Профессионально-педагогический колледж федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Саратовский государственный технический университет имени Гагарина Ю.А.»

Конкурсное задание, разработанное для проведения Всероссийской олимпиады профессионального мастерства обучающихся по специальности 10.02.03 «Информационная безопасность автоматизированных систем» среднего профессионального образования

1. Введение

Всероссийская олимпиада профессионального мастерства обучающихся по специальности 10.02.03 «Информационная безопасность автоматизированных систем» среднего профессионального образования включает выполнение теоретического и профессионального конкурсных заданий. Содержание конкурсных заданий соответствует федеральному государственному образовательному стандарту среднего профессионального образования по специальности 10.02.03 «Информационная безопасность автоматизированных систем», конкурсные задания разработаны с учётом основных требований работодателей.

Теоретическое задание представляется в виде тестов и выполняется на компьютере. Теоретическое задание включает в себя вопросы, охватывающие содержание общепрофессиональных дисциплин и профессиональных модулей по специальности 10.02.03 «Информационная безопасность автоматизированных систем»:

- основы информационной безопасности;
- технические средства информатизации;
- сети и системы передачи информации;
- операционные системы;
- электроника и схемотехника;
- основы алгоритмизации и программирования;
- базы данных;
- ПМ.01 Эксплуатация подсистем безопасности автоматизированных систем;
- ПМ. 02 Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах.

Теоретическое задание насчитывает 270 вопросов.

Вопросы тестового задания могут быть нескольких типов:

- Множественный выбор с одним или несколькими вариантами ответов;
- Вопросы на соответствие;
- Открытые вопросы (требуется ввод ответа).

Содержание профессионального задания нацеливает участников Всероссийской олимпиады на демонстрацию видов профессиональной деятельности, в соответствии с профессиональными модулями по специальности 10.02.03 «Информационная безопасность автоматизированных систем»:

- ПМ.01 Эксплуатация подсистем безопасности автоматизированных систем;
- ПМ. 02 Применение программно-аппаратных средств обеспечения информационной

безопасности в автоматизированных системах.

Профессиональное задание выполняется участниками Всероссийской олимпиады с применением теоретических знаний и практических навыков, заключающихся в проектировании, разработке решения по заданным параметрам с практическим выполнением задания и контролем соответствия результата проектным показателям.

2. Теоретическое задание

Операционные системы

1. **Безопасная информационная система – это система, которая …**
   а. проникает в компьютер под видом легального пользователя;
   б. надежно хранит информацию и гарантирует неизменность данных;
   в. использует чужие пароли, захватывает и анализирует сетевые сообщения.
2. **Конфиденциальность – гарантия того, что …**
   а. обеспечивается запрет изменять, модифицировать, разрушать или создавать данные;
   б. авторизованные пользователи всегда получат доступ к данным;
   в. секретные данные будут доступны только тем пользователям, которым этот доступ разрешен.
3. **Как можно интерпретировать свойство конфиденциальности, примененное к устройству печати?**
   а. устройство готово к использованию всякий раз, когда в этом возникает необходимость;
   б. неизменность параметров настройки данного устройства;
   в. доступ к устройству имеют только те пользователи, которым этот доступ разрешен.
4. **Любое действие, которое направлено на нарушение конфиденциальности, целостности и/или доступности информации, а также на нелегальное использование других ресурсов сети, называется …**
5. **Доступность – гарантия того, что …**
   а. авторизованные пользователи всегда получат доступ к данным;
   б. секретные данные будут доступны только тем пользователям, которым этот доступ разрешен;
   в. обеспечивается запрет изменять, модифицировать, разрушать или создавать данные.
6. **Вероятная оценка величины возможного ущерба, который может понести владелец информационного ресурса в результате успешно проведенной атаки– это …**
7. **Вставьте пропущенные слова в утверждении: «значение риска тем выше, чем … уязвимой является существующая система безопасности и чем … вероятность реализации атаки».**
   а. … менее … ниже;
   б. …. более … выше;
   в. … менее … выше.

8. **Целостность – гарантия того, что …**

а. авторизованные пользователи всегда получат доступ к данным;
б. обеспечивается запрет изменять, модифицировать, разрушать или создавать данные;
в. секретные данные будут доступны только тем пользователям, которым этот доступ разрешен.

