Контрольная работа 1 😀

1. КОНСТИТУЦИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

   статья **23**:

   1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

   2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.

2. Федеральный закон от 27 июля **2006** г. № 149-ФЗ “Об информации, информационных технологиях и о защите информации.”

3. **ФЗ № 152** – ФЗ “О персональных данных” 27.07.2006 г.

4. ФЗ № **98** “О коммерческой тайне” 29.07.2004 г.

5. Указ Президента **№ 188** “Об утверждении перечня сведений конфиденциального характера” 06.03.1997 г.

6. **Информация** – сведения (сообщения, данные) независимо от формы их представления.

7. **Обладатель информации** – лицо, самостоятельно создавшее информацию, либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

8. **Конфиденциальность информации** - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

9. КОДЕКС Российской Федерации об административных правонарушениях:

Глава **13**. Административные правонарушения в области связи и информации

Статья.Нарушение правил защиты информации

п. 2. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну),

п. 4. Использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну

10. Условия деятельности, работы, существования чего-нибудь - это **режим**.

11. любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу - это **персональные данные**

12. **Профессиональная тайна** – информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности.

13. **Служебная тайна** – защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости.

14. режим, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг - это **коммерческая тайна**

15. "**Специальные** требования и рекомендации по технической защите конфиденциальной информации" (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282

16.

Угрозы 1-го типа – связанные с наличием недокументированных возможностей в *системном* ПО.

Угрозы 2-го типа – связанные с наличием недокументированных возможностей в *прикладном* ПО.

Угрозы 3-го типа – *не связанные* с наличием недокументированных возможностей в *системном и прикладном ПО*.

17. Статья **272** Неправомерный доступ к компьютерной информации – **до 7 лет.**

18. Статья **273** Создание, использование и распространение вредоносных программ для ЭВМ – **до 7 лет.**
    Какой максимальный срок лишения свободы можно получить за статью 273 УК РФ**?**
    Ответ: 7 (точная формулировка 18 вопроса)

19. Статья **274** Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. – **до 5 лет.**

20. Статья **274.1** Неправомерное воздействие на критическую информационную инфраструктуру РФ – **до 10 лет.**

21. Статья **274.2** Нарушение правил центрального управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности

функционирования на территории РФ информационно-телекоммуникационной сети “Интернет” и сети связи. – **до 3 лет.**

22. **Закладочное** средство (устройство) – техническое средство (устройство) приема, передачи и обработки информации, преднамеренно установленное на объекте информатизации или в контролируемой зоне в целях перехвата информации или несанкционированного воздействия на информацию и (или) ресурсы автоматизированной информационной системы.

24. Скрытые каналы, основанные на сокрытии информации в **неструктурированных** данных, используют встраивание данных в информационные объекты без учета формально описанной структуры.

    НАПРИМЕР: запись скрытой информации в наименее значимые биты изображения, не приводящая к видимым искажениям изображения.

26. одно или несколько правил, процедур, практических приёмов или руководящих принципов в области безопасности, которым руководствуется организация в области безопасности, которым руководствуется организация в своей деятельности - это Политика безопасности **организации**

27. **Криптографический ключ** – совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

28. **Ключ** – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований.

29. **Пароль** – конфиденциальная информация аутентификации, обычно состоящая из строки знаков.

30. **Пароль доступа** – идентификатор субъекта доступа, который является его (субъекта) секретом.

31. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 “Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных **информационных** системах”

32. Федеральный закон "Об общих принципах организации публичной власти в **субъектах** Российской Федерации" от **21.12.2021** N **414-ФЗ** (чё именно хотели в вопросе не помним в истории браузера осталось 😀)

    - такое ощущение что “в субъектах”, но это не точно

33. совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности - **политика безопасности информации**

34. **Доктрина** информационной безопасности РФ. Утверждена Указом Президента РФ от **05 декабря 2016** года №**646**

35. **Вредоносная программа** - программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы.

36. **Критически важные объекты** — Объекты, нарушение или прекращение функционирования которых приводит:

    — к потере управления, разрушению инфраструктуры,

    — необратимому негативному изменению или разрушению экономики страны, субъекта или административно-территориальной единицы

    — или к существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях длительный период времени.

