МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования«Поволжский государственный университет сервиса»

(ФГБОУ ВО «ПВГУС»)

|  |  |
| --- | --- |
| УТВЕРЖДЕНО |  |
| на заседании Высшей школы интеллектуальных систем и кибертехнологий |
|  |
| Протокол от | 02.12.2022 г. | № | 4 |

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

(фонд оценочных средств) для проведения промежуточной аттестации

по дисциплине

|  |
| --- |
| **«Комплексное обеспечение информационной безопасности автоматизированных систем и объектов информатизации»** |

наименование дисциплины

|  |  |
| --- | --- |
| по образовательной программе высшего образования – программе | **магистратуры** |
| **«Информационная безопасность интеллектуальных и информационно-аналитических систем»** |

наименование образовательной программы

|  |
| --- |
| **10.04.01 «Информационная безопасность»** |
| шифр, наименование направления подготовки / специальности |

|  |  |
| --- | --- |
| Составитель | Филиппова Ольга Александровна, доцент, Высшая школа интеллектуальных систем и кибертехнологий; к.э.н., доцент |
|  | ФИО, должность, структурное подразделение, ученая степень, ученое звание |

Тольятти

 2022

**1. Паспорт фонда оценочных средств (далее – ФОС)**

**1.1. Планируемые результаты обучения по дисциплине**

|  |  |  |  |
| --- | --- | --- | --- |
| Код компетенции | Наименование компетенции | Код и наименование индикаторов достижения компетенции | Основание (ПС) \*для профессиональных компетенций |
| ОПК-2 | Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности | ИОПК-2.2. Проектирует систему обеспечения информационной безопасности, ее компоненты и подсистемы |  |
| ПК-3 | Способен оценить угрозы безопасности информации автоматизированной системы и обосновать необходимость её защиты | ИПК-3.1. Строит модель угроз безопасности информации, обрабатываемой автоматизированной системы;ИПК-3.2. Обосновывает необходимость защиты информации в интеллектуальных и информационно-аналитических системах. | 06.033 Специалист по защите информации в автоматизированных системах |
| ПК-4 | Способен разработать архитектуру системы защиты информации и провести анализ уязвимости и эффективности её модели с учетом специфики деятельности организации и обрабатываемых данных | ИПК-4.3. Разрабатывает архитектуру системы защиты информации автоматизированных систем, а также интеллектуальных и информационно-аналитических систем в частности | 06.033 Специалист по защите информации в автоматизированных системах |

В результате изучения дисциплины обучающийся должен:

**владеть навыками:** разработки технических проектов систем (подсистем либо компонент систем) обеспечения информационной безопасности; мониторинга и аудита угроз информационной безопасности информационных систем, а также методами обоснования необходимости их защиты; разработки архитектуры систем защиты информации автоматизированных информационно-аналитических и интеллектуальных систем с учетом специфики деятельности предприятия (организации) и обрабатываемых данных

**уметь:** проектировать системы обеспечения информационной безопасности, ее компоненты и подсистемы, а также управлять подобными проектами и принимать эффективные проектные решения в условиях неопределенности и риска; проводить мониторинг угроз безопасности информационных систем, а также обосновывать необходимость защиты информации и определять комплекс мер для обеспечения информационной безопасности в интеллектуальных и информационно-аналитических системах; разрабатывать единую архитектуру системы всесторонней защиты информации автоматизированных информационно-аналитических и интеллектуальных систем

**знать:** жизненный цикл и принципы организации информационных систем в соответствии с требованиями по защите информации; методы принятия эффективных проектных решений в условиях неопределенности и риска ПО; методы анализа возникающей неопределенности и риска и оценки их негативных последствий; методику построения модели угроз информационной безопасности, а также принципы формирования комплекса мер по обеспечению информационной безопасности предприятия(организации) и организации информационных систем в соответствии с требованиями по защите информации; принципы, а также современные методологии и технологии построения эффективной и безопасной архитектуры информационно-аналитических систем

**1.2. Содержание дисциплины**

|  |  |  |
| --- | --- | --- |
| № | Тема (раздел дисциплины) (в соответствии с РПД) | Код компетенции и индикаторы достижения компетенций |
|  | Базовые понятия сущности комплексного обеспечения информационной безопасности (КОИБ) | ОПК-2.ИОПК-2.2.ПК-3.ИПК-3.1 |
|  | Сущностная характеристика компонентов КОИБ и определение условий их функционирования | ОПК-2.ИОПК-2.2.ПК-3.ИПК-3.2 |
|  | Разработка модели КОИБ и её архитектуры | ПК-4.ИПК-4.3 |
|  | Выполнение курсового проекта | ОПК-2.ИОПК-2.2.ПК-3.ИПК-3.1ИПК-3.2ПК-4.ИПК-4.3 |

**1.3. Система оценивания по дисциплине**

Дисциплина изучается в течение одного семестра.

Форма промежуточной аттестации по дисциплине – экзамен/защита КП.

|  |  |  |
| --- | --- | --- |
| **Форма проведения****промежуточной аттестации** | **Шкалы оценки уровня****сформированности результатов обучения** | **Шкала оценки уровня****освоения дисциплины** |
| Уровневая шкала оценки компетенций | 100 бальная шкала, % | 100 бальная шкала, % | 5-балльная шкала,дифференцированная оценка/балл |
| **Экзамен / защита КП** | допороговый | ниже 61 | ниже 61 | «неудовлетворительно» / 2 |
| пороговый | 61-85,9 | 61-69,9 | «удовлетворительно» / 3  |
| 70-85,9 | «хорошо» / 4 |
| повышенный  | 86-100 | 86-100 | «отлично» / 5 |

**2. Перечень оценочных материалов для проведения промежуточной аттестации**

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в ходе текущего контроля успеваемости (в процессе проведения практических занятий, тестирования, опросов).

В ходе проведения промежуточной аттестации осуществляется контроль и оценка результатов освоения компетенций.

**Примерная тематика курсовых проектов**

**ОПК-2: ИОПК-2.2; ПК-3: ИПК-3.1, ИПК-3.2; ПК-4: ИПК-4.3**

1. Разработка комплексной системы защиты информации производственного предприятия

2. Организация системы мониторинга информационной безопасности организации

3. Разработка комплекса мероприятий противодействия внутренним угрозам предприятия

4. Особенности использования методов защиты информации при разработке веб-приложения

5. Организация защиты информационных ресурсов корпоративной сети предприятия

6. Методы идентификации субъекта и их применение

7. Разработка комплексной системы защиты информации коммерческого предприятия

8. Проект управления рисками информационной безопасности предприятия

9. Особенности разработки комплексной системы защиты информации в банковской сфере

10. Программно-аппаратные средства шифрования

11. Разработка комплексной системы защиты информации вуза

12. Разработка системы инженерно-технической защиты информации предприятия

13. Разработка политики информационной безопасности в организации

14. Разработка программы проведения аудита безопасности информации в организации.

