Вопрос:

Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

**Сотрудники**

Вопрос:

Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

**Улучшить контроль за безопасностью этой информации**

Вопрос:

Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

**Поддержка высшего руководства**

Что такое защита информации?

**- это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.**

Какой-то вопрос с фразой "точка-в-точку" или "точка-точка"

**VPN(?)**

503 тип ошибки?...

**Причина: Легкие запросы обрабатываются быстро, а тяжёлые проблемные - медленно, тормозя продвижение очереди. Когда длина очереди достигает определенной величины, сервер перестает принимать новые запросы, возвращая ошибку 503 (Service Temporarily Unavailable, сервис временно недоступен).**

**про протоколы безопасности wi-fi: какой эффективнее WEP WPA WPA2…**

**WPA2**

**если буdет вариант WPA3, то он**

вопрос про автоматическое назначение ip-адресов

**там dhcp вроде**

и как настроить общий доступ

**свойства?**

что-то про какими правами обладает первый пользователь?

**Админ**

Реестр открывается через команду **regedit**

Кто является основным ответственным за определение уровня классификации информации?

**Владелец**

Что самое главное должно продумать руководство при классификации данных?

**Необходимый уровень доступности, целостности и конфиденциальности**

Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

**Руководство**

Что такое процедура?

**Пошаговая инструкция по выполнению задачи**

Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

**Поддержка высшего руководства**

Вопрос:

Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

**Когда стоимость контрмер превышает ценность актива и потенциальные потери**

Вопрос:

Что такое политики безопасности?

**Широкие, высокоуровневые заявления руководства**

Вопрос:

Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

**Анализ затрат / выгоды**

Вопрос:

Что лучше всего описывает цель расчета ALE?

**Оценить потенциальные потери от угрозы в год**

Вопрос:

Тактическое планирование – это:

**Среднесрочное планирование**

Вопрос:

Что является определением воздействия (exposure) на безопасность?

**Нечто, приводящее к ущербу от угрозы**

Вопрос:

Эффективная программа безопасности требует сбалансированного применения:

**Технических и нетехнических методов**

Вопрос:

Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

**Уровень доверия, обеспечиваемый механизмом безопасности**

Вопрос:

Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?

**Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности**

Вопрос:

Как рассчитать остаточный риск?

**(Угрозы х Уязвимости х Ценность актива) x Недостаток контроля**

Вопрос:

Что из перечисленного не является целью проведения анализа рисков?

**Делегирование полномочий**

Вопрос:

Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?

**Выполнение анализа рисков**

Вопрос:

Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

**Количественные измерения должны применяться к качественным элементам**

Вопрос:

Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?

**Много информации нужно собрать и ввести в программу**

Вопрос:

Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств?

**Должная забота (Due care)**

Вопрос:

Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?

**Открытый стандарт, определяющий цели контроля**

Вопрос:

Из каких четырех доменов состоит CobiT?

**Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка**

Вопрос:

Что представляет собой стандарт ISO/IEC 27799?

**Стандарт по защите персональных данных о здоровье**

CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO?

**COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень**

OCTAVE, NIST 800-30 и AS/NZS 4360 являются различными подходами к реализации управления рисками в компаниях. В чем заключаются различия между этими методами?

**NIST и OCTAVE ориентирован на ИТ**

Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?

**Анализ сбоев и дефектов**

Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?

**OECD**

Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод:

**перестановки;**

Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:

**гаммирования;**

Защита информации от утечки это деятельность по предотвращению:

**неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;**

Естественные угрозы безопасности информации вызваны:

**воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;**

Искусственные угрозы безопасности информации вызваны:

**деятельностью человека;**

К основным непреднамеренным искусственным угрозам АСОИ относится:

**неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.**

К посторонним лицам нарушителям информационной безопасности относится:

**представители конкурирующих организаций.**

Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п:

**черный пиар;**

Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:

**фишинг**

Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы:

**детектор;**

Антивирус не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние:

**доктор**

Антивирус запоминает исходное состояние программ, каталогов и системных областей диска когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным:

**ревизор;**

Антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов:

**сторож**

Активный перехват информации это перехват, который:

**осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.**

Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:

**аудиоперехват;**

Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:

**пассивный перехват**

Перехват, который осуществляется путем использования оптической техники называется:

**видеоперехват;**

К внутренним нарушителям информационной безопасности относится:

**технический персонал, обслуживающий здание**

Прикладные программы предназначены для:

**Решения каких-либо задач в пределах данной области**

К какому виду ПО относятся программы общего назначения?

**Прикладное ПО**

Выберите верное утверждение:

**Прикладное ПО – совокупность программ для решения прикладных задач**

Главной составной частью системного программного обеспечения является:

**операционная система**

Что не входит в правовое обеспечение информационной безопасности?

**Биометрическая защита данных**

Информационная безопасность – это:

**защита целостности, доступности и конфиденциальности информации**

Какие программы относятся к прикладному ПО:

**MS PowerPoint, Google, Skype**

К формам защиты информации не относится:

**аналитическая**

Наиболее защищенная файловая система – это:

**FAT 16**

Что не входит в виды угроз:

**угроза дублирования**

Программа, которая предназначена для выполнения определенных пользовательских задач и рассчитана на непосредственное взаимодействие с пользователем:

**прикладное ПО**

Комплекс мероприятий, которые направлены на защиту информации:

**защита информации**

Выберите виды информационных угроз:

**доступность, конфиденциальность, целостность**

Программное обеспечение классифицируется на:

**системное, прикладное, системы программирования**

Перечислите основные угрозы при незащищённом использовании сети Интернет:!!!

**спам**

**вирус**

**вредоносное ПО**

**платные подписки**

Назначение операционной системы:

**организовать взаимодействие пользователя с компьютером и выполнение всех других программ**

В состав системного ПО входит Сервисное ПО. К нему относится:

**набор утилит, которые позволяют пользователю управлять ресурсами компьютера**

К биометрической системе защиты относятся:

**идентификация по радужной оболочке глаз**

**идентификация по отпечаткам пальцев**

**Заражение компьютерными вирусами может произойти в процессе ...**

**1. работы с файлами**

**2. форматирования дискеты**

**3. выключения компьютера**

**4. печати на принтере**

**5. правильных ответов нет**

**12. Что необходимо иметь для проверки на вирус жесткого диска?**

**1. защищенную программу**

**2. загрузочную программу**

**3. файл с антивирусной программой**

**4. дискету с антивирусной программой, защищенную от записи**

**5. правильных ответов нет**

**Составные части современного антивируса**

**1. Модем**

**2. Принтер**

**3. Сканер**

**4. Межсетевой экран**

**5. Монитор**

**Варианты ответов:**

**1. 3), 4), 5);**

**2. 1), 2), 5);**

**3. 2), 3), 4);**

**4. 2),3),5),**

**14. Вредоносные программы – это:**

**1.шпионские программы.**

**2. программы, наносящие вред данным и программам, находящимся на компьютере**

**3. антивирусные программы**

**4. программы, наносящие вред пользователю, работающему на зараженном компьютере**

**5. троянские утилиты и сетевые черви**

**RAID-массив это**

**1. Набор жестких дисков, подключенных особым образом**

**2. Антивирусная программа**

**3. Вид хакерской утилиты**

**4. База защищенных данных**

**5. Брандмауэр**

**16 Три составляющие информационной безопасности?**

**1. Доступность, целостность, конфиденциальность**

**2. Неприкосновенность, целостность, устойчивость**

**3. Публичность, доступность, защищённость**

**4. Тайна, охрана, зашифрованность**

**5. Охранность, устойчивость, защищённость**

**6. Конфиденциальность, тайна, публичность.**

**17. Какой стандарт определяет требования к управлению информационной безопасностью?**

**1. ГОСТ Р 15408**

**2. ГОСТ ИСО/МЭК 27001**

**3. ГОСТ ИСО/МЭК 17799**

**4. Нет такого стандарта**

**19 что такое DoS-атака?**

**1. атака, направленная на уязвимости ОС MS-DOS**

**2. атака, осуществляемая обычно при помощи ОС MS-DOS или PC-DOS**

**3. атака типа "отказ в обслуживании"**

**4. распределённая (distributed) атака**

**5.беспокоющая (disturb) атака**

**6.деструктивная атака**

**7. атака, направленная на настольные (desktop) системы**

**20 Какой из русских терминов, соответствующих английскому "firewall", является официальным?**

**1. файервол**

**2.брандмауэр**

**3. межсетевой экран**

**4. сетевой фильтр**

**5. пакетный фильтр**

**6. фильтр**

**7. огненная стена**

**21. Какой из уровней называется транспортным в 7-уровневой модели OSI?**

**1. 1-й**

**2. 2-й**

**3. 3-й**

**4. 4-й**

**5. 5-й**

**6. 6-й**

**7.7-й**

**22. На каком уровне (в 7-уровневой модели OSI) находится протокол ICMP?**

**1. на канальном**

**2. на прикладном**

**3.на сетевом**

**4.на транспортном**

**5. на уровне представлений**

**6. на физическом**

**7. он находится между уровнями**

**23 На каком уровне утверждается политика информационной безопасности предприятия?**

**1.это не имеет значения**

**2. на уровне руководителя функционального подразделения**

**3. на уровне начальника службы ИБ**

**4. на уровне технического директора**

**5. на уровне высшего руководства предприятия**

**6.на уровне вышестоящего или надзирающего органа**

**24. На кого возлагается ответственность за определение подлежащих защите ресурсов на предприятии?**

**1. на высшее руководство**

**2. на руководителей среднего звена**

**3. на рядовых работников**

**4. на службу ИБ**

**5.на вышестоящие или надзирающие органы**

**6. этот вопрос не разрешён в стандарте по ИБ**

**25. Может ли администратор информационной системы предприятия передавать ответственность и полномочия по обеспечению ИБ поставщику услуг?**

