование деятельности по управлению рисками ИБ.

2. Реализация концепции управления информационными рисками на практике. Проработка тестов по анализу и оценке угроз, уязвимостей и информационных рисков организаций. Примерный анализ и моделирование событий и инцидентов информационной безопасности в различных организациях.

3. Принятие решений по обработке и управлению рисками ИБ.

4. Планирование деятельности по управлению рисками ИБ.

Раздел 3 «Основные процессы СУИБ. Обязательная документация СУИБ»

1. Методологические основы управления рисками. Понятия и определения в области управления рисками. Управление рисками в основных международных стандартах информационной безопасности. Модель процессов управления информационными рисками.

2. Обработка рисков информационной безопасности. Практические примеры "из жизни" управления рисками информационной безопасности организации.

3. Идентификация актуальных угроз и уязвимостей.

4. Оценка вероятности реализации угроз и уязвимостей.

Раздел 4 «Теория рисков ИБ»

1. Стратегии анализа информационных рисков организации. Сравнительные методики и основные подходы к анализу рисков ИБ. Инструментальные средства анализа рисков.

2. Роль управления информационными рисками в политике информационной безопасности организации. Управление инцидентами информационной безопасности в организации. Организационные вопросы обеспечения информационной безопасности. Порядок разработки, структура и содержание политик ИБ. Управление информационными рисками на различных стадиях жизненного цикла ИТ.

3. Оценка рисков информационной безопасности.

4. Основные этапы анализа рисков информационной безопасности.

5. Идентификация информационных активов компании.

Раздел 5 «Процесс управление инцидентами безопасности. Процесс обеспечение непрерывности ведения бизнес процессов»

1. Оценка рисков информационной безопасности. Менеджмент-решение. Активы ИС, риски, угрозы и уязвимости. Идентификация активов при анализе рисков ИС. Анализ угроз информационной безопасности организации. Анализ уязвимостей информационной инфраструк-

туры организации.

2. Программные средства, используемые для анализа и управления рисками. Обзор, анализ и сравнение современных программных продуктов по анализу рисков. Проблемы внедрения в России. Практические примеры оценки рисков в ИТ и в бизнесе.

3. Оценивание идентифицированных ресурсов с учётом требований законодательства и бизнеса.

4. Идентификация реализованных и планируемых мер защиты информационных активов.

5. Вычисление и оценивание рисков информационной безопасности.

6. Роли и ответственность в управлении рисками ИБ.

Раздел 6 «Стандарты в области рисков ИБ»

1. Основные положения правового регулирования процессов управления рисками информационной безопасности.

2. Современные методики управления рисками информационной безопасности.

ФОНД ТЕСТОВЫХ ЗАДАНИЙ

1. Команда по разработке политики безопасности обычно включает следующее число человек:
1) от 2 до 5
2) от 2 до 10
3) от 2 до 15
4) от 2 до 20

2. Количество основных правил глобальной политики безопасности равно:
1) трем
2) четырем
3) пяти
4) шести

3. В основные обязанности пользователя данными входит следующее их число:
1) два
2) три
3) четыре
4) пять

4. Какой самый важный вопрос должна решить команда по разработке политики безопасности организации:
1) какие компьютерные и сетевые сервисы требуются для бизнеса
2) зависят ли компьютерные и сетевые сервисы от удаленного доступа к внутренней сети
3) имеется ли требование бизнеса на тот или иной сервис
4) имеются ли требования по доступу к Веб-ресурсам

5. Основные устанавливаемые роли в безопасности сети включают следующее их количество:
1) два
2) три
3) четыре
4) пять

6. Процедура управления конфигурацией определяет:
1) какую информацию следует регистрировать и прослеживать
2) как тестируется и инсталлируется новое аппаратное обеспечение
3) как тестируется и инсталлируется новое программное обеспечение

4) кто должен быть проинформирован, когда вносятся изменения в различные виды обеспечения

7. Первые шаги по разработке политики безопасности включают следующее их число:
1) три
2) четыре
3) пять
4) шесть

8. Процедура реагирования на события определяет:
1) какую информацию следует регистрировать и прослеживать
2) кто имеет полномочия выполнять изменения конфигурации аппаратного и программного обеспечения
3) как обрабатывать исследование отклонений от нормы
4) как следует реагировать на атаки вторжения

9. На этапе анализа рисков осуществляются следующее число действий:
1) три
2) четыре
3) пять
4) шесть

10. При разработке политики ИБ необходимо руководствоваться следующим основным правилом:
1) команда разработчиков политики ИБ не должна превышать 20 человек
2) стоимость защиты конкретного актива не должна превышать стоимости самого актива
3) как следует реагировать на атаки вторжения
4) какую информацию следует регистрировать и прослеживать при функционировании системы защиты

11. Архитектура безопасности включает как минимум следующее число компонентов:
1) два
2) три
3) четыре
4) пять

12. В политике безопасности организации должны быть определены:
1) стандарты
2) правила безопасности
3) операции безопасности
4) процессы безопасности

13. Каждое действие в процессе безопасности включает следующее число компонентов:
1) два
2) три
3) четыре
4) пять

14. Каждое действие в процессе безопасности включает:
1) операцию
2) механизм
3) управление

4) выход

15. Защищаемые ресурсы (данные, файлы, базы данных, программы) могут быть разделены на следующее число групп:
1) два
2) три
3) четыре
4) пять

16. Компоненты архитектуры безопасности включают:
1) физическую безопасность
2) логическую безопасность
3) периметр безопасности сети
4) защиту ресурсов

17. Административные полномочия подразделяются на следующее число категорий:
1) два
2) три
3) четыре
4) пять

18. В основные задачи управления ИБ входят:
1) управление конфигурациями объектов и субъектов доступа;
2) управление доступом к базе данных
3) управление учетными записями и правами доступа к активным сетевым устройствам, рабочим станциям и серверам
4) управление конфигурациями объектов и субъектов доступа

19. Последовательность процессов для обнаружения проблемы и выдачи сигнала тревоги включает следующее число шагов:
1) два
2) три
3) четыре
4) пять

20. Подсистемы управления обновлениями позволяют автоматизировать следующие задачи:
1) возможность назначения обновлений определенным рабочим станциям и серверам или группам рабочих станций и серверов
2) контроль времени обновления ПО
3) автоматическое получение обновлений с сайтов производителей ПО
4) организацию централизованного хранилища обновлений

21. Использование централизованного управления рабочими станциями и серверами позволяет:
1) создавать типовые образы рабочих станций и серверов
2) существенно сократить затраты на обеспечение актуальной конфигурации оборудования
3) распределять административные роли по типам и группам устройств
4) поддерживать соответствие локальных настроек политике безопасности организации

22. Основные задачи управления ИБ включают следующее их число:
1) два
2) три
3) четыре

4) пять

23. Подсистемы управления обновлениями позволяют автоматизировать следующее число задач:
1) два
2) три
3) четыре
4) пять

24. Централизованное управление сетевым оборудованием позволяет:
1) осуществлять мониторинг сетевых устройств
2) производить откат неудачных изменений конфигурации
3) поддерживать соответствие локальных настроек политике безопасности организации
4) централизованно хранить конфигурации активного сетевого оборудования

25. Использование централизованного управления рабочими станциями и серверами позволяет удовлетворить следующее число требований:
1) два
2) три
3) четыре
4) пять

16 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «КОНТРОЛЬ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА»

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ

1. В чем суть понятия защита информации? Какие бывают угрозы и меры защиты?
2. Какие существуют основные виды атак? Что такое сетевые атаки?
3. Какие виды политик информационной безопасности Вы знаете?
4. На чем базируется математическая модель информационной безопасности Бела-Лападула?
5. В чем суть математической модели информационной безопасности Биба?
6. В чем отличительные особенности мандатной модели защиты от угроз?
7. В чем специфика модели Харрисона-Руззо-Ульмана?
8. Перечислите известные Вам стандарты информационной безопасности. Что определяют материалы ФСТЭК России?
9. Как строится классификация компьютерных преступлений по кодификатору Интерпола?
10. Что такое криптография? Назовите основные термины и определения. Каковы основные задачи криптографии?
11. Перечислите ПАК для проведения пентестов?
12. Стандарт 27000, назначение, общие сведения?
13. Каковы основные этапы развития криптографии?
14. Что такое стеганография?
15. В чем суть шифрования данных? Как строится классификация шифрования?
16. Что такое роторные машины?
17. В чем особенности американского стандарта шифрования DES?
18. Каковы режимы работы алгоритма DES?
19. В чем особенности российского стандарта шифрования ГОСТ 28147-89?
20. Что такое симметричная криптосистема AES?
21. Как устроены асимметричные системы шифрования? Каков их основной принцип работы? Что такое однонаправленные функции?
22. В чем особенности системы шифрования RSA?
23. Что такое хэш-функции? Каковы основные требования к ним? Приведите примеры построения.
24. Как устроен алгоритм хэширования SHA?
25. Что такое электронная цифровая подпись RSA?
26. Как происходит генерация ключей?
27. Как осуществляется хранение ключей?
28. Как устроен алгоритм безопасного распределения ключей Диффи-Хэллмана?
29. Что такое сертификаты открытых ключей?
30. Что такое протокол Kerberos?
31. Какие существуют технологии аутентификации?
32. Как организована защита информации в сети? В чем суть семиуровневой моделиOSI? Что такое стек TCP/IP?
33. Что такое протокол IPSec? Каковы его режимы работы?
34. Как построена стратегия безопасности протокола IPSec?
35. Как организуется защита информации в сети при использовании протоколаSSL/TLS?
36. Как организуется защита информации на прикладном уровне при использовании протокола PGP?
37. Как организуется защита информации на прикладном уровне при использовании протокола S/MIME?
38. Что такое система отслеживания вторжений?
39. В чем суть понятия защищенности (безопасности) компьютерной информации? Что такое конфиденциальность, целостность и доступность информации?

40. Что такое угроза безопасности компьютерной информации? Как строится классификация угроз?

41. Таксонометрия угроз безопасности и изъянов (брешей) систем защиты. ГОСТ Р 51275-99.

42. Что такое модель нарушителя безопасности?

43. Что такое субъектно-объектная модель компьютерной системы? В чем суть понятий потока, доступа и правил разграничения доступа. Каковы основные типы политик разграничения доступа?

44. Что такое монитор безопасности КС и как происходит гарантирование выполнение политики безопасности?

45. Что такое изолированная программная среда?

ТИПОВЫЕ ПРАКТИЧЕСКИЕ ЗАДАНИЯ ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ

Задание 1

1. Исходя из требований к ИСПДн 3-го уровня защищённости, организовать и настроить систему регистрации, контроля и разграничения прав доступа к доверенной среде в ОС Windows 10 (по вариантам).
2. Использовать функцию AppLockerОС Windows 10.

Задание 2

1. Используя методику внешнего аудита определить общий порядок сертификации средств защиты информации.
2. Дать рекомендации по СЗИ (по вариантам).

Задание 3

1. Используя приказы, нормативные документы ФСТЭК, дать методику организации средств СЗИ по категориям объектов КИИ.
2. Спроектировать локальную защищённую вычислительную сеть связи (ЛВС) объекта КИИ с использованием уникальных исходных данных (по вариантам).

Задание 4

1. С помощью механизмов проведения контроля защищённости конфиденциальной информации от несанкционированного доступа дать чёткую методику проведения:

*ICMP – echозапросов.

*TCP – Pingзапросов.

*сканирования портов TCPи UDP.

*определение ОС системы.

*определение приложения на основе banner – based.

*принцип работы с SSL/TLS.

Задание 5

1. С помощью средств ПО ViPNet организовать сегмент защищённой локальной сети предприятия с разными видами пользовательских данных (коммерческая тайна, персональные данные)
2. Дать мелодику определения структуры исходящих информационных потоков, циркулирующих в предприятии.

ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

Министерство науки и высшего образования РФ Федеральное государственное бюджетное	10.04.01 Информационная безопасность (код и направление подготовки)

образовательное учреждение высшего образования «Сибирский государственный университет геосистем и технологий» Кафедра: информационной безопасности	Организация и управление информационной безопасности (профиль подготовки) Контроль защищенности информации от несанкционированного доступа (дисциплина)

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

4. Определение бизнес процессов как они связаны с теорией риска.
5. Определение объекта КИИ.
6. Стандарт BS 7799-3.

Составитель _____ И.О.Ф.
(подпись)

Заведующий кафедрой _____ И.О.Ф.
(подпись)

ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ

Раздел 1 «Основные понятия и термины в области защиты информации от несанкционированного доступа»

1. В чем особенности руководящего документа Защита от несанкционированного доступа к информации. Термины и определения. Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г.?
2. ГОСТ Р 50922-96. ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ. Защита информации. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.
3. В чем суть терминов организационные мероприятия; технические средства; программные средства; шифрование?

Раздел 2 «Методы и способы защиты информации от несанкционированного доступа»

1. Какие существуют показатели защищенности?
2. Какие существуют классы защищённости?
3. Как осуществляется контроль отсутствия НДВ в информационных системах.
4. Какие показатели защищенности от НСД к информации Вы знаете?
5. Дайте определение защищенности автоматизированной системы.

