МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВПО «Ивановский государственный университет»

Экономический факультет

Утверждаю:

декан экономического факультета

д.э.н., проф.\_\_\_\_\_\_\_\_\_\_\_\_\_\_Еремин В.Н.

«\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2012 г.

**Рабочая программа дисциплины (модуля)**

Инструментальные средства аудита информационных систем

*Направление подготовки*

230700 «Прикладная информатика»

*Программа специализированной подготовки магистров*

Прикладная информатика в аналитической экономике

*Квалификация (степень) выпускника*

**Магистр**

*Форма обучения*

очная

Иваново 2012

Рабочая программа дисциплины составлена на основании ФГОС ВПО, утвержденного Министерством образования и науки РФ по направлению подготовки 230700 «Прикладная информатика» (квалификация (степень) "магистр") (Приказ Министерства образования и науки РФ от 21 декабря 2009 г. N 762) и учебного плана ИВГУ.

Рабочая программа разработана кафедрой ИТЭ и ОП

Доцент, к.э.н. С.В.Данилова

Рассмотрена и одобрена на заседании кафедры ИТЭ и ОП

протокол № 4 от «10» декабря 2012 г.

Зав. кафедрой ИТЭ и ОП,

доцент, к.т.н. С.М. Голяков

1. **Цели освоения дисциплины**

Целью дисциплины является формирование общепрофессиональных компетенций, знаний, умений, путем получения магистрами теоретических знаний в области аудита и управления информационными системами, а также практических навыков, позволяющих оценивать обеспечение функционирования существующих информационных систем. Освоение дисциплины предполагает сочетание фундаментальной подготовки в области информационных технологий с изучением методик и специализированных программных продуктов аудита информационных систем

Для реализации данной цели при изучении дисциплины решаются следующие задачи:

* дать общие сведения о принципах планирования и проведения аудита информационных систем;
* раскрыть цели и задачи проведения аудита информационных систем;
* провести анализ инструментальных средств аудита ИС.

Задачи, решаемые в процессе изучения дисциплины, направлены на масштабное видение задач управления планированием и организацией информационных систем, развитием систем бизнес-приложений и проведением аудита информационных систем в рамках корпоративного управления предприятием.

Дисциплина изучается на лекциях, практических занятиях и в ходе самостоятельной работы магистров.

На лекциях магистры приобретают теоретические знания по основным подходам к управлению информационными системами и аудиту информационных систем, современным методологиям обеспечения функционирования существующих систем, их стратегической оценке с учетом бизнес целей организации.

На практических занятиях апробируют на практике теоретические, методические вопросы управления информационными системами и аудита информационных систем (ИС), применяют методы оценки систем и практик управления ими, используя стандарты аудита ИС, раскрывая их природу, сущность и основные принципы планирования и управления ИС.

В методическом плане в ходе преподавания данного курса активно используются интерактивные формы работы с магистрами на практических занятиях. С этой целью в программу курса включен ряд заданий, носящих явный практический характер и позволяющих наиболее эффективно закреплять теоретическую информацию.

**2. Место дисциплины в структуре ООП магистратуры.**

**М.2. Профессиональный цикл. М.2.В. Вариативная часть**

Дисциплина «Инструментальные средства аудита информационных систем» относится к дисциплинам вариативной части профессионального цикла.

Для освоения дисциплины обучающиеся используют знания, умения, сформированные в ходе изучения дисциплин: базовой части профессионального цикла «Каноническое проектирование экономических ИС» (М.2.Б).

Освоение данной дисциплины является основой для последующего изучения дисциплины «Автоматизированное создание и адаптация ИСУ» (М.2.Б), «Основы консалтинговой деятельности» (М.2.В), прохождения организационно-управленческой практики, подготовки к итоговой государственной аттестации.

**3. Компетенции обучающегося, формируемые в результате освоения дисциплины**

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих общекультурных (ОК) и профессиональных (ПК) компетенций (см. ФГОС ВПО):

* способен совершенствовать и развивать свой интеллектуальный и общекультурный уровень, самостоятельно обучаться новым методам исследования (ОК-1);
* способен использовать и развивать методы научных исследований и инструментария в области проектирования и управления информационными системами в прикладных областях (ПК-5);
* способен формализовывать задачи прикладной области, при решении которых возникает необходимость использования количественных и качественных оценок (ПК-6);
* способен исследовать применение различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций (ПК-9);
* способен проводить анализ экономической эффективности ИС, оценивать проектные затраты и риски (ПК-10);
* способен выбирать методологию и технологию проектирования ИС с учетом проектных рисков (ПК-11);
* способен проводить маркетинговый анализ ИКТ и вычислительного оборудования для рационального выбора инструментария автоматизации и информатизации прикладных задач (ПК-14);
* способен применять современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС (ПК-15);
* способен проектировать архитектуру и сервисы информационных систем предприятий и организаций в прикладной области (ПК-16);
* способен проектировать информационные процессы и системы с использованием инновационных инструментальных средств, адаптировать современные ИКТ к задачам прикладных ИС (ПК-17);
* способен формировать стратегию информатизации прикладных процессов и создания прикладных ИС в соответствии со стратегией развития предприятий (ПК-19);
* способен организовывать работы по моделированию прикладных ИС и реинжинирингу прикладных и информационных процессов предприятия и организации (ПК-20);
* способен управлять проектами по информатизации прикладных задач и созданию ИС предприятий и организаций (ПК-22);
* способен в условиях функционирования ИС брать на себя ответственность за выполнение производственных задач ИТ-служб, эффективно использовать современные приемы и методы работы с ИТ-персоналом (ПК-24);
* способен использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС (ПК-25);
* способен использовать международные информационные ресурсы и стандарты в информатизации предприятий и организаций (ПК-26);
* способен использовать информационные сервисы для автоматизации прикладных и информационных процессов (ПК-27);
* способен интегрировать компоненты и сервисы информационных систем (ПК-28).

В результате изучения дисциплины магистры должны:

ЗНАТЬ:

* теоретические основы построения и функционирования информационных систем аудита;
* перспективные направления применения новых информационных технологий в аудите.

УМЕТЬ:

* формулировать цели и задачи проведения аудита информационных систем,
* пользоваться современными прикладными программами аудита информационных систем,
* иметь представление о перспективах развития информационных экономических систем и работы фирмы после проведения аудита информационных систем.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Индекс компетенции | Содержание компетенции  (или ее части) | В результате изучения учебной дисциплины обучающиеся должны: | | |
| Знать | Уметь | Владеть |
| 1 | ОК-1 | способен совершенствовать и развивать свой интеллектуальный и общекультурный уровень, самостоятельно обучаться новым методам исследования | * стратегии информационных систем; * организационную структуру информационных систем; * политику ИС, стандарты ИС и процедуры ИС; * управление проектами, управления изменениями; * сетевую инфраструктуру ИС; * информационную безопасность ИС; * управление рисками и управление процессами; * администрирование ИС. | * проводить аудит информационных систем; * управлять планированием и организацией ИС; * оценивать стратегии, политики и стандарты ИС; * оценивать эффективность администрирования ИС; * оценивать сетевую инфраструктуру безопасности ИС; * оценивать эффективность информационных систем; * оценивать управление рисками и управление процессами; * проводить мониторинг ИС; * оценивать риски ИС. | * требованиями к управлению и аудиту ИС; * инструментальными средствами, необходимыми для проведения аудита ИС; * анализом показателей эффективности аудита информационных систем и управления ИС; * организацией работ по проведению аудита ИС и управлению ИС. |
| 3 | ПК-5 | способен использовать и развивать методы научных исследований и инструментария в области проектирования и управления информационными системами в прикладных областях |
| 4 | ПК-6 | способен формализовывать задачи прикладной области, при решении которых возникает необходимость использования количественных и качественных оценок |
| 5 | ПК-9 | способен исследовать применение различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций |
| 6 | ПК-10 | способен проводить анализ экономической эффективности ИС, оценивать проектные затраты и риски |
| 7 | ПК-11 | способен выбирать методологию и технологию проектирования ИС с учетом проектных рисков |
|  | ПК-14 | способен проводить маркетинговый анализ ИКТ и вычислительного оборудования для рационального выбора инструментария автоматизации и информатизации прикладных задач; |
|  | ПК-15 | способен применять современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС; |
|  | ПК-16 | способен проектировать архитектуру и сервисы информационных систем предприятий и организаций в прикладной области ; |
|  | ПК-17 | способен проектировать информационные процессы и системы с использованием инновационных инструментальных средств, адаптировать современные ИКТ к задачам прикладных ИС; |
|  | ПК-19 | способен формировать стратегию информатизации прикладных процессов и создания прикладных ИС в соответствии со стратегией развития предприятий; |
|  | ПК-20 | способен организовывать работы по моделированию прикладных ИС и реинжинирингу прикладных и информационных процессов предприятия и организации; |
|  | ПК-22 | способен управлять проектами по информатизации прикладных задач и созданию ИС предприятий и организаций; |
|  | ПК-24 | способен в условиях функционирования ИС брать на себя ответственность за выполнение производственных задач ИТ-служб, эффективно использовать современные приемы и методы работы с ИТ-персоналом; |
|  | ПК-25 | способен использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС; |
|  | ПК-26 | способен использовать международные информационные ресурсы и стандарты в информатизации предприятий и организаций; |
|  | ПК-27 | способен использовать информационные сервисы для автоматизации прикладных и информационных процессов; |
|  | ПК-28 | способен интегрировать компоненты и сервисы информационных систем. |