9. Как можно интерпретировать свойство доступности, примененное к устройству печати?

а. устройство готово к использованию всякий раз, когда в этом возникает необходимость;
б. неизменность параметров настройки данного устройства;
в. доступ к устройству имеют только те пользователи, которым этот доступ разрешен.

10. Что из перечисленного можно отнести к типовым функциональным дефектам ОС, которые могут привести к созданию каналов утечки данных?

а. идентификация;
б. список паролей;
в. разрыв связей.

11. Угрозы могут быть разделены на …

а. законные и незаконные;
б. легальные и нелегальные;
в. умышленные и неумышленные.

12. Незаконное проникновение может быть реализовано …

а. следствием низкой квалификации лояльных сотрудников;
б. следствием отказа всего файлового сервера;
в. через уязвимые места в системе безопасности.

13. К какому роду угроз относятся последствия ненадежной работы программных и аппаратных средств системы?

а. неумышленные угрозы;
б. незаконное проникновение;
в. незаконное проникновение в один из компьютеров сети под видом легального пользователя.

14. Какие угрозы могут ограничиваться либо пассивным чтением данных или мониторингом системы, либо включать в себя активные действия?

а. незаконные;
б. легальные;
в. умышленные.

15. «Подслушивание» внутрисетевого трафика относится к …

а. нелегальным угрозам;
б. умышленным угрозам;
в. атаке.

16. Разрушение системы с помощью программ-вирусов относится к …

а. нелегальным угрозам;
б. умышленным угрозам;

в. атаке.

17. **Использование специальных программ, которые работают путем перебора слов из некоторого файла, позволяет …**
    а. подобрать пароль;
    б. «подслушать» внутрисетевой трафик;
    в. получить доступ ко всем ресурсам системы.
18. **Программа, работающая без ведома хозяина данного компьютера и выполняющая действия, заданные злоумышленником, называется …**

19. **Программа, которая маскируется под какую-нибудь полезную утилиту или игру и производит действия, разрушающие систему, называется …**
    а. «троянский конь»;
    б. системная программа;
    в. утилита.
20. **Вирусы могут привести к …**
    а. захвату и анализу сетевых сообщений;
    б. повреждению или полной утрате информации;
    в. незаконному проникновению в один из компьютеров сети под видом легального пользователя.
21. **Нелегальные действия легального пользователя …**
    а. это незаконный мониторинг сети, захват и анализ сетевых сообщений;
    б. вызываются ошибочными действиями лояльных сотрудников;
    в. исходят от легальных пользователей сети, которые пытаются выполнять действия, выходящие за рамки их должностных обязанностей.
22. **Что предотвращает доступ к сети нежелательных лиц и разрешает вход для легальных пользователей?**
    а. авторизация;
    б. аудит;
    в. аутентификация.
23. **Когда пользователь вводит свои идентификатор и пароль, которые автономно обрабатываются операционной системой?**
    а. при авторизации доступа;
    б. при локальной аутентификации;
    в. при аудите.

24. **Когда контролируется доступ легальных пользователей к ресурсам системы, предоставляя каждому из них те права, которые ему были определены администратором?**
    а. при авторизации доступа;
    б. при локальной аутентификации;
    в. при аудите.
25. **Фиксация в системном журнале событий, связанных с доступом к защищаемым системным ресурсам – это …**

26. **Аудит используется для того, чтобы …**

а. вся информация делилась на уровни в зависимости от степени секретности;
б. засекать даже неудачные попытки «взлома» системы;
в. пользователи не имели возможности изменить уровень доступности информации.

27. Безопасная информационная система обладает следующими свойствами: *а. конфиденциальности, б. доступности , в. целостности***.**

Каждому свойству поставьте в соответствие его определение:

А. … – это гарантия того, что авторизованные пользователи всегда получат доступ к данным

Б. … – это гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом изменять, модифицировать, разрушать или создавать данные

В. … – это гарантия того, что секретные данные будут доступны только авторизованным пользователям

28. На каких двух компонентах базируется сетевая безопасность?

а. защита данных в момент их передачи по линиям связи ;
б. защита от несанкционированного удаленного доступа в сеть;
в. предотвращение доступа к сети нежелательных лиц;
г. разрешение входа для легальных пользователей.