Раздел 3 «Показатели защищенности. Классы защищенности»

1. Каковы основные исходные данные по обследуемой системе?
2. Каковы дополнительные исходные данные по обследуемой системе?
3. Какие требования предъявляются к автоматизированной системе как к объекту защиты?
4. Охарактеризуйте основные методы тестирования автоматизированных систем?
5. Охарактеризуйте нормативную базу оценки защищенности в России.
6. Каковы основные действующие нормативные документы в области защиты информации?
7. Каковы основные этапы развития «Общих критериев»?
8. Охарактеризуйте использование стандарта ISO 15408 в России.
9. Поясните понятие профиля защиты.
10. Поясните понятие задания по безопасности.

11. Каковы основные цели безопасности согласно «Общим критериям»? Коротко поясните.

12. В чем суть понятия защищенности?

13. Для чего необходимо проводить анализ защищенности?

14. Что является объектами анализа защищенности?

15. Каковы основные требования к автоматизированной системе?

16. В чем суть тестирования по методу «черного ящика»?

17. В чем суть тестирования по методу «белого ящика»?

Раздел 4 «Контроль отсутствия НДВ в информационных системах»

1. Каковы основные конструкции требований безопасности?

2. Что такое политика безопасности системы?

3. Не противоречат ли друг другу свойства защищаемой информации (конфиденциальность и доступность)?

4. Назначение анализаторов сетевых пакетов и их отличие от систем обнаружения вторжений. Примеры использования анализаторов сетевых пакетов при расследовании деятельности, связанной с Интернет.

5. Опишите в терминах ГОСТ Р ИСО/МЭК 15408-2002 и РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» систему контроля доступа на базе СЗИ «SecretNet 5.0», предназначенную для защиты коммерческой тайны в однопользовательском режиме.

6. Опишите в терминах ГОСТ Р ИСО/МЭК 15408-2002 и РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» систему контроля доступа на базе СЗИ «SecretNet 2000», предназначенную для защиты коммерческой тайны в компьютерной сети с разграничением прав доступа.

7. Опишите в терминах ГОСТ Р ИСО/МЭК 15408-2002 и РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» систему контроля доступа на базе СЗИ «Страж 2.5», предназначенную для защиты коммерческой тайны в однопользовательском режиме.

8. Опишите в терминах ГОСТ Р ИСО/МЭК 15408-2002 и РД «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» систему контроля информационных потоков на базе СЗИ «Застава», предназначенную для защиты государственной тайны в компьютерной сети в многопользовательском режиме.

9. Опишите в терминах ГОСТ Р ИСО/МЭК 15408-2002 и РД «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» систему контроля информационных потоков на базе СЗИ «VipNET», предназначенную для защиты коммерческой тайны в компьютерной сети с разграничением прав доступа.

10. Проведите процедуру базового анализа остаточных информационных рисков согласно ГОСТ Р ИСО/МЭК 17799-2005 для системы защиты информации компьютерной сети.

11. Проведите процедуру базового анализа остаточных информационных рисков согласно ГОСТ Р ИСО/МЭК 17799-2005 для системы защиты информации электронного документооборота.

12. Проведите процедуру базового анализа остаточных информационных рисков согласно ГОСТ Р ИСО/МЭК 17799-2005 для системы защиты информации электронного архива.

ФОНД ТЕСТОВЫХ ЗАДАНИЙ

1. К уязвимостям протокола FTP относятся:

А) Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде) Доступ по умолчанию

Б) Наличие двух открытых портов

В) Отсутствие механизма предотвращения перегрузок буфера

Г) Отсутствие аутентификации управляющих сообщений об изменении маршрута

Д) Отсутствие механизма проверки корректности заполнения служебных заголовков пакета

Е) Отсутствие средств проверки аутентификации полученных данных от источника

З) Отсутствие аутентификации сообщений об изменении параметров маршрута

И) Отсутствие поддержки аутентификации заголовков сообщений

2. К уязвимостям протокола telnet относятся:

А) Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде) Доступ по умолчанию

Б) Наличие двух открытых портов

В) Отсутствие механизма предотвращения перегрузок буфера

С) Отсутствие аутентификации управляющих сообщений об изменении маршрута

Д) Отсутствие механизма проверки корректности заполнения служебных заголовков пакета

Е) Отсутствие средств проверки аутентификации полученных данных от источника

З) Отсутствие аутентификации сообщений об изменении параметров маршрута

И) Отсутствие поддержки аутентификации заголовков сообщений

3. К уязвимостям протокола UDP относятся:

А) Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде) Доступ по умолчанию

Б) Наличие двух открытых портов

В) Отсутствие механизма предотвращения перегрузок буфера

Г) Отсутствие аутентификации управляющих сообщений об изменении маршрута

Д) Отсутствие механизма проверки корректности заполнения служебных заголовков пакета

Е) Отсутствие средств проверки аутентификации полученных данных от источника

З) Отсутствие аутентификации сообщений об изменении параметров маршрута

И) Отсутствие поддержки аутентификации заголовков сообщений

4. К уязвимостям протокола ARP относятся:

А) Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде) Доступ по умолчанию

Б) Наличие двух открытых портов

В) Отсутствие механизма предотвращения перегрузок буфера

Г) Отсутствие аутентификации управляющих сообщений об изменении маршрута

Д) Отсутствие механизма проверки корректности заполнения служебных заголовков пакета

Е) Отсутствие средств проверки аутентификации полученных данных от источника

З) Отсутствие аутентификации сообщений об изменении параметров маршрута

И) Отсутствие поддержки аутентификации заголовков сообщений

5. К уязвимостям протокола RIP относятся:

А) Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде) Доступ по умолчанию

Б) Наличие двух открытых портов

В) Отсутствие механизма предотвращения перегрузок буфера

Г) Отсутствие аутентификации управляющих сообщений об изменении маршрута

Д) Отсутствие механизма проверки корректности заполнения служебных заголовков пакета

Е) Отсутствие средств проверки аутентификации полученных данных от источника

З) Отсутствие аутентификации сообщений об изменении параметров маршрута
И) Отсутствие поддержки аутентификации заголовков сообщений

6. К уязвимостям протокола TCP относятся:
А) Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде) Доступ по умолчанию
Б) Наличие двух открытых портов
В) Отсутствие механизма предотвращения перегрузок буфера
Г) Отсутствие аутентификации управляющих сообщений об изменении маршрута
Д) Отсутствие механизма проверки корректности заполнения служебных заголовков пакета
Е) Отсутствие средств проверки аутентификации полученных данных от источника
З) Отсутствие аутентификации сообщений об изменении параметров маршрута
И) Отсутствие поддержки аутентификации заголовков сообщений

7. К уязвимостям протокола DNS относятся:
А) Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде) Доступ по умолчанию
Б) Наличие двух открытых портов
В) Отсутствие механизма предотвращения перегрузок буфера
Г) Отсутствие аутентификации управляющих сообщений об изменении маршрута
Д) Отсутствие механизма проверки корректности заполнения служебных заголовков пакета
Е) Отсутствие средств проверки аутентификации полученных данных от источника
З) Отсутствие аутентификации сообщений об изменении параметров маршрута
И) Отсутствие поддержки аутентификации заголовков сообщений

8. К уязвимостям протокола IGMP относятся:
А) Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде) Доступ по умолчанию
Б) Наличие двух открытых портов
В) Отсутствие механизма предотвращения перегрузок буфера
Г) Отсутствие аутентификации управляющих сообщений об изменении маршрута
Д) Отсутствие механизма проверки корректности заполнения служебных заголовков пакета
Е) Отсутствие средств проверки аутентификации полученных данных от источника
З) Отсутствие аутентификации сообщений об изменении параметров маршрута
И) Отсутствие поддержки аутентификации заголовков сообщений

9. К уязвимостям протокола SMTP относятся:
А) Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде) Доступ по умолчанию
Б) Наличие двух открытых портов
В) Отсутствие механизма предотвращения перегрузок буфера
Г) Отсутствие аутентификации управляющих сообщений об изменении маршрута
Д) Отсутствие механизма проверки корректности заполнения служебных заголовков пакета
Е) Отсутствие средств проверки аутентификации полученных данных от источника
З) Отсутствие аутентификации сообщений об изменении параметров маршрута
И) Отсутствие поддержки аутентификации заголовков сообщений

10. К уязвимостям протокола SNMP относятся:
А) Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде) Доступ по умолчанию
Б) Наличие двух открытых портов
В) Отсутствие механизма предотвращения перегрузок буфера

Г) Отсутствие аутентификации управляющих сообщений об изменении маршрута
Д) Отсутствие механизма проверки корректности заполнения служебных заголовков пакета
Е) Отсутствие средств проверки аутентификации полученных данных от источника
З) Отсутствие аутентификации сообщений об изменении параметров маршрута
И) Отсутствие поддержки аутентификации заголовков сообщений

11. Процедура распознавания субъекта по его идентификатору называется:
А) Идентификацией
Б) Аутентификацией
В) Авторизацией

12. Процедура проверки подлинности называется
А) Идентификацией
Б) Аутентификацией
В) Авторизацией

13.Процедура предоставление доступа к какому-либо ресурсу называется
А) Идентификацией
Б) Аутентификацией
В) Авторизацией

14. К статическим биометрическим системам идентификации и аутентификации относятся:
А) идентификация по форме ладони
Б) идентификация по подписи
В) идентификация по отпечатку пальцев
Г) идентификация по речи
Д) идентификация по радужной оболочке
Е) идентификация по динамики клавиатурного набора
З) идентификация по сетчатке глаза
И) идентификация по форме лица

15 К динамическим биометрическим системам идентификации и аутентификации относятся:
А) идентификация по форме ладони
Б) идентификация по подписи
В) идентификация по отпечатку пальцев
Г) идентификация по речи
Д) идентификация по радужной оболочке
Е) идентификация по динамики клавиатурного набора
З) идентификация по сетчатке глаза
И) идентификация по форме лица
16. Какие защитные механизмы СЗИ Secret Net Studio уровне защиты данных
А) Теневое копирование
Б) Шифрование данных
В) Маркировка документов
Г) Регистрация и контроль запуска
Д) Контроль доступа к сети
Е) Контроль поведения приложения
З) Персональный межсетевой экран
И) VPN-клиент
К) Антивирусная защита
Л) Контроль входа в систему

М) Управление доступом
Н) Контроль целостности
О) Контроль подключения устройств и доступа к устройствам
П) Интеграция со средством доверительной загрузки (ПАК «Соболь»)

17. Какие защитные механизмы СЗИ Secret Net Studio уровне защиты приложений
А) Теневое копирование
Б) Шифрование данных
В) Маркировка документов
Г) Регистрация и контроль запуска
Д) Контроль доступа к сети
Е) Контроль поведения приложения
З) Персональный межсетевой экран
И) VPN-клиент
К) Антивирусная защита
Л) Контроль входа в систему
М) Управление доступом
Н) Контроль целостности
О) Контроль подключения устройств и доступа к устройствам
П) Интеграция со средством доверительной загрузки (ПАК «Соболь»)

18. Какие защитные механизмы СЗИ Secret Net Studio уровне защиты сети
А) Теневое копирование
Б) Шифрование данных
В) Маркировка документов
Г) Регистрация и контроль запуска
Д) Контроль доступа к сети
Е) Контроль поведения приложения
З) Персональный межсетевой экран
И) VPN-клиент
К) Антивирусная защита
Л) Контроль входа в систему
М) Управление доступом
Н) Контроль целостности
О) Контроль подключения устройств и доступа к устройствам
П) Интеграция со средством доверительной загрузки (ПАК «Соболь»)

19. Какие защитные механизмы СЗИ Secret Net Studio уровне защиты операционной системы
А) Теневое копирование
Б) Шифрование данных
В) Маркировка документов
Г) Регистрация и контроль запуска
Д) Контроль доступа к сети
Е) Контроль поведения приложения
З) Персональный межсетевой экран
И) VPN-клиент
К) Антивирусная защита
Л) Контроль входа в систему
М) Управление доступом
Н) Контроль целостности
О) Контроль подключения устройств и доступа к устройствам

П) Интеграция со средством доверительной загрузки (ПАК «Соболь»)

20. Какие защитные механизмы СЗИ Secret Net Studio уровне защиты периферийного оборудования

А) Теневое копирование
Б) Шифрование данных
В) Маркировка документов
Г) Регистрация и контроль запуска
Д) Контроль доступа к сети
Е) Контроль поведения приложения
З) Персональный межсетевой экран
И) VPN-клиент
К) Антивирусная защита
Л) Контроль входа в систему
М) Управление доступом
Н) Контроль целостности
О) Контроль подключения устройств и доступа к устройствам
П) Интеграция со средством доверительной загрузки (ПАК «Соболь»)

21. Межсетевые экраны какого типа могут иметь только программно-техническое исполнение?

А) межсетевой экран уровня сети (тип «А»)
Б) межсетевой экран уровня логических границ сети (тип «Б»)
В) межсетевой экран уровня узла (тип «В»)
Г) межсетевой экран уровня веб-сервера (тип «Г»)
Д) межсетевой экран уровня промышленной сети (тип «Д»)

22. Межсетевые экраны какого типа могут иметь только программное исполнение?

