**Вопросы на зачет**

1. Способность специалиста в области информационной безопасности

определять круг задач в рамках поставленной цели и выбирать

оптимальные способы их решения, исходя из действующих правовых

норм, имеющихся ресурсов и ограничений

Ответ: Разработка и реализация проектов(УК-2)

2. Реализация профессионального стандарта «СПЕЦИАЛИСТ ПО

ИНФОРМАЦИОННЫМ РЕСУРСАМ» в области информационной

безопасности

Ответ: ПК-2

3. Безопасность жизнедеятельности в профессиональной деятельности

Ответ: УК-8. Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов

4. Способность специалиста в области информационной безопасности

администрировать операционные системы, системы управления базами

данных, вычислительные сети

Ответ: Опк 4-2

5. Способность специалиста в области информационной безопасности

создавать и поддерживать в повседневной жизни и в профессиональной

деятельности безопасные условия жизнедеятельности для сохранения

природной среды, обеспечения устойчивого развития общества, в том

числе при угрозе и возникновении чрезвычайных ситуаций и военных

конфликтов

Ответ: УК-8(безопасность жизнедеятельности)

6. Способность специалиста в области информационной безопасности

формировать предложения по оптимизации структуры и функциональных

процессов объекта защиты и его информационных составляющих с целью

повышения их устойчивости к деструктивным воздействиям на

информационные ресурсы

Ответ: ОПК-2.2

7. Способность специалиста в области информационной безопасности

использовать необходимые математические методы для решения задач

профессиональной деятельности

Ответ: ОПК-3

8. Какая категория атак относится к атакам на конфиденциальность?

Ответ: Вмешательство и наблюдение за трафиком и его анализ.

9. Области профессиональной — деятельности и (или) сферы

профессиональной — деятельности бакалавров по — направлению

"Информационная безопасность"

Ответ: Образование и наука. Связь, информационные т коммуникационные технологии. Обеспечение безопасности. Сфера обороны и безопасности. Сфера правоохранительной деятельности

10. Способность специалиста в области информационной безопасности

применять нормативные правовые акты, нормативные и методические

документы, регламентирующие деятельность по защите информации в

сфере профессиональной деятельности

Ответ: ОПК-5

11. Способность специалиста в области информационной безопасности

проводить подготовку исходных данных для проектирования подсистем,

средств обеспечения защиты информации и для технико-экономического

обоснования соответствующих проектных решений

Ответ: ОПК-12

12. Управление информацией из различных источников для обеспечения

информационной безопасности объекта защиты и его информационных

ресурсов

Ответ: ПК-2.1

13. Способность специалиста в области информационной безопасности

осуществлять деловую коммуникацию в устной и письменной формах на

государственном языке Российской Федерации и иностранном(ых)

языке(ах)

Ответ: УК-4

14. Способность специалиста в области информационной безопасности

выбирать технологии обработки информации и проектировать системы

защиты информации автоматизированных систем

Ответ: ПК-2

15. Разработка, изменение и согласование архитектуры программного

обеспечения с системным аналитиком и архитектором программного

обеспечения информационной безопасности

Ответ: ПК-4.2

16. Как определить, в какой момент можно считать свою среду безопасной?

Ответ:

17. Какие факторы можно использовать при реализации схемы

многофакторной аутентификации для пользователей, которые входят на

рабочие станции, находящиеся в защищенной среде и используемые

более чем одним человеком?

Ответ: Фактор знания, фактор владения

18. Формирование задания для устранения выявленных недочётов по

результатам анализа информационной безопасности объекта защиты и

его информационных ресурсов

Ответ: ОПК - 10 (возможно)

19. Гражданская позиция в профессиональной деятельности

Ответ: УК-10. Способен формировать нетерпимое отношение к коррупционному поведению

20. Рассматривая триаду СПА и гексаду Паркера, определите, какие

преимущества и недостатки есть у каждой модели?

Ответ: 1. Преимущества:

Триада CIA гарантирует, что данным или информационной системе можно доверять, и что они редактируется только уполномоченными лицами;

Гексада Паркера предоставляет физический контроль над устройством или другой средой хранения информации только тем, кто имеет на это право.