**1. нет**

**2. полномочия - нет, ответственность – да**

**3. полномочия - да, ответственность – нет**

**4. да**

**5. этот вопрос не разрешён в стандарте по ИБ**

**26 Пользователь компьютера с ОС Windows-XP планирует предоставить к файлам в папке Docs доступ так, чтобы все остальные пользователи имели права на чтение. Как можно это сделать?**

**1. копировать файлы из Docs в папку Shared Documents**

**2. предоставить общий доступ к папке Docs с правами по умолчанию**

**3. копировать файлы из Docs в папку My Documents**

**4. предоставить разрешения NTFS группе "Everyone" на уровне "Читатель"**

**27 Какое минимальное разрешение NTFS требуется пользователю, чтобы пр осмотреть содержимое папки в ОС Windows-XP Professional?**

**1. чтение**

**2. чтение и выполнение**

**3. запись**

**4. изменение**

**5.просмотреть нельзя**

**28. Возможно ли в ОС Windows XP Professional запускать программы от имени другого пользователя не завершая сеанс текущего пользователя?**

**1. возможно только для членов группы Администраторы (Administrators)**

**2. возможно, если известны имя и пароль учетной записи, от имени которой требуется запустить программу**

**3. возможно, кроме программ, работающих неинтерактивно**

**4. возможно за исключением запуска программ от имени пользователя из группы Администраторы (Administrators)**

**5. возможно за исключением запуска программ от имени пользователя**

**6. невозможно**

**29. Какая из перечисленных файловых систем позволяет разграничивать доступ к файлам и папкам?**

**1. FAT-16**

**2.. ISO-9660**

**3. ISO-9660 с расширением Julliet**

**4. FAT-32**

**5. NTFS**

**30. Где хранятся локальные учетные записи в ОС Windows XP Professional?**

**1. в базе RMS**

**2. в файле system32/security/users**

**3. в базе SAM**

**4. в файле user.exe**

**5. локальных учётных записей нет, все учётные записи хранятся на контроллере домена**

**31.Какими методами обнаруживают полиморфные вирусы?**

**1. при помощи сигнатуры**

**2. эвристическими методами и эмуляторами кода**

**3. их невозможно обнаружить**

**32. Какова длина хэш-функции MD5?**

**1. 64 бита**

**2. 128 бит**

**3. 256 бит**

**4. 512 бит**

**5.1024 бита**

**6. 2048 бит**

**7. длина переменная**

**33. Какие вирусы заражают загрузочный сектор гибкого диска или винчестера?**

**1. сетевые вирусы**

**2. загрузочные вирусыв**

**3. макро -вирусы**

**4. все выше перечисленные**

**34. Когда может произойти полное уничтожение информации на дисках?**

**1. При воздействии компьютерных вирусов;**

**2. При форматировании;**

**3. При отказе дисковода жесткого диска;**

**4. Нет правильного ответа**

**35. Какие программы не относится к антивирусным программам?**

**1. AVP**

**2. DrWeb**

**3. NAV**

**4. GIF**

**5. SCAN**

**Варианты ответов:**

**1. AVP, DrWeb, NAV;**

**2. AVP, GIF, SCAN;**

**3, NAV, GIF, SCAN.**

**36. Какие программы не относится к антивирусным программам?**

**1. AVP**

**2. DrWeb**

**3. Spy Sweeper 5.8**

**4. OfficeScan Client 10.0**

**5.SCAN**

**37. Какие программы не относится к антивирусным программам?**

**1. AVP**

**2. Norton AntiVirus 10.1**

**3. Spy Sweeper 5.8**

**4. OfficeScan Client 10.0**

**5.PGP**

**38. Какие программы не относится к антивирусным программам?**

**1. CounterSpy 3.1**

**2. DrWeb**

**3. Spy Sweeper 5.8**

**4. OfficeScan Client 10.0**

**5.КРИПТОН**

**Выберите не верное утверждение.**

**1. От вируса избавится нельзя.**

**2. Вирус замедляет работу на компьютере.**

**3. Вирус может изменить формат данных.**

**4. Вирус выводит посторонние сведения.**

**5. Вирус искажает и уничтожает информацию на компьютере.**

**40. Каким способом компьютер может заразится вирусом?**

**1. Пользователь переписывает на дискету любую информацию с компьютера.**

**2. В процессе форматирования диска.**

**3. Пользователь хотя бы один раз запустить программу, содержащую вирус.**

**4. В процессе неправильной перезагрузки компьютера.**

**5. При запуске программы DRWER.**

**41. Какая программа называется архиватором?**

**1. Программа обнаруживающая и удаляющая вирусы**

**2. Программа, которая может изменить свой объем.**

**3. Программа определяющая и снимающая атрибуты файла.**

**4. Программа уменьшающая объем файла.**

**5. Программа увеличивающая объем файл.**

**42. Как называется процесс включения защиты на ячейках?**

**1. Вирус.**

**2. Блокировка ячеек.**

**3. Защита информации.**

**4. Кодировка.**

**5. Компиляция**

**43. Как называется вирус, который не записывает себя в оперативную память?**

**1. Призрак.**

**2. Невидимый.**

**3. Загрузочный.**

**4. Компьтерный.**

**5. Нерезидентный.**

**44. Как называется вирус, не имеющий ни одного постоянного участка кода в ОЗУ?**

**1. Загрузочный.**

**2. Компьтерный.**

**3. Нерезидентный.**

**4. Резидентный.**

**5.Призрак**

**45. Как называется вирус, который активизируется в оперативную память?**

**1. Призрак.**

**2. Резидентный.**

**3. Загрузочный.**

**4. Сетевой**

**46. Как называется вирус, который распространяется по компьютерной сети?**

**1. Резидентный.**

**2. Сетевой.**

**3. Загрузочный.**

**4.Компьтерный.**

|  |
| --- |
|  |

**Заражение компьютерными вирусами может произойти в процессе ...**

**1. работы с файлами**

**2. форматирования дискеты**

**3. выключения компьютера**

**4. печати на принтере**

**5. правильных ответов нет**

**12. Что необходимо иметь для проверки на вирус жесткого диска?**

**1. защищенную программу**

**2. загрузочную программу**

**3. файл с антивирусной программой**

**4. дискету с антивирусной программой, защищенную от записи**

**5. правильных ответов нет**

**Составные части современного антивируса**

**1. Модем**

**2. Принтер**

**3. Сканер**

**4. Межсетевой экран**

**5. Монитор**

**Варианты ответов:**

**1. 3), 4), 5);**

**2. 1), 2), 5);**

**3. 2), 3), 4);**

**4. 2),3),5),**

**14. Вредоносные программы – это:**

**1.шпионские программы.**

**2. программы, наносящие вред данным и программам, находящимся на компьютере**

**3. антивирусные программы**

**4. программы, наносящие вред пользователю, работающему на зараженном компьютере**

**5. троянские утилиты и сетевые черви**

**RAID-массив это**

**1. Набор жестких дисков, подключенных особым образом**

**2. Антивирусная программа**

**3. Вид хакерской утилиты**

**4. База защищенных данных**

**5. Брандмауэр**

**16 Три составляющий информационной безопасности?**

**1. Доступность, целостность, конфиденциальность**

**2. Неприкосновенность, целостность, устойчивость**

**3. Публичность, доступность, защищённость**

**4. Тайна, охрана, зашифрованность**

**5. Охранность, устойчивость, защищённость**

**6. Конфиденциальность, тайна, публичность.**

**17. Какой стандарт определяет требования к управлению информа-ционной безопасностью?**

**1. ГОСТ Р 15408**

**2. ГОСТ ИСО/МЭК 27001**

**3. ГОСТ ИСО/МЭК 17799**

**4. Нет такого стандарта**

**19 что такое DoS-атака?**

**1. атака, направленная на уязвимости ОС MS-DOS**

**2. атака, осуществляемая обычно при помощи ОС MS-DOS или PC-DOS 3. атака типа "отказ в обслуживании"**

**4. распределённая (distributed) атака**

**5.беспокоющая (disturb) атака**

**6.деструктивная атака**

**7. атака, направленная на настольные (desktop) системы**

**20 Какой из русских терминов, соответствующих английскому "firewall", является официальным?**

**1. файервол**

**2.брандмауэр**

**3. межсетевой экран**

**4. сетевой фильтр**

**5. пакетный фильтр**

**6. фильтр**

**7. огненная стена**

**21. Какой из уровней называется транспортным в 7-уровневой модели OSI?**

**1. 1-й**

**2. 2-й**

**3. 3-й**

**4. 4-й**

**5. 5-й**

**6. 