А) межсетевой экран уровня сети (тип «А»)
Б) межсетевой экран уровня логических границ сети (тип «Б»)
В) межсетевой экран уровня узла (тип «В»)
Г) межсетевой экран уровня веб-сервера (тип «Г»)
Д) межсетевой экран уровня промышленной сети (тип «Д»)

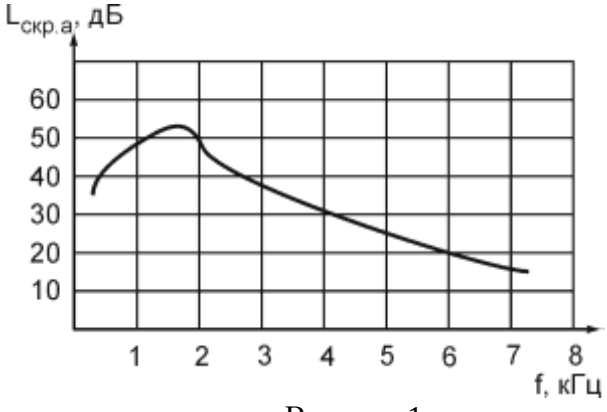
17 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «КОНТРОЛЬ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ»

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ

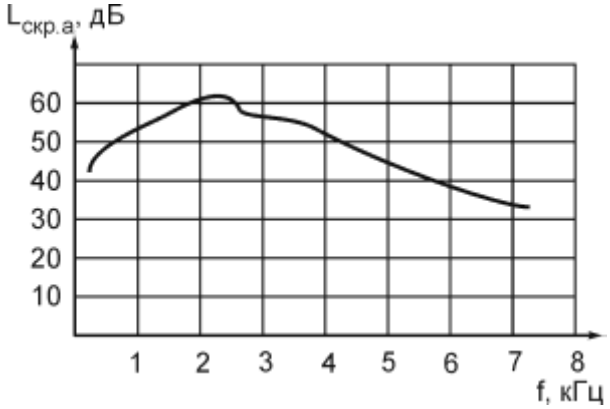
46. В чем суть понятия утечки информации?
47. Каковы цели обеспечения информационной безопасности?
48. Какие существуют методы предотвращения утечки информации?
49. Что значит информационная безопасность с точки зрения бизнеса?
50. Что такое цена информации?
51. В чем суть управления информационной безопасностью?
52. Каковы основные свойства информации?
53. Каковы основные цели защиты информации?
54. Каковы основные виды технических каналов утечки информации?
55. В чем особенности электромагнитного канала утечки информации?
56. В чем особенности индукционного канала утечки информации?
57. В чем особенности оптико-электронного канала утечки информации?
58. В чем особенности виброакустического канала утечки информации?
59. В чем особенности параметрического канала утечки информации?
60. Каковы основные задачи систем защиты информации?
61. Каковы структура и классификация технических каналов утечки информации?
62. Каковы основные характеристики технических каналов утечки информации?
63. В чем особенности технических каналов утечки речевой информации?
64. Каковы основные способы технической защиты?
65. В чем заключаются концепция и методы инженерно-технической защиты информации?
66. Охарактеризуйте требования стандарта (с точки зрения реализации на практике).
67. Какова взаимосвязь стандартов?
68. В чем особенности системы управления рисками по требованию стандарта ISO 27001:2005?

ТИПОВЫЕ ПРАКТИЧЕСКИЕ ЗАДАНИЯ ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ

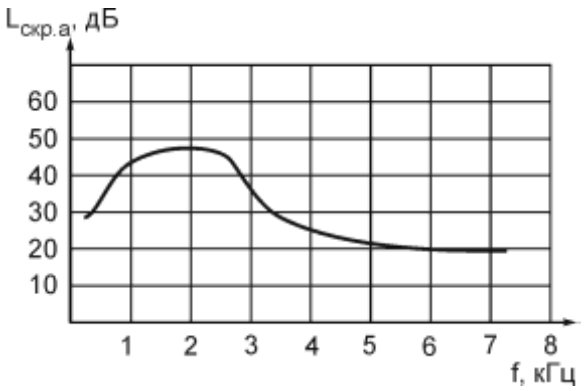
1. По спектру речевого сигнала, измеренному на границах контролируемой зоны (см. рисунок), в соответствии с вариантом, заданным преподавателем, рассчитать словесную разборчивость речевой информации. Уровень шума принять равным Lак.ш = 50 дБ. Сделать вывод о возможности перехвата речевой информации, если Wп = 1.



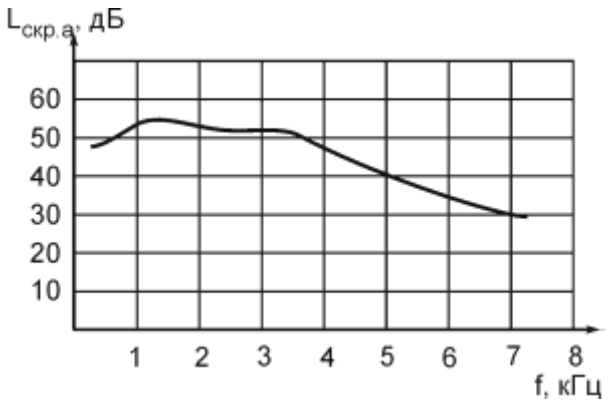
Вариант 1



Вариант 2



Вариант 3



Вариант 4

Спектр речевого сигнала $L_{скр.а}$, измеренного на границах контролируемой зоны

2. Рассчитать эффективность поглощения и глубину проникновения электромагнитного поля в экраны ЭМИ, выполненные из материалов, описанных в таблице в соответствии с вариантом, указанным преподавателем. Толщина каждого из экранов составляет 3 мм. Расчет произвести на частоте 100 МГц. Сделать вывод об эффективности использования рассчитанного экрана на заданной частоте.

Характеристики некоторых металлов и сплавов

Вариант	Металл	Удельное сопротивление $\frac{Ом \cdot мм^2}{м}$	μ
1	Медь	0,0175	1
2	Латунь	0,06	1
3	Алюминий	0,03	1
4	Сталь	0,1	200
5	Пермаллой	0,65	12000

ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

Министерство науки и высшего образования РФ Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет геосистем и технологий» Кафедра: информационной безопасности	10.04.01 Информационная безопасность (код и направление подготовки) Организация и управление информационной безопасности (профиль подготовки) Контроль защищенности информации от утечки по техническим каналам (дисциплина)

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

7. Определение бизнес процессов как они связаны с теорией риска.

8. Определение объекта КИИ.
9. Стандарт BS 7799-3.

Составитель _____ И.О.Ф.
(подпись)

Заведующий кафедрой _____ И.О.Ф.
(подпись)

ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ

Раздел 4 «Методы, способы и средства инженерно-технической защиты информации»

1. В чем особенности акустического канала утечки информации?
2. Каковы наиболее опасные объекты с точки зрения акустической разведки?
3. Каковы основные средства перехвата акустической информации?
4. Каковы особенности использования виброакустического канала?
5. Какие существуют звукопоглощающие материалы и конструкции?
6. Что такое резонансные звукопоглотители?
7. Что такое виброизоляция?
8. Что такое акустические речевые сигналы? Каковы особенности их восприятия
9. Что такое фонемы, октавы и форманты в акустическом речевом сигнале?
10. Как определяется разборчивость речи?
11. Что такое словесная, слоговая и другие виды разборчивости речи?
12. Каковы основные характеристики речевого сигнала?
13. Каковы обстоятельства, влияющие на разборчивость речи?
14. Каков порядок расчёта словесной разборчивости?
15. Что такое направленные микрофоны? Каковы их основные виды?
16. Каковы основные характеристики направленных микрофонов?
17. Чем отличаются трубчатый и щелевой направленный микрофоны?
18. Что такое направленный микрофон органного типа?
19. Что такое параболический направленный микрофон?
20. В чем особенности применения направленных микрофонов на открытой местности и в помещениях?
21. Каковы особенности распространения звука на открытом пространстве?
22. Как влияют атмосфера и погодные условия на распространение звука?

Раздел 5 «Организация инженерно-технической защиты информации»

1. Каковы основные цели канала утечки ПЭМИН?
2. В чем заключаются источники и особенности ПЭМИН?
3. Какие существуют способы защиты информации от утечки через канал ПЭМИН?
4. В чем состоит активная радиотехническая маскировка?
5. Как осуществляется электромагнитное экранирование помещений?
6. Как определяется эффективность экранирования от ПЭМИН?
7. Какие физические процессы происходят при электромагнитном экранировании?
8. Какие материалы применяются при экранировании от ПЭМИН?
9. Каковы основные способы экранирования от ПЭМИН?
10. В чем особенности визуального канала утечки информации?
11. Какие существуют средства скрытого видеонаблюдения?
12. Какие существуют средства управления сигналом в системах видеонаблюдения?
13. Каковы исходные данные для расчета объема видео?
14. Каков порядок расчета?
15. Каковы оптимизировать объем записываемой видеоинформации?
16. Какие существуют видеодетекторы движения?

17. Каковы особенности применения средств визуального наблюдения в ночных условиях?
18. Что такое ПНВ, тепловизоры?
19. Что входит в состав системы телевидения?
20. Каковы основные правила установки камер наблюдения?
21. Как осуществляется выбор мест установки камер наблюдения?
22. Как происходит работа систем управления охранного телевидения? Что такое мультиплексоры?
23. В чем особенности правового обеспечения систем видеонаблюдения?
24. Каковы правовые ограничения применения систем видеонаблюдения?
25. Что такое скрытое видеонаблюдение? Каковы его правовые аспекты?
26. Каков порядок расчета и выбора объективов и матриц камер наблюдения?
27. Каков порядок настройки камеры с переменным фокусом?

ВОПРОСЫ ДЛЯ ЗАЩИТЫ ЛАБОРАТОРНЫХ РАБОТ

Лабораторная работа № 1 «Расчет параметров акустического сигнала»

1. В чем особенности акустического канала утечки информации?
2. Каковы наиболее опасные объекты с точки зрения акустической разведки?
3. Каковы основные средства перехвата акустической информации?
4. Каковы особенности использования виброакустического канала?
5. Какие существуют звукопоглощающие материалы и конструкции?
6. Что такое резонансные звукопоглотители?
7. Что такое виброизоляция?

Лабораторная работа № 2 «Расчет параметров направленного микрофона»

1. Что такое направленные микрофоны? Каковы их основные виды?
2. Каковы основные характеристики направленных микрофонов?
3. Чем отличаются трубчатый и щелевой направленный микрофоны?
4. Что такое направленный микрофон органного типа?
5. Что такое параболический направленный микрофон?
6. В чем особенности применения направленных микрофонов на открытой местности и в помещениях?
7. Каковы особенности распространения звука на открытом пространстве?
8. Как влияют атмосфера и погодные условия на распространение звука?

Лабораторная работа № 3 «Расчет показателя разборчивости речи»

1. Что такое акустические речевые сигналы? Каковы особенности их восприятия
2. Что такое фонемы, октавы и форманты в акустическом речевом сигнале?
3. Как определяется разборчивость речи?
4. Что такое словесная, слоговая и другие виды разборчивости речи?
5. Каковы основные характеристики речевого сигнала?
6. Каковы обстоятельства, влияющие на разборчивость речи?
7. Каков порядок расчёта словесной разборчивости?

Лабораторная работа № 4 «Защита помещений от ПЭМИН»

1. Каковы основные цели канала утечки ПЭМИН?
2. В чем заключаются источники и особенности ПЭМИН?
3. Какие существуют способы защиты информации от утечки через канал ПЭМИН?
4. В чем состоит активная радиотехническая маскировка?
5. Как осуществляется электромагнитное экранирование помещений?
6. Как определяется эффективность экранирования от ПЭМИН?

7. Какие физические процессы происходят при электромагнитном экранировании?
8. Какие материалы применяются при экранировании от ПЭМИН?
9. Каковы основные способы экранирования от ПЭМИН?

Лабораторная работа № 5 «Анализ видеоканала утечки информации, дальность распознавания текста»

1. В чем особенности визуального канала утечки информации?
2. Какие существуют средства скрытого видеонаблюдения?
3. Основные параметры камеры, влияющие на дальность распознавания?

Лабораторная работа № 6 Изучение работы средств охранной сигнализации

1. Типы охранных извещателей
2. Правила установки инфракрасных и радиоволновых извещателей
3. Принцип работы пассивных инфракрасных извещателей
4. Принцип работы активных радиоволновых извещателей
5. Достоинства и недостатки, правила установки акустических ДРС
6. Виды и принципы действия поверхностных ДРС
7. Функционал и способы применения приемно-контрольных приборов

ФОНД ТЕСТОВЫХ ЗАДАНИЙ

1. Технические каналы утечки информации:
e) Акустический;
f) Визуальный;
g) Фотографический;
h) Электромагнитный

2. Промышленный шпионаж – это:
d) Кража деталей из промышленного цеха;
e) Кража конфиденциальной информации;
f) Разведка на поле боя.