***Примечание:*** *В данном пункте рабочей программы учебной дисциплины (модуля) раскрываются ожидаемые результаты освоения учебной дисциплины во взаимосвязи с компетентностной моделью магистра.*

**4.Структура и содержание дисциплины «Инструментальные средства**

**аудита информационных систем»**

**4.1. Структура дисциплины**

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

Таблица

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Индент.  № | Раздел дисциплины | Семестр | Неделя  семестра | Виды учебной работы, включая самостоятельную работу студентов  и трудоемкость (в часах) | | | | Формы  текущ. контр.(по неделям семестра)\*  Форма промежут. аттест. (по семестрам) |
| лекции | семинар,  практич. | лаборат. | самост.  работа |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 1 | Тема 1. Аудит ИС | 2 | 1-2 | 2 | 2 |  | 10 | О |
| 2 | Тема 2. Виды аудита ИС | 2 | 3-5 | 2 | 2 |  | 12 | О |
| 3 | Тема 3. Методика проведения аудита ИС | 2 | 6-8 | 4 | 4 |  | 16 | О, П |
| 4 | Тема 4. Характеристика стандартов аудита ИС | 2 | 9-11 | 2 | 2 |  | 14 | О, П |
| 5 | Тема 5. Оценка бизнес-процессов и риск-менеджмент | 2 | 11-13 | 2 | 2 |  | 14 | О, П |
| 6 | Тема 6. Внутренний контроль | 2 | 13-15 | 2 | 2 |  | 14 | О, П |
| **ИТОГО ЗА 2 СЕМЕСТР:** | |  |  | 14 | 14 |  | 80 | **экзамен** |

\*О – опрос, П – презентация.

**4.2. Содержание дисциплины по разделам**

***Тема 1. Аудит ИС***. История возникновения аудита ИС. Аудит информационных систем, ИТ-аудит: понятие, цели, задачи, стандарты, этапы Особенности финансового аудита и аудита информационных систем: задачи, цели, стандарты, наличие законодательной базы.Состояние рынка ИТ-аудита в России: компании, виды услуг.ИТ-инфраструктура: понятие, состав, безопасность, конфигурация, управление

***Тема 2. Виды аудита ИС***. Основные виды ИТ-аудита: цели, задачи, краткая характеристика. ИТ-аудит при подготовке компании к сертификации по международным стандартам: цель, схема организации, участники, объекты исследования, содержание итогового отчета, структура затрат

ИТ-аудит перед реструктуризацией ИТ-подразделений: цель, схема организации, участники, объекты исследования, содержание итогового отчета, структура затрат

ИТ-аудит перед внедрением информационной системы: цель, схема организации, участники, объекты исследования, содержание итогового отчета, структура затрат

ИТ-аудит перед внедрением систем управления конфигурацией ИТ-инфраструктуры: цель, схема организации, участники, объекты исследования, содержание итогового отчета, структура затрат

***Тема 3. . Методика проведения аудита ИС.*** Методика проведения ИТ-аудита: планирование аудита, этапы, проблемы при проведении аудита и методы их решения, выбор источника финансирования

***Тема 4. Характеристика стандартов аудита ИС.***

Проведение ИТ-аудита в соответствии со стандартом COBIT: основные понятия, структура стандарта, цели, задачи, показатели, этапы аудита

Библиотека ITIL, ITSM.

***Тема 5. Оценка бизнес-процессов и риск-менеджмент.*** Корпоративное управление. Управление ИТ. Управление жизненным циклом ИС. Предоставление сервиса ИТ. Оценка эффективности информационных систем в поддержке бизнес-процессов. Оценка построения и внедрения контроля рисков. Оценка управления рисками и управления процессами. Ресурсы.

***Тема 6. Внутренний контроль.*** Мониторинг. Защита внутренних активов. Внутренний аудит. Информация и коммуникация. Контрольные процедуры. Оценка рисков. Среда контроля.

**5. Образовательные технологии**

При проведении курса широко используются активные и интерактивные формы проведениязанятий, в том числе:

* компьютерная симуляция моделей систем,
* разбор конкретных ситуаций,
* коллективная работа,
* проектная форма выполнения заданий,
* дискуссии,
* учебные мини-конференции,
* элементы дистанционной поддержки обучения,

Удельный вес занятий, проводимых в интерактивной форме, составляет до 80 процентов. Долялекционных занятий от общего числа аудиторных занятий составляет до 40%.

В качестве образовательных технологий используются предметно-ориентированные и личностно-ориентированные:

* для каждого раздела дисциплины определены целевые установки, критерии их достижения;
* сформулированы контрольные вопросы, подготовлены тесты обучающего и контролирующего типов;
* сделан акцент на развитие инициативы и самостоятельности студентов при изучении информационных технологий корпоративного типа;
* написание реферата на теоретические темы, связанные с аудитом ИС;
* студенческие научно-исследовательские работы.

Для организации самостоятельной работы студентов на сервере университета размещены электронные материалы (учебники, статьи, слайды и т.п.).

**6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов**

В течение семестра студент обязан самостоятельно выполнять практическую работу, отчитываться на практических занятиях поэтапно о выполняемой работе.

Для обеспечения текущего контроля прохождения дисциплины применяется балльно-рейтинговая система, которая основана на использовании совокупности контрольных точек, оптимально расположенных на всем временном интервале изучения дисциплины.

Дисциплина разделена на ряд логически завершенных блоков (модулей), по которым проводится промежуточный контроль.

По окончании второго семестра проводится экзамен. Оценивание магистров на экзамене осуществляется в соответствие с требованиями и критериями, установленными в вузе. Учитываются как результаты текущего контроля, так и знания, навыки и умения, непосредственно показанные магистрами в ходе экзамена.

**7. Формы текущего контроля и активных методов обучения**

7.1. Проведение зачета. *Примерный перечень вопросов к зачету.*

Не предусмотрен.