15. Разработка частной модели угроз безопасности персональных данных при их обработке в ИСПДн

16. Разработка мероприятий по контролю эффективности функционирования системы защиты информации в компании

17. Разработка комплекса мер по защите информации от утечки по техническим каналам в организации

18. Разработка организационно-распорядительных документов, регламентирующих обеспечение информационной безопасности сведений, составляющих ПДн

19. Организация обработки персональных данных в компании (организации)

20. Методы и способы защиты информации от утечки по техническим каналам

21. Методы и средства защиты информации от несанкционированного доступа в сети Интернет

22. Разработка предложений по обеспечению безопасности информации в ключевых системах информационной инфраструктуры

23. Разработка предложений по обеспечению безопасности информации в автоматизированных системах управления технологическими процессами

24. Анализ уязвимостей в социальных сетях

25. Исследование безопасности мобильных платформ

26. Разработка рекомендаций по использованию средств защиты от DDOS-атак в корпоративных сетях

27. Разработка рекомендаций по организации защиты информационной системы малого предприятия

28. Совершенствование системы защиты информации производственного предприятия

**Перечень вопросов к защите курсового проекта**

**ОПК-2: ИОПК-2.2; ПК-3: ИПК-3.1, ИПК-3.2; ПК-4: ИПК-4.3**

1. Основная цель курсового проекта. Каковы исходные данные?

2. Актуальность темы проекта

3. Применяемые методы исследования

4. Методы и инструменты, используемые при выполнении курсового проекта

5. Информационные технологии, используемые при выполнении курсового проекта

6. Этапы выполнения курсового проекта

7. Практическая значимость работы

**Перечень вопросов и заданий для подготовки к экзамену**

**ОПК-2: ИОПК-2.2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности**

1. Какие основные компоненты входят в понятие комплексного обеспечения информационной безопасности (КОИБ)?

2. Каким образом определяется сущность комплексного обеспечения информационной безопасности?

3. Какие принципы лежат в основе комплексного обеспечения информационной безопасности?

4. Какие цели и задачи ставит перед собой комплексное обеспечение информационной безопасности?

5. Какие принципиальные отличия между комплексным и частным обеспечением информационной безопасности?

6. Какие проблемы решает комплексное обеспечение информационной безопасности?

7. Какие методы и подходы используются в рамках комплексного обеспечения информационной безопасности?

8. Каким образом комплексное обеспечение информационной безопасности взаимодействует с другими системами и процессами в организации?

9. Какие технологии и инструменты чаще всего применяются в комплексном обеспечении информационной безопасности?

10. Какие риски и угрозы могут быть устранены или снижены с помощью комплексного обеспечения информационной безопасности?

11. Каким образом комплексное обеспечение информационной безопасности способствует защите конфиденциальности, целостности и доступности данных?

12. Какие этапы включает в себя процесс разработки комплексного обеспечения информационной безопасности?

13. Каким образом оценивается эффективность комплексного обеспечения информационной безопасности?

14. В каком документе ФСТЭК РФ регламентируются требования к организации защиты информации, содержащейся в информационной системе?

15. На основании чего осуществляется разработка системы защиты информации информационной системы?

16. Какие этапы работ включает в себя разработка концепции информационной системы в соответствие с ГОСТ 34.601?

17. Какие этапы работ включает в себя разработка технического проекта информационной системы в соответствие с ГОСТ 34.601?

18. Опишите определение комплексной системы защиты информации.

19. Что включают в себя организационно-правовые мероприятия по защите информации?

20. Что представляет собой семирубежная модель защиты информации?

**ПК-3: ИПК-3.1, ИПК-3.2. Способен оценить угрозы безопасности информации автоматизированной системы и обосновать необходимость её защиты**

21. Из каких этапов состоит процесс оценки угроз безопасности информации?

22. Что включает в себя этап определения негативных последствий при оценке угроз информационной безопасности?

23. Что включает в себя этап определения объектов воздействия при оценке угроз информационной безопасности?

24. Что включает в себя этап оценки реализации угроз и определение их актуальности при оценке угроз информационной безопасности?

25. Какие системы управления базами данных соответствуют 6 классу защиты?

26. Какие системы управления базами данных соответствуют 5 классу защиты?

27. Какие системы управления базами данных соответствуют 4 классу защиты?

28. Какие исходные данные используются для определения негативных последствий от реализации угроз безопасности информации?

29. Какие существуют нарушители информационной безопасности в зависимости от уровня их возможностей?

30. В каких случаях возможна угроза безопасности информации по определению?

31. Что относится к программно-аппаратным средствам защиты информации по определению?

32. Что можно назвать уязвимостью в системе информационной безопасности по определению?

33. Что является границей оценки угроз безопасности информации?

34. Каких экспертов рекомендуется включать в состав экспертной группы для оценки угроз безопасности информации?

35. В отношении каких параметров оценки угроз информационной безопасности рекомендуется проводить экспертную оценку?

36. Какие методы оценки угроз безопасности информации вы знаете?

37. В чём сущность метода угроз и уязвимостей (ThreatandVulnerabilityAssessment, TVA)?

38. В чём заключается метод пентестинга?

39. Какие инструменты применяются для анализа уязвимостей системы?

40. Какие шаги вы предпримете для обоснования необходимости защиты информации в вашей автоматизированной системе?

41. Каковы основные угрозы безопасности информации, с которыми сталкиваются автоматизированные системы?

42. Какие методы защиты информации вы бы рекомендовали для минимизации угроз безопасности в автоматизированных системах?

43. Как вы определяете критические активы и данные, требующие особой защиты?

44. Какие действия вы бы предприняли для обнаружения потенциальных угроз безопасности информации?

45. Как оценить эффективность мер безопасности, принятых для защиты информации в системе?

46. Какие технологии и методы шифрования информации используются для обеспечения безопасности данных?

47. Каков процесс анализа уязвимостей и угроз безопасности перед внедрением новых компонентов в автоматизированную систему?

48. Какие меры предосторожности существуют для защиты информации от внутренних угроз?

49. Какие средства мониторинга безопасности используют для оперативного обнаружения инцидентов?

50. Как проводится анализ последствий возможных нарушений безопасности информации в системе?

**ПК-4: ИПК-4.3. Способен разработать архитектуру системы защиты информации и провести анализ уязвимости и эффективности её модели с учетом специфики деятельности организации и обрабатываемых данных**

51. Какие основные принципы следует учитывать при разработке архитектуры системы защиты информации?

52. Какие стадии включает процесс разработки архитектуры системы защиты информации?