3. Направленный микрофон относится к каналу утечки информации:
e) Акустический;
f) Визуальный;
g) Материальный;
h) Электромагнитный.

4. Радиозакладка относится к каналу утечки информации:
d) Акустический;
e) Визуальный;
f) Материальный.

5. Скрытая видеокамера относится к каналу утечки информации:
e) Акустический;
f) Визуальный;
g) Материальный;
h) Электромагнитный.

6. Средства прослушивания телефонной линии относятся к каналу утечки информации:
e) Акустический;

f) Визуальный;
g) Материальный;
h) Электромагнитный.

7. Кража документов относится к каналу утечки информации:
e) Акустический;
f) Визуальный;
g) Материальный;
h) Электромагнитный.

8. Кража образцов химических веществ относится к каналу утечки информации:
e) Акустический;
f) Визуальный;
g) Материальный;
h) Электромагнитный.

9. Явление отражения звуковых волн используется в:
e) Линейной группе микрофонов;
f) В параболическом микрофоне;
g) В трубчатом микрофоне;
h) В фазированной решетке.

10. Трубки разной длины используются в:
f) Линейной группе микрофонов;
g) В параболическом микрофоне;
h) Органном микрофоне;
i) В трубчатом микрофоне;
j) В фазированной решетке.

11. Плоскость с точечными микрофонами используется:
e) Линейной группе микрофонов;
f) В параболическом микрофоне;
g) В трубчатом микрофоне;
h) В фазированной решетке.

12. Типичная дальность применения направленного микрофона в условиях городской шумной улицы:
d) До 100 м;
e) До 25 – 50 м;
f) До 15 – 25 м.

14. Типичная дальность применения направленного микрофона в условиях тихой городской улицы:
d) До 100 м;
e) До 25 – 50 м;
f) До 15 – 25 м.

15. Типичная дальность применения направленного микрофона в условиях загородной местности:
d) До 100 м;
e) До 25 – 50 м;
f) До 15 – 25 м.

16. Что больше всего оказывает влияние на дальность действия микрофона:
e) Осадки;
f) Давление воздуха;
g) Температура воздуха;
h) Турбулентность воздуха.

17. Что больше всего оказывает влияние на дальность действия микрофона:
e) Посторонние шумы;
f) Давление воздуха;
g) Температура воздуха;
h) Турбулентность воздуха.

18. Скорость звука в воздухе. Выберите наиболее близкое значение
e) 784 м/с;
f) 153 м/с;
g) 343 м/с;
h) 1100 м/с.

19. Скорость звука в воде. Выберите наиболее близкое значение
e) 1000 м/с;
f) 1310 м/с;
g) 1440 м/с;
h) 5000 м/с.

20. Скорость звука в стали. Выберите наиболее близкое значение:
e) 1000 м/с;
f) 1500 м/с;
g) 4000 м/с;
h) 5000 м/с.

21. Диапазоны слышимости звука для человека:
e) 100 – 500 Гц;
f) 16 – 20000 Гц;
g) 51 – 14400 Гц;
h) 163 – 9900 Гц.

22. Явление убывания интенсивности звуковой волны с расстоянием описывается:
e) Законом Планка;
f) Законом обратных квадратов;
g) Теоремой Котельникова;
h) Законом Кирхгофа.

23. Интенсивность звука измеряется в:
e) Децибелах;
f) Кг/м^3;
g) вт/м^2;
h) Гц.

24. Уровень интенсивность (громкость) измеряется в:
e) Децибелах;

f) Кг/м^3;
g) вт/м^2;
h) Гц,

25. Порог слышимости человеческого уха в вт/м^2
e) 1;
f) 10^{-5};
g) 10^{-12};
h) 10^{-1}.

18 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «ПРОЦЕССНЫЙ ПОДХОД В УПРАВЛЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ЗАЧЕТУ

1. В чем сущность процесса как системы? Процесс как развивающаяся система.
2. В чем сущность и основные характеристики бизнес-процесса.
3. Сущность и содержание процессного подхода.
4. Опишите организацию как совокупность процессов.
5. Каковы принципы процессного подхода?
6. Каковы принципы формирования управленческой команды в рамках процессного управления?
7. Каковы особенности лидерства и формирования команды в рамках процессной команды?
8. В чем сущность концепции четырехфазного управленческого цикла (модель PDCA)?
9. Какие функции управления Вы знаете?
10. В чем особенности формирования команды по управлению информационной безопасностью?
11. Каковы элементы цикла Ишикавы?
12. В чем сущность концепции Business Process Management?
13. Каковы этапы жизненного цикла управления процессами в BPM?
14. В чем сущность проектирования процессов?
15. Основные этапы реализации процессов?
16. Каковы свойства организации как системы процессов?
17. Иерархическое представление сложной системы.
18. Графическое моделирование сложных систем.
19. В чем сущность процессного подхода к управлению информационной безопасностью?
20. Отечественные и зарубежные стандарты в области управления информационной безопасностью
21. Модель PDCA применительно к процессам СУИБ

ТИПОВЫЕ ПРАКТИЧЕСКИЕ ЗАДАНИЯ ДЛЯ ПОДГОТОВКИ К ЗАЧЕТУ

Описать процесс «Распределение обязанностей и ответственности» при обеспечении информационной безопасности.

Описать процесс «Повышение осведомленности сотрудников в вопросах информационной безопасности» при обеспечении информационной безопасности.

Описать процесс «Обеспечение непрерывности бизнес-процессов» при обеспечении информационной безопасности.

Описать процесс «Мониторинг информационной инфраструктуры» при обеспечении информационной безопасности.

Описать процесс «Безопасное хранение данных» при обеспечении информационной безопасности.

Описать процесс «Управление доступом к данным» при обеспечении информационной безопасности.

ВОПРОСЫ ПО ТЕМАМ / РАЗДЕЛАМ ДИСЦИПЛИНЫ

Раздел 1. Процесс. Процессный подход

8. Определение процесса как системы.

9. Понятие, сущность и основные характеристики бизнес-процесса, процесса обеспечения информационной безопасности.

10. Сущность и содержание процессного подхода.

11. Основные критерии процессного подхода.

12. Этапы реализации процессного подхода.

13. Формирование управленческой команды в рамках процессного управления.

14. Характеристика лидера в рамках процессной команды.

Раздел 2. Модель непрерывного улучшения процессов

1. Сущность концепции четырехфазного управленческого цикла (PDCA).

2. Перечислите основные функции управления.

3. Сущность методики формирования команды по управлению информационной безопасностью.

4. Цикл Ишикавы.

5. Сущность концепции Business Process Management.

6. Этапы жизненного цикла управления процессами в Business Process Management.

7. Алгоритм проектирования и реализации процессов.

8. Непрерывное совершенствование системы посредством измерения и оценки.

9. Способы иерархического представления сложной системы.

10. Способы графического моделирования сложных систем.

Раздел 3. Процессная модель управления информационной безопасностью

1. Сущность процессного подхода к управлению информационной безопасностью.

2. Какие отечественные стандарты в области управления информационной безопасности вы знаете?

3. Какие зарубежные стандарты в области управления информационной безопасности вы знаете?

4. Дайте характеристику стандартам ISO/IEC серии 270XX

5. Дайте характеристику стандарту ГОСТ Р ИСО/МЭК 27001:2006

6. Дайте характеристику стандарту Свод правил Control Objectives for Information and Related Technology (COBIT)

7. Дайте характеристику Библиотеке Information Technology Infrastructure Library (ITIL);

8. Дайте характеристику стандартам Серии National Institute of Standards and Technology (NIST)

9. Особенности модели PDCA применительно к процессам СУИБ

ТЕМЫ РЕФЕРАТОВ

1. Процесс как управляемая система
2. Процессный подход при построении системы информационной безопасности
3. Основные функции управления
4. Сущность процессов в системе информационной безопасности
5. Цикл Деминга и его применении в управлении информационной безопасностью
6. Отечественные стандарты, определяющие структуру процессов при построении системы информационной безопасности
7. Зарубежные стандарты, определяющие структуру процессов при построении системы информационной безопасности

Реферат – краткая запись идей, содержащихся в одном или нескольких источниках, которая требует умения сопоставлять и анализировать различные точки зрения. Реферат – одна из форм интерпретации исходного текста или нескольких источников. Поэтому реферат, в отличие от конспекта, является новым, авторским текстом. Новизна в данном случае подразумевает новое изложение, систематизацию материала, особую авторскую позицию при сопоставлении различных точек зрения.

Реферирование предполагает изложение какого-либо вопроса на основе классификации, обобщения, анализа и синтеза одного или нескольких источников.

Виды рефератов

По полноте изложения	Информативные (рефераты-конспекты)
	Индикативные (рефераты-резюме)
По количеству реферируемых источников	Монографические
	Обзорные

Реферат должен отвечать ряду требований.

Требования по оформлению:

– объем реферата от 10 до 15 страниц формата А4, шрифт Times New Roman, кегль 14 пт, полуторный междустрочный интервал, выравнивание текста – по ширине, нумерация страниц в верхнем колонтитуле по центру, автоматические переносы слов (кроме титульного листа), поля: снизу и сверху – 20 мм, слева – 25 мм, справа – 10 мм;

– на титульном листе указывается: название реферата, Фамилия И.О. обучающегося, номер группы;

– список использованных источников – современная, актуальная литература, не менее трех источников, полное указание выходных данных для книжных и периодических изданий, адреса сайтов с которых заимствован материал, по тексту реферата должны быть ссылки на источники.

Требования по структуре:

– реферат включает титульный лист, оглавление, введение, основной текст, заключение, список литературы, приложения (при необходимости);

– основной текст должен содержать несколько разделов.

Требования по содержанию:

– реферат должен содержать достоверные и актуальные сведения на достаточном научном уровне;

– реферат, кроме текста (формат .doc или .docx), может дополнительно содержать: качественные цветные иллюстрации, фрагменты программного кода и другие материалы, качественно дополняющие основную часть реферата.

19 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «ТЕОРИЯ ПРИНЯТИЯ РЕШЕНИЙ В ВОПРОСАХ ЗАЩИТЫ ИНФОРМАЦИИ»

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ЗАЧЕТУ

30) Понятие и классификация управленческих решений.
31) Методы принятия управленческих решений
32) Методика принятия управленческих решений в экстремальных ситуациях.
33) Риск и его разновидности. Классификация рисков. Уровни рисков. Типы рисков.
34) Анализ и оценка последствий риска.
35) Меры по снижению возможного риска.
36) Методы анализа влияния внешней среды на принятие управленческих решений.
37) Алгоритм разработки управленческих решений в вопросах информационной безопасности.
38) Выбор решений в условиях неопределенности.
39) Анализ организационной структуры как первый этап разработки управленческих решений.
40) Определение видов критической информации при разработке управленческих решений.
41) Анализ критической информации с использованием схемы классификации угроз информационной безопасности DSECCT.
42) Разработка управленческих решений в соответствии с характеристиками угроз информационной безопасности.
43) Проверка управленческих решений на соответствие аспектам информационной безопасности.
44) Критерии принятия управленческих решений.
45) Выбор решений с помощью дерева решений (позиционные игры).
46) Эффективность управленческих решений.
47) Методы оценки экономической эффективности управленческих решений.
48) Организация процесса разработки управленческих решений.
49) Процедуры организации выполнения управленческих решений.
50) Виды ответственности руководителей за управленческие решения в сфере информационной безопасности.
51) Контроль на стадиях разработки и реализации управленческих решений.

ТИПОВЫЕ ПРАКТИЧЕСКИЕ ЗАДАНИЯ ДЛЯ ПОДГОТОВКИ К ЗАЧЕТУ

4. Международный аэропорт «Одесса» был подвергнут хакерской атаке. Все службы аэропорта переведены на усиленный режим работы. Десятки рейсов были задержаны. Какие управленческие решения должны быть предприняты для решения данной ситуации?

5. Из-за хакерской атаки в работе в работе серверов Интерфакса возник сбой. Технические службы принимают все меры для восстановления работы систем. Каковы возможные причины ущерба?

6. Программа- вымогатель WannaCry заразила в МВД России только персональные компьютеры сотрудников, подключавших ПК к интернету. Внутренняя сеть МВД при атаке не пострадала. Каковы возможные причины инцидента и какие управленческие решения необходимо принять?

ВОПРОСЫ ПО ТЕМАМ / РАЗДЕЛАМ ДИСЦИПЛИНЫ

Раздел 1

15. Сущность экспертных методов прогнозирования

16. Сущность логического и функционально-логического прогнозирования.
17. Сущность и содержание структурного прогнозирования.
18. Сущность математических методов прогнозирования.
19. Сущность прогнозирования по аналогии.
20. Анализ внешней среды и ее влияния на реализацию альтернатив.
21. Алгоритм разработки управленческих решений в вопросах информационной безопасности.

Раздел 2. Модель непрерывного улучшения процессов

11. Сущность организации процесса разработки управленческого решения.
12. процедуры организации согласования, утверждения и выполнения решения.
13. Сущность методики формирования команды по управлению информационной безопасностью.
14. Сущность и виды ответственности.
15. Сущность контроля управленческого решения.