7.2. Проведение экзамена. *Примерный перечень экзаменационных вопросов.*

1. Аудит информационных систем, ИТ-аудит: понятие, цели, задачи,
2. Аудит информационных систем: стандарты, этапы
3. Основные виды ИТ-аудита: цели, задачи, краткая характеристика
4. ИТ-аудит при подготовке компании к сертификации по международным стандартам: цель, схема организации, участники, объекты исследования, содержание итогового отчета, структура затрат
5. ИТ-аудит перед реструктуризацией ИТ-подразделений: цель, схема организации, участники, объекты исследования, содержание итогового отчета, структура затрат
6. ИТ-аудит перед внедрением информационной системы: цель, схема организации, участники, объекты исследования, содержание итогового отчета, структура затрат
7. ИТ-аудит перед внедрением систем управления конфигурацией ИТ-инфраструктуры: цель, схема организации, участники, объекты исследования, содержание итогового отчета, структура затрат
8. Методика проведения ИТ-аудита: планирование аудита, этапы, проблемы при проведении аудита и методы их решения, выбор источника финансирования
9. Проведение ИТ-аудита в соответствии со стандартом COBIT: основные понятия, структура стандарта, цели, задачи, показатели, этапы аудита
10. Особенности финансового аудита и аудита информационных систем: задачи, цели, стандарты, наличие законодательной базы
11. Состояние рынка ИТ-аудита в России: компании, виды услуг.
12. Общая характеристика стандартов ИТ-аудита: стандарты СКС, стандарты ИБ, Cobit, ITIL
13. Библиотека ITIL: структура, основные понятия, процессы, история создания
14. ИТ-инфраструктура: понятие, состав, безопасность, конфигурация, управление
15. Структурированные кабельные системы: понятие, преимущества использования, стандартизация, структура, конфигурация
16. История развития и возникновения аудита информационных систем
17. Ассоциация аудита и управления информационными системами (ISACA).
18. Характеристика сертификатов по ИТ-аудиту (ISACA): CISA, CISM, CGEIT
19. Кодекс профессиональной этики аудитора ISACA
20. Аудит информационной безопасности: понятие, цели, задачи, методы проведения и этапы
21. Аудит информационной безопасности: стандарты, сертификаты.
22. Характеристика систем управления конфигурацией ИТ-инфраструктуры: SystemsManagementServer 2003, HP OpenView, IT ServiceBridge, IBM TivoliBusinessSystemsManager
23. Организация аудита информационных систем с помощью ITIL.

7.3. Курсовая работа.

Не предусмотрена.

7.4. Вопросы, выносимые на самостоятельную работу:

1. Аудит информационной безопасности: цели и задачи.
2. Методика проведения аудита информационной безопасности.
3. Организация управления аппаратными ресурсами в организации.
4. Организация управления программными ресурсами в организации.
5. Аудит информационных систем как часть ИТ- стратегии фирмы.
6. Организация управления ресурсами данных на фирме.
7. Организация телекоммуникаций и сетей в организации.
8. Интернет в инфраструктуре новых информационных технологий.
9. Международная ассоциация аудита и контроля информационных систем ISACA.
10. Компании – системные интеграторы.
11. Оформление результатов аудита информационной системы.
12. Методики оценки текущего состояния ИС.

7.5.Тестовые вопросы

1. Аудитор ИС, выполняя проверку контроля приложений, обнаруживает уязвимость в системе программного обеспечения, которая могла реально повлиять на приложения. Аудитор ИС должен:

A*.* неучитывать эту уязвимость контроля как обзор системы программного обеспечения, что является вне поля этой проверки.

B. сопровождать детализированную проверку системы программного обеспечения и составлять отчет о контроле за уязвимостями.

C. включать в отчет заголовка, что аудит был ограничен проверкой контроля приложений.

D. провести аудит контролей систем программного обеспечения как необходимый и рекомендуемый детализированной проверкой системы программного обеспечения.

2. Причина контроля в инфраструктуре ИС:

A. остается неизменной от руководства инфраструктурой, но инструменты контроля могут отличаться.

B. меняется от руководства инфраструктурой, поэтому инструменты контроля могут отличаться.

C. меняется от руководства инфраструктурой, но инструменты контроля могут остаться теми же.

D. остается неизменной от руководства инфраструктурой и выполнения инструментами контроля, который также остается тот же.

3. Который из нижеследующих типов рисков подразумевает компенсацию проверкой в рассматриваемой области?

A. Риск контролей

B. Риск обнаружения

C. Риск наследования

D. Риск примера

4. Аудитор ИС сопровождает нетривиальные тесты новым расчетным модулем. У аудитора весьма загруженный график работы и ограничено время на экспертизу. Который из видов аудита мог бы быть использован в этой ситуации?

A. Тестирование данных

B. Параллельная симуляция

C. Интегрированное средство тестирования

D. Воплощенный модуль аудита

5. Первоначальная цель самооценки контроля или программа контроля самоуверенности это:

A. заменить некоторые внутренние ответственности аудитора.

B. удалить ответственность контролей по линии менеджеров.

C. превзойти мониторинг контроля ответственности по функциональности.

D. улучшить мониторинг общего контроля организации.

6. Который из следующих лучших обзоров описывает раннюю стадию аудита ИС?

A. Делая обзор ключевых организационных средств.

B. Оценивая инфраструктуру ИС.

C. Понимая бизнес-процессы и инфраструктуру применительно к аудиту.

D. Заслушивая предыдущий из докладываемых отчетов аудита ИС.

7. Самая лучшая из инфраструктур в использовании средств интегрированного контроля – это необходимость:

A. изолировать контроль данных от производственных данных.

B. заметить персонального пользователя таким образом, чтобы делать подтверждения на вывод информации.

C. сегрегировать особые записи файлов мастера.

D. собрать транзакцию и записи файлов в отдельной папке.

8. Перед докладом результатов старшему менеджменту по аудиту аудитору ИС следует:

A. подтвердить находки аудита.

B. подготовить исполнительное резюме и послать его в менеджмент по аудиту.

C. определить рекомендации и представить находки в комитет по аудиту.

D. получить аудиторское заключение.

9. В то время как, развивая риск ориентированную программу аудита, который из следующих подойдет больше всего аудитору ИС?

A. Бизнес-процессы.

B. Критические ИТ приложения.

C. Операционные контроли.

D. Бизнес-стратегии.

10. В первую очередь использование общего аудита программного обеспечения – это:

A. аудиторский контроль программного обеспечения.

B. проверка неавторизованного доступа к данным.

C. извлечение необходимых данных для аудита.

D. сокращение необходимости в транзакционном подтверждении.

11. Которая из следующих задач может быть выполнена одним и тем же человеком в хорошо контролируемом информационно-процессорном компьютерном центре?

A. Администрирование безопасности и управление изменениями.

B. Компьютерные вычисления и развитие систем.

C. Развитие систем и управление изменениями.

D. Развитие систем и содержание систем.

12. Который из самых критических контролей находится над администрированием баз данных?

A. Подтверждение функционирования доступа к Базам Данных.

B. Подразделение обязанностей.

C. Проверка доступа к логам и их деятельности.

D. Проверка использования инструментов баз данных.

13. Который из следующих ответов мог бы быть включен в стратегический план ИС?

A. Спецификации по запланированной покупке аппаратного обеспечения.

B. Анализ будущих целей бизнеса.

C. Целевые данные для развития проектов.

D. Ежегодное бюджетирование целей для департамента ИС.

14. Самая большая ответственность офицера безопасности данных в организации – это:

A. давать рекомендации и проводить мониторинг политики информационной безопасности.

B. продвижение безопасности в совокупности с организацией.

C. процедуры установления политики информационной безопасности.

D. администрирование физического и логического контролей доступа.

15. Который из следующих пунктов лучше описывает процесс стратегического планирования ИТ департамента?

A. ИТ департамент будет иметь либо коротко-масштабные либо широко-масштабные планы зависящие от организационных более масштабных планов и целей.

B. Стратегический план ИТ департамента должен быть временно и проектно ориентированным и помочь определить приоритеты, отвечающие нуждам бизнеса.

C. Планирование долгосрочного диапазона для ИТ департамента должно распознать организационные цели, технологические преимущества и регулярные требования.

D. Планирование короткого диапазона для ИТ департамента не нуждается в интеграции в коротко-масштабные планыорганизации с тех пор, как технологические преимущества будут скорее лидерами в планах ИТ департамента, чем в организационных.

16. Когда полное подразделение обязанностей не может быть достигнуто в системе он-лайн, которой из следующих процедур следовало бы отделиться от других?

A. Проектирование

B. Авторизация

C. Записывание

D. Коррекция

17. Первичная выгода от нормализации баз данных - это:

A. минимизация сокращения информации в таблицах, требуемой удовлетворить нужды пользователей.

B. способность удовлетворить больше запросов.

C. максимизация целостности баз данных обеспечивая информацией более, чем одну таблицу.

D. минимизация времени ответа через быструю обработку информации.

18**.** Которая из сетевых топологий дает большое сокращение в случае провала одного узла?

