РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Управление информационной безопасностью

(наименование дисциплины (модуля) по УП)

Закреплена за кафедрой: систем информационной безопасности

Направление подготовки (специальности): 10.05.03 Информационная безопасность автоматизированных систем

Профиль: Обеспечение информационной безопасности распределенных информационных систем
(название профиля по УП)

Часов по УП: 144; Часов по РПД: 144;
Часов по УП (без учета часов на экзамены): 108; Часов по РПД: 108;
Часов на интерактивные формы (ИФ) обучения по УП: -
Часов на интерактивные формы (ИФ) обучения по РПД: -
Часов на самостоятельную работу по УП: 28 (25,9%);
Часов на самостоятельную работу по РПД: **28 (25,9%);**
Общая трудоемкость в ЗЕТ: 4;
Виды контроля в семестрах (на курсах): экзамен – 8;
Форма обучения: очная**;**
Срок обучения: нормативный**.**

Распределение часов дисциплины по семестрам

Вид занятий	**№ семестров, число учебных недель в семестрах**																	
	1 / 18		2 / 18		3 / 18		4 / 18		5 / 18		6 / 20		7 / 18		8 / 10		Итого	
	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД
Лекции											40						40	
Лабораторные											-						-	
Практические											40						40	
Ауд. занятия											80						80	
Сам. работа											28						28	
Итого											108						108	

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	**Цель изучения дисциплины** является изучение основных понятий, методологии и практических приемов управления технической и организационной инфраструктурой обеспечения информационной безопасности на предприятии
1.2	**Для достижения цели ставятся задачи:**
1.2.1	приобретение обучаемыми необходимого объема знаний и практических навыков в области стандартизации и нормотворчества в управлении информационной безопасностью, оценки рисков информационных ресурсов предприятия и аудита информационной безопасности, организации работы и разграничения полномочий персонала, ответственного за информационную безопасность

1.2.2	формирование у обучаемых целостного представления об организации и содержании процессов управления информационной безопасностью на предприятии как результата внедрения системного подхода к решению задач обеспечения информационной безопасности (ИБ) автоматизированных систем

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВПО

Цикл (раздел) ООП: С.3	код дисциплины в УП: С3.Б.16
2.1 Требования к предварительной подготовке обучающегося	
Для успешного освоения дисциплины студент должен иметь базовую подготовку по информатике и математике в пределах программы средней школы, а также дисциплины младших курсов, такие как	
С3.Б.8	Основы информационной безопасности
С3.Б.5	Безопасность операционных систем
С3.Б.18	Информационная безопасности распределённых информационных систем
2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее	
С3.Б.11	Техническая защита информации
С3.Б.19	Методы проектирования защищённых распределённых информационных систем
С3.В.ДВ.1	Управление рисками в распределённых информационных системах

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-21	способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы **Знать:** - основные методы управления информационной безопасностью; - методы аттестации уровня защищенности автоматизированных систем; - основные положения стандартов Единой системы конструкторской документации, Единой системы программной документации; **Уметь:** - оценивать информационные риски в автоматизированных системах; - определять комплекс мер (правила, процедуры, практические приемы, руководящие

	принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем; - применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации; **Владеть:** - навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; - методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; - методами управления информационной безопасностью автоматизированных систем.
ПК-29	способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы **Знать:** - принципы построения систем управления информационной безопасностью (СУИБ); - современные подходы к управлению ИБ объекта и направления их развития; - особенности отдельных процессов управления ИБ в рамках СУИБ **Уметь:** - разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем; - составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем; - используя современные методы и средства, разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность; **Владеть:** - терминологией и процессным подходом построения СУИБ; - методами оценки информационных рисков; - навыками участия в экспертизе состояния защищенности информации на объекте защиты;
ПК-33	способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации **Знать:** - принципы формирования политики информационной безопасности в автоматизированных системах; - модели безопасности компьютерных систем ориентированные на управление доступом и информационные потоки **Уметь**: - разрабатывать частные политики информационной безопасности автоматизированных систем; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; - разрабатывать документальное обеспечение дли процессов управления ИБ, включая различные политики ИБ (ПолИБ) и применять его па практике. **Владеть:** - навыками формализации моделей безопасности компьютерных систем ориентированные на управление доступом и информационные потоки в рамках конкретной СУИБ; - навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом.
ПК-39	способностью управлять информационной безопасностью автоматизированной системы