ТЕМЫ РЕФЕРАТОВ

11. Информационное обеспечение решений и информационная безопасность.
12. Информационная поддержка решений директора.
13. Влияние традиций и специфики предприятия на разработку управленческого решения.
14. Роль человеческого фактора в процессе разработки управленческого решения.
15. Этические основы управленческого решения.
16. Демократизация процессов разработки управленческих решений.
17. Организация и эффективность использования экспертных оценок.
18. Интеллектуальная деятельность при разработке управленческих решений.
19. Организация выполнения принятых решений.
20. Формы разработки и реализации УР.
21. Методика построения сценариев при разработке управленческого решения.
22. Разработка и поддержка стратегических решений.
23. Проверка реализуемости разрабатываемых управленческих решений.
24. Оценка возможной ответственности при разработке управленческого решения.
25. «Прогнозирование – планирование» - единая система методических приемов при разработке управленческого решения.

Реферат – краткая запись идей, содержащихся в одном или нескольких источниках, которая требует умения сопоставлять и анализировать различные точки зрения. Реферат – одна из форм интерпретации исходного текста или нескольких источников. Поэтому реферат, в отличие от конспекта, является новым, авторским текстом. Новизна в данном случае подразумевает новое изложение, систематизацию материала, особую авторскую позицию при сопоставлении различных точек зрения.

Реферирование предполагает изложение какого-либо вопроса на основе классификации, обобщения, анализа и синтеза одного или нескольких источников.

Виды рефератов

По полноте изложения	Информативные (рефераты-конспекты)
	Индикативные (рефераты-резюме)
По количеству реферируемых источников	Монографические
	Обзорные

Реферат должен отвечать ряду требований.

Требования по оформлению:

– объем реферата от 10 до 15 страниц формата А4, шрифт Times New Roman, кегль 14 пт, полуторный междустрочный интервал, выравнивание текста – по ширине, нумерация страниц в верхнем колонтитуле по центру, автоматические переносы слов (кроме титульного листа), поля: снизу и сверху – 20 мм, слева – 25 мм, справа – 10 мм;

– на титульном листе указывается: название реферата, Фамилия И.О. обучающегося, номер группы;

– список использованных источников – современная, актуальная литература, не менее трех источников, полное указание выходных данных для книжных и периодических изданий, адреса сайтов с которых заимствован материал, по тексту реферата должны быть ссылки на источники.

Требования по структуре:

– реферат включает титульный лист, оглавление, введение, основной текст, заключение, список литературы, приложения (при необходимости);

– основной текст должен содержать несколько разделов.

Требования по содержанию:

– реферат должен содержать достоверные и актуальные сведения на достаточном научном уровне;

– реферат, кроме текста (формат .doc или .docx), может дополнительно содержать: качественные цветные иллюстрации, фрагменты программного кода и другие материалы, качественно дополняющие основную часть реферата.

КОМПЛЕКТ КЕЙС-ЗАДАЧ

Кейс 1.

В коммерческой организации, которая занимается поставками компьютерной техники для государственных и муниципальных органов. При сумме потенциального контракта (поставки) более 100 тысяч рублей данная компания должна участвовать в тендере, соответственно сталкиваться с конкурентной борьбой во время проведения торгов. Компания не имеет никаких внутренних документов, касающихся информационной безопасности, в том числе политики безопасности. В процессе участия в одной из процедур торгов ответственный менеджер по торгам получает на корпоративную почту письмо с заголовком "Срочно. Документы" с неизвестного адреса. Данное письмо содержит единственный архивный файл без текста самого письма. Менеджер открывает архив, после чего автоматически запускается вирус, который не только блокирует рабочий компьютер с установленным программным обеспечением для торгов и авторизированной электронной подписью организации, но и пытается распространяться по внутренней сети компании.

Сотрудники ИТ-отдела реагируют достаточно оперативно, локализуют распространение вируса, устраняют сам вирус и последствия его действия на всех зараженных компьютерах в течение 3-х часов. Но за это время торги закрываются, и компания упускает крупный контракт (порядка миллиона рублей)

. Кто, по Вашему мнению, виноват в данной ситуации (менеджер, который открывал неизвестное письмо; сотрудники ИТ-отдела, которые не предприняли превентивных мер)? Кого следует наказать?

Правильный ответ В данном случае: виноват первый руководитель организации (например, генеральный директор), который не инициировал создание и внедрение политики безопасности. В политике безопасности могли быть описаны правила работы с электронной почтой, отдельно могли быть представлены правила организации работы во время проведения торгов, а также правила проведения инструктажа сотрудников. Также в политике безопасности расписываются правила передачи ответственности при проведении определенных действий. Если политика внедрена, инструктаж проведен, менеджер расписался о проведении инструктажа, то он не только 10 раз задумается, стоит ли открывать неизвестные письма, но и будет понимать, что наказание будет грозить непосредственно ему, так как на время торгов на него будет полностью

возложена ответственность за их проведение.

Кейс 2.

«Расчет рисков информационной безопасности»

Описание ситуации: Например, информационная система Компании состоит из двух ресурсов: сервера и рабочей станции, которые находятся в одной сетевой группе, т.е. физически связанны между собой.

На сервере хранятся виды информации: бухгалтерский отчет и база клиентов Компании. На рабочей станции расположена база данных наименований товаров Компании с описанием.

К серверу локальный доступ имеет группа пользователей (к первой информации – бухгалтерский отчет): – главный бухгалтер. К серверу удаленный доступ имеют группы пользователей (ко второй информации – база клиентов Компании): – бухгалтер (с рабочей станции); – финансовый директор (через глобальную сеть Интернет).

К рабочей станции локальный доступ имеет группа пользователей (к базе данных наименований товаров Компании с описанием): – бухгалтер.

По правилам работы модели бухгалтер при удаленном доступе к серверу является группой обычных пользователей, а финансовый директор – группой авторизованных пользователей. Причем, бухгалтер имеет удаленный доступ к серверу через коммутатор.

Задание: Рассчитать риски информационной безопасности на основе модели информационных потоков.

Кейс 3.

Описание ситуации

В одной из компаний был зафиксирован следующий инцидент: при увольнении с работы системный администратор украл разрабатываемый в компании программный продукт и передал его конкурентам, которые выпустили программу на рынок под своим товарным знаком. Кроме этого, он внес изменения в информационную систему, в результате которых после его ухода функционирование определенных ее компонентов было нарушено. Привлечь администратора к ответственности в данном случае оказалось невозможно, так как, во-первых, не выполнялась регистрация его действий, во-вторых, администратор мог удалить все доказательства своих неправомерных действий и, в-третьих, не была налажена процедура сбора улик об инциденте.

Задание. 1. Определите возможные причины инцидента и степень ответственности сотрудника. 2. Определите меры, направленные на предотвращение повторных инцидентов. 3. Подготовьте проекты соответствующих документов.

Кейс 4.

Описание ситуации

В одной из компаний сотрудник хранил на мобильном компьютере конфиденциальные сведения компании без применения средств шифрования. После работы он забрал компьютер домой и забыл его в машине, которую оставил под окнами дома, а ночью машину взломали, и компьютер был украден. Злоумышленники получили доступ к конфиденциальной информации компании и могли продать ее конкурентам. Кроме этого, на компьютере хранилась ценная информация, которая не была зарезервирована на другом носителе.

Задание. 1. Определите возможные причины инцидента и степень ответственности сотрудника. 2. Определите меры, направленные на предотвращение повторных инцидентов. 3. Подготовьте проекты соответствующих документов.

Кейс 5.

Описание ситуации.

В Белозерске Вологодской области врач центральной районной больницы выписал список медицинских препаратов на «черновике». за разглашение персональных данных. Чернови-

ком оказался талон амбулаторного больного, где были указаны персональные данные другого пациенты: ФИО, год рождения, номер паспорта, домашний адрес и диагноз.

Задание. 1. Определите возможные причины инцидента и степень ответственности сотрудника. 2. Определите меры, направленные на предотвращение повторных инцидентов. 3. Подготовьте проекты соответствующих документов.

Кейс 5.

Описание ситуации.

В больнице поселка Всеволодо-Вильва Пермского края пациентке вместе с результатами ЭКГ выдали список других пациентов. На черновике, к которому приклеили расшифровку кардиограммы, указаны фамилии, имена, даты рождения, домашние адреса и паспортные данные.

Задание. 1. Определите возможные причины инцидента и степень ответственности сотрудника. 2. Определите меры, направленные на предотвращение повторных инцидентов. 3. Подготовьте проекты соответствующих документов.

20 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «ТЕХНИЧЕСКИЕ, ОРГАНИЗАЦИОННЫЕ И КАДРОВЫЕ АСПЕКТЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ЗАЧЕТУ С ОЦЕНКОЙ

1. Охарактеризуйте особенности АСУ ТП с точки зрения информационной безопасности.
2. Какие методы используются при организации и проведения высокотехнологичных исследований?
3. Охарактеризуйте методы и способы управления информационной безопасностью.
4. Как осуществляется организация управления информационной безопасностью?
5. Охарактеризуйте предприятие с позиции поведенческого и структурного подхода.
6. Охарактеризуйте принципы и методы управления персоналом высокотехнологичного предприятия с учетом этапов инновационной деятельности.
7. Охарактеризуйте методы разработки и реализации мероприятий по совершенствованию организации труда персонала для комплексного решения инновационных проблем.
8. Как осуществляется формирование требований к защите информации в информационно-аналитических системах.
9. Приведите примеры организации процесса управления информационной безопасностью: опыт разных стран.
10. Охарактеризуйте предприятие с позиции структурного подхода.
11. Какое место и роль занимают подразделения НИОКР в структуре управления: линейно-функциональной, дивизиональной, матричной.
12. Охарактеризуйте принципы и методы управления персоналом высокотехнологичного предприятия с учетом этапов инновационной деятельности.
13. Назовите и охарактеризуйте методы разработки и реализации мероприятий по совершенствованию организации труда персонала для комплексного решения инновационных проблем - от идеи до серийного производства.
14. Назовите фундаментальные свойства оцифрованной информации.
15. Назовите причины появления киберпреступности.
16. Назовите причины, по которым совершенная защита информации невозможна
17. Назовите методы и инструменты анализа и контроля информационных рисков
18. Назовите преимущества и недостатки количественной оценки соотношения потерь от угроз безопасности и затрат на создание системы защиты.
19. Перечислите нормативно-правовые документы предприятия, касающиеся вопросов информационной безопасности.
20. Назовите требования действующего российского законодательства - руководящие документы ФСТЭК (Гостехкомиссии), СТР-К, требования ФСБ РФ, ГОСТы и др.
21. Охарактеризуйте кратко рекомендации международных стандартов - ISO 17799, OCTAVE, CoBIT и др.

ТИПОВЫЕ ЗАДАЧИ ДЛЯ ЗАЧЕТА С ОЦЕНКОЙ

Задача 1. Определить среднюю продолжительность процесса «НИР-ОКР-О» по трем научным направлениям на основании исходных данных:

Таблица 1 – Сроки выполнения отдельных стадий по годам

Научное направление	Название темы	НИР		ОКР		Освоение	
		начало	окончание	начало	окончание	начало	окончание
I	А	2002	2004	2003	2004	2005	2007
	Б	2003	2005	2005	2006	2007	2008

II	В Г	2005 2006	2005 2007	2006 2007	2008 2008	2007 2008	2008 2009
III	Д Е	2005 2003	2007 2005	2005 2004	2006 2005	2007 2006	2009 2008

Необходимо рассчитать:

- среднюю продолжительность каждой стадии по научным направлениям;
- среднюю продолжительность перерывов между стадиями процесса;
- среднюю продолжительность проведения работ по стадиям процесса;
- коэффициенты параллельного проведения работ по стадиям процесса;
- среднюю продолжительность всего процесса по каждому научному направлению.

Задача 2. Определить среднюю продолжительность процесса «НИР-ОКР-О» по трем научным направлениям на основании исходных данных:

Таблица 1 – Сроки выполнения отдельных стадий по годам

Научное направление	Название темы	НИР		ОКР		Освоение	
		начало	окончание	начало	окончание	начало	окончание
I	А Б	2003 2004	2004 2006	2005 2005	2005 2007	2005 2007	2007 2008
II	В Г	2003 2006	2005 2006	2007 2008	2008 2009	2007 2009	2008 2010

Необходимо рассчитать:

- среднюю продолжительность каждой стадии по научным направлениям;
- среднюю продолжительность перерывов между стадиями процесса;
- среднюю продолжительность проведения работ по стадиям процесса;
- коэффициенты параллельного проведения работ по стадиям процесса;
- среднюю продолжительность всего процесса по каждому научному направлению.

Задача 3. Определить на основании исходных данных среднюю продолжительность каждой стадии процесса создания и освоения новой продукции и рассчитать предельную нормативную длительность этого процесса, используя следующие дополнительные условия: продолжительность стадии более 3,5 лет считается нерациональной; поправка на развертывание производства равна 0,4 года, поправка на ускорение темпов обновления производства 1 год.