29. С помощью каких биохарактеристик аутентифицируемый может доказать свою идентичность?

а. электронная магнитная карта;
б. отпечатки пальцев;
в. рисунок радужной оболочки глаза;

30. Термин «аутентификация» в переводе с латинского означает …

<u>Основы информационной безопасности</u>

1. Установите соответствие между основными методами обеспечения информационной безопасности.

а. сервисы сетевой безопасности;	А. защита авторских прав;
б. теоретические методы;	Б. протоколирование и аудит;
в. инженерно – технические методы;	В. обоснование корректности и адекватности систем обеспечения ИБ;
г. правовые методы.	Г. защита информации от утечки по техническим каналам.

2. Установление полномочий субъектов для последующего контроля санкционированного использования ресурсов, доступных в системе это …

а. разграничение полномочий;
б. разграничение доступа;
в. аутентификация;
г. аудит.

3. **Продолжите предложение**

Принято выделять два основных метода разграничения доступа: …

4. **Продолжите предложение**

… выполняет функции разграничения информационных потоков на границе защищаемой автоматизированной системы.

5. **Механизм подтверждения подлинности и целостности цифровых документов**
   а. пароль;
   б. аутентификация пользователей;
   в. цифровая подпись;
   г. асимметричные криптосистемы.
6. **Защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.**
   а. информационная безопасность;
   б. информационная война;
   в. информационный ресурс;
   г. конфиденциальность информации.
7. **Ознакомление с информацией, ее обработка, в частности копирование, модификация или уничтожение информации.**
   а. получение информации;
   б. доступ к информации;
   в. защита информации;
   г. обработка информации.
8. **Доступ к информации, не нарушающий установленные правила разграничения доступа**
   а. анонимный доступ к информации;
   б. несанкционированный доступ к информации;
   в. открытый доступ к информации;
   г. санкционированный доступ к информации.
9. **Продолжите фразу: «Статус, предоставленный данным и определяющий требуемую степень их защиты – это …»**

Запишите ответ: _____

10. **Некоторое неудачное свойство системы, которое делает возможным возникновение и реализацию угрозы.**
    а. целостность системы;
    б. конфиденциальность системы;
    в. уязвимость системы;
    г. защищенность системы.
11. **Реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него.**
    а. гриф секретности;

б. степень секретности;
в. цифровая подпись;
г. реквизиты секретности.

12. Продолжите фразу: «Научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства «ноу-хау»), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам – это …»

Запишите ответ: _____

13. К формам защиты информации не относится…

а. аналитическая;
б. правовая;
в. организационно-техническая;
г. страховая.

14. Информация, составляющая государственную тайну, не может иметь гриф…

а. «для служебного пользования»;
б. «секретно»;
в. «совершенно секретно»;
г. «особой важности».

15. Элементы знака охраны авторского права:

а. буквы С в окружности или круглых скобках;
б. буквы Р в окружности или круглых скобках;
в. наименования (имени) правообладателя;
г. наименование охраняемого объекта.

16. Укажите соответствие для всех 4 вариантов ответа:

а. комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны за счет электромагнитных полей побочного характера и наводок;	А. защита информации от утечки по акустическому каналу;
б. комплекс мероприятий, исключающих или уменьшающих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны в виде производственных или промышленных отходов;	Б. защита информации от утечки по визуально-оптическому каналу;
в. комплекс мероприятий, исключающих или уменьшающих	В. защита информации от утечки по электромагнитным каналам;
	Г. защита информации от утечки по материально-вещественному каналу.

возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей;

г. комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет распространения световой энергии.

17. Продолжите фразу: " Последовательность символов, недоступная для посторонних, предназначенная для идентификации и аутентификации субъектов и объектов между собой - это..."

Запишите ответ: _____

18. Какие законы существуют в России в области компьютерного права? Выберите несколько из 4 вариантов ответа:

а. о государственной тайне;
б. об авторском праве и смежных правах;
в. о гражданском долге;
г. о правовой охране программ для ЭВМ и БД.

19. Укажите соответствие для всех 4 вариантов ответа:

а. наука о скрытой передаче информации путем сохранения в тайне самого факта передачи;

б. наука скрывающая содержимое секретного сообщения;

в. наука, занимающаяся методами шифрования и дешифрования;

г. наука о методах расшифровки зашифрованной информации без предназначенного для такой расшифровки ключа.