6-й**

**7.7-й**

**22. На каком уровне (в 7-уровневой модели OSI) находится протокол ICMP?**

**1. на канальном**

**2. на прикладном**

**3.на сетевом**

**4.на транспортном**

**5. на уровне представлений**

**6. на физическом**

**7. он находится между уровнями**

**23 На каком уровне утверждается политика информационной безопасности предприятия?**

**1.это не имеет значения**

**2. на уровне руководителя функционального подразделения**

**3. на уровне начальника службы ИБ**

**4. на уровне технического директора**

**5. на уровне высшего руководства предприятия**

**6.на уровне вышестоящего или надзирающего органа**

**24. На кого возлагается ответственность за определение подлежащих защите ресурсов на предприятии?**

**1. на высшее руководство**

**2. на руководителей среднего звена**

**3. на рядовых работников**

**4. на службу ИБ**

**5.на вышестоящие или надзирающие органы**

**6. этот вопрос не разрешён в стандарте по ИБ**

**25. Может ли администратор информационной системы предприятия передавать ответственность и полномочия по обеспечению ИБ поставщику услуг?**

**1. нет**

**2. полномочия - нет, ответственность – да**

**3. полномочия - да, ответственность – нет**

**4. да**

**5. этот вопрос не разрешён в стандарте по ИБ**

**26 Пользователь компьютера с ОС Windows-XP планирует предоставить к файлам в папке Docs доступ так, чтобы все остальные пользователи имели права на чтение. Как можно это сделать?**

**1. копировать файлы из Docs в папку Shared Documents**

**2. предоставить общий доступ к папке Docs с правами по умолчанию**

**3. копировать файлы из Docs в папку My Documents**

**4. предоставить разрешения NTFS группе "Everyone" на уровне "Читатель"**

**27 Какое минимальное разрешение NTFS требуется пользователю, чтобы пр осмотреть содержимое папки в ОС Windows-XP Professional? 1. чтение**

**2. чтение и выполнение**

**3. запись**

**4. изменение**

**5.просмотреть нельзя**

**28. Возможно ли в ОС Windows XP Professional запускать программы от имени другого пользователя не завершая сеанс текущего пользователя?**

**1. возможно только для членов группы Администраторы (Administrators)**

**2. возможно, если известны имя и пароль учетной записи, от имени которой требуется запустить программу**

**3. возможно, кроме программ, работающих неинтерактивно**

**4. возможно за исключением запуска программ от имени пользователя из группы Администраторы (Administrators)**

**5. возможно за исключением запуска программ от имени пользователя**

**6. невозможно**

**29. Какая из перечисленных файловых систем позволяет разграничивать доступ к файлам и папкам?**

**1. FAT-16**

**2.. ISO-9660**

**3. ISO-9660 с расширением Julliet**

**4. FAT-32**

**5. NTFS**

**30. Где хранятся локальные учетные записи в ОС Windows XP Professional?**

**1. в базе RMS**

**2. в файле system32/security/users**

**3. в базе SAM**

**4. в файле user.exe**

**5. локальных учётных записей нет, все учётные записи хранятся на контроллере домена**

**31.Какими методами обнаруживают полиморфные вирусы?**

**1. при помощи сигнатуры**

**2. эвристическими методами и эмуляторами кода**

**3. их невозможно обнаружить**

**32. Какова длина хэш-функции MD5?**

**1. 64 бита**

**2. 128 бит**

**3. 256 бит**

**4. 512 бит**

**5.1024 бита**

**6. 2048 бит**

**7. длина переменная**

**33. Какие вирусы заражают загрузочный сектор гибкого диска или винчестера?**

**1. сетевые вирусы**

**2. загрузочные вирусыв**

**3. макро -вирусы**

**4. все выше перечисленные**

**34. Когда может произойти полное уничтожение информации на дисках?**

**1. При воздействии компьютерных вирусов;**

**2. При форматировании;**

**3. При отказе дисковода жесткого диска;**

**4. Нет правильного ответа**

**35. Какие программы не относится к антивирусным программам?**

**1. AVP**

**2. DrWeb**

**3. NAV**

**4. GIF**

**5. SCAN**

**Варианты ответов:**

**1. AVP, DrWeb, NAV;**

**2. AVP, GIF, SCAN;**

**3, NAV, GIF, SCAN.**

**36. Какие программы не относится к антивирусным программам?**

**1. AVP**

**2. DrWeb**

**3. Spy Sweeper 5.8**

**4. OfficeScan Client 10.0**

**5.SCAN**

**37. Какие программы не относится к антивирусным программам?**

**1. AVP**

**2. Norton AntiVirus 10.1**

**3. Spy Sweeper 5.8**

**4. OfficeScan Client 10.0**

**5.PGP**

**38. Какие программы не относится к антивирусным программам?**

**1. CounterSpy 3.1**

**2. DrWeb**

**3. Spy Sweeper 5.8**

**4. OfficeScan Client 10.0**

**5.КРИПТОН**

**Выберите не верное утверждение.**

**1. От вируса избавится нельзя.**

**2. Вирус замедляет работу на компьютере.**

**3. Вирус может изменить формат данных.**

**4. Вирус выводит посторонние сведения.**

**5. Вирус искажает и уничтожает информацию на компьютере.**

**40. Каким способом компьютер может заразится вирусом?**

**1. Пользователь переписывает на дискету любую информацию с компьютера.**

**2. В процессе форматирования диска.**

**3. Пользователь хотя бы один раз запустить программу, содержащую вирус.**

**4. В процессе неправильной перезагрузки компьютера.**

**5. При запуске программы DRWER.**

**41. Какая программа называется архиватором?**

**1. Программа обнаруживающая и удаляющая вирусы**

**2. Программа, которая может изменить свой объем.**

**3. Программа определяющая и снимающая атрибуты файла.**

**4. Программа уменьшающая объем файла.**

**5. Программа увеличивающая объем файл.**

**42. Как называется процесс включения защиты на ячейках?**

**1. Вирус.**

**2. Блокировка ячеек.**

**3. Защита информации.**

**4. Кодировка.**

**5. Компиляция**

**43. Как называется вирус, который не записывает себя в оперативную память?**

**1. Призрак.**

**2. Невидимый.**

**3. Загрузочный.**

**4. Компьтерный.**

**5. Нерезидентный.**

**44. Как называется вирус, не имеющий ни одного постоянного участка кода в ОЗУ?**

**1. Загрузочный.**

**2. Компьтерный.**

**3. Нерезидентный.**

**4. Резидентный.**

**5.Призрак**

**45. Как называется вирус, который активизируется в оперативную память?**

**1. Призрак.**

**2. Резидентный.**

**3. Загрузочный.**

**4. Сетевой**

**46. Как называется вирус, который распространяется по компьютерной сети?**

**1. Резидентный.**

**2. Сетевой.**

**3. Загрузочный.**

**4.Компьтерный.**

**1. Вирус, который не записывает себя в оперативную память называется нерезидентным.**

**2. Вирус, который активизируется в оперативную память называется резидентным.**

**3. Вирус, который распространяющийся по компьютерной сети называется сетевым.**

**4. Вирус, имеющий свойство модификации своего тела называется "невидимым"**

**48. Для того, чтобы компьютер заразился вирусом, необходимо:**

**1. Переписать на дискету любую информацию с компьютера**

**2. Отформатировать дискету**

**3. Хотя бы один раз выполнить программу, содержащую вирус**

**4. Перезагрузить компьютер**

**5. Запустить программу drweb**

**49. Вирус – это программа, которая**

**1. Мешает нормальной работе компьютера**

**2. Увеличивает память компьютера**

**3. Мешает выведению информации на принтер**

**4. Мешает хранить информацию в сжатом виде**

**5. Входит в состав некоторых компьютерных игр**

**50. Какое высказывание о вирусе не верно?**

**1. Вирус может уменьшать свободную оперативную память компьютера**

**2. Вирус может замедлять работу компьютера**

**3. Вирус выводит посторонние сведения на экран**

**4. Вирус мешает введению дискеты в дисковод**

**5. Вирус искажает и уничтожает информацию в компьютере**

**51. Какие признаки не указывают на наличие вирусов?**

**1. Сильно замедляется работа вычислительной системы; без видимой причины изменяются размеры, содержание и количество файлов.**