53. Что представляет собой архитектура системы информационной безопасности?

54. Каким базовым принципам должна соответствовать оптимальная система информационной безопасности?

55.Какие средства являются основными компонентами системы информационной безопасности?

56. Какие виды обеспечения информационно-вычислительной системы, необходимы для создания и поддержания функционирования системы защиты информации?

57.В чём заключается основная цель архитектуры системы безопасности?

58. Каковы основные задачи архитектуры системы безопасности?

59. В чём заключается принцип построения архитектуры системы безопасности «защиты в глубину»?

60. В чём заключается принцип построения архитектуры системы безопасности «минимизации привилегий»?

61. В чём заключается принцип построения архитектуры системы безопасности «разделения обязанностей»?

62. В чём заключается принцип построения архитектуры системы безопасности «аутентификации и авторизации»?

63. В чём заключается принцип построения архитектуры системы безопасности «непрерывности работы»?

64. В чём заключается принцип построения архитектуры системы безопасности «постоянного обновления и адаптации»?

65. Какова особенность архитектуры системы безопасности «Периметр»?

66. Какова особенность архитектуры системы безопасности «Защита по уровням»?

67. Какова особенность архитектуры системы безопасности «Централизованная»?

68. Какова особенность архитектуры системы безопасности «Распределенная»?

69. В чём заключается процесс анализа уязвимостей ИС?

70. Какие методы анализа уязвимостей можно выделить в сфере информационной безопасности?

71. Какие минимальные требования защиты от несанкционированного доступа к данным устанавливает документация ФСТЭК РФ?

72. Как обеспечить совместимость новой модели защиты информации с уже существующими системами и приложениями?

73. В чём особенность автоматизированной системы в защищенном исполнении?

74. Как осуществляется защита информации от утечки по техническим каналам утечки информации?

75. Какие мероприятия по защите от утечки информации по техническим каналам относятся к организационным?

76. Какие мероприятия по защите от утечки информации по техническим каналам относятся к техническим мероприятиям с использованием пассивных средств защиты информации?

77.Какие мероприятия по защите от утечки информации по техническим каналам относятся к техническим мероприятиям с использованием активных средств защиты информации?

78. Как провести анализ эффективности мер по предотвращению угроз безопасности информации в рамках модели защиты данных?

79. Какие этапы разработки системы защиты информации выделяют на предпроектной стадии и стадии проектирования?

80. Какие этапы разработки системы защиты информации выделяют на стадии ввода в эксплуатацию?