Таблица 1 - Распределение работ по продолжительности и стадиям процесса «НИР-ОКР-О»

№ п/п	Длительность стадий в годах	Количество работ по стадиям			№ п/п	Длительность стадий в годах	Количество работ по стадиям		
		НИР	ОКР	О			НИР	ОКР	О
1	0,5	2	1	3	8	4,0	1	2	2
2	1,0	7	4	8	9	4,5	1	2	2
3	1,5	8	6	9	10	5,0	1	1	2
4	2,0	2	12	10	11	5,5	-	1	1
5	2,5	2	4	9	12	6,0	1	1	-
6	3,0	2	3	8	13	6,5	-	1	1
7	3,5	2	2	7	14	7,0	-	1	-

Задача 4. Вы руководитель трудового коллектива, состоящего из двух отделов, примерно

равных по численности, но имеющих разную социальную структуру. На предприятии в качестве конечных результатов приняты выручка от реализованной продукции, производительность труда и качество продукции. Критерий эффективности - валовая прибыль. В отчетном квартале Ваш коллектив выполнил основные конечные показатели, хотя были проблемы с качеством продукции. Виноват в этом оказался отдел А, который состоит в основном из молодых мужчин. Отдел Б не виноват в снижении качества, но допустил ряд упущений в трудовой дисциплине, о которых известно в коллективе. Отдел Б преимущественно женский, там часто бывают конфликты. Заводская премия Вашему подразделению была снижена за упущения по качеству и рассчитана пропорционально численности сотрудников, как давно принято на предприятии.

Каким образом, и в каких пропорциях Вы распределите премию?

Задача 5 Отдел управления человеческими ресурсами завода «Сигнал» провел анонимный опрос сотрудников с целью выяснения их отношения к процедуре аттестации, проводимой по классической схеме:

а) ежегодное аттестационное собеседование с руководителем;

б) специальные формы оценки и план развития;

в) повышение базового оклада в соответствии с аттестационной оценкой.

Собрать мнение сотрудников завода было достаточно сложно, тем не менее, почти половина опрашиваемых представили свои ответы на вопросы анкеты. Всего было собрано 70 из 154 розданных анкет.

Результаты опроса сотрудников показали, что:

– 65% сотрудников не удовлетворены, аттестацией как методом оценки их работы;

– 50% сотрудников считают, что руководители не могут объективно оценить их работу, поскольку не располагают необходимой для этого информацией;

– 45% сотрудников считают аттестационное собеседование формальным оглашением заранее принятого решения;

– 12% утверждают, что их руководители вообще не проводят собеседования, а просят подписать заполненную заранее форму;

– 68% сотрудников не чувствуют, что результаты, аттестации используются для чего-либо помимо повышения оклада.

Результаты опроса проводивших аттестацию руководителей завода «Сигнал» показали, что:

– 75% руководителей пожаловались на недостаток времени для ее подготовки и проведения;

– 25% руководителей признались, что испытывают сложности в случаях, когда необходимо критиковать аттестуемых и регулярно завышают аттестационные оценки.

1. Оцените результаты опроса.

2. Предложите меры, которые необходимо реализовать отделу управления человеческими ресурсами завода «Сигнал», по совершенствованию системы оценки персонала.

3. Какие информационные системы можно рекомендовать?

ФОНД ТЕСТОВЫХ ЗАДАНИЙ

Укажите букву выбранного Вами ответа. В каждом вопросе только **один правильный ответ.**

Вариант 1

1. Персонал – это...

А) личный (штатный) состав организации, объединенный по профессиональным или другим признакам, выполняющий производственные или управленческие функции;

Б) трудоспособная часть населения страны;

В) часть работников организации (юридически оформленных), выполняющая управленческие операции;

Г) часть работников организации (юридически оформленных), выполняющая только производственные операции;

2. В практическое управление персоналом в любой организации включены:

А) только служба управления персоналом;

Б) все работники и все службы на предприятии;

В) только линейные менеджеры;

Г) все лица и все службы на предприятии, несущие ответственность за работу с персоналом.

3. Планирование человеческих ресурсов - это...

А) процесс определения потребности организации в человеческих ресурсах и разработки методов ее покрытия;

Б) процесс выбора методов планирования;

В) совокупность балансовых, нормативных и математико-статистических методов планирования персонала;

Г) совокупность различных планов.

4. Должностная инструкция:

А) перечень выполняемых задач, описание рабочих требований к исполнению, права, ответственность работника;

Б) перечень функций работника;

В) описание рабочего места и требований к работнику,

Г) только описание рабочего места.

5. Профессиограмма...

А) раскрывает как содержание профессии, так и требования, которые она предъявляет к человеку;

Б) это «портрет» идеального сотрудника;

В) тоже, что и должностная инструкция;

Г) все выше перечисленное.

6. Методы построения системы управления персоналом:

А) системный анализ, метод сравнений, декомпозиции и т. д.;

Б) поисков и решений;

В) «разделяй и властвуй»;

Г) ничего из выше перечисленного.

7. Стадии организационного проектирования системы управления персоналом:

А) проектная подготовка, организационный общий проект, организационный рабочий проект;

Б) миссия, цели, задачи, проект;

В) проектная подготовка, проектирование, внедрение;

Г) все выше перечисленное.

8. Рациональный режим труда:

А) научно обоснованное чередование труда и отдыха;

Б) жесткий распорядок дня;

В) гибкий график работы;

Г) минимальная загруженность работника в рабочее время.

Вариант 2

1. Определите правильную последовательность работы с персоналом в организации:

Вариант А:

1. Собрать информацию о персонале.
2. Определить цели планирования производства.
3. Спланировать потребность в персонале.
4. Спланировать использование персонала.
5. Спланировать расходы на персонал организации.

Вариант Б:

1. Спланировать потребность в персонале.
2. Спланировать использование персонала.
3. Определить цели планирования производства.
4. Собрать информацию о персонале.
5. Спланировать расходы на персонал организации.

Вариант В:

1. Спланировать расходы на персонал организации.
2. Спланировать использование персонала.
3. Определить цели планирования производства.
4. Собрать информацию о персонале.
5. Спланировать потребность в персонале.

Вариант Г:

1. Спланировать использование персонала.
2. Определить цели планирования производства.
3. Собрать информацию о персонале.
4. Спланировать расходы на персонал организации.
5. Спланировать потребность в персонале.

2. К внешнему движению персонала относят...

А) текучесть кадров;

Б) квалификационное;

В) межцеховое;

Г) все выше перечисленное.

3. Набор персонала - это...

А) совокупность методов работы с персоналом;

Б) создание резерва претендентов для занятия вакантных должностей;

В) отбор из некоторого числа претендентов;

Г) определение источников покрытия потребности в персонале.

4. Компетенция персонала:

А) знания, навыки, способность к общению;

Б) уровень общих знаний;

В) способности к работе;

Г) уровень интеллекта

5. Маркетинг персонала включает:

А) выбор путей покрытия потребности в персонале;

Б) уточнение данных, представленных претендентом на вакансию;

В) проведение тестирования;

Г) проведение кадрового интервью.

6. Какие методы обучения на рабочем месте наиболее эффективны в процессе профессионального развития персонала?

А) ротация, использование инструкций, копирование, наставничество, делегирование полномочий;

Б) ротация, ролевые игры, учебные ситуации;

В) копирование, деловые игры, моделирование, ротация;

Г) деловые и ролевые игры.

7. В результате собеседования руководителя кадровой службы и претендента на занятие вакантной должности руководителя отдела

рекламы, фирмы по торговле устройствами малой полиграфии, определены такие характеристики претендента:

1. Возраст —35 лет, мужчина;
2. Высшее образование в области станкостроения;
3. Опыт практической работы в качестве оператора ПЭВМ - 7 лет;

4. Опыт работы на руководящих должностях отсутствует;

5. Высокое умение работать на компьютере (на системном уровне);

6. Уровень коммуникабельности выше среднего;

7. Логическое мышление.

Определить возможные действия руководителя кадровой службы совместно с линейным менеджером в отношении претендента.

А) необходимо взять на работу с испытательным сроком;

Б) необходимо пригласить на работу, выполнив большинство встречных требований претендента;

В) необходимо взять на работу без испытательного срока;

Г) отказать в приеме, но занести данные в базу данных для дальнейшего сотрудничества.

8. Трудовые ресурсы как экономическая категория это...

А) физические и интеллектуальные способности в соответствии с условиями воспроизводства;

Б) отражают отношения по поводу населения в соответствии с условиями воспроизводства рабочей силы;

В) цена труда;

Г) стоимость рабочей силы.

9. Составляющие стратегии управления персоналом:

А) отбор, оценка, стимулирование, развитие персонала;

Б) идеи, мысли, правила, процедуры;

В) миссия, цели, задачи;

Г) генеральная стратегия управления организацией.

10. Расходы на персонал:

А) интегральный показатель, включающий все расходы, связанные с функционированием человеческого фактора;

Б) один из показателей по труду;

В) заработная плата;

Г) государственные дотации.

11. Содержательные теории мотивации основываются на:

А) концепции потребностей работника;

Б) оценке соотношения усилий и получаемого результата;

В) анализе процесса выполнения работы;

Г) представлении о справедливости вознаграждения.

12. Процессуальные теории мотивации основываются на:

А) представлении, что человек по природе своей ленив;

Б) иерархии потребностей;

В) концепции значимости для человека процесса и выполнения работы;

Г) концепции «гигиенических факторов».

13. Процесс воздействия на человека в целях побуждения его к определенным действиям путем пробуждения в нем определенных мотивов называется...

А) мотивированием;

Б) поощрением;

В) манипулированием;

Г) стимулированием.

14. Согласно теории «Х», менеджер должен:

А) принуждать подчиненных к работе;

Б) быть внимательным к подчиненным;

В) понять их и стимулировать их работу;

Г) уважать подчиненных.

15. Согласно теории «У»:

А) работа не противна природе человека;

Б) работа не дает людям удовлетворение;
В) работники пытаются получить от компании все, что можно;
Г) работники не могут влиться в организацию.

Вариант 3

1. Современные концепции управления персоналом базируются ...

А) в основном на принципах и методах административного управления;
Б) только на возрастающей роли личности работника;
В) с одной стороны, на принципах и методах административного управления, а с другой стороны, на концепции всестороннего развития личности;
Г) в большей мере на необходимости директивного управления персоналом.

2. Суть делегирования состоит:

А) передаче ответственности на более низкий уровень управления;
Б) передаче властных полномочий вниз и принятии их менеджером низшего звена;
Б) в установлении приоритетов;
Г) в доверии к своим подчиненным.

3. Ключевые факторы, оказывающие воздействие на людей в процессе производства:

А) заработная плата, отношения с начальством;
Б) имидж организации, должность;
В) взаимоотношения с коллегами и подчиненными.
Г) иерархическая структура, культура, рынок;

4. Источники покрытия потребности в персонале:

А) незаконная коммерческая деятельность;
Б) «свои» люди и зарубежные партнеры;
В) биржи труда, учебные заведения, сотрудники организации;
Г) обязательное государственное распределение молодых специалистов.

5. Методами управления персоналом выступают...

А) организационно-распорядительные, демократические, либеральные;
Б) административно-командные, демократические;
В) организационно-распорядительные, экономические, социально-психологические;
Г) все выше перечисленное.

6. Корпоративная культура основана на:

А) разделяемых большинством членов организации убеждениях и ценностях;
Б) особенностях производства;
В) принятых в обществе формах поведения;
Г) правилах, определяемых только руководством организации.

ТЕМЫ ДОКЛАДОВ

1. Специфика АСУ ТП. Угрозы и примеры.
2. Особенности АСУ ТП с точки зрения информационной безопасности.
3. Формирование требований к защите информации в автоматизированной системе управления.
4. Разработка системы защиты автоматизированной системы управления.
5. Внедрение системы защиты автоматизированной системы управления и ввод ее в действие.
6. Обеспечение защиты информации в ходе эксплуатации автоматизированной системы управления.
7. Обеспечение защиты информации при выводе из эксплуатации автоматизированной системы управления
8. Российская нормативная база. Стандарт NIST SP 800-82
9. Классификация решений для информационной безопасности АСУТП.

10. Системы мониторинга активности и обнаружение угроз.
11. Системы предотвращения угроз (или управления доступом). Выводы и прогнозы.
12. Инструкции, журналы, приказы, типовые формы.
13. Основные термины и определения в защите информации на КВО
14. Порядок работ по обеспечению безопасности информации в АСУ ТП.
15. Западный и российский подходы к защите АСУ ТП
16. Решения по обеспечению информационной безопасности для АСУ ТП
17. Шаблоны ОРД, регламентирующие работу по обеспечению информационной безопасности.
18. Анализ информационной безопасности КВО.
19. Составление и оформление организационно-распорядительных документов

Пользуясь законодательными документами, рекомендуемыми источниками, в том числе периодическими изданиями и интернет-ресурсами, необходимо раскрыть тему доклада. Материал излагается четко, ясно, технически грамотно. Требуется систематизировать, исследуемые данные, привести современные сведения по теме. В выступлении необходимо представить аргументировано свое мнение. Объем работы: 3-5 страниц машинописного текста (размер шрифта 14, межстрочный интервал 1,5).