A. сетчатая

B. звезда

C. кольцо

D. шина

19**.** Исполнитель договора против соглашений уровня сервиса должен быть оценен:

A. покупателем.

B. участником договора.

C. третьей стороной.

D. исполнительным менеджментом.

20**.** Который из следующих пунктов обеспечивает лучший метод определения уровня исполнения договора?

A. удовлетворение пользователя

B. достижение цели

C. квалификация

D. планирование роста и мощности

21**.** Когда аудитор ИС должен проверить наличие безопасности базы данных клиент-сервера:

A. системные утилиты.

B. генераторы программных приложений.

C. документация систем безопасности.

D. доступ к хранимым процедурам.

22**.** Который из следующих мог бы позволить компании расширить ее корпоративную сеть через Интернет к бизнес-партнерам?

A. виртуальная частная сеть

B. клиент-сервер

C. телефонная линия

D. сетевой сервис-провайдер

23. Аудитор ИС, проверяя аппаратное обеспечение процедурой мониторинга должен оценивать:

A. отчеты наличия систем.

B. отчеты прибыли и убытков.

C. отчеты о времени ответов.

D. отчеты утилизации баз данных.

24. Которая из следующих передач информации обеспечивает устойчивость к проникновению осветления?

A. Витая пара

B. Оптический кабель

C. Коаксиальный кабель

D. Радио системы

25. Который из следующих заголовков относится к пакетной передаче данных по сети?

A. Пакеты с сообщением передаются по одному и тому же маршруту.

B. Пароли не могут быть переданы с пакетом.

C. Длина пакетов переменна и каждый пакет содержит одно и то же количество информации

D. Стоимость затрат по передаче основана на пакетах, но дистанция или маршрут изменяется.

26. Аудитор ИС когда проверяет сеть, используя интернет коммуникации, будет в первую очередь тестировать:

A. частоту замены пароля.

B. архитектуру клиент-серверного приложения.

C. архитектуру сети.

D. межсетевой экран защиты и прокси-серверы.

8. Методы преподавания (традиционные и (или) инновационные).

Традиционные и инновационные.

*Перечень используемых инновационных методов и разработок.*

Электронная рабочая программа, рейтинговая система учета академической активности магистров при изучении дисциплины, индивидуальное взаимодействие со студентами по электронной почте для предварительного ознакомления с их разработками при подготовке к аудиторным занятиям, использование на лекциях и практических занятиях мультимедийного оборудования для демонстрации электронных документов, презентаций, работы программ, авторские презентации к лекциям.

*Методические рекомендации преподавателю дисциплины*

Основными видами обучения студентов являются лекции, практические занятия в дисплейном классе и самостоятельная работа магистров.

При чтении лекций особое внимание следует уделить выработке у студентов понимания того, что в современном информационном обществе все сколь-нибудь значимые решения должны приниматься на основе многовариантного выбора, причем, по возможности, с использованием широкого спектра формализованных методов. Компьютерные технологии создают для этого наилучшие возможности. Необходимо широко использовать мультимедийную технику, демонстрировать не только статичные иллюстрационные материалы, но и вести непосредственно компьютерное моделирование, обсуждая с аудиторией его ход и результаты.

Самостоятельная работа ориентирована на домашнюю или классную работу как с компьютером, так и без него. Магистры должны систематически работать с литературой и конспектом лекций, с материалами Интернет. Оценка самостоятельной работы должна входить в оценку контрольных точек практикума с учётом контроля остаточных знаний по тестовым вопросам.

*Методические указания для магистров*

Основными методами обучения являются лекции, практические занятия в дисплейном классе и самостоятельная работа. При этом самостоятельная работа является ведущей.

При прослушивании и проработке лекций особое внимание следует уделить терминологии, используемой в дисциплине, и основным понятиям. Записывать следует только основные положения, формулируемые преподавателем и ссылки на информационные источники, которые вы проработаете самостоятельно. Необходимо активно участвовать в обсуждении предлагаемых преподавателем тем, высказывать собственные соображения.

На практических занятиях необходимо осваивать соответствующие методы в бескомпьютерном, «ручном» варианте, приучаясь при этом грамотно оформлять промежуточные расчеты.

При подготовке к практикуму необходимо по заданию сделать заготовки к будущему занятию и согласовать их в начале занятия с преподавателем, чтобы не терять время на переделки и доработки программы. Если в размещенной в Интернете технологической карте указано, что вы должны до занятия отправить преподавателю информацию по электронной почте, нужно сделать это не в последний момент, а заблаговременно, чтобы преподаватель успел с нею ознакомиться.

Следует учесть, что без самостоятельной работы по подготовке выполнить график практикума практически невозможно, так как работы достаточно трудоемки. Кроме того, практические работы включают элемент творчества и исследований, а не просто демонстрируют возможности какой-либо системы.

Документирование и формирование итоговой отчётности следует начинать заблаговременно и вести в соответствии со стандартами оформления учебных документов и научно-исследовательских отчётов. Без предоставления отчётов магистры не могут быть аттестованы по дисциплине в целом.

Важной частью промежуточной аттестации является контроль остаточных знаний, соответствующие вопросы следует попросить у преподавателя заранее и самостоятельно к ним подготовиться.

**9. Учебно-методическое и информационное обеспечение дисциплины**

а) Основная литература:

1. Ананьева Т.Н. Информационный консалтинг: учебное пособие. – М.: ЗАО «Издательство «Экономика», 2006
2. Артюшенко В.М., Аббасова Т.С. Структурированные кабельные системы: Учебное пособие / Под ред. В.М. Артюшенко, ГОУ ВПО «МГУС». – М.: 2005.
3. Мишенин А.И. Теория экономических информационных систем: Учебник. - 4-е изд., доп. и перераб. - М.: Финансы и статистика, 2005.
4. **Лодон Дж., Лодон К. Управление информационными системами – СПб: Питер, 2005**
5. **Якутский А. Энциклопедия полезных программ – М.: Бестселлер, 2005**
6. **Ткалич А.И. Консалтинговый сервис: учебное пособие.- М.: Альфа-М: ИНФРА-М, 2007**