37. одно или несколько правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности - это Политика безопасности **организации** *(ДУБЛЬ 26ОГО ВОПРОСА)*

38. *2 варианта вопроса*

    Характеристика ГОСТ Р 53113.1-2008 В настоящем стандарте использованы нормативные ссылки на следующие стандарты: — ГОСТ Р ИСО/МЭК **15408**-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности — ГОСТ Р ИСО/МЭК **17799**-2006 Информационная технология. Практические правила управления информационной безопасностью

39. Закон РФ "О государственной тайне" от 21.07.**1993** N 5485-1

    Закон РФ № 5485-1 от 21 июля **1993** г. «О государственной тайне

40. Условия деятельности, работы, существования чего-нибудь - это **режим**. *(дубль 10ого)*

41. Приказ Минкомсвязи РФ от 27.10.2011 N 282 Об утверждении Положения о Департаменте государственной политики в области создания и развития электронного **правительства** Министерства связи и массовых коммуникаций Российской Федерации

42. Судебное дело: Иванова И.И. обвиняется в неправомерном доступе к компьютерной информации, находящейся под защитой закона, что привело к блокировке, изменению и копированию данных. в течение 6 минут, с 00:22 по 00:28 23 июня 2017 года… НОМЕР СТАТЬИ УК РФ **272**

43. *Одна тема, из которой вылезают несколько вопросов*:

Формулируя концептуальные задачи обеспечения безопасности предприятия, следует выделить следующие принципы построения и оптимизации системы внутриобъектового режима объекта защиты: 1. **универсальность**, предполагающая, что все решения должны быть отработаны и унифицированы; 2. **комплексность**, предполагающая, что используемые приемы работы и применяемые ТС взаимоувязаны между собой, дополняют друг друга по функциональным и техническим показателям; 3. разумная **достаточность**, означающая, что мероприятия по обеспечению безопасности объекта должны быть адекватны возможным угрозам со стороны вероятного нарушителя по финансовым, материально-техническим и кадровым ресурсам; 4. **оперативность**, предполагающая приоритет методов и средств защиты, обеспечивающих быстрое обнаружение и последующую нейтрализацию возможных угроз; 5. **адаптивность**, предусматривающая, что методы и средства защиты могут быть достаточно гибко приспособлены к изменениям организационных и технических условий функционирования объекта; 6. **непрерывность, систематичность**, означающие, что выбранные решения обеспечат достаточно эффективную круглосуточную защиту объекта; 7. **целеустремленность** - сосредоточение усилий на защиту наиболее ценных ресурсов фирмы или наиболее уязвимых участков объекта; 8. **многорубежность**, предполагающая использование дополнительных пространственных рубежей безопасности или методов защиты для наиболее ответственных, с точки зрения безопасности, помещений и зон объекта; 9. **равнопрочность** создаваемых границ безопасности; 10. **последовательность** в использовании соответствующих методов и средств при обнаружении, отражении и ликвидации угроз безопасности объекта (так называемая эшелонированность безопасности); 11. **совместимость** с существующими системами; 12. **простота, экологическая чистота и незаметность** ("дружественность"), предполагающие, что развертываемая система не создаст дополнительных препятствий для нормального функционирования организации, не потребует очень высокой квалификации и длительной подготовки обслуживающего персонала, не причинит вреда защищаемым ценностям объекта; 13. **неуязвимость** — способность противостоять предпринимаемым попыткам выведения системы из строя; 14. **документированность**, предполагающая регистрацию интересующих событий, связанных с защищаемым объектом, что необходимо для последующего анализа тревожных и нештатных ситуаций и достигнутого уровня защищенности объекта; 15. **законность**, означающая, что все применяемые меры организационного и технического характера легальны и юридически обоснованы.

Формулируя концептуальные задачи обеспечения безопасности предприятия, следует выделить следующие принципы построения и оптимизации системы внутриобъектового режима объекта защиты:

1. универсальность
2. комплексность
3. достаточность
4. оперативность
5. адаптивность
6. непрерывность, систематичность
7. целеустремленность
8. многорубежность
9. равнопрочность
10. последовательность
11. совместимость
12. простота, экологическая чистота и незаметность
13. неуязвимость
14. документированность
15. законность

45. Указ Президента РФ от 16 августа 2004 г. N 1085 "Вопросы Федеральной службы по техническому и **экспортному** контролю"

48. *Было несколько вариков про “классификация скрытых каналов”*

СК по памяти основаны на наличии памяти, в которую передающий субъект записывает информацию, а принимающий — считывает ее (Классификация скрытых каналов по **памяти** делятся на

— СК, основанные на **сокрытии информации в структурированных данных**;

— СК, основанные на сокрытии информации в неструктурированных данных).