**Вопросы для подготовки к экзамену с «ключами» правильных ответов**

| **№** | **Содержание вопроса** | **Правильный ответ** |
| --- | --- | --- |
| **ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности** |
|  | Какие основные компоненты входят в понятие комплексного обеспечения информационной безопасности (КОИБ)? | Основные компоненты комплексного обеспечения информационной безопасности (КОИБ) включают в себя:1. технические средства защиты информации;2. организационные меры безопасности;3. физическая защита информации;4. управление рисками и угрозами;5. контроль и мониторинг;6. соблюдение законодательства и стандартов.Эти компоненты взаимодействуют между собой для обеспечения комплексной защиты информации организации от угроз и рисков. |
|  | Каким образом определяется сущность комплексного обеспечения информационной безопасности? | Сущность комплексного обеспечения информационной безопасности определяется как системный подход к защите информации в организации. Она включает в себя не только отдельные технические решения или организационные и процессуальные меры, но и их взаимодействие и согласованное применение для обеспечения полноценной защиты информации от различных угроз. |
|  | Какие принципы лежат в основе комплексного обеспечения информационной безопасности? | Основные принципы комплексного обеспечения информационной безопасности:1. Принцип защиты по всем аспектам, включая технические, организационные, процессуальные и человеческие.2. Принцип целостности.3. Принцип конфиденциальности.4. Принцип доступности только тем пользователям, которые имеют на это право.5. Принцип управления рисками.6. Принцип непрерывности: постоянного мониторинга, анализа и обновления мер защиты.7. Принцип соответствия законодательству. |
|  | Какие цели и задачи ставит перед собой комплексное обеспечение информационной безопасности? | Комплексное обеспечение информационной безопасности ставит перед собой следующие цели и задачи:1. Защита конфиденциальности информации.2. Обеспечение целостности информации.3. Гарантирование надёжного и стабильного доступа к информации.4. Предотвращение угроз и рисков.5. Обеспечение непрерывности работы организации.6. Соответствие законодательству и нормативам.7. Обучение и осведомленность сотрудников по вопросам безопасности информации. |
|  | Какие принципиальные отличия между комплексным и частным обеспечением информационной безопасности? | Частное обеспечение информационной безопасности обычно фокусируется на конкретных аспектах безопасности, таких как защита от вирусов, шифрование данных, контроль доступа и т.д. Комплексное обеспечение информационной безопасности включает в себя широкий спектр мер и методов защиты информации, охватывая все аспекты безопасности: конфиденциальность, целостность, доступность, управление рисками и т.д. |
|  | Какие проблемы решает комплексное обеспечение информационной безопасности? | Основные проблемы, которые решает комплексное обеспечение информационной безопасности: защита конфиденциальности; гарантирование целостности данных и информационных систем; обеспечение непрерывной доступности информационных ресурсов и сервисов для пользователей; установление подлинности пользователей и управление доступом к информационным ресурсам; идентификация, оценка и управление угрозами; мониторинг и анализ безопасности обучение и осведомленность пользователей; соблюдение законодательства и стандартов. |
|  | Какие методы и подходы используются в рамках комплексного обеспечения информационной безопасности? | Основные методы и подходы для обеспечения защиты информации: использование нескольких уровней защиты; применение шифрования данных для защиты конфиденциальности и целостности информации при передаче и хранении; использование методов идентификации и аутентификации пользователей; строгое управление доступом к информационным ресурсам на основе принципа минимальных привилегий; постоянный мониторинг сетевого трафика, журналов событий, уязвимостей и аномалий для обнаружения инцидентов безопасности и своевременного реагирования на угрозы. |
|  | Каким образом комплексное обеспечение информационной безопасности взаимодействует с другими системами и процессами в организации? | Системы безопасности информации интегрируются с ИТ-инфраструктурой организации для обеспечения защиты сетей, серверов, баз данных и других информационных ресурсов. Комплексное обеспечение информационной безопасности встраивается в бизнес-процессы организации и помогает соблюдать требования законодательства и стандартов. Системы мониторинга и анализа безопасности взаимодействуют с процессами управления инцидентами для своевременного обнаружения и реагирования на угрозы безопасности. |
|  | Какие технологии и инструменты чаще всего применяются в комплексном обеспечении информационной безопасности? | Наиболее распространенные технологии и инструменты: системы управления доступом (IAM – IdentityandAccessManagement); системы обнаружения вторжений (IDS/IPS – IntrusionDetection/PreventionSystems); системы защиты от вредоносного ПО (Antivirus, Anti-Malware); системы мониторинга безопасности (SIEM – SecurityInformationandEventManagement); файрволы; технологии шифрования; системы управления уязвимостями; системы резервного копирования и восстановления данных. |
|  | Какие риски и угрозы могут быть устранены или снижены с помощью комплексного обеспечения информационной безопасности? | Комплексное обеспечение информационной безопасности позволяет снизить риск возникновения различных угроз и защитить информационные ресурсы организации от разнообразных атак: несанкционированный доступ к данным, вредоносное ПО и кибератаки, утечка конфиденциальной информации, сетевые угрозы и утеря или повреждение данных. |
|  | Каким образом комплексное обеспечение информационной безопасности способствует защите конфиденциальности, целостности и доступности данных? | Для защиты конфиденциальности данных применяют шифрование данных, управление доступом (IAM), а также мониторинг и аудит.Для защиты целостности данных - системы контроля целостности и резервное копирование.Для обеспечения доступности данных - защиту от отказа обслуживания (DDoS) и планирование бизнес-континуитета.Комплексное обеспечение информационной безопасности комбинирует различные технологии, методы и процедуры, чтобы обеспечить полную защиту конфиденциальности, целостности и доступности данных организации. |
|  | Какие этапы включает в себя процесс разработки комплексного обеспечения информационной безопасности? | Процесс разработки комплексного обеспечения информационной безопасности включает в себя следующие этапы:1. Анализ и планирование.2. Проектирование.3. Разработка.4. Тестирование.5. Внедрение.6. Поддержка и сопровождение. |
|  | Каким образом оценивается эффективность комплексного обеспечения информационной безопасности? | Для оценки эффективности комплексного обеспечения информационной безопасности определяются: уровень угроз и рисков, уровень защиты, уровень уязвимостей, уровень реагирования системы безопасности, проверяется соответствие комплексного обеспечения информационной безопасности действующим стандартам и требованиям законодательства, проводится тестирование и аудит системы безопасности. |
|  | В каком документе ФСТЭК РФ регламентируются требования к организации защиты информации, содержащейся в информационной системе? | Приказ ФСТЭК России от 11 февраля 2013 г. N 17. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах |
|  | На основании чего осуществляется разработка системы защиты информации информационной системы? | Разработка системы защиты информации информационной системы осуществляется в соответствии с техническим заданием на создание информационной системы и (или) техническим заданием (частным техническим заданием) на создание системы защиты информации информационной системы с учетом ГОСТ 34.601 "Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания", ГОСТ Р 51583 и ГОСТ Р 51624 |
|  | Какие этапы работ включает в себя разработка концепции информационной системы в соответствие с ГОСТ 34.601? | Разработка концепции информационной системы (ИС) включает в себя следующие этапы работ:1. Изучение объекта2. Проведение необходимых научно-исследовательских работ3. Разработка вариантов концепции ИС и выбор варианта концепции ИС, удовлетворяющего требованиям пользователя4. Оформление отчета о выполненной работе |