**б) Дополнительная литература:**

1. Газета «Компьютер-Информ» (<http://www.ci.ru/> )
2. Журнал "CIO/Сhief Information Officer" (<http://www.cio-world.ru/>)
3. Журналы издательства «Открытые системы» (<http://www.osp.ru/> )
4. СЕТЕВОЙ online – журнал для ИТ- профессионалов (<http://www.setevoi.ru/>).
5. Публикации электронной библиотеки "Технологии информационного общества в России» (<http://rusg2b.ru/library/useful/> , <http://library.infosoc.ru> )
6. **Электронная библиотека образовательных и просветительских изданий (**<http://www.iqlib.ru/> **)**
7. Полезные материалы на тему аудита и управления информационными системами. **ООО «Инфотехника» (**<http://www.isaudit.ru/> **)**
8. Библиотека исследований Лиги независимых экспертов  
   в области информационных технологий (<http://www.linex.ru/alib.html> )
9. Библиотека по информационным технологиям (<http://www.itexpert.ru/rus/biblio/cobit> )
10. **Стандарт COBIT (**<http://www.isaca.org>, <http://www.itgi.org>)
11. "IT Audit School" (<http://www.microinform.ru/mis/news_itae.htm> )
12. Digital Security Аудит (http://www.dsec.ru/consult/audit/ )
13. Softline – Аудит (<http://soft.softline.ru/groups.php?id=311>)
14. Астахов А. «Введение в COBIT» //Директор информационной службы, № 7–8/2003.
15. Астахов A. M. Аудит безопасности информационных систем. ISACA.RU, 2002
16. Аудит информационной безопасности. Компания «Микротест» (<http://www.microtest.ru/services/information_security_audit/> )
17. Аудит информационной безопасности. Компания «ДиалогНаука» (<http://www.dials.ru/main.phtml?/services/audit> )
18. Аудит и консалтинг информационных систем (<http://www.icand.ru/index.php?option=com_content&task=view&id=54> )
19. Аудит информационной системы компании на соответствие стандарту PaymentCardIndustryDataSecurityStandard (<http://www.infosec.ru/themes/default/content.asp?folder=2142>).
20. Аудит ИТ-инфраструктуры. Компания «Микротест» (<http://www.microtest.ru/services/it-department_audit/> )
21. Аудит ИТ-инфраструктуры (<http://www.rbcsoft.ru/ru/services/consulting/audit/> )
22. Аудит информационной системы. Компания «Ай-Теко» (<http://www.i-teco.ru/audit4.html> )
23. Аудит информационной системы. Компания "Тех-Системс": (<http://tech-systems.ru/> ).
24. Аудит информационной системы. Схема проведения аудита. Компания S4b Group (<http://www.s4b-group.ru/audit.htm> )
25. Аудит автоматизированной информационной системы Аудиторская фирма «И.С.К.» (<http://www.isk.yaroslavl.ru/services/it/audit.html>)
26. Аудит информационной системы. Компания [TechExpert](http://it.techexpert.ua/Pages/default1.aspx) (<http://it.techexpert.ua/consult/audit/Pages/Default.aspx> )
27. Аудит информационных систем (<http://www.arti.ru/solution/audit_IS.php> ).
28. Аудит информационных систем. Компания Арсис  
    (<http://www.arsis.ru/index.php?option=com_content&task=view&id=47&Itemid=55>)
29. Аудит ИС (<http://www.amphora-group.ru/solutions/itconsulting/itperfection/itgovernance_moreinfo/itaudit.html> )
30. Аудит ИС. Компания «Информационно-техническая лаборатория» (<http://www.itl.nnov.ru/departments/itcons/audit/> )
31. Аудит ИС. Гос. сектор. РБС-ИТ. (<http://www.rbsys.ru/it_consult/?state_sector/audit_datasistem/> )
32. БулкинД. ITIL // Журнал "CIO/Сhief Information Officer" №2,2006 (<http://www.cio-world.ru/print/weekly/251017/> )
33. ВнедрениеITIL. Компания [TechExpert](http://it.techexpert.ua/Pages/default1.aspx). (<http://it.techexpert.ua/consult/itil/Pages/Default.aspx> )
34. **Внутренний аудит информационных систем. (**<http://www.robertsonblums.com/rbconsulting/audit.html> **)**
35. Голов А., Кузнецов В. Вопросы сертификационного аудита систем управления информационной безопасностью // Журнал "CIO/СhiefInformationOfficer" №2,2006 (<http://offline.cio-world.ru/2006/45/253564/> )
36. Гузик С. Зачем проводить аудит информационных систем?  
    (<http://www.nestor.minsk.by/sr/2001/01/10111.html>, <http://www.info-system.ru/pj_managment/article/pj_audit_is.html> , <http://www.itexpert.ru/rus/biblio/auditIS/print> )
37. Гузик С. Информационная система под лупой аудита // Сетевой журнал №9.2001 (<http://www.setevoi.ru/cgi-bin/text.pl/magazines/2001/9/46>)
38. Компания "Сфера АйТи Системы" (<http://www.sferatel.ru/audit.shtml> )
39. Компания EdipService – анализ и аудит информационной системы (<http://1-se.ru/analysis/>)
40. Консалтинг и аудит информационных систем. Компания «СтинсКоман» (<http://www.stinscoman.com/consult> )
41. Консалтинг управления ИТ и аудит информационных систем. Компания **КРЕЧЕТ**  (<http://www.crechet.ru/audit_and_consulting.php> )
42. КРОК – системный интегратор (<http://www.croc.ru>.)
43. Колесников С. Аудит информационных систем: сетевая инфраструктура // Газета «Компьютер-Информ» № 06, 07/2005 (<http://www.ci.ru/inform06_05/p_10.htm>, <http://www.ci.ru/inform07_05/p_25.htm> )
44. КонеевИ. Зачем нужен аудит информационных систем? //Директор ИС №5/2005 (<http://www.osp.ru/cio/2005/05/173971/_p1.html> )
45. Маркевич М. Принципы проведения активного аудита информационной безопасности компании // "InformationSecurity/Информационная безопасность" № 2/2007 (<http://www.dsec.ru/about/articles/active_audit/> ).
46. Медведовский И.Практические аспекты проведения аудита информационной безопасности в соответствии с лучшей западной практикой// ["Connect! Мир связи" №10/2006](http://www.connect.ru/article.asp?id=7158) (<http://www.dsec.ru/about/articles/practice/> ).
47. ПачинИ. ITSM // Журнал "CIO/Сhief Information Officer" №6,2006 (<http://www.cio-world.ru/print/weekly/271909/>
48. Потоцкий М. О ценности улучшений, или Зачем нужен ITSM //Директор ИС №5/2005 (<http://www.osp.ru/cio/2005/05/173968/_p1.html>)
49. Прохоров А. Специалисты по аудиту информационных систем в России нужны как никогда (<http://www.compress.ru/article.aspx?id=12325&iid=471>)
50. Рабочая группа ISACA.ru – Управление, Сопровождение и Аудит Информационных Систем и Технологий (<http://www.isaca.ru/>)
51. Решения BindView по обеспечению соответствия требованиям информационной безопасности (<http://www.isecurity.ru/technologies/auditu.php> )
52. Сакун Ю. Аудит ИС (<http://www.ibusiness.ru/19367/index.html> )
53. Стандартные действия ИТ- аудита (<http://www.lankey.ru/?id=714> )
54. **Управление ИТ-инфраструктурой на предприятии //** Журнал "CIO/СhiefInformationOfficer" №8,2006  **(**<http://www.cio-world.ru/weekly/280383/> **)**

г) Программное обеспечение:

В качестве прикладных программных средств для данной дисциплины используются: стандартные программы базового комплекта ОС Windows; пакет прикладных программ MS Excel; «1С: Предприятие» (фирма 1С), AIDA32 (для диагностики и оптимизации системы); SandraStandart 2004.2.9 (для диагностики и оптимизации системы.

**10. Материально-техническое обеспечение дисциплины**

Аудиторный фонд факультета.

На факультете имеется 4 компьютерных класса, а также мультимедиа-проектор, позволяющие успешно проводить лекционные и практические занятия по данной дисциплине (демонстрация и защита презентаций в рамках занятий, защита проектов).Структура и состав компьютерных классов приведены в ООП.

Автор

доцент кафедры ИТЭиОП \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Данилова С.В.

Программа рассмотрена на заседании кафедры ИТЭ и ОП

от «\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_2012 г., протокол № \_\_\_\_\_\_\_\_

Программа одобрена на заседании Ученого совета экономического факультета

от «\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_2012 г., протокол № \_\_\_\_\_\_\_

1. Аудитор ИС, выполняя проверку контроля приложений, обнаруживает уязвимость в системе программного обеспечения, которая могла реально повлиять на приложения. Аудитор ИС должен:

A*.* неучитывать эту уязвимость контроля как обзор системы программного обеспечения, что является вне поля этой проверки.

B. сопровождать детализированную проверку системы программного обеспечения и составлять отчет о контроле за уязвимостями.

C. включать в отчет заголовка, что аудит был ограничен проверкой контроля приложений.

D. провести аудит контролей систем программного обеспечения как необходимый и рекомендуемый детализированной проверкой системы программного обеспечения.

2. Причина контроля в инфраструктуре ИС:

A. остается неизменной от руководства инфраструктурой, но инструменты контроля могут отличаться.

B. меняется от руководства инфраструктурой, поэтому инструменты контроля могут отличаться.

C. меняется от руководства инфраструктурой, но инструменты контроля могут остаться теми же.

D. остается неизменной от руководства инфраструктурой и выполнения инструментами контроля, который также остается тот же.

3. Который из нижеследующих типов рисков подразумевает компенсацию проверкой в рассматриваемой области?

A. Риск контролей

B. Риск обнаружения

C. Риск наследования

D. Риск примера

4. Аудитор ИС сопровождает нетривиальные тесты новым расчетным модулем. У аудитора весьма загруженный график работы и ограничено время на экспертизу. Который из видов аудита мог бы быть использован в этой ситуации?