СК по времени предполагают, что передающий информацию субъект модулирует с помощью передаваемой информации некоторый изменяющийся во времени процесс, а субъект, принимающий информацию, в состоянии демодулировать передаваемый сигнал, наблюдая несущий информацию процесс во времени.

Скрытый статистический канал использует для передачи информации изменение параметров распределений вероятностей любых характеристик системы, которые могут рассматриваться как случайные и описываться вероятностно-статистическими моделями.

Есть еще классификация по пропускной способности: Скрытый канал с низкой пропускной способностью; Скрытый канал с высокой пропускной способностью)

49. Иван Иванович Иванов осуществил незаконный доступ к защищенной компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, повлекший причинение вреда критической

информационной инфраструктуре Российской Федерации. С 2 октября 2018 года по 17 апреля 2019 Статья **274.1**

50. В течение периода с лета 2019 по весну 2020 года было выявлено, что Иванов И.И., занимавший должность старшего следователя в Отделе полиции России по районам Ромашково Статья **272** и **286**

51. Компания с ограниченной ответственностью "Азия" (в дальнейшем в тексте обозначается как истец) обратилась в арбитражный суд с требованием к индивидуальному предпринимателю И.И. Иванов Статья **183**

52. Подсудимый Иванов И.И. виновен в нарушении правил эксплуатации средств хранения и обработки охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре РФ, информационных систем, относящихся к критической информационной инфраструктуре РФ, правил доступа к указанной информации и информационным системам, что повлекло причинение вреда критической информационной инфраструктуре РФ Статья **274.1**

53. Иванов И.И. нарушил закон, раскрыв сведения, являющиеся коммерческой тайной, без разрешения их правообладателя несмотря на то, что эти данные были ему доверены в рамках рабочей деятельности Статья **183** и **272**

54. Н.Н. Иванова незаконно получила доступ к компьютерным данным, охраняемым законом, и, в случае копирования этой информации, её действия стали нарушением. В определенный момент времени, о котором следственные действия пока не предоставили точных данных, Иванова Н.Н. получила надежные указания о том, что «Потерпевший» использует электронную почту с адресом «xxxx». Статья **272**

55. Иванов И.И. нарушил закон, осуществив незаконный доступ к защищенной законом информации в электронном виде, что привело к её изменению. Это произошло в целях личного обогащения в Цветочном районе Цветочного. Статья **272**

56. Работник оборонного завода Иванов И.И. решил оказать помощь своей знакомой, которая переходила на обучение в онлайн режиме, и помочь ей найти программу для активации офисного программного комплекса от известной компании. Используя компьютер Статья **273**

57. УК РФ Статья 284. Утрата документов, содержащих **государственную тайну**

58. **Защищенность** - атрибуты программного обеспечения, относящиеся к его способности предотвращать несанкционированный доступ, случайный или преднамеренный, к программам и данным.

59. Информационные системы интеллектуального здания хозяйствующего субъекта можно условно разделить на следующие системы:

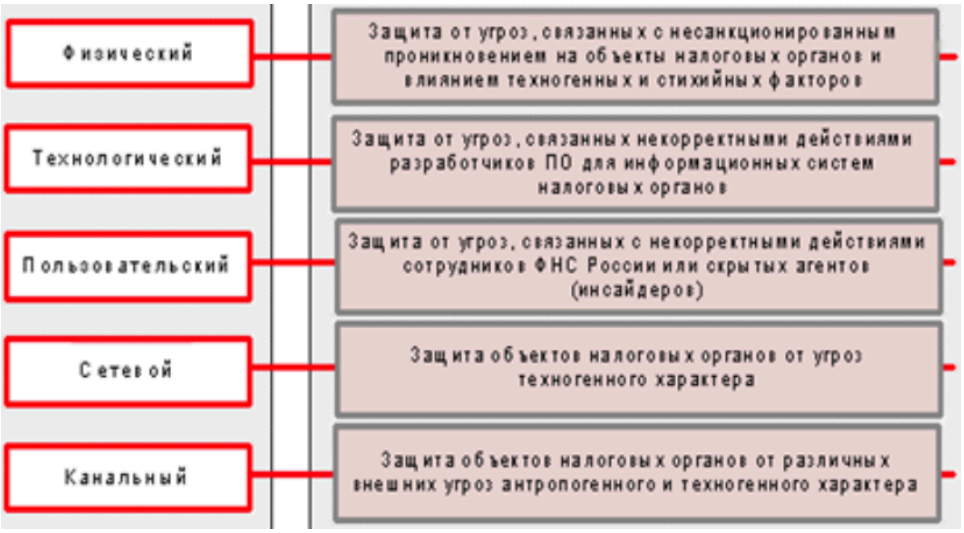
Интегрированная техническая система охраны - в ее состав ориентировочно входят системы:

- контроля и управления доступом (СКУД);

- пожарной сигнализации (СПС);
- аварийного оповещения и управление эвакуацией персонала и посетителей (СОУЭ);
- охранной сигнализации (включая защиту периметра и тревожную сигнализацию) (СОС);
- **видеоконтроля** (СВК)

60. УК РФ Статья 276: **Шпионаж**

61. Подуровни **исполнительского** уровня системы обеспечения безопасности информации **Ответ: Исполнительского**



62. Скрытый канал является каналом с **низкой** пропускной способностью, если его пропускной способности достаточно для передачи ценных информационных объектов минимального объема (например криптографические ключи, пароли) или команд за промежуток времени, на протяжении которого данная передача является актуальной.

63. **Об утверждении доктрины** информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 5 декабря 2016 г. № 646

64. **Доверие** - основание для уверенности в том, что объект соответствует целям безопасности

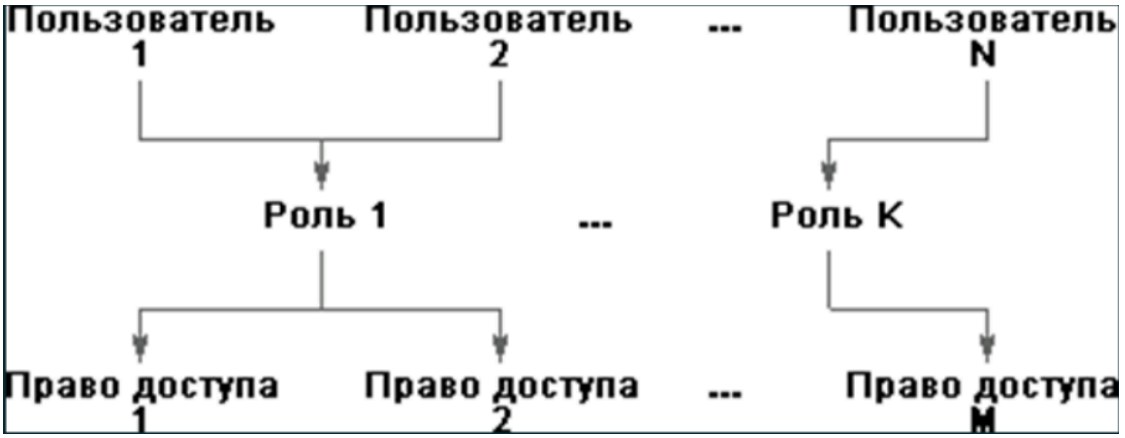
65. Приемы, способы и методы применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных - это **информационная технология**

67. ГОСТ 34.12-2018. “Межгосударственный стандарт. Информационная технология. **Криптографическая** защита информации. Блочные шифры”

68. ГОСТ 34.13-2018 “Межгосударственный стандарт. Информационная технология. Криптографическая защита информации. **Режимы** работы блочных шифров.

69. “**Методика** оценки угроз безопасности информации” М., 2004

70. На рисунке представлена “Схема **ролевого** управления доступом”