**2. Уменьшается объем доступной оперативной памяти; появляются сбои в работе операционной системы, в том числе зависание и прекращение работы.**

**3. На экране монитора появляются необычные сообщения; необычно функционирует клавиатура; форматируется диск без команды пользователя.**

**4. Зажигается лампочка дисковода, когда на диск ничего не должно записываться и читаться с него.**

**5. Западание клавиш на клавиатуре**

**52. Защита информации это:**

**1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;**

**2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;**

**3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;**

**4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;**

**53. Защита информации это:**

**1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;**

**2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;**

**3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;**

**4. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.**

**54. Информационные процессы это:**

**1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;**

**2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;**

**3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;**

**4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;**

**55. Шифрование информации это:**

**1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;**

**2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;**

**3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;**

**4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;**

**56. Доступ к информации это:**

**1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;**

**2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;**

**3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;**

**4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;**

**57. Защита информации от утечки это деятельность по предотвращению:**

**1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;**

**2. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;**

**3. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;**

**58. Защита информации от несанкционированного воздействия это деятельность по предотвращению:**

**1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;**

**2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;**

**3. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;**

**4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;**

**59. Защита информации от непреднамеренного воздействия это деятельность по предотвращению:**

**1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;**

**2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;**

**3. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;**

**4. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.**

**60. Защита информации от разглашения это деятельность по предотвращению:**

**1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;**

**2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию 3. доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;**

**3. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;**

**4. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.**

**61. Защита информации от несанкционированного доступа это деятельность по предотвращению:**

**1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;**

**2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;**

**3. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;**

**4. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.**

**62. Субъект доступа к информации это:**

**1. физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;**

**2. субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;**

**3. субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;**

**4. субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами;**

**63. Носитель информации это:**

**1. физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;**

**2. субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;**

**3. субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;**

**4. субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами;**

**64. Собственник информации это:**

**1. физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;**

**2. субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;**

**3. субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;**

**4. субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами;**

**65. Владелец информации это:**

**1. субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;**

**2. субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;**

**3. субъект, в полном объеме реализующий полномочия, пользования, распоряжения информацией в соответствии с законодательными актами;**

**4. участник правоотношений в информационных процессах.**

**66. Пользователь (потребитель) информации это:**

**1. субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;**

**2. субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;**

**3. субъект, в полном объеме реализующий полномочия, пользования, распоряжения информацией в соответствии с законодательными актами;**

**4. участник правоотношений в информационных процессах.**

**67. Естественные угрозы безопасности информации вызваны:**

**1. деятельностью человека;**

**2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;**

**3. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;**

**4. корыстными устремлениями злоумышленников;**

**5. ошибками при действиях персонала.**

**68. Искусственные угрозы безопасности информации вызваны:**

**1. деятельностью человека;**

**2. . ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;**

**3. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;**

**4. корыстными устремлениями злоумышленников;**

**5. ошибками при действиях персонала.**

**69. К основным непреднамеренным искусственным угрозам АСОИ относится:**

**1. физическое разрушение системы путем взрыва, поджога и т.п.;**

**2. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;**

**3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;**

**4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;**

**5. неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.**

**70. К основным непреднамеренным искусственным угрозам АСОИ относится:**

**1. физическое разрушение системы путем взрыва, поджога и т.п.;**

**2. неправомерное отключение оборудования или изменение режимов работы устройств и программ;**

**3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;**

**4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;**

**5. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.**

**71. К основным непреднамеренным искусственным угрозам АСОИ относится:**

**1. физическое разрушение системы путем взрыва, поджога и т.п.;**

**2. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;**

**3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;**

**4. неумышленная порча носителей информации;**

**5. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.**

**72. К основным непреднамеренным искусственным угрозам АСОИ относится:**

**1. запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы;**

**2. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;**

**3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;**

**4. физическое разрушение системы путем взрыва, поджога и т.п.;**

**73. К основным непреднамеренным искусственным угрозам АСОИ относится:**

**1. физическое разрушение системы путем взрыва, поджога и т.п.;**

**2. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;**

**3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;**

**4. нелегальное внедрение и использование неучтенных программ игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения служебных обязанностей;**

**5. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.**

**74. К основным непреднамеренным искусственным угрозам АСОИ относится:**

**1. физическое разрушение системы путем взрыва, поджога и т.п.;**

**2. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;**

**3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;**

**4. неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной;**

**75. К основным непреднамеренным искусственным угрозам АСОИ относится:**

**1. физическое разрушение системы путем взрыва, поджога и т.п.;**

**2. разглашение, передача или утрата атрибутов разграничения доступа;**

**3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;**

**4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;**

**5. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.**

**76. К основным непреднамеренным искусственным угрозам АСОИ относится:**

**1. физическое разрушение системы путем взрыва, поджога и т.п.;**

**2. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;**

**3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;**

**4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;**

**5 проектирование архитектуры системы, с возможностями, представляющими опасность для работоспособности системы и безопасности информации.**

**77. К основным непреднамеренным искусственным угрозам АСОИ относится:**

**1. игнорирование организационных ограничений при работе в системе;**

**2. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;**

**3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;**

**4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;**

**5. физическое разрушение системы путем взрыва, поджога и т.п..**

**78. К основным непреднамеренным искусственным угрозам АСОИ относится:**

**1. изменение режимов работы устройств или программ, забастовка,**

**2. саботаж персонала, постановка мощных активных помех и т.п.;**

**3. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;**

**4. вход в систему в обход средств защиты;**

**5. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;**

**6. физическое разрушение системы путем взрыва, поджога и т.п..**

**79. К основным непреднамеренным искусственным угрозам АСОИ относится:**

**1. изменение режимов работы устройств или программ, забастовка,**

**2. саботаж персонала, постановка мощных активных помех и т.п.;**

**3. некомпетентное использование, настройка или отключение средств защиты;**

**4. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;**

**5. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;**

**6. физическое разрушение системы путем взрыва, поджога и т.п..**

**80. К основным непреднамеренным искусственным угрозам АСОИ относится:**

**1. изменение режимов работы устройств или программ, забастовка,**

**2. саботаж персонала, постановка мощных активных помех и т.п.;**

**чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;**

**3.перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;**

**4. пересылка данных по ошибочному адресу абонента;**

**5. физическое разрушение системы путем взрыва, поджога и т.п.**

**81. К основным непреднамеренным искусственным угрозам АСОИ относится:**

**1. ввод ошибочных данных;**

**2. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;**

**3. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;**

**4. изменение режимов работы устройств или программ, забастовка, 5. саботаж персонала, постановка мощных активных помех и т.п.;**

**5. физическое разрушение системы путем взрыва, поджога и т.п..**

**82. К основным непреднамеренным искусственным угрозам АСОИ относится:**

**1. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;**

**2. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;**

**3. неумышленное повреждение каналов связи;**

**4. изменение режимов работы устройств или программ, забастовка,**

**5. саботаж персонала, постановка мощных активных помех и т.п.;**

**6. физическое разрушение системы путем взрыва, поджога и т.п..**

**83. К основным преднамеренным искусственным угрозам АСОИ относится:**

**1. неправомерное отключение оборудования или изменение режимов работы устройств и программ;**

**2. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);**

**3. физическое разрушение системы путем взрыва, поджога и т.п.;**

**4. игнорирование организационных ограничений (установленных правил) при работе в системе;**

**5. пересылка данных по ошибочному адресу абонента.**

**84. К основным преднамеренным искусственным угрозам АСОИ относится:**

**1. отключение или вывод из строя систем электропитания, охлаждения и вентиляции, линий связи и т.п.;**

**2. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);**

**3. неправомерное отключение оборудования или изменение режимов работы устройств и программ;**

**4. игнорирование организационных ограничений (установленных правил) при работе в системе;**

**5. пересылка данных по ошибочному адресу абонента.**

**85. К основным преднамеренным искусственным угрозам АСОИ относится:**

**1. пересылка данных по ошибочному адресу абонента;**

**2. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);**

**3. неправомерное отключение оборудования или изменение режимов работы устройств и программ;**

**4. игнорирование организационных ограничений (установленных правил) при работе в системе;**

**5. действия по дезорганизации функционирования системы (изменение режимов работы, забастовка, саботаж персонала, и т.п.).**