A. Тестирование данных

B. Параллельная симуляция

C. Интегрированное средство тестирования

D. Воплощенный модуль аудита

5. Первоначальная цель самооценки контроля или программа контроля самоуверенности это:

A. заменить некоторые внутренние ответственности аудитора.

B. удалить ответственность контролей по линии менеджеров.

C. превзойти мониторинг контроля ответственности по функциональности.

D. улучшить мониторинг общего контроля организации.

6. Который из следующих лучших обзоров описывает раннюю стадию аудита ИС?

A. Делая обзор ключевых организационных средств.

B. Оценивая инфраструктуру ИС.

C. Понимая бизнес-процессы и инфраструктуру применительно к аудиту.

D. Заслушивая предыдущий из докладываемых отчетов аудита ИС.

7. Самая лучшая из инфраструктур в использовании средств интегрированного контроля – это необходимость:

A. изолировать контроль данных от производственных данных.

B. заметить персонального пользователя таким образом, чтобы делать подтверждения на вывод информации.

C. сегрегировать особые записи файлов мастера.

D. собрать транзакцию и записи файлов в отдельной папке.

8. Перед докладом результатов старшему менеджменту по аудиту аудитору ИС следует:

A. подтвердить находки аудита.

B. подготовить исполнительное резюме и послать его в менеджмент по аудиту.

C. определить рекомендации и представить находки в комитет по аудиту.

D. получитьаудиторскоезаключение.

9. В то время как, развивая рискориентированную программу аудита, который из следующих подойдет больше всего аудитору ИС?

A. Бизнес-процессы.

B. Критические ИТ приложения.

C. Операционные контроли.

D. Бизнес-стратегии.

10. В первую очередь использование общего аудита программного обеспечения – это:

A. аудиторский контроль программного обеспечения.

B. проверка неавторизованного доступа к данным.

C. извлечение необходимых данных для аудита.

D. сокращениенеобходимости в транзакционном подтверждении.

11. Которая из следующих задач может быть выполнена одним и тем же человеком в хорошо контролируемом информационно-процессорном компьютерном центре?

A. Администрирование безопасности и управление изменениями.

B. Компьютерныевычисления и развитие систем.

C. Развитиесистемиуправление изменениями.

D. Развитие систем и содержание систем.

12. Который из самых критических контролей находится над администрированием баз данных?

A. Подтверждение функционирования доступа к Базам Данных.

B. Подразделение обязанностей.

C. Проверка доступа к логам и их деятельности.

D. Проверка использования инструментов баз данных.

13. Которыйизследующих ответовмогбыбытьвключенвстратегический план ИС?

A. Спецификации по запланированной покупке аппаратного обеспечения.

B. Анализ будущих целей бизнеса.

C. Целевые данные для развития проектов.

D. Ежегодное бюджетирование целей для департамента ИС.

14. Самаябольшаяответственностьофицерабезопасностиданных в организации – это:

A. давать рекомендации и проводить мониторинг политики информационной безопасности.

B. продвижениебезопасностивсовокупности с организацией.

C. процедуры установления политики информационной безопасности.

D. администрирование физического и логического контролей доступа.

15. Которыйизследующих пунктовлучшеописываетпроцесс стратегического планирования ИТ департамента?

A. ИТдепартаментбудетиметьлибокоротко-масштабныелибошироко-масштабные планы зависящие от организационных более масштабных планов и целей.

B. СтратегическийпланИТдепартаментадолженбытьвременноипроектноориентированным и помочь определить приоритеты, отвечающие нуждам бизнеса.

C. Планирование долгосрочного диапазона для ИТ департамента должно распознать организационные цели, технологические преимущества и регулярные требования.

D. ПланированиекороткогодиапазонадляИТ департамента не нуждается в интеграции в коротко-масштабные планыорганизации с тех пор, как технологические преимущества будут скорее лидерами в планах ИТ департамента, чем в организационных.

16. Когда полное подразделение обязанностей не может быть достигнуто в системе он-лайн, которой из следующих процедур следовало бы отделиться от других?

A. Проектирование

B. Авторизация

C. Записывание

D. Коррекция

17. Первичнаявыгодаотнормализациибазданных - это:

A. минимизация сокращения информации в таблицах, требуемой удовлетворить нужды пользователей.

B. способность удовлетворить больше запросов.

C. максимизация целостности баз данных обеспечивая информацией более, чем одну таблицу.

D. минимизация времени ответа через быструю обработку информации.

18**.** Которая из сетевых топологий дает большое сокращение в случае провала одного узла?

A. сетчатая

B. звезда

C. кольцо

D. шина

19**.** Исполнитель договора против соглашений уровня сервисадолжен быть оценен:

A. покупателем.

B. участником договора.

C. третьей стороной.

D. исполнительнымменеджментом.

20**.** Который из следующих пунктов обеспечивает лучший метод определения уровня исполнения договора?

A. удовлетворениепользователя

B. достижение цели

C. квалификация

D. планированиеростаимощности

21**.** Когда аудитор ИС должен проверить наличие безопасности базы данных клиент-сервера:

A. системные утилиты.

B. генераторы программных приложений.

C. документация систем безопасности.

D. доступ к хранимым процедурам.

22**.** Который из следующих мог бы позволить компании расширить ее корпоративную сеть через Интернет к бизнес-партнерам?

A. виртуальная частная сеть

B. клиент-сервер

C. телефоннаялиния

D. сетевой сервис-провайдер

23. Аудитор ИС, проверяя аппаратное обеспечение процедурой мониторинга должен оценивать:

A. отчетыналичиясистем.

B. отчеты прибыли и убытков.

C. отчеты о времени ответов.

D. отчеты утилизации баз данных.

24. Которая из следующих передач информации обеспечивает устойчивость к проникновению осветления?

A. Витая пара

B. Оптический кабель

C. Коаксиальный кабель

D. Радио системы

25. Который из следующих заголовков относится к пакетной передаче данных по сети?

A. Пакеты с сообщением передаются по одному и тому же маршруту.

B. Пароли не могут быть переданы с пакетом.

C. Длина пакетов переменна и каждый пакет содержит одно и то же количество информации

D. Стоимость затрат по передаче основана на пакетах, но дистанция или маршрут изменяется.

26. Аудитор ИС когда проверяет сеть, используя интернет коммуникации, будет в первую очередь тестировать:

A. частоту замены пароля.

B. архитектуру клиент-серверного приложения.

C. архитектуру сети.

D. межсетевой экран защиты и прокси-серверы.

1. Который из следующих лучше обеспечивает контроль доступа к обработке данных на локальном севере?

A. Регистрирующий доступ к информации пользователя

B. Отдельный пароль для конфиденциальных сообщений

C. Программное обеспечение ограничивает доступ правилами авторизации персоналаf

D. Доступ в систему ограничен рабочими часами

2. Который из следующих мог бы быть адресован цифровой подписи со значением безопасности электронного сообщения?

A. Неавторизованное чтение

B. Кража

C. Неавторизованное копирование

D. Внесение изменений

3. Самый эффективный антивирус контролирует:

A. сканирование почтовых приложений на почтовом сервере.

B. восстановление систем с чистых копий.

C. блокирование мягких дисков.

D. онлайновый антивирус сканирует с современными определителями вируса.

4. Который из следующих предложений лучше определяет, что полное шифрование и аутентификация протоколов по защите информации существует пока передается?

A. Цифровая подпись с RSA была выполнена.

B. Работа будучи сделанной в туннельном режиме с представленными сервисамиAH и ESP.

C. Цифровые сертификаты с RSA применены.

D. Работа выполненная в транспортном режиме с сервисами AH и ESP.

5. Который из следующих мог бы быть наиболее подходящим удостовериться в конфиденциальности транзакций, инициируемых через Интернет?

A. Цифровая подпись

B. Стандарт Шифрования Данных (DES)

C. Виртуальные частные сети(VPN)

D. Общийключшифрования

6. Который из следующих является операционной системой контроля доступа?

A. Протоколирование деятельности пользователя

B. Протоколирование коммуникации доступа к данным

C. Различая авторизацию пользователя на уровне поля

D. Обмен файлами данных

7***.*** Если злоумышленники наметили несанкционированное проникновение в систему, то на кого рассчитывать аудитору ИС, в случае проверки журнала регистрации при попытке входа в систему?