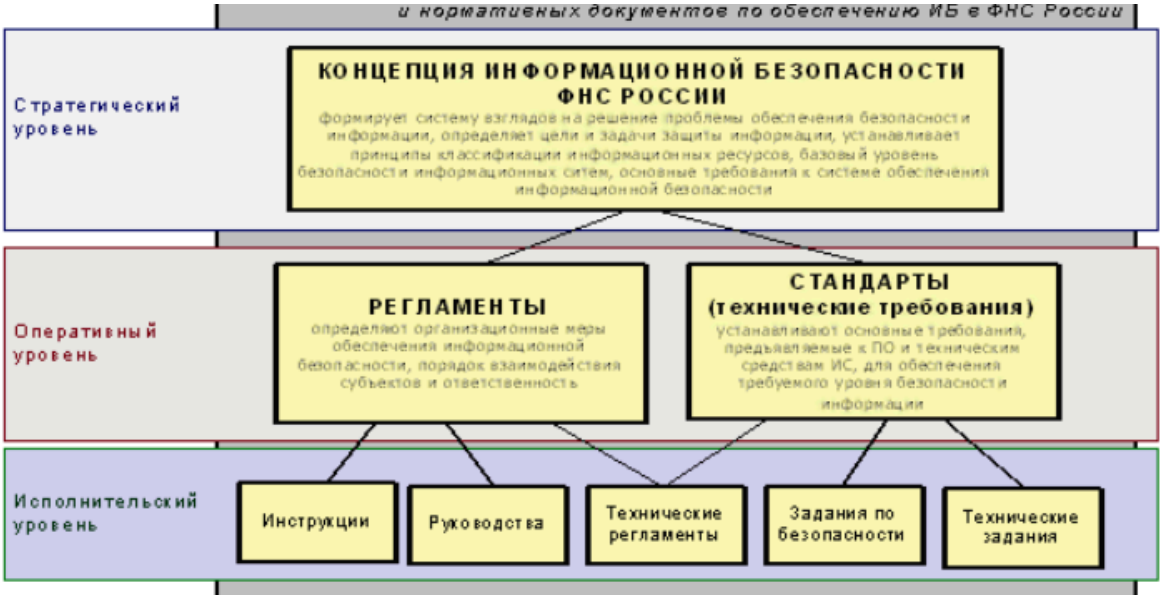


71. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 “Вопросы Федеральной службы по техническому и **экспортному** контролю.

72. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 “Об утверждении Требований о защите информации, не составляющих государственную тайну, содержащейся в государственных **информационных** системах”

73. Структура организационной базы системы обеспечения безопасности информации (далее - СОБИ) ФОИВ строится: **Матричность** предполагает создание разветвленной горизонтальной структуры взаимодействия с подразделениями ФОИВ.

74. Укрупненная структура **Политики безопасности информации** органа власти



75. комплекс, состоящий из процессов, технических и программных средств, устройств и персонала, обладающий возможностью удовлетворять установленным потребностям или целям - это **система**

76. **Система** — специфическое воплощение информационной технологии с конкретным назначением и условиями эксплуатации

77. **Физическая защита** - средства, используемые для обеспечения физической защиты ресурсов от преднамеренной или случайной угрозы

78. Основные направления **правового** обеспечения защиты информации

    1. Права собственности, владения и распоряжения информацией
    2. Степень открытости информации
    3. Порядок отнесения информации к категории ограниченного доступа
    4. Организация работ по защите информации
    5. Государственное лицензирование деятельности в области защиты информации
    6. Порядок создания специальных служб
    7. Права и ответственность должностных лиц за защиту информации

79. Особый класс активов, которые уязвимы с точки зрения угроз, реализуемых с использованием СК с низкой пропускной способностью: Класс **А** — активы, связанные с функционированием критически важных объектов. Класс **Б** — активы, содержащие ключевую/парольную информацию, в том числе ключи криптографических систем защиты информации и пароли доступа к иным активам.

80. непредусмотренный разработчиком системы информационных технологий и автоматизированных систем коммуникационный канал, который может быть применен для нарушения политики безопасности - это **скрытый канал**

81. **Агент нарушителя** — это лицо, программное, программно-аппаратное или аппаратное средство, действующие в интересах нарушителя.

82. Политика ИБ ФОИВ является собирательным понятием, предполагающим создание совокупности взаимоувязанных нормативных и организационно-распорядительных документов, • как единых для всех участников информационного обмена (Общая политика), • так и специализированных, для территориальных органов и подведомственных учреждений ФОИВ (**Частная политика**).

83. **Специальные** требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282 *(ДУБЛЬ 15ОГО ВОПРОСА)*

84. Судебное дело: Водитель электровоза Иванов И.И., стремясь обеспечить своему подчинённому успешное прохождение экзамена по знаниям технико-диспетчерского руководства на железнодорожных путях, прибег к использованию внешней программной разработки, которая позволяет напрямую вмешиваться в итоги тестирования. Подсудимый признал свою вину и

самостоятельно направил личные финансовые средства на счёт местной общеобразовательной школы. Согласно вердикту суда, этот поступок компенсировал вред, который был нанесен его незаконными действиями. В ходе расследования по уголовному делу не было выявлено какого-либо материального ущерба. Данный объект является КИИ. **274.1** (дубль 46 вопроса)