Недостатки:

у триады CIA обеспечивается доступ к данным или информационной системе только уполномоченному лицу;

Гексада Паркера не позволяет пользователю выдать себя за другого, что не даёт ему оставаться анонимным

21. Способность специалиста в области информационной безопасности

разрабатывать, внедрять и сопровождать комплекс мер по обеспечению

безопасности объекта защиты с применением локальных нормативных

актов и стандартов информационной безопасности

Ответ: ОПК-2.3. Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению

безопасности объекта защиты с применением локальных нормативных актов и стандартов

информационной безопасности;

22.Способность специалиста в области информационной безопасности

проводить эксперименты по заданной методике и обработку их

результатов

Ответ: ОПК-11. Способен проводить эксперименты по заданной методике и обработку их результатов

23.Способность специалиста в области информационной безопасности

управлять своим временем, выстраивать и реализовывать траекторию

саморазвития на основе принципов образования в течение всей жизни

Ответ: УК-6. Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни./ Самоорганизация и саморазвитие (в том числе здоровьесбережение)

24. Способность специалиста в области информационной безопасности

проводить анализ функционального процесса объекта защиты и его

информационных составляющих с целью выявления возможных

источников информационных угроз, их возможных целей, путей

реализации и предполагаемого ущерба

Ответ: ОПК-2.1. Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба

25. Самоорганизация и саморазвитие в профессиональной деятельности

Ответ: Самоорганизация и саморазвитие (в том числе здоровьесбережение) УК-6. Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни

УК-7. Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности

26. Как называется процесс, в котором клиент аутентифицируется на сервере,

а сервер аутентифицируется на клиенте?

Ответ: Аунтификация

27. Коммуникация в профессиональной деятельности

Ответ: Коммуникация. УК-4. Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)

28. Способность специалиста в области информационной безопасности

применять необходимые физические законы и модели для решения задач

профессиональной деятельности

Ответ: ОПК-4. Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности

29. Управление (менеджмент) информационными ресурсами в области

информационной безопасности

Ответ: ГОСТ Р ИСО/МЭК 27004-2021 Система менеджмента информационной безопасности (СМИБ) представляет собой руководство, управление, администрирование, разработку и создание, а также эффективное использование и контроль методов и средств, направленных на обеспечение информационной безопасности (ИБ) предприятия.

Ответ\_2: **ПК-2**

30. Если вы разрабатываете систему многофакторной аутентификации для

среды, в которой число травмированных или пользователей с

инвалидностью выше обычного, например в больнице, какие факторы

аутентификации Вы могли бы использовать, а какие нет?Почему?

Ответ: Обычно это пароль, PIN-код или кодовая фраза, или набор секретных вопросов и соответствующие ответы на них, известные только человеку.

То, что у вас есть (фактор владения)

До смартфонов пользователи носили токены или смарт-карты, которые генерировали одноразовый пароль или код доступа (OTP), который можно было ввести в онлайн-приложение.

То, что вы есть (фактор неотъемлемости)

Биометрические данные о человеке варьируются от отпечатков пальцев, сканирования сетчатки глаза, распознавание лиц , а также распознавание голоса для поведения (например, насколько сильно или быстро человек набирает текст или проводит пальцем по экрану).

То, где вы находитесь. ( фактор расположения).

Физическое местоположение пользователя.

31. Оформление документов по ГОСТу

Ответ: ГОСТ Р 7.0.97-2016

32. Как измерить частоту, с которой Вам не удается аутентифицировать

«правильных» пользователей в биометрической системе?

Ответ: **Количество ложных приемов делённое на количество попыток идентификации**

33. Здоровьесбережение в профессиональной деятельности

Ответ: УК-7. Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности

34. Объясните разницу между уязвимостью и угрозой

Ответ: Угрозы как возможные опасности совершения какого-либо действия, направленного против объекта защиты, проявляются не сами по себе, а через уязвимости, приводящие к нарушению безопасности информации на конкретном объекте информатизации.