А. стеганография;

Б. криптоанализ;

В. криптология;

Г. криптография.

20. Расположите в порядке возрастания ущерб от атаки фирмы

а. фирма прекращает существование;
б. ущерб от атаки есть, но он незначителен, основные финансовые операции и положение фирмы на рынке не затронуты;
в. значительные потери на рынке и в прибыли, от фирмы уходит ощутимая часть клиентов;
г. раскрытие информации принесет ничтожный моральный и финансовый ущерб фирме.

21. Преднамеренно внесенные в ПО функциональные объекты, которые при определенных условиях (входных данных) инициируют выполнение не описанных в документации функций ПО, приводящих к нарушению конфиденциальности, доступности или целостности обрабатываемой информации называются

а. вирус;
б. троян;
в. вредоносное ПО;
г. программная закладка.

22. Биометрические характеристики относятся к средствам…

а. аутентификации;
б. идентификации;
в. протоколирования ;
г. аудита.

23. Сбор и накопление информации о событиях, происходящих в информационной системе, называется…

а. экранированием;
б. аудитом;
в. протоколированием;
г. криптографией.

24. Укажите в правильном порядке этапы допуска в вычислительную систему

а. установление подлинности;
б. идентификация;
в. определение полномочий для последующего контроля и разграничения доступа.

25. Восстановите последовательность действий процедуры опознания с использованием простого пароля

а. система запрашивает пароль;
б. пользователь вводит пароль;
в. пользователь посылает запрос на доступ к компьютерной системе и вводит свой идентификатор;
г. система сравнивает полученный пароль с паролем пользователя, хранящимся в базе эталонных данных системы защиты, и разрешает доступ, если пароли совпадают; в противном случае пользователь к ресурсам компьютерной системы не допускается.

26. Основные угрозы доступности информации:

а. непреднамеренные ошибки пользователей;
б. хакерская атака;
в. разрушение или повреждение помещений;
г. перехват данных.

27. Разделы современной криптографии:

а. симметричные криптосистемы;
б. криптосистемы с открытым ключом;
в. управление паролями;
г. управление ключами;

28. Основные угрозы конфиденциальности информации:

а. маскарад;
б. переадресовка;
в. перехват данных;
г. злоупотребления полномочиями.

29. Преднамеренная угроза безопасности информации

а. кража;
б. наводнение;
в. повреждение кабеля, по которому идет передача, в связи с погодными условиями;
г. ошибка разработчика.

30. Вставьте пропущенное слово:

Информация может быть защищена без аппаратных и программных средств защиты с помощью _____ преобразований.
Запишите ответ:
_____

Технические средства информатизации

1. **Сетевое устройство, объединяющее сети на существенно разных программных и аппаратных платформах, называется**
   а. шлюз;
   б. мост;
   в. концентратор.
2. **Что может стать причиной сброса настроек в микросхеме BIOS?**
   а. действие вируса типа Kido;
   б. разгон процессора;
   в. переустановка ОС.
3. **Единица измерения частоты дискретизации -**
   а. Мб;
   б. Кб;
   в. Гц;
   г. Кц.
4. **Качество кодирования непрерывного звукового сигнала зависит:**
   а. от частоты дискретизации и глубины кодирования;
   б. от глубины цвета и разрешающей способности монитора;
   в. от международного стандарта кодирования.
5. **Совокупность условий и правил обмена информацией называется ...**
   а. выделенным каналом связи;
   б. компьютерной сетью;
   в. протоколом.
6. **Укажите, где нельзя хранить резервные копии?**
   а. запись резервных данных на компактные диски;
   б. запись резервных данных на жёсткий диск компьютера;
   в. внутри локальной сети;
   г. запись резервных данных на FTP-серверы;
   д. запись резервных данных на любое USB-совместимое устройство (такое, как флэш-карта или внешний жёсткий диск).
7. **Как называется процедура извлечения информации с запоминающего устройства в случае, когда она не может быть прочитана обычным способом.**

а. восстановление данных;
б. образ;
в. резервное копирование.

8. Многопроводная шина информационного обмена внутри материнской платы называется:

а. портом;
б. магистралью;
в. адаптером;
г. линией внутренней связи.