	Знать: - современные подходы к управлению ИБ объекта и направления их развития; - подходы к интеграции СУИБ в общую систему управления организации; - основные международные и российские стандарты, регламентирующие управление ИБ; **Уметь**: - анализировать текущее состояние ИЬ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ; - определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ; **Владеть:** - навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем; - навыками анализа бизнес-активов организации, угроз ИБ и уязвимости в рамках области действия СУИБ; - навыками построения отдельных процессов управления ИБ, относящихся к области технических, организационных и кадровых аспектов управления ИБ.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

№ П./п	Наименование раздела дисциплины	Семестр	Неделя семестра	Вид учебной нагрузки и их трудоемкость в часах				
				Лекции	Практические занятия	Лабораторные. работы	СРС	Всего часов
1	Основные понятия и подходы к управ-	8	1-3	6	6	-	6	6

	лению информационной безопасностью							
2	Стандартизация систем и процессов управления информационной безопасностью	8	4-6	6	6	-	4	16
3	Политика информационной безопасности	8	7-9	6	6	-	4	16
4	Модели управления доступом и информационными потоками	8	10-13	8	8	-	4	12
5	Управление и система управления информационной безопасностью	8	14-17	8	8	-	4	12
6	Организационные и кадровые вопросы управления информационной безопасностью	8	18-20	6	6	-	2	14
Итого				40	40	-	28	108

4.1 Лекции

Неделя семестра	Тема и содержание лекции	Объем часов	В том числе, в интерактивной форме (ИФ)
Основные понятия и подходы к управлению информационной безопасностью		6	
1-3	Базовая терминология. Системный и процессный подходы к управлению ИБ. Управление логическим доступом к активам организации. Управление защищенной передачей данных и организационной деятельностью. Управление конфигурациями, изменениями и обновлениями. *Самостоятельное изучение*. Физическая защита и защита от воздей-	6	

	ствий окружающей среды		
Стандартизация систем и процессов управления информационной безопасностью		**6**	
4-6	Серия стандартов ISO/IEC 27000 «Информационные технологии. Методы обеспечения безопасности». Стандарты на отдельные процессы управления ИБ и оценку безопасности ИТ. Отраслевые стандарты в области управления ИБ. *Самостоятельное изучение.* Стандарты банковской системы РФ в области управления ИБ	6	
Политика информационной безопасности		6	
7-9	Понятие политики обеспечения ИБ и политики ИБ организации. Причины разработки политики. Основные требования и принципы, учитываемые при разработке и внедрения политики ИБ. Содержание политики ИБ. Жизненный цикл политики ИБ. Ответственность за исполнение политики. *Самостоятельное изучение.* Ответственность за исполнение политики.	6	
Модели управления доступом и информационными потоками		8	
10-13	Модели дискреционного управления доступом. Модели изолированной программной среды. Модели с мандатным управлением доступом. Модели безопасности информационных потоков. Модели с ролевым управлением доступом *Самостоятельное изучение.* Модели мандатного ролевого управления	8	
Управление и система управления информационной безопасностью		**8**	
14-17	Необходимость управления обеспечением ИБ организации. Деятельность по обеспечению ИБ организации как процесс. Определение управления ИБ организации. Управление ИБ информационно-телекоммуникационных технологий организации. Система управления ИБ организации. Область действия СУИБ. Документальное обеспечение СУИБ. Документальное обеспечение СУИБ. Процессный подход в рамках управления ИБ. Работа с процессами СУИБ организации. Стратегии построения и внедрения СУИБ. *Самостоятельное изучение.* Поддержка СУИБ со стороны руководства организации	8	
Организационные и кадровые вопросы управления информационной безопасностью		6	
18-20	Модели организационного управления ИБ. Организационная инфраструктура ИБ. Служба ИБ организации. Компетентностные уровни профессионалов в области ИБ *Самостоятельное изучение.* Учет вопросов ИБ при работе с персоналом	6	
Всего		**40**	