Ответ\_2: Уязвимость - это любая характеристика или свойство информационной системы, использование которой нарушителем может привести к реализации угрозы.(Можно контролировать.) Угроза - это потенциально возможное событие, явление или процесс, которое посредством воздействия на компоненты информационной системы может привести к нанесению ущерба чьим-либо интересам.(Как правило, не поддается контролю.)

35. Способность специалиста в области информационной безопасности

управлять информационными ресурсами в задачах информационной

безопасности

Ответ: ОПК-2. Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;

36. Способность специалиста в области информационной безопасности

выполнять работы по установке, настройке, администрированию,

обслуживанию и проверке работоспособности отдельных программных,

программно-аппаратных (в том числе криптографических) и технических

средств защиты информации автоматизированных систем

Ответ: ОПК-4.3. Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем;

37. Сущность экспериментально-исследовательской деятельности

Ответ: Сущность экспериментального метода состоит в том, что он направлен на исследование причинно-следственных отношений между изучаемыми объектами (на определение – вызывает ли изменение одной переменной изменение другой переменной). В нем присутствуют черты, характерные для теоретического познания, - выделение стороны объекта, явления, интересующей исследователя, и абстрагирование от других его сторон.

38. Анализ изменения угроз информационной безопасности объекта защиты

в процессе эксплуатации объекта защиты

Ответ: Приказ ФСТЭК России от 25.12.2017 N 239 (ред. от 20.02.2020) Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (Зарегистрировано в Минюсте России 26.03.2018 N 50524)

Построение систем защиты информации начинается с создания модели угроз. Для предприятий риски зависят от сферы деятельности и готовности информационной системы к отражению атак. Модель необходимо строить, с учетом результатов анализа угроз информационной безопасности и после классификации типов нарушителей.

39. Автоматизация подготовки документов

Ответ: В практическом смысле – это внедрение системы, позволяющей с минимальным участием человека создавать, проводить и хранить договоры, платежки, счета, акты, приказы, а также контролировать все этапы их редактирования, согласования или исполнения. Также это способ модернизировать порядок ведения дел в компании, сделать его более простым, эффективным, прозрачным, лучше защищенным от ошибок.

40. Обработка результатов аналитической деятельности по анализу

информационной безопасности объекта защиты и его информационных

ресурсов

Ответ: Анализ состояния информационной безопасности (или оценка защищенности информационных систем) представляет собой структурированный повторяемый процесс, который помогает компаниям вовремя находить и устранять возникающие опасности. По результатам анализа формируются рекомендации, направленные на изменение внутренних процессов компании. Также анализ необходим для определения вероятности возникновения опасности и масштаба возможного ущерба.

Анализ информационной безопасности помогает понять, какой должна быть система защиты для дальнейшего ее проектирования, модернизации, внедрения необходимых средств защиты, что, в свою очередь, позволит обеспечить требуемый уровень защиты данных предприятия от неправомерного доступа. Существует несколько различных методологий, которые можно использовать при анализе защищенности. Давайте рассмотрим их подробнее.

41. Способность специалиста в области информационной безопасности

осуществлять разработку требований и проектирование программного

обеспечения в сфере информационной безопасности

Ответ: **ПК-4**

42. Реализация профессионального стандарта «ПРОГРАММИСТ» в области информационной безопасности

Ответ:

43. Способность специалиста в области информационной безопасности при

решении профессиональных задач организовывать защиту информации

ограниченного доступа в соответствии с нормативными правовыми

актами, нормативными и методическими документами Федеральной

службы безопасности Российской Федерации, Федеральной службы по

техническому и экспортному контролю

Ответ: ОПК-6

44. Применение языка Рушоп для задач автоматизации профессиональной

деятельности

Ответ: Автоматизация тестирования

Ответ\_2: **Генерация документов на основе входных данных с применением шаблонов, парсинг информации из публичных источников**

45. Разработка принципиальных вариантов концептуальной архитектуры

системы информационной безопасности объекта защиты, выбор и

обоснование выбранного варианта концептуальной архитектуры

Ответ:

46. Разработка и реализация проектов в профессиональной деятельности

Ответ: УК-2 (без разветвлений)