|  | Какие этапы работ включает в себя разработка технического проекта информационной системы в соответствие с ГОСТ 34.601? | Разработка технического проекта информационной системы (ИС) включает в себя следующие этапы работ:1. Разработка проектных решений по системе и ее частям2. Разработка документации на ИС и ее части3. Разработка и оформление документации на поставку изделий для комплектования ИС и (или) технических требований (технических заданий) на их разработку4. Разработка заданий на проектирование в смежных частях проекта объекта автоматизации |
|  | Опишите определение комплексной системы защиты информации. | Комплексная система защиты информации (КСЗИ) – это совокупность организационно-правовых и инженерно-технических мероприятий, направленных на обеспечение защиты информации от разглашения, утечки и несанкционированного доступа. |
|  | Что включают в себя организационно-правовые мероприятия по защите информации? | Организационно-правовые мероприятия включают в себя создание концепции информационной безопасности, а также: составление должностных инструкций для пользователей и обслуживающего персонала; создание правил администрирования компонент информационной системы, учета, хранения, размножения, уничтожения носителей информации, идентификации пользователей; разработку планов действий в случае выявления попыток несанкционированного доступа к информационным ресурсам системы, выхода из строя средств защиты, возникновения чрезвычайной ситуации и обучение правилам информационной безопасности пользователей. |
|  | Что представляет собой семирубежная модель защиты информации? | В соответствии с семирубежной моделью ЗИ при организации защиты информации на предприятии в качестве объектов защиты рассматриваются:1)прилегающая к предприятию территория;2)здания предприятия;3)рабочие помещения и помещения, предназначенные для обработки информации с ограниченным доступом; помещения, предназначенные для ведения переговоров, в ходе которых оглашаются сведения ограниченного доступа; хранилища носителей информации;4)физические поля; системы, линии и средства связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации с ограниченным доступом;5)аппаратные средства, средства и системы информатизации и другие технические средства защиты информации;6)программные средства;7)информационные ресурсы, содержащие конфиденциальную информацию; сведения, отнесенные любому виду тайн; носители информации и средства их транспортировки |
|  | **ПК-3. Способен оценить угрозы безопасности информации автоматизированной системы и обосновать необходимость её защиты** |
|  | Из каких этапов состоит процесс оценки угроз безопасности информации? | Оценка угроз безопасности информации включает следующие этапы:1) определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации;2) определение возможных объектов воздействия угроз безопасности информации;3) оценку возможности реализации (возникновения) угроз безопасности информации и определение их актуальности. |
|  | Что включает в себя этапопределения негативных последствий при оценке угроз информационной безопасности? | Этап определения негативных последствийпри оценке угроз информационной безопасности включает в себя: анализ документации систем и сетей и иных исходных данных, а также определение негативных последствий от реализации угроз |
|  | Что включает в себя этапопределения объектов воздействия при оценке угроз информационной безопасности? | Этап определения объектов воздействия при оценке угроз информационной безопасности включает в себя: анализ документации систем и сетей и иных исходных данных; инвентаризацию систем и сетей; определение групп информационных ресурсов и компонентов систем и сетей. |
|  | Что включает в себя этапоценки реализации угроз и определение их актуальности при оценке угроз информационной безопасности? | Этап оценки реализации угроз и определение их актуальности при оценке угроз информационной безопасности включает в себя: определение источников угроз; оценку способов реализации угроз; оценку актуальности угроз. |
|  | Какие системы управления базами данных соответствуют 6 классу защиты? | Системы управления базами данных, соответствующие 6 классу защиты, применяются в значимых объектах критической информационной инфраструктуры 3 категории значимости, в государственных информационных системах 3 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 3 класса защищенности, в информационных системах персональных данных при необходимости обеспечения 3 и 4 уровня защищенности персональных данных. |
|  | Какие системы управления базами данных соответствуют 5 классу защиты? | Системы управления базами данных соответствующие 5 классу защиты, применяются в значимых объектах критической информационной инфраструктуры 2 категории значимости, в государственных информационных системах 2 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 2 класса защищенности, в информационных системах персональных данных при необходимости обеспечения 2 уровня защищенности персональных данных. |
|  | Какие системы управления базами данных соответствуют 4 классу защиты? | Системы управления базами данных, соответствующие 4 классу защиты, применяются в значимых объектах критической информационной инфраструктуры 1 категории значимости, в государственных информационных системах 1 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности, в информационных системах персональных данных при необходимости обеспечения 1 уровня защищенности персональных данных, в информационных системах общего пользования II класса. |
|  | Какие исходные данные используются для определения негативных последствий от реализации угроз безопасности информации? | 3.2. Исходными данными для определения негативных последствий от реализации угроз безопасности информации являются:а) общий перечень угроз безопасности информации, содержащийся в банке данных угроз безопасности информации ФСТЭК России, а также отраслевые модели угроз безопасности информации;б) нормативные правовые акты РФ, в соответствии с которыми создаются и функционируют системы и сети, содержащие в том числе описание назначения, задач (функций) систем и сетей, состав обрабатываемой информации и ее правовой режим;в) документация на сети и системы (в части сведений о назначении и функциях систем и сетей, о составе и архитектуре систем и сетей);г) технологические, производственные карты или иные документы, содержащие описание основных процессов обладателя информации, оператора;д) результаты оценки рисков (ущерба), проведенной обладателем информации или оператором. |
|  | Какие существуют нарушители информационной безопасности в зависимости от уровня их возможностей? | В зависимости от уровня возможностей нарушители подразделяются на нарушителей, обладающих:1. базовыми возможностями по реализации угроз безопасности информации (Н1);2. базовыми повышенными возможностями по реализации угроз безопасности информации (Н2);3. средними возможностями по реализации угроз безопасности информации (Н3);4. высокими возможностями по реализации угроз безопасности информации (Н4). |
|  | В каких случаях возможна угроза безопасности информации по определению? | Угроза безопасности информации возможна, если имеются нарушитель или иной источник угрозы, объект, на который осуществляются воздействия, способы реализации угрозы безопасности информации, а реализация угрозы может привести к негативным последствиям. |
|  | Что относится к программно-аппаратным средствам защиты информации по определению? | Программно-аппаратное средство - это устройство, состоящее из аппаратного обеспечения и функционирующего на нем программного обеспечения, участвующее вформировании, обработке, передаче или приеме информации. |
|  | Что можно назвать уязвимостью в системе информационной безопасности по определению? | Уязвимость - это недостаток программного (программно-технического) средства или системы и сети в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации. |
|  | Что является границей оценки угроз безопасности информации? | Граница оценки угроз безопасности информации - это совокупность информационных ресурсов и компонентов систем и сетей, в пределах которой обеспечивается защита информации в соответствии с едиными правилами и процедурами, а также контроль за реализованными мерами защиты информации. |
|  | Каких экспертов рекомендуется включать в состав экспертной группы для оценки угроз безопасности информации? | В состав экспертной группы для оценки угроз безопасности информации рекомендуется включать экспертов из:1. подразделения по защите информации;2. подразделения, ответственного за цифровую трансформацию (ИТ-специалистов);3. подразделения, ответственного за эксплуатацию сетей связи;4. подразделения, ответственного за эксплуатацию автоматизированных систем управления;5. подразделения обладателя информации или оператора, ответственного за выполнение основных процессов. |