4.2 Практические занятия

Неделя семестра	Наименование практической работы	Объем часов	В том числе в интерактивной форме (ИФ)	Виды контроля
6-ой семестр		**40**	**-**	

1	Модель решётки	2		отчет
3	Дискреционное управлением доступом (модели Харрисона-Руззо-Ульмана и типизированная матрицы доступов)	6		отчет
6	Управление распространением прав доступа на основе классической модели Take-Grant	6		отчет
8	Управление распространением прав доступа на основе расширенной модели Take-Grant	4		отчет
10	Модель Белла-ЛаПадулы. Мандатное управление доступом	**4**		отчет
13	Ролевое и мандатное ролевое управление доступом	6		отчет
16	Изучение средств управления безопасностью на уровне операционной системы на примере Windows Server 2003. Управления учетными записями пользователей	6		отчет
19	Изучение средств управления безопасностью на уровне операционной системы на примере Windows Server 2003. Настройка политик безопасности	6		отчет
Итого за 2-ой семестр		**40**		

4.3. Лабораторные работы

Не предусмотрены

4.4 Самостоятельная работа студента (СРС)

Неделя семестра	Содержание СРС	Виды контроля	Объем часов
2 семестр		**Зачет**	**28**
3	Физическая защита и защита от воздействий окружающей среды	проверка домашнего задания	6
6	Стандарты банковской системы РФ в области управления ИБ	проверка домашнего задания	4
9	Ответственность за исполнение политики безопасности	проверка домашнего задания	4
13	Модели мандатного ролевого управления	проверка домашнего задания, допуск к выполнению лабораторной работы	4
17	Поддержка СУИБ со стороны руководства организации	проверка домашнего задания	4
20	Учет вопросов ИБ при работе с персоналом	проверка домашнего задания	2

4.5. Темы курсовых работ

Курсовые работы не предусмотрены

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

	В рамках изучения дисциплины предусмотрены следующие образовательные технологии:
5.1	**Информационные лекции**;
5.2	**лабораторные работы**: – информационные технологии, – работа в команде;

	– проблемное обучение; – контекстное обучение;
5.3	**самостоятельная работа студентов**: – изучение теоретического материала, – подготовка к лекциям, лабораторным работам и практическим занятиям, – работа с учебно-методической литературой, – оформление конспектов лекций, подготовка реферата, отчетов, – подготовка к текущему контролю успеваемости и к экзамену;
5.4	**консультации** по всем вопросам учебной программы.

6. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

6.1	**Контрольные вопросы и задания**
6.1.1	Используемые формы текущего контроля: – реферат; – отчет и защита выполненных практических работ.
6.1.2	Рабочая программа дисциплины обеспечена фондом оценочных средств для проведения текущего контроля знаний.
6.2	**Другие виды контроля**
6.2.1	Реферат по тематике, касающейся основных нововведений в области развития операционных систем. Темы рефератов представлены учебно – методическом комплексе дисциплины.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1 Рекомендуемая литература

№ п/п	**Авторы, составители**	Заглавие	Годы издания. Вид издания	Обеспеченность
7.1.1. Основная литература				
7.1.1.1	Курило А.П., Милославская Н.Г.,	Основы управления информационной безопасностью: Учеб. пособие. - М. : Горячая линия -	2012 печат.	

	Сенаторов М.Ю., Толстой А.И.	Телеком, - 244 с. : ил . - (Вопросы управления информационной безопасностью. Кн.1).		
7.1.1.2	Девянин П.Н.	Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. – 2-е изд. –М.: Горячая линия – Телеком, 338 с. (ЭБС «Лань»)	2013 печат.	
7.1.2. Дополнительная литература				
7.1.2.1	Милославская Н.Г., Сенаторов М.Ю., Толстой А.И.	Технические, организационные и кадровые аспекты управления информационной безопасностью : Учеб. пособие. - М. : Горячая линия - Телеком, - 214 с. : ил . - (Вопросы управления информационной безопасностью. Кн.4).	2012 печатн.	
7.1.2.2	Милославская Н.Г. Сенаторов М.Ю.; Толстой А.И.	Проверка и оценка деятельности по управлению информационной безопасностью : Учеб. пособие. - Воронеж : Горячая линия -Телеком, - 166 с. : ил . - (Вопросы управления информационной безопасностью. Кн.5).	2012 печатн.	
7.1.3. Методическая литература				
7.1.3.1	Разинкин К.А.	Методические указания № 336-2014 к практическим занятиям № 1–4 по дисциплине «Управление информационной безопасностью» для студентов специальности 090303 «Информационная безопасность»	2014 Эл.рес	
7.1.3.2	Разинкин К.А.	Методические указания № 335-2014 к практическим занятиям № 5,6 по дисциплине «Управление информационной безопасностью» для студентов специальности 090303 «Информационная безопасность»	2014 Эл.рес	