47. Способность специалиста в области информационной безопасности в

качестве технического специалиста принимать участие в формировании

политики — информационной — безопасности, организовывать и

поддерживать выполнение комплекса мер по — обеспечению

информационной безопасности, управлять процессом их реализации на

объекте защиты

Ответ: ОПК-10

48. Способность специалиста в области информационной безопасности

осуществлять поиск, критический анализ и синтез информации,

применять системный подход для решения поставленных задач

Ответ: УК-1

49. Составление комплекса правил, процедур, практических приёмов,

принципов и методов, средств обеспечения информационной

безопасности объектазащиты

Ответ: Профиль “Организация и технологии защиты информации”

50. Какой термин Вы могли бы использовать для описания полезности

данных?

Ответ: Статистика

Ответ\_2: “Ценные данные”

Ответ\_3: **Полезные данные – это данные с частой обращаемостью. Поэтому подойдёт термин «горячие» данные.**

51. Способность специалиста в области информационной безопасности

осуществлять концептуальное, функциональное и логическое

проектирование систем среднего и крупного масштаба и сложности в

сфере информационной безопасности

Ответ:

52. Сущность проектно-технологической деятельности

Ответ: сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности; проведение проектных расчетов элементов систем обеспечения информационной безопасности;

участие в разработке технологической и эксплуатационной документации;

проведение предварительного технико-экономического обоснования проектных расчетов;

53. Концептуальное, функциональное и логическое проектирование систем

среднего и крупного масштаба и сложности в области информационной

безопасности

Ответ: профессиональный стандарт СИСТЕМНЫЙ АНАЛИТИК 06.022 ( пс 6)

54. Системноеи критическое мышление в профессиональной деятельности

Ответ: ук-5 (без разветвлений)

Ответ\_2: УК-1

55. Способность специалиста в области информационной безопасности

осуществлять диагностику и мониторинг систем защиты

автоматизированных систем

Ответ: ОПК - 4.4

56. Межкультурное взаимодействие в профессиональной деятельности

Ответ: УК - 5 Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах (Межкультурные взаимодействия)

57. Сущность организационно-управленческой деятельности

Ответ: это особый вид деятельности, который начал изучаться, описываться и нормироваться только во второй половине XX века. До этого времени управление существовало как «искусное действие» – индивидуальное мастерство человека или группы лиц.

Ответ: осуществление организационно-правового обеспечения информационной безопасности объекта защиты;

организация работы малых коллективов исполнителей;

участие в совершенствовании системы управления информационной безопасностью;

изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа; контроль эффективности реализации политики информационной безопасности объекта защиты

58. Если Вы используете пароль из восьми символов, содержащий только

строчные буквы, даст ли увеличение длины до десяти символов

значительный прирост безопасности? Почему?

Ответ: Даёт, потому что время на подбор пароля значительно увеличивается

Ответ\_2: да, тк при 8 символах вариаций пароля окло 36 триллионов а при 10 около 1 секстилиона

Ответ\_3: **Да, так как количество комбинаций вырастает, что влечёт за собой увеличение времени подбора**

59. Разработка требований и проектирование программного обеспечения в

области информационной безопасности

Ответ: ПК – 4.0

60. В вашей среде установлены серверы Microsoft Internet Information Sevices(IIS) и обнаружен новый червь, атакующий веб-серверы Apache, чего у Вас нет?

Ответ: нет брандмауэра, черви через него не должны проходить на сервер

61. Способность специалиста в области информационной безопасности выполнять экспериментальные исследования защищенности автоматизированных систем.

Ответ: ПК-3

62. Назовите три причины, почему одного лишь паспорта недостаточно для идеальной аутентификации.

Ответ: паспорт можно купить, подделать и украсть

63. Проектирование структур данных, баз данных и программных интерфейсов систем информационной безопасности.