A. Сетевой администратор

B. Системный администратор

C. Администратор данных

D. Администратор баз данных

8. Аудитор только что ознакомился с организацией, которая имеет мэйнфрейм и клиент-серверное оборудование, где находятся все данные. Какая из уязвимостей считается наиболее серьёзной*?*

*A. Офицер по безопасности также выполняет роль и администратора баз данных*

*B. Контроль паролей не администрируется в клиент-серверной архитектуре.*

*C. Не существует плана непрерывности бизнеса для системы мейнфреймов автоматических приложений.*

*D. Большинство ЛВС не делают резервные копии с дисков сервера.*

9. Организация предлагает установить средство SSO,предоставляющее доступ к любым системам. В организации должны знать, что:

A. максимальнонеавторизированныйдоступ мог бы быть возможен, если пароль известен.

B. права доступа пользователя могли бы быть урезаны дополнительными параметрами безопасности.

C. загруженность работой администратора по безопасности увеличилась.

D. Права доступа пользователя могут быть расширены.

10. СайтэлектроннойкоммерцииB-to-Cкак часть программ информационной безопасности требует защиты и предотвращения хакерской деятельности и оповещения системным администратором, когда подозрительные действия случаются. Которые из предложенных инфраструктурных компонентов могут использоваться для этих целей?

A***.*** Системы обнаружения вторжений

B. Межсетевые экраны

C. Маршрутизаторы

D. Ассиметричное шифрование

***Тема 5. Восстановление после катастроф и непрерывность бизнеса***. Бизнес кейс для непрерывного планирования. Процесс планирования адекватного восстановления и непрерывности. Важность менеджмента информационной безопасности. Логический доступ. Сетевая инфраструктура безопасности. Менеджмент аудита информационной безопасности. Аудит сетевой инфраструктуры безопасности. Физический доступ и контроль. Оценка планов по восстановлению, документированию и эксплуатации. Оценка методов тестирования, результатов ведения отчетов, и их обработка.

*Литература*

[1.1], [1.2], [2.1], [2.2], [2.3]

*Контрольные вопросы*

1***.*** Которое из замечаний в плане непрерывности бизнеса самое важное?

A. поставщики оборудования.

B. агенты страховых компаний.

C. договорные сервисы для персонала.

D. приоритезированный контактный лист.

2***.*** Аудитор ИС выявляет, что план непрерывности бизнеса организации обеспечивает альтернативный сайт обработки, который будет вмещать 50 процентов первоначальной способности обработки. Основанный на этом, который из предложенных действий аудитор ИС предпримет?

A. Ничего не делать, так как в общем, менее чем 25 % всей обработки для организации критично и мощности резервного копирования, поэтому это адекватно.

B. Определит приложения, которые могут быть обработаны на альтернативном сайте и распознает процедуры по инструктажу резервного копирования***.***

C. Удостоверится, что критические приложения определены и что альтернативный сайт мог бы обработать все подобные приложения.

D. Рекомендует, что массив средств обработки информации для альтернативного сайта с мощностью обработки по крайней мере составляет 75 процентов.

3***.*** ЗакоторуюизследующихкомпонентплананепрерывностибизнесаответственендепартаментИСорганизации в первую очередь?

A. развиватьпланнепрерывностибизнеса

B. выбирать и подтверждать стратегию плана непрерывности бизнеса

C. декларировать катастрофы, уязвимости

D. восстанавливать информационные системы и данные после катастроф

4.Которое из следующих замечаний должно быть включено в план непрерывности бизнеса?

A. требуемыйперсоналдолженподдерживатькритическиефункции бизнеса в кратковременных, средних и продолжительных отношениях

B. Потенциальныйинцидент, чтопроизошел как катастрофа, - землетрясение

C. Катастрофические события оказывающие влияние на информационные системы обработки и функций конечного пользователя

D. Анализ рисков, который предполагает неправильную работу системы, удаление случайных файлов или другие неудачи

5***.*** В аудите план непрерывности бизнеса, который из следующих предложений самый логичный?

A. Не существует страховки для дополнения активов в течение года.

B. BCPинструкция не совершенствуется регулярно.

C. Проверка резервного копирования данных не выполняется регулярно.

D. Регистрациядоступаксистеменебылавыполнена.

6. Классификация информационных систем является существенной в плане непрерывности бизнеса. Которая из следующих типов систем не может быть перемещена методами инструкций?

A. Критические системы

B. Необходимыми системами

C. Чувствительными системами

D. Некритичными системами

7. Аудитор ИС должен быть вовлечен в:

A. рассмотрение проверок плана по восстановлению системы после катастроф.

B. разработка плана по восстановлению системы после катастроф.

C. утверждение плана по восстановлению системы после катастроф.

D. пересмотртребованийпо восстановлению системы после катастроф.

8. Временнойлагпоспособностиквосстановлениюинформациипослекатастроф основывается на:

A. критичность процессов оказывает влияние.

B. качествообработанныхданных.

C. природа катастроф.

D. приложения основывающиеся на мейнфреймах.

9. Вовремяаудиторскойпроверкикрупногобанка, выобнаруживаете, чтоне было выполненоупражненийпооценкерисков различных бизнес-приложений с целью вернуть их относительную важность и восстановить временные требования. Риск, которым руководствуется банк заключается в том, что:

A. план по непрерывности бизнеса может быть не отнесен к соответствующему риску, так что разрушение каждого из приложений позиционируется по отношению к организации.

B. план по непрерывности бизнеса может не включать все соответствующие приложения и поэтому может отсутствовать завершенность в отношении его покрытия.

C. влияниекатастрофнабизнесможетбытьнеправильновоспринятоменеджментом.

D. план непрерывности бизнеса может не иметь эффективности в собственности у владельцев бизнеса таких приложений.

10. Которыйизследующихнеобходимоиметьвпервуюочередьвразвитии плана непрерывностибизнеса?

A. классификацию систем, основанную на рисках.

B. проверка всех активов.

C. полная документация всех нарушений.

D. наличие аппаратного и программного обеспечений.

***Тема 6. Развитие систем бизнес-приложений, приобретение, ввод в эксплуатацию и обеспечение функционирования***. Оценочный подход. Непрерывность бизнеса. Планирование развития систем бизнес-приложений. Аудит непрерывности бизнеса. Функциональные требования. Анализ функционирования ИС. Системные спецификации. Построение системы. Развитие системы. Приобретение. Внедрение. Эксплуатация.

*Литература*

[1.1], [1.3], [1.5], [1.6], [2.1], [2.2], [2.22], [2.36]

*Контрольные вопросы*

1. Планыпотестированиюприложенийразвиты, вкоторыхизперечисленных следующих фаз жизненного цикла развития систем (SDLC) они присутствуют?

A. Создание

B. Проверка (тестирование)

C. Требование

D. Развитие

2. Который из следующих тестов подтверждает, что новая система может управлять своей целевой инфраструктурой?

A. Открытое тестирование

B. Регрессионное тестирование

C. Действительное тестирование

D. Тестирование черным ящиком

3. Уверенностьвкачествепрограммногообеспечения(SQA) – это процесс менеджмента, который дополняет:

A. правильностьвразработке стандартов.

B. выполнение проверок (тестов) системы.

C. идентификациясистемныхтребований.

D. спецификация детализированной разработки.

4. Первоначальная цель, предпринимая параллельный запуск новой системы, - это:

A. доказать, что система обеспечивает необходимую бизнес-функциональность.

B. утвердить операцию новой системы в противовес предшествующей.

C. устранитьлюбыеошибкивпрограммеифайловом интерфейсе.

D. доказать, что система может обрабатывать загружаемую информацию.

5. Процедуры контроля изменениями чтобы вовремя предотвратить масштаб распространения развития приложений следовало бы определить в течение:

A. архитектуру.

B. выполнимость (осуществимость).

C. обеспечение выполнимости.

D. определение требований.

6. Котороеизследующихпредложениймоглобылучше подтвердить, что система развития проектов отвечает бизнес-требованиям?