**86. К основным преднамеренным искусственным угрозам АСОИ относится:**

**1. пересылка данных по ошибочному адресу абонента;**

**2. внедрение агентов в число персонала системы, в том числе в административную группу, отвечающую за безопасность;**

**3. неправомерное отключение оборудования или изменение режимов работы устройств и программ;**

**4. игнорирование организационных ограничений (установленных правил) при работе в системе;**

**5. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).**

**87. К основным преднамеренным искусственным угрозам АСОИ относится:**

**1. пересылка данных по ошибочному адресу абонента;**

**2. игнорирование организационных ограничений (установленных правил) при работе в системе;**

**3. неправомерное отключение оборудования или изменение режимов работы устройств и программ;**

**4. вербовка персонала или отдельных пользователей, имеющих необходимые полномочия;**

**5. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).**

**88. К основным преднамеренным искусственным угрозам АСОИ относится:**

**1. пересылка данных по ошибочному адресу абонента;**

**2. игнорирование организационных ограничений (установленных правил) при работе в системе;**

**3. применение подслушивающих устройств, дистанционная фото- и видеосъемка и т.п.;**

**4. неправомерное отключение оборудования или изменение режимов работы устройств и программ;**

**5. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).**

**89. К основным преднамеренным искусственным угрозам АСОИ относится:**

**1. пересылка данных по ошибочному адресу абонента;**

**2. игнорирование организационных ограничений (установленных правил) при работе в системе;**

**3. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;**

**4. неправомерное отключение оборудования или изменение режимов работы устройств и программ;**

**5. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).**

**90. К основным преднамеренным искусственным угрозам АСОИ относится:**

**1. перехват данных, передаваемых по каналам связи;**

**2. игнорирование организационных ограничений (установленных правил) при работе в системе;**

**3. пересылка данных по ошибочному адресу абонента;**

**4. неправомерное отключение оборудования или изменение режимов работы устройств и программ;**

**5. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).**

**91. К основным преднамеренным искусственным угрозам АСОИ относится:**

**1. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);**

**2. игнорирование организационных ограничений (установленных правил) при работе в системе;**

**3. пересылка данных по ошибочному адресу абонента;**

**4. неправомерное отключение оборудования или изменение режимов работы устройств и программ;**

**5. хищение носителей информации.**

**92. К основным преднамеренным искусственным угрозам АСОИ относится:**

**1. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);**

**2. игнорирование организационных ограничений (установленных правил) при работе в системе;**

**3. несанкционированное копирование носителей информации;**

**4. неправомерное отключение оборудования или изменение режимов работы устройств и программ;**

**5. пересылка данных по ошибочному адресу абонента.**

**93 К основным преднамеренным искусственным угрозам АСОИ относится:**

**1. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);**

**2. игнорирование производственных отходов (распечаток, записей, списанных носителей информации и т.п.);**

**3. игнорирование организационных ограничений (установленных правил) при работе в системе;**

**4. неправомерное отключение оборудования или изменение режимов работы устройств и программ;**

**5. пересылка данных по ошибочному адресу абонента.**

**94 К основным преднамеренным искусственным угрозам АСОИ относится:**

**1. игнорирование остаточной информации из оперативной памяти и с внешних запоминающих устройств;**

**2. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);**

**3. игнорирование организационных ограничений (установленных правил) при работе в системе;**

**4. неправомерное отключение оборудования или изменение режимов работы устройств и программ;**

**5. пересылка данных по ошибочному адресу абонента.**

**95. К основным преднамеренным искусственным угрозам АСОИ относится:**

**1. неправомерное отключение оборудования или изменение режимов работы устройств и программ;**

**2. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);**

**3. игнорирование организационных ограничений (установленных правил) при работе в системе;**

**4. незаконное получение паролей и других реквизитов разграничения доступа;**

**5. пересылка данных по ошибочному адресу абонента.**

**96 К основным преднамеренным искусственным угрозам АСОИ относится:**

**1. неправомерное отключение оборудования или изменение режимов работы устройств и программ;**

**2. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);**

**3. игнорирование организационных ограничений (установленных правил) при работе в системе;**

**4. пересылка данных по ошибочному адресу абонента;**

**5. несанкционированное использование терминалов пользователей, имеющих локальные физические характеристики.**

**97. К основным преднамеренным искусственным угрозам АСОИ относится:**

**1. неправомерное отключение оборудования или изменение режимов работы устройств и программ;**

**2. раскрытие шифров криптозащиты информации;**

**3. игнорирование организационных ограничений (установленных правил) при работе в системе;**

**4. пересылка данных по ошибочному адресу абонента;**

**5. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).**

**98. К основным преднамеренным искусственным угрозам АСОИ относится:**

**1. неправомерное отключение оборудования или изменение режимов работы устройств и программ;**

**2. пересылка данных по ошибочному адресу абонента;**

**3. игнорирование организационных ограничений (установленных правил) при работе в системе;**

**4. внедрение аппаратных спецвложений, программных "закладок" и "вирусов";**

**5. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).**

**99. К основным преднамеренным искусственным угрозам АСОИ относится:**

**1. неправомерное отключение оборудования или изменение режимов работы устройств и программ;**

**2. незаконное подключение к линиям связи с целью работы "между строк";**

**3. игнорирование организационных ограничений (установленных правил) при работе в системе;**

**4. пересылка данных по ошибочному адресу абонента;**

**5. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).**

**100. К основным преднамеренным искусственным угрозам АСОИ относится:**

**1. неправомерное отключение оборудования или изменение режимов работы устройств и программ;**

**2. игнорирование организационных ограничений (установленных правил) при работе в системе;**

**3. незаконное подключение к линиям связи с целью подмены законного пользователя путем его отключения после входа в систему;**

**4. пересылка данных по ошибочному адресу абонента;**

**5. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).**

**101. К внутренним нарушителям информационной безопасности относится:**

**1. клиенты;**

**2. пользователи системы;**

**3. посетители;**

**4. любые лица, находящиеся внутри контролируемой территории;**

**5. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации.**

**102. К внутренним нарушителям информационной безопасности относится:**

**1. клиенты;**

**2. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;**

**3. посетители;**

**4. любые лица, находящиеся внутри контролируемой территории;**

**5. персонал, обслуживающий технические средства.**

**103. К внутренним нарушителям информационной безопасности относится:**

**1. сотрудники отделов разработки и сопровождения ПО;**

**2. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;**

**3. посетители;**

**4. любые лица, находящиеся внутри контролируемой территории;**

**клиенты.**

**104. К внутренним нарушителям информационной безопасности относится:**

**1. посетители;**

**2. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;**

**3. технический персонал, обслуживающий здание;**

**4. любые лица, находящиеся внутри контролируемой территории;**

**5. клиенты.**

**105. К внутренним нарушителям информационной безопасности относится:**

**1. посетители;**

**2. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;**

**3. любые лица, находящиеся внутри контролируемой территории;**

**4. сотрудники службы безопасности;**

**5. клиенты.**

**106. К внутренним нарушителям информационной безопасности относится:**

**1. посетители;**

**руководители различных уровней;**

**2. любые лица, находящиеся внутри контролируемой территории;**

**3. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;**

**4. клиенты.**

**107. К посторонним лицам нарушителям информационной безопасности относится:**

**1. пользователи;**

**2. персонал, обслуживающий технические средства;**

**3. клиенты;**

**4. технический персонал, обслуживающий здание;**

**5. сотрудники службы безопасности.**

**108. К посторонним лицам нарушителям информационной безопасности относится:**

**1. пользователи;**

**2. персонал, обслуживающий технические средства;**

**3. технический персонал, обслуживающий здание;**

**4. посетители;**

**5. сотрудники службы безопасности.**

**109. К посторонним лицам нарушителям информационной безопасности относится:**

**1. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;**

**2. персонал, обслуживающий технические средства;**

**3. технический персонал, обслуживающий здание;**

**4. пользователи;**

**5. сотрудники службы безопасности.**

**110. К посторонним лицам нарушителям информационной безопасности относится:**

**1. сотрудники службы безопасности;**

**2. персонал, обслуживающий технические средства;**

**3. технический персонал, обслуживающий здание;**

**4. пользователи;**

**5.. представители конкурирующих организаций.**

**111. К посторонним лицам нарушителям информационной безопасности относится:**

**1. сотрудники службы безопасности;**

**2. лица, нарушившие пропускной режим;**

**3. технический персонал, обслуживающий здание;**

**пользователи;**

**4. персонал, обслуживающий технические средства.**

**112. По характеру воздействия удаленные атаки делятся на:**

**1. условные и безусловные;**

**3. атаки с обратной связью и без обратной связи;**

**4. внутрисегментные и межсегментные;**

**5. пассивные и активные;**

**6. атаки, которые могут реализо­вываться на всех семи уровнях – физическом, канальном, сете­вом, транспортном, сеансовом, представительном и прикладном.**

**113. По цели воздействия удаленные атаки делятся на:**

**1. условные и безусловные;**

**2. атаки с обратной связью и без обратной связи;**

**3. внутрисегментные и межсегментные;**

**4. пассивные и активные;**

**5. атаки в зависимости от нарушения конфиденциальности, целостности и доступности.**

**114. По наличию обратной связи с атакуемым объектом удаленные атаки делятся на:**

**1. условные и безусловные;**

**2. атаки с обратной связью и без обратной связи;**

**3. внутрисегментные и межсегментные;**

**4. пассивные и активные;**

**5. атаки в зависимости от нарушения конфиденциальности, целостности и доступности.**

**115. По расположению субъекта атаки относительно атакуе­мого объекта удаленные атаки делятся на:**

**1. условные и безусловные;**

**2. атаки с обратной связью и без обратной связи;**

**3. внутрисегментные и межсегментные;**

**4. пассивные и активные;**

**5. атаки в зависимости от нарушения конфиденциальности, целостности и доступности.**

**116. По уровню эталонной модели взаимосвязи открытых сис­тем OSI Международной организации стандартизации (ISO) удаленные атаки делятся на:**