Ответ:

64. Способность специалиста в области информационной безопасности определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

Ответ: УК-2

65. Способность специалиста в области информационной безопасности проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах

Ответ: ОПК-4.1

66. Командная работа и лидерство в профессиональной деятельности

Ответ: УК-3

67. Способность специалиста в области информационной безопасности анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма

Ответ: ОПК-13

68. Типы задач профессиональной деятельности

Ответ: стереотипные, диагностические, типовые, тренировочные, графические

69. Способность специалиста в области информационной безопасности применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числеотечественного производства, для решения задач профессиональной деятельности

Ответ: ОПК-2

70. Анализ возможности реализации требований к программному обеспечению информационной безопасности

Ответ: ПК - 4.1

71. Способность специалиста в области информационной безопасности использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности

Ответ: ОПК-7

72. Описание системного контекста и границ системы информационной безопасности объекта защиты, определение ключевых свойств и ограничений системы информационной безопасности объектазащиты

Ответ: ПК - 3.1

73. Способность специалиста в области информационной безопасности поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности

Ответ: УК-7

74. Если можно использовать паспорт в качестве основы схемы аутентификации, какие шаги можно добавить в процесс, чтобы перейти к многофакторной аутентификации?

Ответ: номер моб. телефона, электронной почты и ответ на контрольный вопрос

75. На основании гексады Паркера объясните, какие принципы будут затронуты, если Вы потеряете партию зашифрованных резервных лент, содержащих персональные данные и данные о платежах ваших клиентов?

Ответ: конфиденциальность, целостность, доступность, владение, полезность

76. Если вы разрабатываете для своей среды новую политику, которая требует от вас использования сложных и автоматически сгенерированных паролей, уникальных для каждой системы и длиной не менее 30 символов, например «!Ра8}В955@%417$3РТ,24п4а#!КВ537,!», что пострадает от такого подхода?

Ответ: Такой пароль невозможно запомнить, а значит где-то придется его записать

77. Язык разметки Мarkdown

Ответ: синтаксис форматирования обычного текста

Ответ\_2: Markdown — удобочитаемый язык разметки, который прозрачно конвертируется в HTML. Его можно открывать и изменять в любом редакторе текста. Широко используется для написания документаций и README файлов

78. Сущность эксплуатационной деятельности

Ответ:

79. Установление категории важности проблем с информационной безопасностью объекта защиты с использованием оценки последствий, установление причины проблем в области информационной безопасности, которые могут быть устранены за счёт автоматизации

Ответ:

80. Какой биометрический фактор описывает, насколько хорошо характеристика сопротивляется изменениям с течением времени?

Ответ: **Неизменность**

81. Способность специалиста в области информационной безопасности

осуществлять подбор, изучение и обобщение научно-технической

литературы, нормативных и методических документов в целях решения

задач профессиональной деятельности

Ответ: ОПК-8.2.

82. Способность специалиста в области информационной безопасности

воспринимать межкультурное разнообразие общества в социально-

историческом, этическом и философском контекстах

Ответ: УК-5

83. В чем разница между проверкой и аутентификацией личности?

Ответ: Аутентификация используется для подтверждения личности зарегистрированного пользователя. Проверка подлинности – это процесс проверки учетных данных: идентификатора пользователя (имени, адреса электронной почты, номера телефона) и пароля.

84. Профессиональный стандат «СПЕЦИАЛИСТ ПО ЗАЩИТЕ

ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ»

Ответ:

85. Назовите шесть логических мер контроля

Ответ: **пароли, шифрование, контроль доступа, брандмауэры и системы обнаружения вторжений**

86. Способность специалиста в области информационной безопасности

проводить аудит защищенности объекта информатизации в соответствии с нормативными документами

Ответ: ОПК-6

87. Управление защитой информации в автоматизированных системах

Ответ: **Для управления защитой информации (ЗИ) создается система ЗИ: программные и аппаратные средства ЗИ, митинги, спецперсонал и т.д.**

88. Классификация и оценка угроз безопасности информации в процессе

эксплуатации объекта защиты

Ответ: Антропогенные источники. Техногенные источники.Стихийные источники.Угрозы информационной безопасности могут быть классифицированы по различным признакам:

1) По аспекту информационной безопасности, на который направлены угрозы:

---угрозы конфиденциальности (неправомерный доступ к информации). Под угрозой конфиденциальности понимается возможность получения неправомерного доступа к конфиденциальной информации, процессам и устройствам. Подобные угрозы могут возникать вследствие человеческого фактора, сбоев работе программных и аппаратных средств.