7.1.4 Программное обеспечение и интернет ресурсы	
7.1.4.1	Методические указания к выполнению лабораторных работ **представлены на сайте:** Интернет ресурсы: http://www.eios.vorstu.ru (электронная информационно-обучающая система ВГТУ) http://e.lanbook.com/ (ЭБС Лань) http://znanium.com/ (ЭБС Знаниум) http://IPRbookshop.ru/ (ЭБС IPRbooks (Айбукс))
7.1.4.2	**Компьютерные практические работы**: – система компьютерной математики MATLAB. – интегрированная среда языка имитационного моделирования GPSS PS – инструментальная система имитационного моделирования AnyLogic PLE

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1	**Специализированная лекционная аудитория**, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой
8.2	**Дисплейный класс**, оснащенный компьютерными программами для проведения лабораторного практикума

ПРИЛОЖЕНИЕ1

Карта обеспеченности рекомендуемой литературой

№ п/п	Авторы, составители	Заглавие	Год издания. Вид издания.	Обеспеченность
1. Основная литература				
Л1.1				
Л1.2				
2. Дополнительная литература				
Л2.1				
3. Методические разработки				
Л3.1				
Л3.2				

Зав. кафедрой _____ / А.Г. Остапенко /

Директор НТБ _____ / Т.И. Буковшина /

Утверждаю
зав. кафедрой СИБ
_____А. Г. Остапенко

Контрольно-измерительные материалы для проведения текущего контроля и промежуточной и итоговой аттестации по дисциплине «Управление информационной безопасностью»

Контрольно-измерительные материалы текущего контроля

1. Дайте определение понятия «система»?
2. Каковы основные свойства системы?
3. В чем заключается системный подход к исследованию объектов?
4. Каковы особенности рассмотрения системного подхода применительно к управлению?
5. Какие элементы процесса могут быть исключены из определения: входные данные процесса, выходные данные процесса, управляющее воздействие, ресурсы?
6. Какие виды деятельности в организации можно назвать процессом (или бизнес-процессом)?
7. Какую роль играют процессы в терминах системного подхода к организации?