**1. условные и безусловные;**

**2. атаки с обратной связью и без обратной связи;**

**3. внутрисегментные и межсегментные;**

**4. пассивные и активные;**

**5. атаки, которые могут реализо­вываться на всех семи уровнях.**

**117. Атака, которая позволяет изучить логику работы сети:**

**1. подмена доверенного объекта или субъекта распределенной вычислительной сети;**

**2. ложный объект распределенной вычислительной сети;**

**3. анализ сетевого трафика;**

**4. отказ в обслуживании;**

**5. удаленный контроль над станцией в сети.**

**118. Атака позволяющая перехватить поток передаваемых данных, которыми обме­ниваются компоненты сетевой ОС:**

**1. подмена доверенного объекта или субъекта распределенной вычислительной сети;**

**2. ложный объект распределенной вычислительной сети;**

**3. анализ сетевого трафика;**

**4. отказ в обслуживании;**

**5. удаленный контроль над станцией в сети.**

**119. Атака эффективно реализующаяся в системах, где применяются нестойкие алгоритмы идентификации/аутентификации хостов, пользователей:**

**1. подмена доверенного объекта или субъекта распределенной вычислительной сети;**

**2. ложный объект распределенной вычислительной сети;**

**3. анализ сетевого трафика;**

**4. отказ в обслуживании;**

**5. удаленный контроль над станцией в сети.**

**120. Атака, которая заключается в навязывании ложного маршрута из-за недостатков в алго­ритмах маршрутизации:**

**1. подмена доверенного объекта или субъекта распределенной вычислительной сети;**

**2. ложный объект распределенной вычислительной сети;**

**3. анализ сетевого трафика;**

**4. отказ в обслуживании;**

**5. удаленный контроль над станцией в сети.**

**121. Основные угрозы доступности информации:**

**1. непреднамеренные ошибки пользователей**

**2. злонамеренное изменение данных**

**3. хакерская атака**

**4. перехват данных**

**122. Основные угрозы доступности информации:**

**1. злонамеренное изменение данных**

**2. хакерская атака**

**3.отказ программного и аппаратно обеспечения**

**4. перехват данных**

**123. Основные угрозы доступности информации:**

**2. злонамеренное изменение данных**

**3. хакерская атака**

**4. разрушение или повреждение помещений**

**5. перехват данных**

**124. Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ)**

**1.МЭ были разработаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения;**

**2. МЭ были разработаны для активного или пассивного обнаружения, а СОВ – для активной или пассивной защиты;**

**3. МЭ работают только на сетевом уровне, а СОВ – еще и на физическом.**

**124. Сервис безопасности:**

**1. идентификация и аутентификация**

**2. инверсия паролей**

**3. регулирование конфликтов**

**4.кэширование записей**

**125 Сервис безопасности:**

**1. шифрование**

**2. инверсия паролей**

**3. регулирование конфликтов**

**4. кэширование записей**

**126. Сервис безопасности:**

**1. инверсия паролей**

**2. контроль целостности**

**3. регулирование конфликтов**

**4. кэширование записей**

**127. Сервисы безопасности:**

**1.инверсия паролей**

**2. регулирование конфликтов**

**3. экранирование**

**4. кэширование записей**

**128 Под угрозой удаленного администрирования в компьютерной сети понимается угроза ...**

**1. несанкционированного управления удаленным компьютером**

**2. внедрения агрессивного программного кода в рамках активных объектов Web-страниц**

**3. перехвата или подмены данных на путях транспортировки**

**вмешательства в личную жизнь**

**4. поставки неприемлемого содержания**

# **К формам защиты информации не относится…**

# **1. Правовая**

**2. организационно-техническая**

**3. страховая**

**130. К формам защиты информации не относится...**

**1. аналитическая**

**2. правовая**

**3.организационно-техническая**

**131. К вредоносным программам относятся:**

**1) Потенциально опасные программы**

**2) Вирусы, черви, трояны**

**3) Шпионские и рекламмные программы**

**4) Вирусы, программы-шутки, антивирусное программное обеспечение**

**5) Межсетевой экран, брандмауэр**

**Варианты ответов:**

1. **1), 2), 3);**
2. **2), 4), 5);**
3. **1), 4),5);**
4. **3), 4), 5).**

**132. Сетевые черви это:**

**1) Вирусы, которые проникнув на компьютер, блокируют работу сети**

**2) Вредоносные программы, устанавливающие скрытно от пользователя другие вредоносные программы и утилиты**

**3) Вирусы, которые внедряются в документы под видом макросов**

**4) Хакерские утилиты управляющие удаленным доступом компьютера**

**5) Вредоносные программы, которые проникают на компьютер, используя сервисы компьютерных сетей**

**Вредоносная программа, которая подменяет собой загрузку некоторых программ при загрузке системы называется...**

**1) Загрузочный вирус**

**2) Макровирус**

**3) Троян**

**4) Сетевой червь**

**5) Файловый вирус**

**134. Программа, осуществляющая несанкционированные действия по сбору, и передаче информации злоумышленнику, а также ее разрушение или злонамеренную модификацию?**

**1) Троян**

**2) Загрузочный вирус**

**3) Макровирус**

**4) Сетевой червь**

**5) Файловый вирус**

**Руткит - это...**

**1. программа для скрытого взятия под контроль взломанной системы**

**2. вредоносная программа, выполняющая несанкционированные действия по передаче управления компьютером удаленному пользователю**

**3. разновидность межсетевого экрана**

**4. программа использующая для распространения Рунет (Российскую часть Интернета)**

**5) вредоносная программа, маскирующаяся под макрокоманду**

**136. Компьютерные вирусы это…**

**1) Программы, которые могут размножаться, и скрыто внедрять свои копии в файлы, загрузочные сектора дисков, документы**

**2) Вредоносные программы, наносящие вред данным.**

**3) Программы, уничтожающие данные на жестком диске**

**.**

**4) Программы, заражающие загрузочный сектор дисков и препятствующие загрузке компьютера**

**5) Это крипты, помещенные на зараженных интернет-страничках**

**137. Антивирусный сканер:**

**1. находит зараженные вирусами файлы, "лечит" их, т.е. удаляет из файла тело вируса, возвращая файлы в исходное состояние;**

**2. обеспечивает поиск вирусов путем подсчета и сравнения с эталоном контрольной суммы;**

**3. запоминает исходное состояние, когда компьютер не заражен вирусом, затем периодически сравнивает текущее состояние с исходным;**

**4. просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок;**

**5. обнаруживает подозрительные действия при работе компьютера, характерные для вирусов.**

**138. Антивирусный детектор:**

**1. просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок;**

**2. обеспечивает поиск вирусов путем подсчета и сравнения с эталоном контрольной суммы;**

**3. находит зараженные вирусами файлы, "лечит" их, т.е. удаляет из файла тело вируса, возвращая файлы в исходное состояние;**

**4. запоминает исходное состояние, когда компьютер не заражен вирусом, затем периодически сравнивает текущее состояние с исходным;**

**5. обнаруживает подозрительные действия при работе компьютера, характерные для вирусов.**

**139. Антивирусный доктор:**

**1. находит зараженные вирусами файлы и удаляет из файла тело вируса, возвращая файлы в исходное состояние;**

**2. обеспечивает поиск вирусов путем подсчета и сравнения с эталоном контрольной суммы;**

**3. запоминает исходное состояние, когда компьютер не заражен вирусом, затем периодически сравнивает текущее состояние с исходным;**

**4. просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок;**

**5. обнаруживает подозрительные действия при работе компьютера, характерные для вирусов.**

**140. Антивирусный ревизор:**

**1. запоминает исходное состояние, когда компьютер не заражен вирусом, затем периодически сравнивает текущее состояние с исходным;**

**2. обеспечивает поиск вирусов путем подсчета и сравнения с эталоном контрольной суммы;**

**3. находит зараженные вирусами файлы и удаляет из файла тело вируса, возвращая файлы в исходное состояние;**

**4. просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок;**

**5. обнаруживает подозрительные действия при работе компьютера, характерные для вирусов.**

**141. Антивирусный сторож:**

**1. постоянно находятся в ОП и обеспечивают проверку файлов в процессе их загрузки в ОП ;**

**2. находит зараженные вирусами файлы и удаляет из файла тело вируса, возвращая файлы в исходное состояние;**

**3. запоминает исходное состояние, когда компьютер не заражен вирусом, затем периодически сравнивает текущее состояние с исходным;**