|  | В отношении каких параметров оценки угроз информационной безопасности рекомендуется проводить экспертную оценку? | Экспертную оценку рекомендуется проводить в отношении следующих параметров:а) негативного последствия от реализации угроз безопасности информации;б) целей нарушителей по реализации угроз безопасности информации;в) сценария действий нарушителей при реализации угроз безопасности информации. |
|  | Какие методы оценки угроз безопасности информации вы знаете? | Основными методами оценки угроз безопасности информации можно назвать следующие:1. Метод оценки угроз уязвимостей (Threat and Vulnerability Assessment, TVA);2. Анализ рисков (RiskAnalysis);3. Методика моделирования угроз безопасности информации;4. Методология анализа безопасности приложений (ApplicationSecurityAssessment);5. Пентестинг (PenetrationTesting). |
|  | В чём сущность метода угроз и уязвимостей (ThreatandVulnerabilityAssessment, TVA)? | Методология угроз и уязвимостей (ThreatandVulnerabilityAssessment, TVA) - это метод, который позволяет идентифицировать угрозы и уязвимости в информационной системе, оценить их потенциальные последствия и разработать соответствующие меры защиты. |
|  | В чём заключается метод пентестинга? | Пентестинг (PenetrationTesting) - метод проверки безопасности информационной системы путем имитации реальных атак для выявления уязвимостей и оценки эффективности защитных мер. |
|  | Какие инструменты применяются для анализа уязвимостей системы? | Для анализа уязвимостей системы существует множество специализированных инструментов, которые помогают выявить потенциальные проблемы в безопасности и обеспечить безопасность информационной системы. Некоторые из наиболее распространенных инструментов для анализа уязвимостей: 1. Nessus - один из самых популярных инструментов для сканирования уязвимостей в сетевых устройствах, операционных системах и приложениях.2. OpenVAS - открытый инструмент для сканирования уязвимостей и анализа уязвимостей в сетевых устройствах и приложениях.3. Qualys - облачный сервис для обнаружения и анализа уязвимостей в реальном времени.4. Metasploit - инструмент для тестирования на проникновение, который используется для проведения эксплойтов и тестирования безопасности системы путем имитации атак.5. BurpSuite - инструмент для тестирования безопасности веб-приложений. |
|  | Какие шаги вы предпримете для обоснования необходимости защиты информации в вашей автоматизированной системе? | Для обоснования необходимости защиты информации в автоматизированной системе можно провести следующие шаги:1. Оценка ценности информации.2. Оценка угроз и уязвимостей3. Оценка последствий нарушения безопасности.4. Сравнение с законодательством и стандартами безопасности.5. Разработка стратегии защиты информации.6. Обоснование бюджета и вложения ресурсов в обеспечение безопасности информации. |
|  | Каковы основные угрозы безопасности информации, с которыми сталкиваются автоматизированные системы? | Существует множество угроз безопасности информации, с которыми автоматизированные системы могут столкнуться. Некоторые из основных угроз включают в себя: кибератаки и хакерские атаки, утечки данных, отказ в обслуживании системы (DDoS), физические угрозы, социальная инженерия - мошеннические практики, недостаточная защита данных, внутренние угрозы. |
|  | Какие методы защиты информации вы бы рекомендовали для минимизации угроз безопасности в автоматизированных системах? | Для минимизации угроз безопасности в автоматизированных системах рекомендуется применять комплексный подход, включающий следующие методы защиты информации: шифрование данных, многоуровневая защита данных, регулярное обновление программного обеспечения, сложные пароли и механизмы аутентификации, резервное копирование данных, мониторинг безопасности, обучение сотрудников, физическая безопасность, аудит безопасности, разработка политики безопасности предприятия. |
|  | Как вы определяете критические активы и данные, требующие особой защиты? | Определение критических активов и данных, требующих особой защиты, зависит от специфики бизнеса и отрасли компании. Однако, обычно такие активы и данные могут включать в себя следующие категории: конфиденциальная информация, персональные данные, инфраструктура и оборудование, ключевые процессы и приложения, системы защиты от кибератак. |
|  | Какие действия вы бы предприняли для обнаружения потенциальных угроз безопасности информации? | Для обнаружения потенциальных угроз безопасности информации, можно применить следующие действия: 1. Постоянный мониторинг журналов событий, системных и сетевых логов;2. Использование систем обнаружения вторжений (IDS/IPS).3. Проведение регулярного сканирования системы на наличие уязвимостей.4. Обучение сотрудников правилам безопасности.5. Мониторинг сетевого трафика.6. Регулярные аудиты безопасности систем и приложений 7. Использование системы управления угрозами. |
|  | Как оценить эффективность мер безопасности, принятых для защиты информации в системе? | оценить эффективность мер безопасности, принятых для защиты информации в системе необходимо использовать следующие методы:1. Проведение пенетрационного тестирования.2. Постоянный мониторинг событий и журналов, а также анализ сетевого трафика 3. Регулярные аудиты безопасности систем и приложений.4. Использование метрик безопасности для количественной оценки эффективности принятых мер.5. Использование систем отчетности о состоянии безопасности системы, ее уязвимостях, инцидентах и принятых мерах. |
|  | Какие технологии и методы шифрования информации используются для обеспечения безопасности данных? | Наиболее распространенные методы шифрования данных: симметричное шифрование, асимметричное шифрование, хэширование, цифровые подписи, протоколы безопасной передачи данных и квантовое шифрование. |
|  | Каков процесс анализа уязвимостей и угроз безопасности перед внедрением новых компонентов в автоматизированную систему? | Процесс анализа уязвимостей и угроз безопасности перед внедрением новых компонентов в автоматизированную систему включает следующие шаги:1. Идентификация угроз и уязвимостей.2. Оценка рисков утечки информации.3. Разработка стратегии защиты данных.4. Выбор подходящих мер защиты безопасности.5. Тестирование системы безопасности.6. Мониторинг и аудит систем безопасности.7. Обучение персонала. |
|  | Какие меры предосторожности существуют для защиты информации от внутренних угроз? | Для защиты информации от внутренних угроз на предприятии можно применить следующие меры безопасности:1. Ограничить доступ к конфиденциальной информации только тем сотрудникам, которым это необходимо.2. Установить систему мониторинга и аудита доступа к информации.3. Проводить постоянное обучение сотрудников правилам соблюдения информационной безопасности.4. Разделить обязанности сотрудников таким образом, чтобы никто не имел полный контроль над всеми аспектами информационных систем. 5. Усложнить систему шифрования данных.6. Установить систему предупреждения об утечках данных.7. Постоянно обновлять политику безопасности. |
|  | Какие средства мониторинга безопасности используют для оперативного обнаружения инцидентов? | Наиболее распространенные средства мониторинга безопасности:1. Системы управления журналами событий (SIEM).2. Системы обнаружения вторжений (IDS/IPS).3. Антивирусное программное обеспечение.4. Системы обнаружения утечек данных (DLP).5. Системы мониторинга доступа к данным.6. Системы аналитики безопасности.7. Средства мониторинга эндпоинтов.8. Системы регистрации событий в системе (Elasticsearch, Logstash, Kibana). |
|  | Как проводится анализ последствий возможных нарушений безопасности информации в системе? | Анализ последствий возможных нарушений безопасности информации в системе проводится в несколько этапов:1. Идентификация нарушения.2. Оценка ущерба.3. Изоляция и устранение уязвимости.4. Восстановление данных и систем.5. Анализ причин и рекомендации по предотвращению.51 Это может включать в себя обновление политик безопасности, проведение обучения сотрудников и другие меры. |
|  | **ПК-4. Способен разработать архитектуру системы защиты информации и провести анализ уязвимости и эффективности её модели с учетом специфики деятельности организации и обрабатываемых данных** |