8. Кто в организации может и должен определить цели бизнес-процессов?
9. Что понимается под ресурсами в рамках определения понятия процесса?
10. Что понимается под управляющим воздействие в рамках определения понятии процесса?
11. В чем заключайся процессный подход?
12. Дайте определение понятия «управление» с позиций системного подхода.
13. Дайте определение понятия «менеджмент».
14. В чем отличия понятий «управление» и «менеджмент»?
15. Каковы основные функции управления?
16. Что такое метод управления?
17. Что такое система управления?
18. Что такое система управления, основанная на процессном подходе?
19. Каковы особенности рассмотрения процессного подхода применительно к управлению?
20. К каким процессам организации может быть применена циклическая модель PDCA?
21. В чем состоят основные преимущества использования циклической модели PDCA?
22. В чем отличие терминов «защита информации» и «информационная безопасность»?
23. Какие свойства ИБ в современных условиях должны приниматься во внимание? Расшифруйте что понимается под каждым из свойств.
24. Какой стандарт (серия стандартов) счал основоположником стандартизации систем управления ИБ?
25. Для организации какой сферы применимы стандарты серии ISO/IEC 27000?
26. Каковы отличительные черты серии стандартов ISO/IEC 27000?
27. Какой из стандартов серии ISO/IEC 27000 содержится руководство к внедрению, эксплуатации, мониторингу, анализу, сопровождению и совершенствованию СУИБ?
28. В чем состоит основные различия и сходства стандартов ISO/IEC 27001 и ITU-T X.1051?
29. Какой из стандартов серии ISO/IEC 27000 признан каталогом «лучших» практик по ИБ?
30. В каком стандарте серии 1SO/IEC 27000 содержится руководство но внедрению СУИБ?
31. На основании чего может проводиться оценка эффективности СУИБ?
32. Можно ли проводить, аудит (или сертификацию) на соответствие стандарту ISO/IEC 27002 (бывший ISO/IKC 17799)?
33. Каковы основные идеи руководства по аудиту СУИБ и средств управления ИБ, реализованных в СУИБ?
34. Почему подход к приведению аудитов систем менеджмента качества и окружающей среды, изложенный в стандарте ISO/IEC 19011. может быть применен для проведения внутренних аудитов СУИБ?
35. В каком стандарте серии ISO/IEC 27000 описана инфраструктура руководства ИБ?
36. Какой стандарт серии ISO/IEC 27000 рассматривает вопросы управления безопасностью сетей?
37. В чем состоят преимущества использования (учета) требований российских и международных стандартов по управлению ИБ при построении СУИБ или отдельных процессов управления ИБ?
38. Каковы преимущества одновременного учета требований стандартов. предъявляемых как к СУИБ в целом, так и стандартов, предъявляющих требования к отдельным процессам, разрабатываемым в рамках СУИБ?
39. В чем состоят основные сходства и различия между стандартами па СУИБ и на отдельные процессы управления ИБ?
40. Какие методы и средства ОИБ для ИГ рассматриваются в стандартах ISO/IEC 13335 и идентичных им ГОСТ Р ИСО/МЭК 13335?
41. Как оценивается ИБ ИГ согласно стандартам ISO/IEC 15408 и 18045 и идентичных им ГОСТ Г ИСО/МЭК?
42. Какие из рассмотренных стандартов затрагивают аспекты анализа рисков ИБ?
43. Каковы основные цели построения системы УНБ, соответствующей требованиям стандартов BS 25999 и 25777?

44. В чем может заключаться различие между требованиями *к* системам управления непрерывностью бизнеса и к процессу управления непрерывностью бизнеса?

45. Каковы основные цели следования модели PDCA при построении процесса управления инцидентами ИБ в соответствии с требованиями ГОСТ Р ИСО/МЭК ТО 18044?

Контрольно-измерительные материалы промежуточного контроля

1. Какие определения ПолИБ даются и различных международных стандартах?
2. В чем различие политик, стандартов, правил и процедур ОИБ?
3. Что такое трастовые модели?
4. С каких точек зрении и как можно описать виды ПолИБ?
5. Что понимают под ПолИБ и широким и узком смыслах?
6. Для чего разрабатываются организационные (административные) и технические ПолИБ?
7. Перечислите основные требования, предъявляемые в различных источниках к ПолИБ?
8. Каковы основные принципы позволяющие разработать эффективную ПолИБ?
9. Каково содержание документа, описывающего корпоративную ПолИБ? Что излагается в каждом из разделов этой политики?
10. Назовите типовые цели корпоративной ПолИБ.
11. 11.Каковы отличительные особенности содержания частной ПолИБ для отдельной области, требующей ОИБ, и для отдельной системы, используемой в организации? Что общего между ними подтипами? Что излагается в каждом из разделов этих политик?
12. 12.Назовите основные стадии жизненного цикла ПолИБ? Из каких шагов они состоят? Какие из этик шагов выполняются итерационно и почему?
13. 13.Отдельно сформулируйте цель к основным мероприятия, осуществляемые на каждом шаге жизненною цикла ПолИБ.
14. Как происходит процесс информирования в отношении ПолИБ?
15. Для чего и кем осуществляются ревизия, мониторинг и аудит ПолИБ? В чем отличия этих шагов жизненного цикла ПолИБ?
16. Что понимаемся под исключениями в ПолИБ?
17. Зачем необходим пересмотр ПолИБ?
18. В каких случаях ПолИБ может быть аннулирована?
19. Что такое «роль»? Какие роли связаны с использованием ПолИБ?
20. Какие виды ответственности связаны со всеми стадиями жизненного цикла ПолИБ?
21. Какими принципами необходимо руководствоваться при установлении ответственности в отношении соблюдения ПолИБ?
22. Дайте определения «ОИБ», «управления ИБ» и «СУИБ» организации.
23. Опишите деятельность по ОИБ организации как процесс. Каковы его входные и выходные данные, ресурсы и управляющие воздействия?
24. Как процесс ОИБ организации связан с процессами основной деятельности организации?
25. Каковы основные этапы процесса управления ИБ ИТТ
26. Что является хорошей практикой при выборе области действия СУИБ? Какие стратегии выбора области действии СУИБ существуют?
27. Какие факторы необходимо учитывать при выборе области действия СУИБ?
28. Какие параметры процессов являются наиболее значимыми при выборе области действия проектируемой СУИБ?
29. Что входит в документальное обеспечение СУИБ? Каковы этапы его жизненного цикла?
30. Какие уровни документов включает в себя иерархия документов СУИБ? Какие виды конкретных документа создаются на каждом из уровней?