9. Какие из накопителей информации применяемые в составе технических средств информации классифицированы верно?

а. по способу хранения информации выделяют: накопители прямого, последовательного и блочного доступа, а так же оптические;
б. по типу устройства хранения информации выделяют: встраиваемые (внутренние), внешние, автономные, мобильные (носимые) и др;
в. по виду носителя информации выделяют: магнитоэлектрические накопители, встраиваемые накопители, накопители блочного доступа.

10. Данное устройство выполняет основную работу по переработке информации, а также все арифметические действия, логические операции, сравнение данных и т. д.

а. арифметико - логическое устройство;
б. устройство управления;
в. регистр;
г. транзистор.

11. Данное устройство обеспечивает организацию выполнения программы обработки информации и согласованное взаимодействие всех узлов машин

а. арифметико - логическое устройство;
б. устройство управления;
в. регистр;
г. транзистор;

12. Технические средства информатизации - это ...

а. совокупность систем, машин, приборов, механизмов, устройств и прочих видов оборудования, предназначенных для автоматизации различных технологических процессов информатики, причем таких, выходным продуктом которых является информация, используемые для удовлетворения информационных потребностей в разных областях деятельности общества;
б. электронное устройство, выполненное в виде платы расширения (может быть интегрирован в системную плату) с разъемом для подключения к линии связи;
в. средство информации.

13. Сетевой адаптер - это:

а. специальная программа, через которую осуществляется связь нескольких компьютеров;
б. специальное аппаратное средство для эффективного взаимодействия персональных компьютеров сети;
в. специальная система управления сетевыми ресурсами общего доступа;
г. система обмена информацией между компьютерами по локальным сетям.

14. Для соединения компьютеров в сетях используются кабели различных типов. По какому из них передаётся информация, закодированная в пучке света.

а. витая пара;

б. телефонный;
в. коаксиальный;
г. оптико – волоконный.

15. Домен-это...

а. часть адреса, определяющая адрес компьютера пользователя в сети;
б. название программы, для осуществления связи между компьютерами;
в. название устройства, осуществляющего связь между компьютерами;
г. единица скорости информационного обмена.

16. Укажите верное(ые) высказывание(я):

а. внешняя память - это память высокого быстродействия и ограниченной емкости;
б. внешняя память предназначена для долговременного хранения информации независимо от того, работает ЭВМ или нет;
в. внешняя память предназначена для долговременного хранения информации, только когда работает ЭВМ.

17. Как называется содержимое энергонезависимой памяти компьютера или любого цифрового вычислительного устройства.

а. прошивкой;
б. конфигурация устройства;
в. моддинг.

18. Отличительными особенностями компьютерного вируса являются:

а. значительный объем программного кода;
б. необходимость запуска со стороны пользователя;
в. способность к повышению помехоустойчивости операционной системы;
г. маленький объем; способность к самостоятельному запуску и многократному копированию кода, к созданию помех корректной работе компьютера.

19. Загрузочные вирусы характеризуются тем, что:

а. поражают загрузочные сектора дисков;
б. поражают программы в начале их работы;
в. запускаются при загрузке компьютера;
г. изменяют весь код заражаемого файла;
д. всегда меняют начало и длину файла.

20. Автоматизированное, отдельно поставляемое программное средство, используемое для устранения проблем в программном обеспечении или изменения его функционала называется

а. автоматическое программное обеспечение;
б. заплатка или патч;
в. деинсталляция программного обеспечения.

21. Назовите наиболее популярный формат для хранения несжатых аудио данных

а. MPEG;
б. MP 3;
в. JPEG;
г. WAV.

22. Устройство, принимающее сигнал из одного порта и распределяющее его по всем остальным портам, называется

а. маршрутизатор;
б. коммутатор;
в. шлюз;
г. концентратор.

23. Шина, предназначенная для обмена цифровой информацией между ПК и другими электронными устройствами, особенно для подключения жёстких дисков и устройств обработки аудио- и видеоинформации?

а. шина VESA;

б. шина AGP;
в. шина SCSI;
г. шина IEEE 1394.

24. Что является характеристикой монитора? ...

а. цветовое разрешение
б. тактовая частота
в. дискретность
г. время доступа к информации

25. Что определяется произведением глубины адресного пространства на количество линий ввода/вывода?