---угрозы целостности. Угрозы нарушения целостности – это угрозы, связанные с вероятностью модификации той или иной информации, хранящейся в информационной системе. Нарушение целостности может быть вызвано различными факторами – от умышленных действий персонала до выхода из строя оборудования.

---угрозы доступности. Нарушение доступности представляет собой создание таких условий, при которых доступ к услуге или информации будет либо заблокирован, либо возможен за время, которое не обеспечит выполнение тех или иных целей [3].

2) По расположению источника угроз: внутренние (источники угроз располагаются внутри системы); внешние (источники угроз находятся вне системы).

3) По размерам наносимого ущерба: общие (нанесение ущерба объекту безопасности в целом); локальные (причинение вреда отдельным частям объекта безопасности); частные (причинение вреда отдельным свойствам элементов объекта безопасности).

4) По степени воздействия на информационную систему: пассивные (структура и со- держание системы не изменяются); активные (структура и содержание системы подвергается изменениям).

5) По природе возникновения:

---естественные (объективные) — вызванные воздействием на информационную среду объективных физических процессов или стихийных природных явлений, не зависящих от воли человека;

---искусственные (субъективные) — вызванные воздействием на информационную сферу человека.

89. Способность специалиста в области информационной безопасности

формировать нетерпимое отношение к коррупционному поведению

Ответ: УК-10

90. Администрирование систем защиты информации автоматизированных

систем

Ответ:

91. Способность специалиста в области информационной безопасности

осуществлять социальное взаимодействие и реализовывать свою роль в

команде

Ответ: УК-3

92. Способность специалиста в области информационной безопасности

выполнять организационные мероприятия по защите информации и

управлять процессом их реализации

Ответ: **ОПК-4.1**

93. Способность специалиста в области информационной безопасности

применять средства криптографической и технической защиты

информации для решения задач профессиональной деятельности

Ответ: ОПК-9

94. Способность специалиста в области информационной безопасности

оценивать роль информации, информационных технологий и

информационной безопасности в современном обществе, их значение для

обеспечения объективных потребностей личности, общества и

государства

Ответ: ОПК-1.

95. К какому фактору аутентификации относится ключ?

Ответ: Фактор знаний.

96. LaTeX-разметка документов. Преимущества системы LaTeX

Ответ: Страница в печатном документе состоит из трех частей: верхнего колонтитула, тела страницы и нижнего колонтитула. Преимущества: готовые профессионально выполненные макеты, делающие документы действительно выглядящими “как изданные”. Удобно поддержана верстка математических формул. Пользователю нужно выучить лишь несколько понятных команд, задающих логическую структуру документа. Ему практически никогда не нужно возиться собственно с макетом документа. Легко изготавливаются даже сложные структуры, типа примечаний, оглавлений, библиографий и прочее.

97. Способность специалиста в области информационной безопасности

администрировать системы защиты информации автоматизированных

систем

Ответ: **ОПК-4,3**

98. Реализация профессионального стандарта «СИСТЕМНЫЙ АНАЛИТИК» в области информационной безопасности

Ответ: Разработка, восстановление и сопровождение требований к программному обеспечению продукту, средству, программно-аппаратному комплексу, автоматизированной информационной системе или автоматизированной системе управления на протяжении их жизненного цикла

99. Используя концепцию глубокой защиты, объясните, какие уровни

защиты можно использовать, чтобы обезопаситься от перемещения

конфиденциальных данных из Вашей среды на USB-накопитель?

Ответ: Физ уровень понятно, он самый юзелесс

Тех уровень, можно поставить условный DLP в компанию

Админ уровень, тоже юзелесс, он не защитит от внутреннего

100. Способность специалиста в области информационной безопасности

управлять защитой информации в процессе эксплуатации объекта защиты

Ответ: ИБшник может управлять средствами ИБ, выполнять аудиты, определять угрозы и выполнять функции администратора системы

1 группа сосет