31. И чем состоит основное отличие между понятиями документ и запись?

32. В чем заключается процесс управления документами и записями?

33. Какова взаимосвязь между понятиями ПолИБ и политика СУИБ?

34. Что должна включать в себя политика СУИБ?

35. На каких панах руководство организации должно продемонстрировать свою приверженность к разработке, реализации, эксплуатации, мониторингу, анализу, сопровождению и совершенствованию СУИБ?

36. В чем состоит основная необходимость участия высшего руководства в жизненном цикле СУИБ?

37. Каким образом при использовании циклической модели PDCA применительно к СУИБ требования и ожидания к результатам ОИБ преобразуются я управляемую ИБ?

38. Дате определение «процесс управления ИБ» организации.

39. Какие действия и процессы выполняются на стадии планировании СУИБ? Каковы задачи данного этапа?

40. Специалистов каких подразделении необходимо включать в рабочую группу по построению СУИБ и почему?

41. Какие действия и процессы выполняются на стадии реализации и внедрения СУИБ? Каковы задачи данного этапа?

42. Какие действия и процессы выполняются на стадии проверки СУИБ? Каковы задачи данною этапа?

43. Какие действия и процессы выполняются на стадии совершенствования СУИБ. Каковы задачи данного этана?

44. В чем разница и сходство между понятиями корректирующего и предупреждающего действия?

45. Почему в рамках процесса подхода к управлению ИБ следует особое внимание уделять мониторингу и анализу результативности и эффективности СУИБ?

46. В чем состоят различия между основными свойствами процессов: эффективность и результативностъ?

47. Что входит в понятие «задание процесса у правления ИБ»?

48. Какие этапы включает в себя идентификация процессов управления ИБ в организации и какие действия необходимо предпринять в рамках этих этапов?

49. Каковы основные преимущества документировании процессов управления ИБ в организации и наличия подробных карт процессов организации?

50. Каковы основные элементы процесса мониторинга процессов управления ИБ организации?

Контрольно-измерительные материалы итогового контроля

1. Почему так важны организационный и кадровый аспекты управления ИБ?
2. Какова главная цель организационного управления ИБ?
3. Какие два основные вида деятельности составляют основу управления ИБ?
4. Как можно проиллюстрировать централизацию и децентрализацию руководства ИБ?
5. Каковы четыре базовые модели организационного управления ИБ? Рассмотрите их подробно и сравните их достоинства и недостатки.
6. Каковы участники процесса управления ИБ в организации и их зоны ответственности?
7. Каковы обязанности высшего руководства организации по управлению ИБ?
8. Каковы основное назначение и функции Управляющего совета по вопросам ИБ?
9. Чем должен заниматься Координационный комитет по вопросам управления ИБ?

10. Рассмотрите четыре группы организационных мероприятий по управлению ИБ.

11. Расскажите о Службе ИБ - целях ее создания, стоящих перед ней задачах, статусе в организации, нормативно-правовой базе деятельности.

12. Какие разделы должны содержаться в Положении о Службе ИБ?

13. Перечислены полномочия Службы ИБ.

14. Назовите основные функции Службы ИБ.

15. Рассмотрите и сравните различные варианты создания Службы ИБ.