а. объём микросхемы памяти;
б. быстродействие микросхемы динамической памяти;
в. циклограмма;
г. разрядность шины ввода/вывода.

26. Что определяется суммой времени последовательного выполнения элементарных действий между 2-мя операциями чтения либо записи данных?

а. быстродействие микросхемы динамической памяти;
б. циклограмма;
в. разрядность шины ввода/вывода;
г. объём микросхемы памяти.

27. Количество бит информации, которое хранится в ячейках памяти?

а. объём микросхемы памяти;
б. глубина адресного пространства;
в. банк памяти;
г. верного ответа нет.

28. Какое устройство обеспечивает наиболее полную защиту от перебоев в сети электропитания?

а. сетевой фильтр;
б. линейный стабилизатор;
в. источник бесперебойного питания.

29. Как называется точная копия всего раздела или носителя (устройства), хранящаяся в одном файле

а. образ;
б. записанный диск;
в. раздел жесткого диска;

30. Какое устройство предназначено для подключения к компьютерной сети?

а. центральный процессор;
б. блок питания;
в. видеокарта;
г. сетевая карта;
д. системная плата.

Сети и системы передачи информации

1. Аналоговый сигнал – это…

а. сигнал данных, у которого каждый из представляющих параметров описывается функцией дискретного времени и конечным множеством возможных значений;
б. сигнал данных, у которого каждый из представляющих параметров описывается функцией времени и непрерывным множеством возможных значений;

в. информационный сигнал, который может принимать лишь конечное число значений.

2. **Амплитудная модуляция — …**
   а. вид модуляции, при которой изменяемым параметром несущего сигнала является его амплитуда;
   б. вид аналоговой модуляции, при котором информационный сигнал управляет частотой несущего колебания;
   в. один из видов модуляции колебаний, при которой фаза несущего колебания управляется информационным сигналом.

3. **В каких единицах измеряется относительное напряжение?**
   а. в вольтах;
   б. в милливольтах;
   в. в децибелах.

4. **Что определяет значение логической переменной при импульсном кодировании?**
   а. амплитуда сигнала;
   б. фаза сигнала;
   в. перепад напряжения.

5. **Как называется информационный блок SDH?**
   а. кадр;
   б. пакет;
   в. блок;
   г. сообщение.

6. **Радиорелейная связь —….**
   а. один из видов спутниковой радиосвязи, основанный на многократной ретрансляции радиосигналов;
   б. один из видов наземной радиосвязи, основанный на многократной ретрансляции радиосигналов;
   в. один из видов наземной радиосвязи, основанный на сотовой связи.

7. **Выберите утверждения, касающиеся глобальной сети:**
   а. соединяется с другими сетями, образуют одну всемирную сеть;
   б. объединение множества локальных сетей и отдельных компьютеров;
   в. охватывающая большие территории и включающая в себя большое число компьютеров;
   г. все компьютеры выполняют одинаковые функции, нет преимущества ни у одного персонального компьютера.

8. **Общий стандарт на представление и преобразование передаваемой информации по сети, название.**
   а. сервер-программа;
   б. клиент-программа;
   в. протокол;
   г. интернет.

9. **Комплекс аппаратных и программных средств, позволяющих компьютерам обмениваться данными:**

а. интерфейс;
б. магистраль;
в. компьютерная сеть;
г. адаптеры.

10. Укажите межсетевой протокол (протокол INTERNET) семейства протоколов TCP/IP

а. ARP (Address Resolution Protocol);
б. IP (Internet Protocol);
в. ICMP (Internet Control Message Protocol).

11. Укажите уровень модели OSI, который не подписан на рисунке

а. информационный;
б. представительский;
в. коммутационный.

12. Цифровой сигнал — это…

а. сигнал данных, у которого каждый из представляющих параметров описывается функцией дискретного времени и конечным множеством возможных значений;
б. информационный сигнал, который может принимать лишь конечное число значений;
в. сигнал данных, у которого каждый из представляющих параметров описывается функцией времени и непрерывным множеством возможных значений.

13. Частотная модуляция— …

а. вид модуляции, при которой изменяемым параметром несущего сигнала является его амплитуда;
б. вид аналоговой модуляции, при котором информационный сигнал управляет частотой несущего колебания;
в. один из видов модуляции колебаний, при которой фаза несущего колебания управляется информационным сигналом.