85. ОБЛАДАТЕЛЬ ИНФОРМАЦИИ, ОПЕРАТОР информационной системы в случаях, установленных законодательством, обязаны обеспечить РЕЖИМНЫЕ меры:

1) ПРЕДОТВРАЩЕНИЕ несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное **обнаружение** фактов несанкционированного доступа к информации;

3) ПРЕДУПРЕЖДЕНИЕ возможности неблагоприятных ПОСЛЕДСТВИЙ нарушения порядка доступа к информации;

4) НЕДОПУЩЕНИЕ ВОЗДЕЙСТВИЯ на технические средства обработки информации, в результате которого нарушается их функционирование;

5) ВОЗМОЖНОСТЬ незамедлительного ВОССТАНОВЛЕНИЯ информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) ПОСТОЯННЫЙ КОНТРОЛЬ за обеспечением уровня защищенности информации.

86. Структура организационной базы системы обеспечения безопасности информации (далее - СОБИ) ФОИВ строится:
Иерархичность предполагает создание в ФОИВ многоуровневой вертикальной структуры, позволяющей своевременно довести управляющее воздействие до исполнительных механизмов….

Контрольная работа 2

1. Шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций:

   - создание электронной подписи,

   - проверка электронной подписи,

   - создание ключа электронной подписи и ключа проверки электронной подписи.

- это средства **электронной подписи**

2. **Средства шифрования** – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации от несанкционированного доступа при ее передаче по каналам связи и(или) при её обработке и хранении

3. **Угрозы безопасности персональных данных** - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

4. Основными видами нарушителей - **конкурирующие организации.**

   Вопрос теперь звучит так:

   Допишите одно из двух определений, которое тут отсутствует в списке. Основными видами нарушителей, подлежащих оценке, являются:

   террористические, экстремистские группировки;

   преступные группы (криминальные структуры);

   отдельные физические лица (хакеры);

   разработчики программных, программно-аппаратных средств;

   лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем;

   поставщики услуг связи, вычислительных услуг;

   лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ;

   лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.);

   авторизованные пользователи систем и сетей;

   системные администраторы и администраторы безопасности;

бывшие (уволенные) работники (пользователи).

5. **Технический канал утечки информации (ТКУИ)** - совокупность объектов разведки, которые содержат информацию, технических средств разведки (ТСР) , с помощью которых добывается информация, и физической среды, в которой распространяется информативный сигнал (циркулируют данные).

   ВСТРЕЧАЕТСЯ ЕЩЕ ОДНО ОПРЕДЕЛЕНИЕ

   совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация - это **технический канал утечки информации**

6. **Криптографическая стойкость (или криптостойкость - ЗАСЧИТАЛИ ТАК)** – способность криптографического алгоритма противостоять возможным атакам на него или оценка алгоритма, способного взломать шифр.

7. **Криптоанализ** – анализ криптографической системы и/или её входов и выходов с целью получения конфиденциальных переменных и/или чувствительных данных, включая открытый текст.

8. **Криптосредство** – шифровальное средство, предназначенное для защиты информации, не содержащей сведений, составляющих гостайну.

9. **Идентификация** – процесс опознания субъекта или объекта по присущему ему или присвоенному ему идентификационному признаку. Под идентификацией подразумевается также присвоение субъектам и объектам доступа дидентификатора и(или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

10. **Аутентификация** – процесс опознания субъекта или объекта путем сравнения введенных идентификационных данных с *эталоном* (образцом), хранящимся в памяти системы для данного субъекта или объекта.

11. **Цели обработки персональных данных:**

    − ведение кадрового учета

    − учет рабочего времени

    - **учет работников**

    − расчет заработной платы работников

    − **ведение налогового учета**

− представление отчетности в государственные органы

− архивное хранение данных

12. Перечень персональных данных, на обработку которых дается согласие:

- фамилия, имя, отчество

- год, месяц, дата и место рождения;

- свидетельство о гражданстве (при необходимости);

- реквизиты документа, удостоверяющего личность;

- идентификационный номер налогоплательщика, дата постановки его на учет, реквизиты свидетельства постановки на учет в налоговом органе;

- номер свидетельства обязательного пенсионного страхования, дата регистрации в системе обязательного пенсионного страхования;

- номер полиса обязательного медицинского страхования;

- адрес фактического места проживания и регистрации по месту жительства и (или) по месту пребывания;

- почтовый и электронный адреса;

- **номера телефонов;**

- фотографии;

- сведения об образовании, профессии, специальности и квалификации, реквизиты документов об образовании;

- сведения о семейном положении и составе семьи;

- сведения об имущественном положении, доходах, задолженности;

- сведения о занимаемых ранее должностях и стаже работы, воинской обязанности, воинском учете;

13. **Ключевой документ** – физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости – контрольную, служебную и технологическую информацию.