Доклад обучающийся представляет в форме устного выступления с презентацией основных понятий, выводов и доказательств. Эта форма удобна для приобретения навыков ведения полемики.

Порядок представления доклада:

1. Выступление (доклады-сообщения) по основным вопросам.
2. Ответы на вопросы к выступающему.
3. Обсуждение содержания доклада, его теоретических и методических достоинств и недостатков, дополнения и замечания по нему.
4. Заключительное слово докладчика.
5. Заключение и оценивание преподавателем выступления докладчика и дополнений обучающихся группы.

Требования к выступлению обучающегося-докладчика:

1. Изложение основных положений доклада.
2. Раскрытие сущности проблемы.
3. Умение представить примеры во взаимосвязи и взаимообусловленности, отбирать наиболее существенные из них.
4. Точные формулировки, последовательность аргументации данной проблемы, безусловная доказательная база и содержательное использование понятий и терминов.
5. Методологическое значение для научной, профессиональной и практической деятельности.

Обучающийся может выбрать тему индивидуального задания из предложенных выше тем или предложить собственную тему:

21 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ «МОДЕЛИРОВАНИЕ И УПРАВЛЕНИЕ ЖИЗНЕННЫМ ЦИКЛОМ ИНФОРМАЦИОННЫХ СИСТЕМ»

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ЗАЧЕТУ С ОЦЕНКОЙ

1) Какова роль и место дисциплины в образовательной программе?

2) В чем заключается предмет, метод и содержание курса «Управление жизненным циклом ИС»?

3) В чем суть понятия и каковы виды систем?

4) В чем сущность законов развития систем?

5) Что включает в себя понятие жизненного цикла ИС?

6) Каковы этапы жизненного цикла ИС?

1) В чем сущность системного анализа как инструмента для прогнозирования жизненного цикла ИС?

2) В чем сущность метода анализа иерархии в системе (МАИ)?

3) В чем сущность метода «дерево»?

4) Какие модели жизненного цикла ИС существуют?

5) В чем сущность каскадной модели; каскадной модель с промежуточным контролем; спиральной модели; модель разработки через тестирование (V-модель)?

6) Какие стандарты существуют для описания жизненного цикла ИС?

7) В чем сущность стандартов: ГОСТ 34.601-90; ISO/IEC 12207:2008 (ГОСТ Р ИСО/МЭК 12207-2010); ISO/IEC 15288 (ГОСТ Р ИСО/МЭК 15288-2005)?

8) В чем заключается планирование проекта ИС? В чем сущность этапов: экспресс-обследование; технико-экономическое обоснование; оценка целесообразности проекта (TELOS); выбор программного решения? Какие работы осуществляются на каждом этапе и как они должны быть организованы?

9) В чем заключается анализ и постановка задачи в жизненном цикле ИС? Что включают в себя этапы: информационное обследование предприятия; описание бизнес-процессов; основные нотации / методологии моделирования; программные продукты моделирования деятельности организации; сбор требований; подготовка технического задания? Какие работы выполняются на данных этапах и как они должны быть организованы?

10) В чем сущность проектирования и на какие этапы оно подразделяется? Что включают в себя этапы: техническое проектирование; рабочее проектирование / прототипирование при заказной разработке?

11) В чем заключается фаза разработки ИС? Какие работы осуществляются на этапах: закупка ПО; настройка конфигураций; создание ролей пользователей; миграция данных; разработка контрольного примера; тестовая эксплуатация; доработка по результатам тестирования; прием результатов испытаний? Как должна быть организована работа по поддержанию жизненного цикла ИС на данных этапах?

12) В чем заключается фаза жизненного цикла ИС: развертывание и внедрение? Какие работы выполняются на этапе закупки и настройки требуемой ИТ–инфраструктуры? Как осуществляется ввод начальных остатков; обучение пользователей; развертывание системы на рабочих местах; основные виды тестирования; опытно-промышленная эксплуатация; приемо-сдаточные испытания? Как должны быть организованы данные виды работ?

13) Что происходит на стадии эксплуатации? Как должны быть организованы работы в процессе эксплуатации?

14) Как осуществляется сопровождение эксплуатации? В чем заключается авторский надзор; техническая поддержка; постгарантийное сопровождение? Как должны быть организованы данные виды работ?

15) В чем сущность модернизации? В чем заключаются: стратегии управления legacy-системами; виртуализация как стратегия модернизации решений? Каковы особенности проектов по модернизации? Как должны быть организованы данные виды работ?

16) Что происходит на стадии жизненного цикла – утилизация? Какие технические аспекты влияют на выполнение работ на данной стадии? Какие организационные аспекты влияют на выполнение работ на данной стадии? Какие коммерческие аспекты влияют на выполнение работ на данной стадии? Какие юридические вопросы влияют на выполнение работ на данной стадии?

17) Какие факторы внешней и внутренней среды влияют на продолжительность этапов жизненного цикла ИС?

18) Какое влияние оказывает НТП?

19) Какие существуют направления и методы анализа факторов внешней и внутренней среды, влияющие на жизненный цикл ИС?

20) В чем сущность прогнозирования продолжительности жизненного цикла ИС? Какие различают методы прогнозирования и каковы условия их использования?

21) В чем сущность и каковы этапы процесса прогнозирования?

22) Какие рекомендации можно дать для принятия решений в сложных системах?

23) В чем сущность и содержание неопределенности и риска при принятии решений относительно жизненного цикла ИС?

24) Что такое износ ИС? Какие формы износа различают и как они влияют на жизненный цикл ИС?

25) Как определить стоимость износа?

26) Что такое нематериальные активы? Как они учитываются в деятельности предприятия?

27) Как осуществляются амортизационные отчисления от стоимости нематериальных активов? Какие методы амортизации существуют?

28) Как определяется эффективность использования технических систем в течение их жизни?

29) Как должны быть организовано выполнение работ по поддержанию жизненного цикла систем и средств обеспечения информационной безопасностью?

30) Какие типы организационно-управленческих структур различают и в чем их сущность?

31) Кто такие стейкхолдеры? Какие методы управления стейкхолдерами рекомендуется применять в процессе жизненного цикла ИС?

32) В чем сущность управления человеческими ресурсами и как оно меняется в процессе жизненного цикла ИС?

33) В чем заключается управление финансами в процессе жизненного цикла ИС?

34) В чем сущность управления коммуникациями в процессе жизненного цикла ИС?

35) Как осуществляется управление качеством ИС? Как оно изменяется в процессе жизненного цикла ИС?

36) Что включает в себя управление содержанием ИС? Как оно реализуется организационно?

37) В чем сущность управления рисками в процессе жизненного цикла ИС?

38) Как осуществляется управление программой проектов? В чем сущность сбалансированной системы показателей (BSC)?

39) В чем сущность сетевых моделей? Как создать и рассчитать сетевую модель жизненного цикла проекта ИС?

ТИПОВЫЕ ПРАКТИЧЕСКИЕ ЗАДАНИЯ ДЛЯ ЗАЧЕТА С ОЦЕНКОЙ

Задание 1.

Определить процент и стоимость физического износа компьютера в течение срока его эксплуатации на предприятии, если его годовой износ составляет 11,5%, амортизация начисляется линейным методом. Определить физический износ за весь срок службы компьютера. Изобразить на графике зависимость годности оборудования от срока его эксплуатации.

Номер года службы прибора	Стоимость прибора, руб.	Стоимость физического износа, руб.	Остаточная стоимость, руб.	Коэффициент физического износа, %	Коэффициент годности, %
1	279000				
2					
3					
4					
5					
6					
7					

Задание 2.

1. Выбрать факторы внешней среды, оказывающие влияние на угрозы или возможности для фирмы, внедряющей и использующей ИС.

2. Выделить причины возникновения угроз или возможностей внешней среды и отобразить их в соответствующей колонке таблицы.

3. Предложить решения по использованию возможностей внешней среды либо предотвращению или снижению риска, которые можно предпринять как со стороны фирмы, так и со стороны государства.

4. По результатам выполненного анализа, сформулировать цели фирмы, учитывающие влияние внешней среды.

5. Составить отчет.

Исходные данные представлены в таблице.

Форма документа по оценке рисков внешних факторов

Факторы риска	Причины возникновения риска		Решения по использованию возможностей либо нейтрализации угроз
	составляющие угрозу	дающие возможность	
1. Экономические			
2. Политические			
3. Рыночные			
4. Технологические			
5. Международные			
б. Конкуренция			
7.Социального поведения			

Задание 3.

Определить величину годовых амортизационных отчислений, процент амортизационных отчислений нематериальных активов предприятия.

Первоначальная стоимость нематериальных активов предприятия составляет 250 тыс.у.е. Срок службы - не определен.

Задание 4.

Построить сетевой график проекта ИС для максимальной продолжительности всех его работ, рассчитать наиболее ранние и наиболее поздние сроки наступления событий, найти критический путь.

Пути сетевого графика:

L1: 0-1, 1-2, 2-5, 5-7, 7-8

L2: 0-1, 1-4, 4-7, 7-8
L3: 0-1, 1-4, 4-5, 5-7, 7-8
L4: 0-1, 1-3, 3-6, 6-7, 7-8
Продолжительность работ (в рабочих днях):

0-1	3,0
1-2	3,0
1-3	3,0
1-4	4,0
2-5	4,0
3-6	5,0
4-5	3,5
4-7	6,0
5-7	4,5
6-7	5,5
7-8	1,0

Задание 5.

Составить смету затрат на проведение мероприятий и определить стоимость работ по совершенствованию системы защиты информации.

Исходные данные.

Для повышения безопасности при работе в интернете фирма приобрела новое программное обеспечение, стоимостью 25 тыс. руб.

Настройка программно-технических средств в фирме будет осуществляться в течение 2-х рабочих дней. Этой работой занимаются 2 специалиста, заработная плата каждого из них составляет 170 руб./час.

Техническую поддержку производственного персонала при внедрении средств защиты будет осуществлять 1 специалист в течение недели. Его месячный оклад 25 тыс. руб.

Обслуживание программно-технических средств защиты в течение недели по 2 часа в день будет осуществлять 1 специалист, заработная плата которого составляет 220 руб./час.

Обучение персонала в вопросах пользования имеющихся средств защиты займет 2 дня. Обучением будут заниматься 2 специалиста, заработная плата каждого из них составляет 200 руб./час.

Всего должно быть обучено 40 человек персонала.

ДЕЛОВАЯ ИГРА

Принятие решений по проектированию организационно-управленческой структуры предприятия»

Цель деловой игры. Освоение теоретических основ построения структуры организации.

Задание. Учебная группа делится на три команды. Из каждой группы выбирается эксперт, который входит в состав экспертной комиссии. Каждая команда должна подготовить характеристику предприятия и заполнить таблицу 1:

Таблица 1 - Характеристика предприятия

Показатели	Наименование предприятия		
	1	2	3
1. Организационно-правовая форма предприятия			
2. Направление специализации			
3. Краткое описание технологии производства			
4. Краткое описание основных элементов внешней и внутренней среды предприятия			
5. Численность работников, чел., в том числе аппарата управления			
6. Объем производимой продукции (работ, услуг)			
7. Расходы на производство и реализацию продукции,тыс. руб.			
8. Расходы по организации и управлению предприятием в расчете на одного работника аппарата управления, тыс.руб.			

Командам рекомендуется выполнение деловой игры в следующей последовательности:

1) определение функциональной структуры предприятия. Для этого определяются все задачи, необходимые для достижения конечной цели предприятия. В зависимости от решаемых задач выделяются объекты деятельности с определенной специализацией. В зависимости от технологии производства и специализации определяются этапы деятельности (например, транспортировка). Все работы разделяются на отдельные задачи и определяется последовательность их выполнения. В результате команды получают функциональную диаграмму исследуемого предприятия.

2) определение должностей сотрудников предприятия. Должности на исследуемом предприятии определяются в зависимости от функциональных задач, которые может и должен решать каждый сотрудник, а также от уровня и сложности выполняемых работ. Каждая команда должна свести полный перечень должностей в таблицу 2, привести их сранительную характеристику и указать положительные и отрицательные стороны этих должностей.

Таблица 2 – Характеристика должностей на предприятии

№ п/п	Наименование должности	Характеристика должности	Положительные стороны	Отрицательные стороны
1.				
2.				

3) определение подразделений предприятия. Подразделения создаются на основе однотипной специализации должностей. Команды должны определить схему взаимосвязей между должностями и полученные результаты свести в таблицу 3.

Таблица 3 – Подразделения предприятия

№ п/п	Наименование должностей	Наименование заданий	Наименование подразделений
1.			
2.			

4) определение уровней подразделений на предприятии и построение общей структурной схемы. Команды должны построить вертикаль подчинения с помощью таблицы 4.

Таблица 4 – Функциональная характеристика подразделений

№п/п	Наименование подразделения	Функциональная характеристика	Количество подразделений	С какими подразделениями связано?
1.				
2.				