14. Какой из перечисленных видов трафика наиболее чувствителен к задержкам электрического сигнала?

а. речевой;
б. видео;
в. все выше перечисленные.

15. Как называется единица скорости передачи информации в телеграфных сетях?

а. бонд;
б. байт;

в. бод;
г. бод/с.

16. Какие устройства образуют канал связи?

а. источник сообщения; передатчик сообщения, приемник сообщения;
б. источник сообщения; преобразователь сигнал - сообщение, передатчик; линия связи;
в. приемник сообщения;
г. передатчик сигнала; приемник сигнала; приемник сообщения;
д. передатчик сообщения, линия связи, приемник сообщения.

17. Канал связи это – …

а. совокупность линий передачи данных и блоков взаимодействия, предназначенных для передачи данных между станциями данных;
б. средства односторонней передачи данных;
в. устройство преобразования кодов и представляющих их электрических сигналов при взаимодействии аппаратуры окончания канала данных и линий связи;
г. система односторонней связи, при которой передаваемое сообщение поступает на пейджер пользователя, извещая его о необходимости предпринять то или действие или просто информируя его о тех или иных текущих событиях.

18. Технические средства, связывающие компьютеры в сетях, называются…

а. хост-машинами;
б. пропускной способностью;
в. скоростью передачи информации;
г. каналами связи.

19. Служба FTP в Интернете предназначена:

а. для создания, приёма и передачи Web-страниц;
б. для удалённого управления техническими системами;
в. для приёма и передачи файлов любого формата;
г. для обеспечения работы телеконференций.

20. Группа компьютеров, связанных каналами передачи информации и находящимися в пределах здания называется:

а. глобальной компьютерной сетью;
б. информационной системой с гиперсвязями;
в. локальной компьютерной сетью;
г. электронной почтой.

21. Укажите протокол пересылки файлов стека протоколов TCP/IP

а. FTP (File Transfer Protocol);
б. ICMP (Internet Control Message Protocol);
в. IP (Internet Protocol).

22. Укажите уровень модели OSI, который не подписан на рисунке

а. информационный;
б. коммутационный;
в. транспортный.

23. Параметры виртуальных локальных сетей определяются стандартом:

а. IEEE 802.1;
б. IEEE 802.2;
в. IEEE 802.1Q;
г. IEEE 802.2Q;
д. IEEE 802.3Q.

24. Маршрутизацию между виртуальными локальными сетями обеспечивает:

а. транковое соединение между коммутаторами;
б. транковое или обычное соединение между коммутаторами;
в. транковое или обычное соединение между коммутатором и маршрутизатором;
г. только транковое соединение между коммутатором и маршрутизатором.

25. По умолчанию управляющей сетью является:

а. первая сеть VLAN 1;
б. сеть, которой назначили IP-адрес;
в. сеть расширенного диапазона идентификаторов VLAN;
г. сеть, определенная стандартом 802.1.

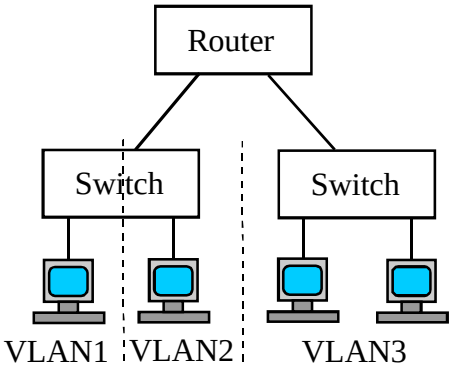
26. Кабель, представляющий собой световод на кремниевой или пластмассовой основе, который защищен материалом с низким коэффициентом преломления

а. Витая пара
б. Оптоволоконный кабель
в. Коаксиальный кабель

27. После удаления одной из виртуальных локальных сетей приписанные к ней порты будут иметь следующий статус:

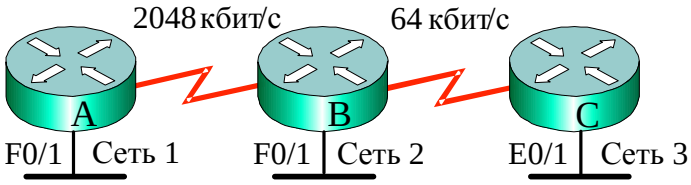
а. порты перейдут в пассивное состояние;
б. порты административно выключены;
в. порты будут связанными с удаленной сетью, пока не будут переназначены другой виртуальной сети;
г. порты удаленной сети будут автоматически переназначены сети VLAN1.