|  | Какие основные принципы следует учитывать при разработке архитектуры системы защиты информации? | Следует выделить следующие основные принципы построения систем компьютерной безопасности, которые необходимо учитывать при их проектировании и разработке: системность подхода; комплексность решений; непрерывность защиты; разумная достаточность средств защиты; простота и открытость используемых механизмов защиты; минимум неудобств пользователям и минимум накладных расходов на функционирование механизмов защиты. Системный подход к защите компьютерных систем предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ИС. |
|  | Какие стадии включает процесс разработки архитектуры системы защиты информации? | При первоначальной разработке и реализации системы защиты ИС обычно выделяют три стадии:1.Первая стадия — выработка требований к системе защиты информации.2.Вторая стадия - определение способов защиты информации.3. Третья стадия - построение системы информационной безопасности, т.е. реализация механизмов защиты как комплекса процедур и средств обеспечения безопасности информации. |
|  | Что представляет собой архитектура системы информационной безопасности? | Архитектура системы информационной безопасности — это совокупность технических средств защиты и организационных мер, направленных на противодействие актуальным угрозам и на снижение рисков для защиты активов компании. |
|  | Каким базовым принципам должна соответствовать оптимальная система информационной безопасности? | Оптимальная архитектура СИБ должна соответствовать нескольким базовым принципам:1. Воплощать в себе концепцию многоэшелонированной защиты.2. Иметь возможности для расширения и роста, горизонтального и вертикального масштабирования.3. Быть простой в эксплуатации и диагностике.4. Иметь возможности для интеграции со всеми необходимыми инфраструктурными системами компании.5. Реально повышать уровень защищённости. |
|  | Какие средства являются основными компонентами системы информационной безопасности? | Основными компонентами СИБ являются:- Средства защиты периметра.- Средства криптографической защиты информации.- Средства защиты внутренней сетевой инфраструктуры.- Средства защиты серверной инфраструктуры и рабочих мест.- Средства мониторинга состояния средств защиты, сбора и корреляции событий ИБ, сканеры уязвимостей. |
|  | Какие виды обеспечения информационно-вычислительной системы, необходимы для создания и поддержания функционирования системы защиты информации (СЗИ)? | Состав и содержание видов обеспечения для создания СЗИ определяются следующим образом:1) техническое обеспечение - совокупность технических средств, необходимых для технической поддержки решения всех тех задач защиты информации, решение которых может потребоваться в процессе функционирования СЗИ; 2) математическое обеспечение - совокупность математических методов, моделей и алгоритмов, необходимых для оценок уровня защищенности информации и решения других задач защиты;3) программное обеспечение - совокупность программ, реализующих программные средства защиты, а также программ, необходимых для решения задач управления механизмами защиты. К ним должны быть! отнесены также сервисные и вспомогательные программы СЗИ;4) информационное обеспечение - совокупность систем классификации и кодирования данных о защите информации, массивы данных СЗИ, а также входные и выходные документы СЗИ;5) лингвистическое обеспечение - совокупность языковых средств, необходимых для обеспечения взаимодействия компонентов СЗИ между собой, с компонентами АСОД и с внешней средой.6) организационно-правовое обеспечение, как компонент СЗИ, представляет собою организованные совокупности организационно-технических мероприятий и организационно-правовых актов. |
|  | В чём заключается основная цель архитектуры системы безопасности? | Цель архитектуры системы безопасности – обеспечить конфиденциальность, целостность и доступность информации, а также защитить систему от несанкционированного доступа, вредоносных программ и других угроз. |
|  | Каковы основные задачи архитектуры системы безопасности? | Основные задачи архитектуры системы безопасности:1. должна предоставлять механизмы идентификации и аутентификации пользователей и устройств;2. должна определять права доступа пользователей и устройств к различным ресурсам и функциям системы; 3. должна обеспечивать конфиденциальность, целостность и доступность данных;4. должна включать механизмы обнаружения и предотвращения инцидентов безопасности;5. должна включать механизмы обучения и осведомления пользователей о правилах безопасности, угрозах и методах защиты;6. должна включать механизмы управления уязвимостями, такие как сканирование уязвимостей, патч-управление и управление обновлениями; 7. должна включать механизмы управления инцидентами безопасности. |
|  | В чём заключается принцип построения архитектуры системы безопасности «защиты в глубину»? | Принцип «защиты в глубину» предполагает использование нескольких уровней защиты для обеспечения безопасности системы. Каждый уровень должен иметь свои механизмы и методы защиты, чтобы в случае преодоления одного уровня, другие уровни могли предотвратить или ограничить возможные угрозы. |
|  | В чём заключается принцип построения архитектуры системы безопасности «минимизации привилегий»? | Согласно принципу «минимизации привилегий», каждый пользователь или процесс должен иметь только необходимые привилегии для выполнения своих задач. Это ограничивает возможности злоумышленников и снижает риск несанкционированного доступа или злоупотребления привилегиями. |
|  | В чём заключается принцип построения архитектуры системы безопасности «разделения обязанностей»? | Принцип «разделения обязанностей» предполагает разделение различных функций и обязанностей между разными пользователями или процессами. Например, администратор системы не должен иметь полный доступ ко всей информации, а только к той, которая необходима для выполнения его задач. Это помогает предотвратить возможность злоупотребления полномочиями и уменьшает риск внутренних угроз. |
|  | В чём заключается принцип построения архитектуры системы безопасности «аутентификации и авторизации»? | Принцип «аутентификации и авторизации» предполагает проверку подлинности пользователей и предоставление им соответствующих прав доступа. Аутентификация подтверждает, что пользователь является тем, за кого себя выдает, а авторизация определяет, какие ресурсы и функции доступны пользователю. Это помогает предотвратить несанкционированный доступ и защищает конфиденциальность и целостность данных. |
|  | В чём заключается принцип построения архитектуры системы безопасности «непрерывности работы»? | Принцип «непрерывности работы» предполагает наличие механизмов и процедур для обеспечения непрерывной работы системы даже в случае возникновения инцидентов безопасности или сбоев. Резервное копирование данных, репликация системы и мониторинг состояния системы являются примерами мер, принимаемых для обеспечения непрерывности работы. |
|  | В чём заключается принцип построения архитектуры системы безопасности «постоянного обновления и адаптации»? | Принцип «постоянного обновления и адаптации» предполагает постоянное обновление и адаптацию архитектуры системы безопасности в соответствии с новыми угрозами и технологическими изменениями. Это включает в себя регулярное обновление программного обеспечения, применение патчей безопасности, анализ новых уязвимостей и принятие соответствующих мер для устранения рисков. |
|  | Какова особенность архитектуры системы безопасности «Периметр»? | В архитектуре «Периметр» основной упор делается на защиту периметра сети. Она включает в себя использование брандмауэров, интранетов и экстранетов для контроля доступа к сети и защиты от внешних угроз. Внутри сети также могут быть использованы дополнительные меры безопасности, такие как системы обнаружения вторжений и антивирусные программы. |
|  | Какова особенность архитектуры системы безопасности «Защита по уровням»? | В архитектуре «Защита по уровням» безопасность обеспечивается на разных уровнях системы. Каждый уровень имеет свои механизмы защиты и контроля доступа. Например, на уровне сети могут быть установлены брандмауэры и системы обнаружения вторжений, на уровне операционной системы – антивирусные программы и системы контроля доступа, а на уровне приложений – механизмы аутентификации и шифрования. |
|  | Какова особенность архитектуры системы безопасности «Централизованная»? | В архитектуре «Централизованная» все механизмы безопасности управляются и контролируются централизованно. Это позволяет обеспечить единые политики безопасности и централизованное управление доступом к ресурсам. Например, централизованная архитектура может включать в себя центральный сервер аутентификации, систему управления доступом и систему мониторинга безопасности. |