**4. просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок;**

**5. обнаруживает подозрительные действия при работе компьютера, характерные для вирусов.**

**142. Антивирусный иммунизатор:**

**1. модифицирует программу или диск таким образом, чтобы вирус воспринимал их зараженными и поэтому не внедрялся;**

**2. обеспечивает поиск вирусов путем подсчета и сравнения с эталоном контрольной суммы;**

**3. находит зараженные вирусами файлы и удаляет из файла тело вируса, возвращая файлы в исходное состояние;**

**4. просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок;**

**5. обнаруживает подозрительные действия при работе компьютера, характерные для вирусов.**

**143. Метод защиты информации ограничение доступа заключается в:**

**1. разделении информации, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;**

**2. контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления;**

**3. создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями;**

**4. том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;**

**5. проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.**

**144. Метод защиты информации контроль доступа к аппаратуре заключается в:**

**1. создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями;**

**2. контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления;**

**3. разделении информации, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;**

**4. том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;**

**5. проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.**

**145. Метод защиты информации разграничение и контроль доступа к информации заключается в:**

**1. том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;**

**2. разделении информации, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;**

**3. контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления;**

**4. создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями;**

**5. проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.**

**146. Метод защиты информации предоставление привилегий на доступ заключается в:**

**1. разделении информации, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;**

**2. контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления;**

**3. создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями;**

**том, что из числа допущенных к ней должностных лиц выделяется группа, 4. которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;**

**5.проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.**

**147. Метод защиты информации идентификация и установление подлинности заключается в:**

**1. проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.**

**2. контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления;**

**3. создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями;**

**4. разделении информации, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;**

**5. том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;**

**148. Шифрование методом подстановки:**

**1. символами, взятыми из одного или нескольких алфавитов;символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста;**

**2. символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности;**

**3. шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор;**

**4. символы шифруемого текста заменяются другими**

**5. замена слов и предложений исходной информации шифрованными.**

**149. Шифрование методом перестановки:**

**1. символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста;**

**2. символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности;**

**3. шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор;**

**4. символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов;**

**5. замена слов и предложений исходной информации шифрованными.**

**150. Шифрование методом гаммирования:**

**1. символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности;**

**2. символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста;**

**3. шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор;**

**4. символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов;**

**5. замена слов и предложений исходной информации шифрованными.**

**151. Шифрование методом аналитических преобразований:**

**1. шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор;**

**2. символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста;**

**3. символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности;**

**4. символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов;**

**5. замена слов и предложений исходной информации шифрованными.**

**152. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод:**

**1. перестановки;**

**2. гаммирования;**

**3. подстановки;**

**4. кодирования;**

**5. аналитических преобразований.**

**153. Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов, это метод:**

**1. подстановки;**

**2. гаммирования;**

**3. кодирования;**

**4. перестановки;**

**5. аналитических преобразований.**

**154. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:**

**1. гаммирования;**

**2. подстановки;**

**3. кодирования;**

**4. перестановки;**

**5. аналитических преобразований.**

**155. Шифрование заключается в получении нового вектора как результата. умножения матрицы на исходный вектор, это метод:**

**1. аналитических преобразований.**

**2. гаммирования;**

**3. подстановки;**

**4. кодирования;**

**5. перестановки;**

**155. Шифр DES это:**

**1. симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16 кратной перестановке данных, для зашифровывания использует ключ в 56 бит.**

**2. система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки;**

**3. система с открытым ключом предназначенная как для шифрования, так и для аутентификации основана на трудности разложения очень больших целых чисел на простые сомножители;**

**4. блочные шифры с ключом переменной длины.**

**5. шифр состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами;**

**156. Шифр IDEA это:**

**1. шифр состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами;**

**2. система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки;**

**3. система с открытым ключом предназначенная как для шифрования, так и для аутентификации основана на трудности разложения очень больших целых чисел на простые сомножители;**

**4. блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны;**

**5. симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16 кратной перестановке данных, для зашифровывания использует ключ в 56 бит.**

**157. Шифр RC2 или RC4 это:**

**1. блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны;**

**2. система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки;**

**3. система с открытым ключом предназначенная как для шифрования, так и для аутентификации основана на трудности разложения очень больших целых чисел на простые сомножители;**

**4. шифр состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами;**

**5. симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16 кратной перестановке данных, для зашифровывания использует ключ в 56 бит.**

**158. Шифр RSA это:**

**1. система с открытым ключом предназначенная как для шифрования, так и для аутентификации основана на трудности разложения очень больших целых чисел на простые сомножители;**

**2. система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки;**

**3. блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны;**

**4. шифр состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами;**

**5. симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16 кратной перестановке данных, для зашифровывания использует ключ в 56 бит.**

**159. Шифр ГОСТ 28147-89 это:**

**1. система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки;**

**2. система с открытым ключом предназначенная как для шифрования, так и для аутентификации основана на трудности разложения очень больших целых чисел на простые сомножители;**

**3. блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны;**

**4. шифр состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами;**

**5. симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16 кратной перестановке данных, для зашифровывания использует ключ в 56 бит.**

**160. Система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки – это шифр:**

**1. ГОСТ 28147-89;**

**2. IDEA;**

**3. RSA;**

**4. RC2 или RC4;**

**5. DES.**

**161. Система с открытым ключом предназначенная как для шифрования, так и для аутентификации основана на трудности разложения очень больших целых чисел на простые сомножители – это шифр:**

**1. IDEA;**

**2. RSA;**

**3. ГОСТ 28147-89;**

**4. RC2 или RC4;**

**5. DES.**

**162. Блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны – это шифр:**

**1. IDEA;**

**2. RSA;**

**3. ГОСТ 28147-89;**

**4. RC2 или RC4;**

**5. DES.**

**163. Шифр состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами – это шифр:**

**1. IDEA;**

**2. RSA;**

**3. ГОСТ 28147-89;**

**4. RC2 или RC4;**

**5.DES.**

**164. Симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16 кратной перестановке данных, для зашифровывания использует ключ в 56 бит – это шифр:**

**1. IDEA;**

**2. RSA;**

**3. ГОСТ 28147-89;**

**4. RC2 или RC4;**

**5. DES.**

# **К формам защиты информации не относится...**

**[⇐ Предыдущая](https://lektsii.org/15-11748.html)**

**[1](https://lektsii.org/15-11747.html)**

**[2](https://lektsii.org/15-11748.html)**

**3**

|  |
| --- |
|  |

**1. Правовая**

**2. организационно-техническая**

**3. страховая**

**130. К формам защиты информации не относится...**

**1. аналитическая**

**2. правовая**

**3.организационно-техническая**

**131. К вредоносным программам относятся:**

**1) Потенциально опасные программы**

**2) Вирусы, черви, трояны**

**3) Шпионские и рекламмные программы**

**4) Вирусы, программы-шутки, антивирусное программное обеспечение**

**5) Межсетевой экран, брандмауэр**

**Варианты ответов:**

1. **1), 2), 3);**
2. **2), 4), 5);**
3. **1), 4),5);**
4. **3), 4), 5).**

**132. Сетевые черви это:**

**1) Вирусы, которые проникнув на компьютер, блокируют работу сети**

**2) Вредоносные программы, устанавливающие скрытно от пользователя другие вредоносные программы и утилиты**

**3) Вирусы, которые внедряются в документы под видом макросов**

**4) Хакерские утилиты управляющие удаленным доступом компьютера**

**5) Вредоносные программы, которые проникают на компьютер, используя сервисы компьютерных сетей**

**Вредоносная программа, которая подменяет собой загрузку некоторых программ при загрузке системы называется...**

**1) Загрузочный вирус**

**2) Макровирус**

**3) Троян**

**4) Сетевой червь**

**5) Файловый вирус**

**134. Программа, осуществляющая несанкционированные действия по сбору, и передаче информации злоумышленнику, а также ее разрушение или злонамеренную модификацию?**

**1) Троян**

**2) Загрузочный вирус**

**3) Макровирус**

**4) Сетевой червь**

**5) Файловый вирус**

**Руткит - это...**

**1. программа для скрытого взятия под контроль взломанной системы**

**2. вредоносная программа, выполняющая несанкционированные действия по передаче управления компьютером удаленному пользователю**

**3. разновидность межсетевого экрана**

**4. программа использующая для распространения Рунет (Российскую часть Интернета)**

**5) вредоносная программа, маскирующаяся под макрокоманду**

**136. Компьютерные вирусы это…**

**1) Программы, которые могут размножаться, и скрыто внедрять свои копии в файлы, загрузочные сектора дисков, документы**