В зависимости от специализации и выполняемых функций подразделения предприятия относят: либо к линейным, либо к штабным. Состав и количество подразделений, выполняющих одноименные работы, зависит от масштабов производства, территориального размещения предприятия, технологии производства.

5) определение организационно - управленческой структуры. Команды разрабатывают организационную структуру исследуемого предприятия и изображают ее схему.

6) определение степени децентрализации подразделений. Команды должны определить связи между подразделениями, а также рассмотреть вопросы делегирования полномочий в разработанной структуре управления.

7) определение эффективности разработанной организационной структуры. Для этого необходимо использовать нормы управляемости руководителей. Определение эффективности структуры управления в большей степени будет носить качественный характер и зависеть от количества подчиненных у одного руководителя. Данные для определения эффективности представлены в таблице 5.

Таблица 5 – Нормы управляемости руководителей

Уровень производства	Тип организации производства		
	Массовое и крупносерийное	Индивидуальное и мелкосерийное	Серийное
Высший (штабной)	5-6 чел.	3-4 чел.	4-5 чел.
Низший (линейный)	11-15 чел.	7-11 чел.	9-13 чел.

8) определение победителя деловой игры. Представитель каждой команды делает доклад с презентацией. Другие команды задают вопросы, отвечать на которые может любой член команды. Итоговая оценка подводится экспертами. При оценке учитываются следующие факторы: регламент выполнения игры, активность членов команды, построение организационной структуры и ее соответствие требованиям отрасли предприятия.

ФОНД ТЕСТОВЫХ ЗАДАНИЙ

1. Жизненный цикл информационной системы – … процесс, началом которого становится момент принятия решения о необходимости системы, а завершением – ее изъятие из эксплуатации.

(впишите слово)

2. Расположите фазы жизненного цикла по порядку их реализации.

1) Эксплуатация
2) Разработка
3) Утилизация
4) Анализ и постановка задачи
5) Развертывание и внедрение
6) Замысел
7) Поддержка
8) Проектирование

3. По результатам проведения информационного обследования, должны быть подготовлены:

(выберите один или несколько вариантов ответа)

1) Полное описание текущей бизнес-модели предприятия заказчика

2) Краткое описание текущей бизнес-модели предприятия

3) Коммерческое предложение со сформулированными проблемами, а также ориентировочными сроками и бюджетом работ по дальнейшему информационному обследованию и непосредственно внедрению системы.

4) Утвержденный план работ по разработке и внедрению (включая состав группы внедрения с обеих сторон).

5) Утвержденный план работ по дальнейшему информационному обследованию и непосредственно внедрению системы.

4. Решаемый вопрос на фазе анализа и постановки задачи.

(выберите один вариант ответа)

1) «Как должна работать будущая система?»

2) «Что должна делать будущая система?»

3) «Кто будет заниматься разработкой ИС?»

4) «Каков порядок действий при разработке ИС?»

5. Аспекты стадии сопровождения, приводящие к изменениям в системе в процессе эксплуатации.

(выберите несколько вариантов ответа)

1) Обеспечение безусловного выполнения условий готовности модулей системы к сдаче в опытно-промышленную эксплуатацию.

2) Увеличение производительности системы.

3) Устранение замечаний, не затрагивающее изменение ТЗ.

4) Подготовка и издание приказа по предприятию заказчика о передаче модуля системы в эксплуатацию.

5) Обновления (по сути – новые версии системы), выпускаемые при накоплении критического объема доработок.

6. ... предполагает переход на следующий этап после полного окончания работ по предыдущему этапу и характеризуется четким разделением данных и процессов их разработки внедрения созданной ИС и обучении пользователей.

(выберите один вариант ответа)

1) Каскадная модель.

2) Спиральная модель.

3) Икрементная модель.

4) Итеративная модель.

7. ... предполагает увеличенное время, отведенное на разработку, за счет проведения промежуточных корректировок между фазами жизненного цикла.

(выберите один вариант ответа)

1) Каскадная модель.

2) Каскадная модель с промежуточным контролем

3) Итеративная модель.

4) Спиральная модель.

8. Фазы жизненного цикла данной модели непоследовательны, то есть допустимо (но не обязательно!) начало работ над следующим этапом до завершения предыдущего.

(выберите один вариант ответа)

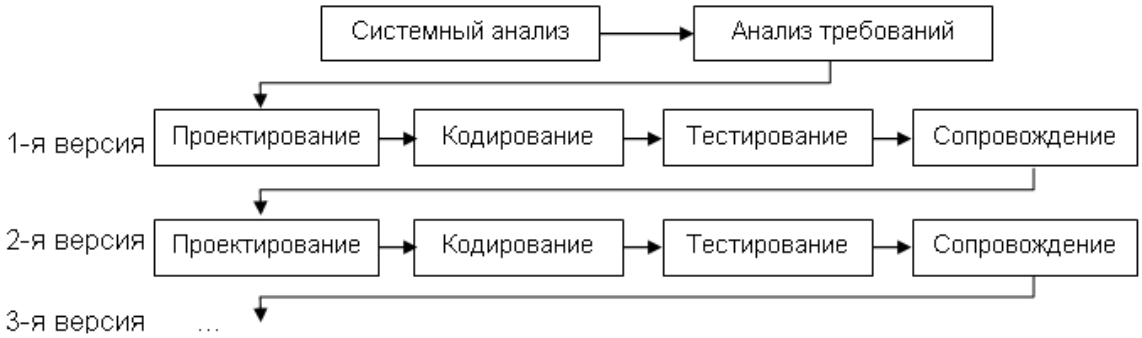
1) Каскадная модель.

2) Спиральная модель.

3) Итеративная модель.

4) Каскадная модель с промежуточным контролем.

9. (выберите один вариант ответа)



1) Каскадная модель.

2) Спиральная модель.

3) Итеративная модель.

4) Каскадная модель с промежуточным контролем.

10. Жизненный цикл информационной системы – ... процесс, началом которого становится момент принятия решения о необходимости системы, а завершением – ее изъятие из эксплуатации.

(впишите слово)

11. Жизненный цикл ИС регламентирует стандарт ISO/IEC 12207. IEC – это...

(выберите один вариант ответа)

1) Международная организация по стандартизации.

2) Международная комиссия по электротехнике.

3) Международная организация по информационным системам.

4) Международная организация по программному обеспечению.

12. Согласно стандарту, структура жизненного цикла ИС состоит из процессов ...

(выберите один вариант ответа)

1) Основных и вспомогательных процессов жизненного цикла и организационных процессов.

2) Разработки и внедрения.

3) Программирования и отладки.

4) Создания и использования ИС.

*13. Согласно ISO 12207, объединение одного или нескольких процессов, аппаратных средств, программного обеспечения, оборудования и людей для удовлетворения определённым потреб*ностям или целям это …

(выберите один вариант ответа)

1) вычислительный центр

2) информационная система

3) полнофункциональный программно-аппаратный комплекс

4) система

14. Проект – это ... предприятие, предназначенное для создания уникальных продуктов, услуг или результатов.

(впишите слово)

15. Установите соответствие:

1) Задача

2) Ресурсы

3) Назначения

4) Веха

А) Исполнители, оборудование и материалы, необходимые для выполнения задачи.

Б) Связь конкретной задачи с ресурсами, выделенными для ее выполнения.

В) Деятельность, осуществляемая в рамках проекта, для достижения определенного результата

Г) Задача, достижение результата которой особенно важно для проекта, используется для обозначения окончания основных этапов проекта.

16. К бизнес-рискам относятся…

(выберите несколько вариантов ответа)

1) Контрактные риски.
2) Сбытовые риски
3) Управленческие риски
4) Инвестиционные риски
5) Эксплуатационные риски

17. Выберите бюджетную форму из ниже перечисленных, которая не существует.

(выберите один вариант ответа)

1) Бюджет доходов и расходов
2) Бюджет движения денежных средств
3) Прогнозный баланс
4) Бюджет затрат

18. Член команды управления проектом, лично отвечающий за все результаты проекта.

(выберите один вариант ответа)

1) Заказчик проекта
2) Куратор проекта
3) Руководитель проекта
4) Инициатор проекта

19. Участники проекта, задействованные в его реализации.

(выберите один вариант ответа)

1) Команда проекта
2) Потребители продукта проекта
3) Команда управления проектом
4) Заказчики проекта

20. Управление риском проекта это…

(выберите один вариант ответа)

1) Системное применение политики, процедур и методов управления к задачам определения ситуации, идентификации, анализа, оценки, обработки, мониторинга риска и обмена информацией, для обеспечения снижения потерь и увеличения рентабельности.

2) Системное применение политики, процедур и методов управления целями проекта, анализа, оценки, обработки, мониторинга информацией, для обеспечения снижения потерь и увеличения рентабельности.

3) Системное применение политики, процедур и методов управления командой проекта и обмена информацией, для обеспечения снижения потерь и увеличения рентабельности.

4) Системное применение политики, процедур и методов управления к задачам определения ситуации, мониторинга риска и обмена информацией, для обеспечения снижения потерь.

ТЕМЫ РЕФЕРАТОВ

1. Жизненный цикл ИС и ПО
2. Модели ЖЦИС
3. Стандарты жизненного цикла ИС
4. Фазы ЖЦИС «Планирование проекта», «Анализ и постановка задачи» и их специфика
5. Фазы ЖЦИС «Проектирование» и «Разработка» и их специфика
6. Фаза ЖЦИС «Развертывание и внедрение» и ее специфика
7. Фазы ЖЦИС «Эксплуатация» и «Сопровождение эксплуатации» их специфика
8. Фазы ЖЦИС «Модернизация» и «Утилизация» и их специфика
9. Управление стейкхолдерами в процессе жизненного цикла информационных систем

10. Управление человеческими ресурсами в процессе жизненного цикла информационных систем
11. Управление финансами в процессе жизненного цикла информационных систем
12. Управление коммуникациями в процессе жизненного цикла информационных систем
13. Управление содержанием проектов
14. Управление программой проектов
15. Сбалансированная система показателей (BSC)
16. Программные средства поддержки жизненного цикла
17. Организация процесса разработки программного обеспечения
18. Управление ресурсами и проектами в жизненном цикле информационных систем
19. Управление рисками в жизненном цикле информационных систем
20. Управление качеством и документирование информационных систем

Реферат должен отвечать ряду требований.

Требования по оформлению:

– объем реферата от 10 до 15 страниц формата А4, шрифт TimesNewRoman, кегль 14 пт, полуторный междустрочный интервал, выравнивание текста – по ширине, нумерация страниц в верхнем колонтитуле по центру, автоматические переносы слов (кроме титульного листа), поля: снизу и сверху – 20 мм, слева – 25 мм, справа – 10 мм;

– на титульном листе указывается: название реферата, Фамилия И.О. обучающегося, номер группы;

– список использованных источников – современная, актуальная литература, не менее трех источников, полное указание выходных данных для книжных и периодических изданий, адреса сайтов с которых заимствован материал, по тексту реферата должны быть ссылки на источники.

Требования по структуре:

– реферат включает титульный лист, оглавление, введение, основной текст, заключение, список литературы, приложения (при необходимости);

– основной текст должен содержать несколько разделов.

Требования по содержанию:

– реферат должен содержать достоверные и актуальные сведения на достаточном научном уровне;

– реферат, кроме текста (формат .doc или .docx), может дополнительно содержать: качественные цветные иллюстрации, фрагменты программного кода и другие материалы, качественно дополняющие основную часть реферата.

КОМПЛЕКТ КОНТРОЛЬНЫХ ЗАДАНИЙ ПО ВАРИАНТАМ

Этап 1 по теме «Жизненный цикл ИС»

1) Собрать предварительную информацию об исследуемом предприятии.
2) Сформулировать видение выполнения проекта и границы проекта.
3) Составить отчет об обследовании.
4) Получить следующие данные:
- Краткая информация о компании (профиль клиента).
- Цели проекта.
- Подразделения и пользователи системы.

5) На основе предварительной информации сформировать и согласовать с заказчиком общее представление о проекте.
6) Оформить результаты в виде отдельного документа – отчета обследовании.

Этап 2 по теме «Разработка документации на ИС»

1) Составить эскизный план разработки ИС.
2) Выбрать модель ЖЦ ИС, которая будет использоваться для разработки.

3) Для этапа «Анализ требований» составить документ «Техническое задание» с подробным описанием функциональных требований к ИС.

4) Для этапа «Проектирование» составить документ «Технический проект» с описанием проектных решений (архитектура системы, логическая структура базы данных, решения по реализации пользовательского интерфейса и т.д.).

5) Для этапа «Тестирование» составить документ «План тестирования» с описанием методики тестирования и контрольных тестов.

6) Для этапа «Внедрение» составить документ «План ввода ИС в эксплуатацию».

7) Уточнить параметры календарного плана разработки ИС, учитывая ограничения и условия разработки.

8) Объединить календарный план разработки и составленные документы в единый отчёт «Разработка ИС».

Этап 3 по теме «Управление проектами ИС»

1) Составить сетевой график разработки проекта.
2) Составить календарный план.
3) Рассчитать стоимость разработки.