|  | Какова особенность архитектуры системы безопасности «Распределенная»? | В архитектуре «Распределенная» механизмы безопасности распределены по разным узлам или уровням системы. Это позволяет обеспечить отказоустойчивость и более эффективное использование ресурсов. Например, распределенная архитектура может включать в себя распределенные брандмауэры, системы обнаружения вторжений и системы контроля доступа. |
|  | В чём заключается процесс анализа уязвимостей ИС? | Анализ уязвимостей – процесс, направленный на обнаружение всевозможных угроз, уязвимых мест и рисков вероятного несанкционированного проникновения третьих лиц в инфосистему компании. Уязвимость выступает в качестве слабого места информационной системы компании. Угроза – фактор оказания отрицательного воздействия со стороны киберпреступника, которое потенциально становится причиной компрометации конфиденциальных и других видов защищаемых данных. |
|  | Какие методы анализа уязвимостей можно выделить в сфере информационной безопасности? | Существует несколько основных методов анализа уязвимостей в сфере информационной безопасности:1. Сканирование уязвимостей сети и приложений.2. Пентестинг (PenetrationTesting): это контролируемое тестирование системы на наличие уязвимостей путем моделирования атаки злоумышленника. 3. Анализ программного кода приложений.4. Анализ настроек системы, сетевых устройств и приложений с целью выявления ошибок конфигурации.5. Моделирование угроз (ThreatModeling).6. Аудит безопасности системы защиты информации. |
|  | Какие минимальные требования защиты от несанкционированного доступа к данным устанавливает документация ФСТЭК РФ? | Для противодействия киберугрозам ФСТЭК регулярно обновляет базу уязвимостей, вносит новые рекомендации в аттестацию, сертификацию оборудования, программного обеспечения.Выполнение требований регулятора по технической защите информации обязательно при:- оказании услуг информационной безопасности (ТЗКИ, СКЗИ);- проведении работ по обеспечению государственной и банковской тайн;- выполнении обязанностей оператора персональных данных (ПД);- передаче информации посредством сети Интернет. |
|  | Как обеспечить совместимость новой модели защиты информации с уже существующими системами и приложениями? | Чтобы обеспечить совместимость новой модели защиты информации с уже существующими системами и приложениями необходимо следующее:1. Провести анализ уже существующих систем, приложений и инфраструктуры, чтобы понять их особенности, требования к безопасности и возможные уязвимости.2. Разработать детальный план внедрения новой модели защиты, учитывая особенности уже существующих систем и приложений. Определите этапы внедрения, риски и меры по их снижению.3. Убедиться, что новые решения по защите информации могут интегрироваться с уже существующими системами и приложениями. Провести тестирование совместимости.4. Обучить персонал работе с новой моделью защиты информации и объяснить им особенности интеграции с уже существующими системами. Это поможет предотвратить ошибки при внедрении. |
|  | В чём особенность автоматизированной системы в защищенном исполнении? | Автоматизированная система в защищенном исполнении (АСЗИ) - автоматизированная система, реализующая информационную технологию выполнения установленных функций в соответствии с требованиями стандартов и/или иных нормативных документов по защите информации. |
|  | Как осуществляетсязащита информации от утечки по техническим каналам утечки информации? | Защита информации от утечки по техническим каналам утечки информации достигается проведением организационных и технических мероприятий.Организационное мероприятие - это мероприятие по защите информации, проведение которого не требует применения специально разработанных технических средств.Техническое мероприятие - это мероприятие по защите информации, предусматривающее применение специальных технических средств, а также реализацию технических решений. |
|  | Какие мероприятия по защите от утечки информации по техническим каналам относятся к организационным? | К основным организационным мероприятиям по защите от утечки информации по техническим каналам относятся:- определение границ контролируемой зоны;- привлечение к проведению работ по защите информации организаций, имеющих лицензию на ТЗКИ;- категорирование и аттестация объектов ОТСС и выделенных для проведения закрытых мероприятий помещений по выполнению требований обеспечения защиты информации;- использование на объекте сертифицированных ОТСС и ВТСС;- организация контроля и ограничение доступа к ИС и в защищаемые помещения;- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;- отключение на период закрытых мероприятий технических средств, имеющих элементы, выполняющие роль электроакустических преобразователей, от линий связи и т.д. |
|  | Какие мероприятия по защите от утечки информации по техническим каналам относятсяктехническим мероприятиям с использованием пассивных средств защиты информации? | К техническим мероприятиям по защите от утечки информации по техническим каналам с использованием пассивных средств защиты информации относятся:- контроль и ограничение доступа к ИС и в выделенные помещения с помощью технических средств и систем;- локализация излучений: экранирование ОТСС и их соединительных линий; заземление ОТСС и экранов их соединительных линий; звукоизоляция выделенных помещений.- развязывание информационных сигналов: установка специальных средств защиты в ВТСС, обладающих «микрофонным эффектом»; установка специальных диэлектрических вставок в оплетки кабелей электропитания, труб систем отопления, водоснабжения и канализации, имеющих выход за пределы контролируемой зоны; установка автономных или стабилизированных источников электропитания ОТСС; установка устройств гарантированного питания ОТСС; установка в цепях электропитания ОТСС, а также в линиях осветительной и розеточной сетей выделенных помещений помехоподавляющих фильтров. |
|  | Какие мероприятия по защите от утечки информации по техническим каналам относятсяк техническим мероприятиям с использованием активных средств защиты информации? | К техническим мероприятиям по защите от утечки информации по техническим каналам с использованием активных средств защиты информации относятся:- пространственное зашумление: пространственное электромагнитное зашумление с использованием генераторов шума или создание прицельных помех; создание акустических и вибрационных помех с использованием генераторов акустического шума; подавление диктофонов в режиме записи с использованием подавителей диктофонов.- линейное зашумление: линейное зашумление линий электропитания; линейное зашумление посторонних проводников и соединительных линий ВТСС, имеющих выход за пределы контролируемой зон.- уничтожение закладных устройств: уничтожение закладных устройств, подключенных к линии, с использованием специальных генераторов импульсов (выжигателей "жучков"). |
|  | Как провести анализ эффективности мер по предотвращению угроз безопасности информации в рамках модели защиты данных? | Анализ эффективности мер по предотвращению угроз безопасности информации в рамках модели защиты данных состоит из следующих этапов:1. Определение ключевых показателей эффективности мер по предотвращению угроз безопасности информации.2. Сбор данных о реализации мер по предотвращению угроз безопасности информации. 3. Анализ данных, оценка эффективности мер по предотвращению угроз безопасности информации, выявление слабых мест и уязвимости.4. Оценка рисков, связанных с угрозами безопасности информации.5. Сравнение с лучшими практиками в области информационной безопасности. 6. Разработка плана улучшений мер по предотвращению угроз безопасности информации. 7. Мониторинг и корректировка. |
|  | Какие этапы разработки системы защиты информации выделяют на предпроектной стадии и стадии проектирования? | Выделяют следующие этапы разработки системы защиты информации:1. на предпроектной стадии:- разработка технико-экономического обоснования- разработка технического задания.2. на стадии проектирования:- разработка технического проекта- разработка рабочего проекта |
|  | Какие этапы разработки системы защиты информации выделяют на стадии ввода в эксплуатацию? | На стадии ввода в эксплуатациювыделяют следующие этапы разработки системы защиты информации:1. ввод в действие отдельных элементов системы2. комплексная стыковка элементов системы3. опытная эксплуатация4. приёмочные испытания и сдача в эксплуатацию. |