14. **Ключевой носитель** – физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации). Различают разовый ключевой носитель (таблицы, перфолента, перфокарта и т.п.) и ключевой носитель многократного использования

(магнитная лента, дискета, компакт-диск, Data Key, Smart Card, Touch Memory и т.п.).

15. Ключевой **блокнот** – набор бумажных ключевых документов одного вида (таблиц, перфолент, перфокарт и т.п., сброшюрованных и упакованных по установленным правилам.

16. **Менеджмент** риска – это скоординированные действия по руководству и управлению организацией в отношении риска.

    Обычно включает в себя:

    — оценку риска,

    — обработку риска,

    — принятие риска и

    — коммуникацию риска

17. Какого уровня не бывает в модели Carnegie Mellon University?

    a. Анархия

    b. Фольклор

    c. Стандарты

    d. **Законы**

18. Сколько уровней в модели зрелости **Gartner Group – 4 уровня.**

19. **Самая высокая** категория шифровальных средств – **А**

21. Интегрированная техническая система охраны - в ее состав входят системы: **СКУД, СПС, СОС, СОУЭ, СВК**

    Интегрированная техническая система охраны - в ее состав ориентировочно входят системы: • контроля и управления доступом (СКУД); • пожарной сигнализации (СПС); • аварийного оповещения и управление эвакуацией персонала и посетителей (СОУЭ); • охранной сигнализации (включая защиту периметра и тревожную сигнализацию) (СОС); • видеоконтроля (СВК).

22. *У многих были подобные вопросы, которые связаны одной темой (спрашивался один из терминов), поэтому запихнула сюда сразу весь слайд:*

    В соответствии с механизмами реагирования на угрозы, определяют следующие уровни защиты информации:

Предотвращение — это внедрение служб контроля доступа к информации и технологии;

Обнаружение — это раннее обнаружение угрозы, даже в случае обхода механизмов защиты;

Ограничение — это уменьшение размера информационных потерь, в случае уже произошедшего преступления;

Восстановление — обеспечение эффективного восстановления информации в нслучае её утраты или уничтожения.

23.

Аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства (за исключением средств шифрования), реализующие алгоритмы криптографического преобразования информации для ее защиты от навязывания ложной информации, в том числе защиты от модифицирования, для обеспечения ее достоверности и некорректируемости, а также обеспечения возможности выявления изменений, имитации, фальсификации или модифицирования информации - это средства **имитозащиты**

24. **Сертификация** - форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров.

25. Подготовка системы управления информационной безопасностью к сертификации в соответствии с ГОСТ Р ИСО/МЭК 27001-2006 осуществляется по следующим этапам.

    Этап 1. Оценка текущего состояния СУИБ.
    Этап 2. Оценка эффективности СУИБ.
    Этап 3. **Инспекции** СУИБ.

26. **Уязвимость** - это слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами.

27. **Потенциал нарушителя** - мера усилий, затрачиваемых нарушителем при реализации угроз безопасности информации в информационной системе. Примечание, Различают высокий, средний и низкий потенциалы нарушителя. Высокий потенциал подразумевает наличие возможностей уровня предприятия/группы предприятий/государства по разработке и использованию специальных средств эксплуатации уязвимостей.

28. **Категория нарушителя** - краткая характеристика основных возможностей нарушителя по реализации угроз безопасности информации в части его оснащенности, знаний, мотивации или краткое обоснование невозможности нарушителем реализовать угрозы безопасности информации.

29. *Одна тема на несколько вопросов, поэтому инфа общая:*

1. Персональные данные 1 категории (специальные ПД). 1.1. Сведения о состоянии здоровья и интимной жизни, о расовой и национальной принадлежности, политических взглядах, религиозных или философских убеждениях (данные справок и медицинских заключений о состоянии здоровья, данные диспансеризации, данные листов о временной нетрудоспособности в части диагнозов заболеваний, признаки причастности клиентов к террористам или экстремистам, к влиятельным политическим лицам).