A. Обеспечение замены журналов регистрации программ

B. Разработкапланапроекта, определяющего развитие ИС

С. Удаление изменений приложений в определенное время года

D. Вовлечение пользователя в системную спецификацию и принятие

7. Котораяизследующихизмеряетсяразмероминформационныхсистем, основанныхнаколичествеисложностиввода, выводасистемыифайлов?

A. Функциональная точка (FP)

B. Оценка обзора технических программ (PERT)

C. Быстрое построение приложений (RAD)

D. Метод критического пути (CPM)

8. Когдаопределяется фазатребованийаудитапрограммного обеспечения, аудитор ИС должен:

A. оценить выполнимость проекта вовремя.

B. оценить качество процессов, предложенных вендором.

C. удостовериться, что требуется самый лучший пакет программного обеспечения.

D. обзорполнотыспецификаций.

9. Цельзагрузкипрограмм - это:

A. генерированиеслучайныхданныхможетбытьиспользовано для проверки программ перед запуском их.

B. защитавовремяфазыпрограммирования, действительные изменения от перезаписи изменений.

C. определениеразвитияпрограммиобеспечениезатрат, включенныхв организуемое обучение.

D. удостовериться, чтоошибочныеоперациии недостатки кодированияпрограмм защищены и скорректированы.

10. Обеспечениепрограммногообеспечениявпервуюочередьотноситсякследующим атрибутам программного обеспечения?

A. Необходимы ресурсы способствуют особым изменениям.

B. Необходимыедостиженияиспользуютсяпрограммными приложениями.

C. Необходимое взаимодействие между функционированиемПОиресурсами.

D. Выполнение нужд пользователя.

***Тема 7. Оценка бизнес-процессов и риск-менеджмент.*** Корпоративное управление. Управление ИТ. Управление жизненным циклом ИС. Предоставление сервиса ИТ. Оценка эффективности информационных систем в поддержке бизнес-процессов. Оценка построения и внедрения контроля рисков. Оценка управления рисками и управления процессами. Ресурсы.

*Литература*

[1.1], [1.2], [1.5], [1.7], [1.8], [1.9], [2.3], [2.4], [2.25], [2.28]

*Контрольныевопросы*

1. Управление ИТ подтверждает, что организациявыстраивает свою ИТстратегиюв соответствии с:

A. целями предприятия.

B. целями ИТ.

C. целями аудита.

D. целями контроля.

2. Котораяизследующихпроверок используетсядляудостоверения, чтогруппа данных полностью и аккуратно передается между двумя системами?

A. Цифровая проверка

B. Полный контроль

C. Проверка суммы

D. Проверка счета

3. Втечениекоторогоизследующихшаговвреинжинирингебизнес-процессовследовало бы квалифицировать команду инструктированием на минимальном уровне достижений?

A. Наблюдение

B. Планирование

C. Анализ

D. Адаптация

4. Котораяизследующихпроцедурдолжнабытьвыполнена, чтобыпомочьудостовериться в компетенции возврата транзакций через электронный обмен данными (EDI)?

A. Сегментныеитоги, построенныенанаборе следа транзакций

B. Набор ряда сообщений получен, что периодически подтверждается с транзакционныминициатором

C. Электронный аудит по финансам и операциямалгоритмически выполняется

D. Совершаясоответствующие транзакции, полученные из набора сообщений EDI

5. Утилитывсостоянииусовершенствоватькритическиеобласти в случае несовместимости данных. Этаутилитаможетбытьвыполненапо запросу ОС как одна из опций приложения. Лучшаяпроверканауменьшениерисканеавторизованнаяманипуляциясданными, - это:

A. удалить утилиту программного обеспечения и инсталлировать ее как и когда потребуется.

B. обеспечить доступ к утилите по требованию ее использования.

C. обеспечитьдоступкутилитек пользовательскому управлению.

D. определитьдоступтакимобразом, чтобы утилита могла быть выполнена только в опции меню.

6. Когдасопровождаяреинжинирингбизнес-процессов, аудиторИСнаходит, чтоключпредупреждающего контроля был удален. В этом случае аудитор ИС должен:

A. информироватьуправлениенаходкойиподтверждениемлибоменеджментимеет возможность принять потенциальный материальный риск не имея того предварительного контроля.

B. определитьесликонтрольобнаружения переместился наконтрольпредотвращенияв течениепроцесса и если так, то нет отчета на удаление.

C. рекомендовать, чтоэтиивсеконтрольныепроцедуры, которыесуществовалидоэтогопроцессанад ними был проведенреинжиниринг чтобы быть включенным в новый процесс.

D. разработать к непрерывному аудиту с тем, чтобы отследить эффекты удаления превентивного контроля.

7. Который из последующих является выходом целевой проверки?

A. Обеспечение регистров необходимым количеством

B. Завершение количества обработки

C. Соответствующий расчет по отказам и исключениям

D. Авторизацияусовершенствованийфайлов

8. Всистеме, которая записывает все данные для компании, получатели зарегистрированы ежедневной базе. Который из следующих мог быть уверен, что балансо получатели неизменны среди рассылок?

A. Контроль диапазона

B. Проверка записей

C. Контроль последовательности

D. От управления-к-управлению общий контроль

9. Котороеизследующихзаявленийсамоеважное для аудитора ИС в проекте реинжиниринга бизнес-процессов?

A. Отсутствиесреднегоменеджмента, которыйчастоявляетсярезультатомпроектареинжинирингабизнес-процессов.

B. То, что контролирует обычно дает низкий приоритет в проекте БПР.

C. Разумноенегативноевлияние, котороезащитаинформациимоглабыиметь на РБП.

D. Рискнеудачсвязансогромнымразмеромвыполняемыхзадач обычно решаемых в проекте БПР

10. Чтобы отвечать предопределенным критериям, какие средства и методы могли бы лучше определять непрерывные транзакции аудита?

A. Файл обзора систем контроля аудита и модули внедрения аудита (SCARF/EAM)

B. Непрерывное и скачкообразное моделирование (CIS)

C. Интегрированные средства проверки (ITF)

D. Аудиторские уловки

***Тема 8. Внутренний контроль.*** Мониторинг. Защита внутренних активов. Внутренний аудит. Информация и коммуникация. Контрольные процедуры. Оценка рисков. Среда контроля.

*Литература*

[1.1], [1.2], [1.3], [1.8], [1.9], [1.10], [1.11], [1.13], [2.1], [2.2], [2.5], [2.8], [2.11], [2.23]

*Контрольные вопросы*

1. Вмаленькойорганизации, гдеразделениеобязанностейнепрактикуется,служащийвыполняетфункциюоператоранакомпьютереиприкладногопрограммиста. Которыйизследующихконтролейпорекомендуетаудитор ИС?

A. Автоматизированнаязагрузкаизмененийвразвивающиеся библиотеки.

B. Дополнительный обслуживающий персонал обеспечивает разделение обязанностей

C. Процедуры, которые различаются тем, что оправдывают программные изменения, выполняются.

D. Контроль доступа выполняется с целью предотвращения внесения изменений оператором.

2. Котороеизследующих самых подходящих действий предназначено для администратора по безопасности?

A. Подтверждение политики безопасности.

B. Тестирование прикладного программного обеспечения.

C. Подтверждение целостности данных.

D. Инструкция по правам доступа.

3. Аудитор ИС проводит тестирование контролей, относящихся к терминалу служащего. Который из следующих самый важный аспект в проведении аудита?

A. Относящийся к компании персонал нацелен на результат.

B. Пользовательидентификационныхданных и служебных паролей был удален.

C. Деталислужащегобылиудалены из активированных рабочих папок.

D. Приобретенная собственность компанией была возвращенаслужащему.

4. Когдапроводитсяпроверкапо соглашению уровня сервиса для аутсорсингового компьютерного центрааудитором ИС следует в первую очередь определить, что:

A. предлагаемая стоимость услуг разумна.

B. механизмы безопасности определены в соглашении.

C. услуги в соглашении основываются на анализе нужд бизнеса.

D. доступ к компьютерному центру разрешается по аудиторскому соглашению.

Авторы программы: Н.Н.Гусева