**2) Вредоносные программы, наносящие вред данным.**

**3) Программы, уничтожающие данные на жестком диске**

**.**

**4) Программы, заражающие загрузочный сектор дисков и препятствующие загрузке компьютера**

**5) Это крипты, помещенные на зараженных интернет-страничках**

**137. Антивирусный сканер:**

**1. находит зараженные вирусами файлы, "лечит" их, т.е. удаляет из файла тело вируса, возвращая файлы в исходное состояние;**

**2. обеспечивает поиск вирусов путем подсчета и сравнения с эталоном контрольной суммы;**

**3. запоминает исходное состояние, когда компьютер не заражен вирусом, затем периодически сравнивает текущее состояние с исходным;**

**4. просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок;**

**5. обнаруживает подозрительные действия при работе компьютера, характерные для вирусов.**

**138. Антивирусный детектор:**

**1. просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок;**

**2. обеспечивает поиск вирусов путем подсчета и сравнения с эталоном контрольной суммы;**

**3. находит зараженные вирусами файлы, "лечит" их, т.е. удаляет из файла тело вируса, возвращая файлы в исходное состояние;**

**4. запоминает исходное состояние, когда компьютер не заражен вирусом, затем периодически сравнивает текущее состояние с исходным;**

**5. обнаруживает подозрительные действия при работе компьютера, характерные для вирусов.**

**139. Антивирусный доктор:**

**1. находит зараженные вирусами файлы и удаляет из файла тело вируса, возвращая файлы в исходное состояние;**

**2. обеспечивает поиск вирусов путем подсчета и сравнения с эталоном контрольной суммы;**

**3. запоминает исходное состояние, когда компьютер не заражен вирусом, затем периодически сравнивает текущее состояние с исходным;**

**4. просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок;**

**5. обнаруживает подозрительные действия при работе компьютера, характерные для вирусов.**

**140. Антивирусный ревизор:**

**1. запоминает исходное состояние, когда компьютер не заражен вирусом, затем периодически сравнивает текущее состояние с исходным;**

**2. обеспечивает поиск вирусов путем подсчета и сравнения с эталоном контрольной суммы;**

**3. находит зараженные вирусами файлы и удаляет из файла тело вируса, возвращая файлы в исходное состояние;**

**4. просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок;**

**5. обнаруживает подозрительные действия при работе компьютера, характерные для вирусов.**

**141. Антивирусный сторож:**

**1. постоянно находятся в ОП и обеспечивают проверку файлов в процессе их загрузки в ОП ;**

**2. находит зараженные вирусами файлы и удаляет из файла тело вируса, возвращая файлы в исходное состояние;**

**3. запоминает исходное состояние, когда компьютер не заражен вирусом, затем периодически сравнивает текущее состояние с исходным;**

**4. просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок;**

**5. обнаруживает подозрительные действия при работе компьютера, характерные для вирусов.**

**142. Антивирусный иммунизатор:**

**1. модифицирует программу или диск таким образом, чтобы вирус воспринимал их зараженными и поэтому не внедрялся;**

**2. обеспечивает поиск вирусов путем подсчета и сравнения с эталоном контрольной суммы;**

**3. находит зараженные вирусами файлы и удаляет из файла тело вируса, возвращая файлы в исходное состояние;**

**4. просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок;**

**5. обнаруживает подозрительные действия при работе компьютера, характерные для вирусов.**

**143. Метод защиты информации ограничение доступа заключается в:**

**1. разделении информации, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;**

**2. контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления;**

**3. создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями;**

**4. том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;**

**5. проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.**

**144. Метод защиты информации контроль доступа к аппаратуре заключается в:**

**1. создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями;**

**2. контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления;**

**3. разделении информации, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;**

**4. том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;**

**5. проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.**

**145. Метод защиты информации разграничение и контроль доступа к информации заключается в:**

**1. том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;**

**2. разделении информации, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;**

**3. контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления;**

**4. создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями;**

**5. проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.**

**146. Метод защиты информации предоставление привилегий на доступ заключается в:**

**1. разделении информации, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;**

**2. контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления;**

**3. создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями;**

**том, что из числа допущенных к ней должностных лиц выделяется группа, 4. которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;**

**5.проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.**

**147. Метод защиты информации идентификация и установление подлинности заключается в:**

**1. проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.**

**2. контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления;**

**3. создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями;**

**4. разделении информации, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;**

**5. том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;**

**148. Шифрование методом подстановки:**

**1. символами, взятыми из одного или нескольких алфавитов;символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста;**

**2. символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности;**

**3. шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор;**

**4. символы шифруемого текста заменяются другими**

**5. замена слов и предложений исходной информации шифрованными.**

**149. Шифрование методом перестановки:**

**1. символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста;**

**2. символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности;**

**3. шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор;**

**4. символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов;**

**5. замена слов и предложений исходной информации шифрованными.**

**150. Шифрование методом гаммирования:**

**1. символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности;**

**2. символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста;**

**3. шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор;**

**4. символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов;**

**5. замена слов и предложений исходной информации шифрованными.**

**151. Шифрование методом аналитических преобразований:**

**1. шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор;**

**2. символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста;**

**3. символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности;**

**4. символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов;**

**5. замена слов и предложений исходной информации шифрованными.**

**152. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод:**

**1. перестановки;**

**2. гаммирования;**

**3. подстановки;**

**4. кодирования;**

**5. аналитических преобразований.**

**153. Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов, это метод:**

**1. подстановки;**

**2. гаммирования;**

**3. кодирования;**

**4. перестановки;**

**5. аналитических преобразований.**

**154. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:**

**1. гаммирования;**

**2. подстановки;**

**3. кодирования;**

**4. перестановки;**

**5. аналитических преобразований.**

**155. Шифрование заключается в получении нового вектора как результата. умножения матрицы на исходный вектор, это метод:**

**1. аналитических преобразований.**

**2. гаммирования;**

**3. подстановки;**

**4. кодирования;**

**5. перестановки;**

**155. Шифр DES это:**

**1. симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16 кратной перестановке данных, для зашифровывания использует ключ в 56 бит.**

**2. система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки;**

**3. система с открытым ключом предназначенная как для шифрования, так и для аутентификации основана на трудности разложения очень больших целых чисел на простые сомножители;**

**4. блочные шифры с ключом переменной длины.**

**5. шифр состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами;**

**156. Шифр IDEA это:**

**1. шифр состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами;**

**2. система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки;**

**3. система с открытым ключом предназначенная как для шифрования, так и для аутентификации основана на трудности разложения очень больших целых чисел на простые сомножители;**

**4. блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны;**

**5. симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16 кратной перестановке данных, для зашифровывания использует ключ в 56 бит.**

**157. Шифр RC2 или RC4 это:**

**1. блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны;**

**2. система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки;**

**3. система с открытым ключом предназначенная как для шифрования, так и для аутентификации основана на трудности разложения очень больших целых чисел на простые сомножители;**

**4. шифр состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами;**

**5. симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16 кратной перестановке данных, для зашифровывания использует ключ в 56 бит.**

**158. Шифр RSA это:**

**1. система с открытым ключом предназначенная как для шифрования, так и для аутентификации основана на трудности разложения очень больших целых чисел на простые сомножители;**

**2. система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки;**

**3. блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны;**

**4. шифр состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами;**

**5. симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16 кратной перестановке данных, для зашифровывания использует ключ в 56 бит.**

**159. Шифр ГОСТ 28147-89 это:**

**1. система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки;**

**2. система с открытым ключом предназначенная как для шифрования, так и для аутентификации основана на трудности разложения очень больших целых чисел на простые сомножители;**

**3. блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны;**

**4. шифр состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами;**

**5. симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16 кратной перестановке данных, для зашифровывания использует ключ в 56 бит.**

**160. Система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки – это шифр:**

**1. ГОСТ 28147-89;**

**2. IDEA;**

**3. RSA;**

**4. RC2 или RC4;**

**5. DES.**

**161. Система с открытым ключом предназначенная как для шифрования, так и для аутентификации основана на трудности разложения очень больших целых чисел на простые сомножители – это шифр:**

**1. IDEA;**

**2. RSA;**

**3. ГОСТ 28147-89;**

**4. RC2 или RC4;**

**5. DES.**

**162. Блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны – это шифр:**

**1. IDEA;**

**2. RSA;**

**3. ГОСТ 28147-89;**

**4. RC2 или RC4;**

**5. DES.**

**163. Шифр состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами – это шифр:**

**1. IDEA;**

**2. RSA;**

**3. ГОСТ 28147-89;**

**4. RC2 или RC4;**

**5.DES.**

**164. Симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16 кратной перестановке данных, для зашифровывания использует ключ в 56 бит – это шифр:**

**1. IDEA;**

**2. RSA;**

**3. ГОСТ 28147-89;**

**4. RC2 или RC4;**

**5. DES.**