2. Персональные данные 2 категории (биометрические ПД). Персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1: 2.1. Сведения о биометрических персональных данных, характеризующих физиологические особенности человека, за исключением персональных данных, относящихся к 1 категории (видеозаписи систем охранного телевидения, банковских терминальных устройств, ксерокопии с документов, удостоверяющих личность и имеющих фотографию владельца, фотографии сотрудников и клиентов Банка, данные в устройствах, использующих для идентификации биометрические данные человека).

3. Персональные данные 3 категории (общие ПД). Персональные данные, позволяющие идентифицировать субъекта персональных данных: 3.1. Фамилия, имя, отчество, год, месяц, дата и место рождения, паспортные данные (номер, серия, данные о выдаче), сведения о месте и дате регистрации (месте жительства). 3.2. Сведения о номере и серии страхового свидетельства государственного пенсионного страхования. 3.3. Сведения из страховых полисов обязательного (добровольного) медицинского страхования (в т.ч. данные соответствующих карточек медицинского страхования). 3.4. Сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу.

4. Персональные данные 4 категории (общедоступные ПД). Обезличенные и (или) общедоступные персональные данные: 4.1. Сведения о семейном положении (состояние в браке, наличие брачного контракта, дата регистрации, фамилия, имя и отчество супруга (и) и его (ее) социальный статус, наличие детей и их возраст, семейные доходы и расходы, долги и другие сведения). 4.2. Данные о трудовой деятельности (данные о трудовой занятости на текущее время, стаж работы, наличие трудового договора, организации, занимаемые в них должности и время работы в этих организациях, а также другие сведения). 4.3. Сведения об образовании, квалификации, о наличии специальных знаний или специальной подготовки (образовательная категория, ученая степень, образовательное учреждение, дата начала и завершения обучения, квалификация и специальность по окончании учебного заведения и другие сведения). 4.4. Сведения об имуществе (имущественное положение): - автотранспорт (вид владения, марка, модель, производство, год выпуска, способ получения и другие сведения, кроме указанных в соответствующем пункте раздела 3); - недвижимое имущество (вид, тип, способ получения, общие характеристики, стоимость и другие сведения).

30. Электронное **сообщение** — это информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

31. Электронный **документ** - это документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах

32. **Риск** - сочетание вероятности появления опасного события и его последствий.

33. Под **аккредитацией** понимается официальное признание органом по аккредитации компетентности физического или юридического лица в части выполнения работы в определенной области оценки соответствия, включая испытания, калибровки, экспертизы, сертификацию и контроль.

34. **Аккредитация -** это официальное признание компетентности физического или юридического лица выполнять работы в определенной области оценки соответствия (еще один вариант вопроса)

35. **СКЗИ** - сертифицированные средства криптографической защиты конфиденциальной информации.x

36. *Вопрос был в подобном духе:*

    К **СКЗИ** относятся: — реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, обеспечивающие безопасность информации при ее обработке, хранении и передаче по каналам связи, включая СКЗИ;
    — реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от несанкционированного доступа к информации при ее обработке и хранении;

37. **Сертификат соответствия** - документ, удостоверяющий соответствие объекта требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров.

38. Классы СКЗИ различаются по уровням защитных свойств: **Уровни А, В, С**

39. Пересмотр установленных категорий значимости или решений об отсутствии необходимости присвоения указанным объектам таких категорий осуществляется в случае изменения показателей **критериев значимости**

40. Что формируется на объект информатизации по рекомендуемому образцу из приказа в соответствии со служебной запиской? **Технический паспорт**

41. Перечень разрешенных к использованию доверенных носителей - **журнал учета съемных носителей**

42. **Жизненный цикл** автоматизированной системы — совокупность взаимосвязанных процессов создания и последовательного изменения состояния АС от

формирования исходных требований к ней до окончания эксплуатации и утилизации комплекса средств автоматизации АС.

43. **Документированная информация** - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель

44. Совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к защищаемой информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение защищаемой информации, а также иных несанкционированных действий при их обработке в информационной системе - это **УБИ**

45. При отнесении заказчиком нарушителя к типу **Н1** криптосредство должно обеспечить криптографическую защиту по уровню КС1

46. Идентификационный номер угрозы безопасности информации в соответствии с открытым банком угроз безопасности информации ФСТЭК России - это **номер УБИ**