16. Какие сотрудники должны входить в состав Службы ИБ?

17. Каковы основные задачи руководителя Службы ИБ?

18. Какие квалификационные характеристики и направления, относящиеся к области ИБ, рассмотрены в Едином квалификационном справочнике, утвержденном Приказом Министерства здравоохранения и социального развития РФ от 22 апреля 2009 г. № 205?

19. Какая информация по квалификационным характеристикам в области ИБ представлена в Государственном классификаторе направлений и специальностей в разделе укрупненного направления 090000 - «Информационная безопасность»?

20. По каким группам компетенций должно осуществляться обучение специалистов в области ИБ? На основании какого документа синтезирован этот список?

21. Какие обобщенные названия должностей этих специалистов сегодня можно встретить в зарубежных и российских организациях?

22. Как может быть наглядно представлена взаимосвязь обобщенных должностей, групп компетенций и направлений ПД в области ОИБ? Рассмотрите более подробно эту связь на любом примере группы компетенций.

23. Как отражаются вопросы ИБ в должностных обязанностях работников организации?

24. Как осуществляется учет вопросов ИБ при найме персонала на работу?

25. Определите задачи, функции, обязанности, права и ответственность администратора ИБ подразделения организации.

26. Для чего необходимо сотрудничество между организациями и консультации со специалистами в области ИБ?

27. Дайте определения управления доступом (логическим), правил разграничения доступа, объекта и субъекта доступа.

28. Каковы назначение и основные достоинства унифицированных систем управления идентификацией?

29. Рассмотрите основное содержание политики в отношении логического доступа.

30. На основе каких документов, процедур и средств осуществляется управление доступом пользователей к активам организации?

31. Как должны назначаться и использоваться привилегированные права доступа?

32. Руководствуясь какими рекомендациями пользователи должны выбирать и изменять свои пароли?

33. Как осуществляется управление паролями?

34. В чем заключается политика чистого стола/экрана?

35. Каковы особенности сетевой аутентификации (по сравнению с аутентификацией при доступе к отдельному компьютеру)? Какие виды такой аутентификации рекомендуется использовать?

36. Какие средства защиты применяются в современных сетях - интранетах и экстранетах?

37. Какими защитными мерами осуществляется управление доступом к прикладным системам (приложениям)?

38. Как и на основе чего обеспечить ИБ при работе пользователей с переносными устройствами и в дистанционном режиме?

39. Какие процедуры при управлении защищенной передачей данных и операционной деятельности должны быть регламентированы?

40. В чем заключается принцип разделений полномочий пользователей?

41. Какие мероприятия по управлению ИБ обеспечивают разделение сред разработки и про-

мышленной эксплуатации систем?

42. Какие специальные вопросы требуется решить при управлении СОИ сторонними лицами и организациями?

43. Что важно учитывать при планировании нагрузки и приемке систем?

44. На что необходимо обратить внимание при защите ПО и СОИ от вредоносных программ?

45. На основе чего осуществляется управление сетевыми ресурсами?

46. Как организуется защита носителей информации?

47. Каков порядок обмена информацией и ПО?

48. Что дает резервирование информации? Как правильно его организовать?

49. Подробно рассмотрите процесс выработки требований к ИБ систем. Какие виды требований ИБ обычно должны быть определены?

50. Каковы области формулирования требований для эшелонированной защиты вычислительной среды организации?

51. Как обеспечивается ИБ системных файлов?

52. Кратко перечислите основные средства криптографической информации, используемые в сетевой среде.

53. Каковы основные цели и функции процессов управления конфигурациями, изменениями и обновлениями? Что между ними общего и в чем различия?

54. Опишите жизненный цикл процесса управления обновлениями ИБ.

55. Как осуществляется физическая защита и защита от воздействия окружающей среды? В чем разница понятий логического и физического доступа?

56. Как в организации создаются охраняемые зоны? Что такое периметр безопасности?

57. Как защитить оборудование организации от различных видов угроз?

58. Каковы основные функции монитора безопасности объектов (МБО) и монитора безопасности субъектов (МБС) в изолированной программное среде (ИПС), в чём их отличие друг от друга.

59. Почему для реализации ИПС необходимо требовать наличия в КС контроля порождения объектов?