28. Сколько широковещательных доменов существует в сети (см. рис.)?



Ответ запишите цифрой:

29. Метрики пути из Сети 1 в Сеть 2 и из Сети 3 в Сеть 1 (см. рисунок) составляют:



а. 50 и 1621;
б. 48 и 1562;
в. 49 и 1563;
г. 1562 и 50;
д. 1562 и 10.

30. В строке таблицы маршрутизации

- 192.168.4.48 [110/2344] via 200.50.50.10, 00:00:10, Serial1/1

via 200.50.50.10 означает: (выбрать два ответа)

а. адрес сети назначения;
б. адрес выходного интерфейса маршрутизатора на пути к сети назначения;
в. адрес входного интерфейса соседнего маршрутизатора на пути к сети назначения;
г. адрес запасного пути (feasible succcessor) к сети назначения;
д. адрес преемника (succcessor).

Электроника и схемотехника

1. **Какие диоды работают в режиме электрического пробоя?**
   а. варикапы;
   б. туннельные;
   в. стабилитроны.

2. **Укажите маркировку интегральной микросхемы**.
   а. КП103Е;
   б. К140УД1Б ;

в. КН102Г.

3. **В каком случае коэффициент усиления по мощности биполярного транзистора меньше или равен 1?**
   а. во всех случаях он больше 1;
   б. в схеме с общим эмиттером ;
   в. во всех случаях он меньше 1.

4. **Для отрицательной обратной связи, применяемой в усилителях, сдвиг фаз между входным напряжением и напряжением обратной связи равен**
   а. 0 градусов;
   б. 90 градусов;
   в. 180 градусов.

5. **Какими причинами можно объяснить завал амплитудно-частотной характеристики УНЧ в области низких частот**
   а. собственными шумами;
   б. реактивными элементами в схеме;
   в. влиянием температуры.

6. **Длительность формируемых мультивибратором прямоугольных импульсов определяется**
   а. элементами RC-цепей;
   б. величиной напряжения питания;
   в. выбором транзисторов.

7. **Какое электронное устройство имеет два устойчивых состояния?**
   а. мультивибратор;
   б. блокинг-генератор;
   в. триггер.

8. **С какой целью выпрямительные диоды включают последовательно?**

   а. для уменьшения габаритов и массы;
   б. чтобы использовать диоды с меньшим Uобрмах;
   в. чтобы использовать диоды с меньшим Iпрсред.

9. **Какое свойство p-n переходов используют в варикапах?**
   а. односторонняя электропроводность;
   б. частотные свойства;
   в. емкостные свойства.

10. **Какие значения параметров стабилизатора предпочтительнее?**
    а. Rвых = 0,5 Ом, Кст и = 300;
    б. Rвых = 0,5 Ом, Кст и = 100;
    в. Rвых = 50 Ом, Кст и = 300.

11. **Какой пробой опасен для p-n-перехода?**
    а. тепловой;
    б. электрический;
    в. тот и другой.

12. У какого транзистора входное сопротивление максимально?

а. у биполярного;
б. у полевого с затвором в виде p-n-перехода;
в. у МДП-транзистора.

13. Как влияют примесные зоны на процесс образования пар свободных носителей заряда в полупроводниках?

а. не влияют;
б. облегчают;
в. затрудняют.

14. В каком случае разрешенный энергетический уровень в атоме расщепляется на большее количество уровней?

а. если атом имеет несколько электронов;
б. если атом входит в состав молекул;
в. если атом находится в кристалле.

15. Как влияет дефекты кристаллической решетки на проводимость кристалла?

а. не влияют;
б. увеличивают;
в. уменьшают.

16. Выходные двухтактные каскады УНЧ обычно работают в экономичном режиме класса

а. А;
б. АВ;
в. В.

17. Какое из указанных свойств характерно для схемы ОК – эмиттерного повторителя?

а. коэффициент усиления по напряжению ≈ 1;
б. малое значение Rвх;
в. большое значение Rвых.

18. Для самовозбуждения автогенератора гармонических колебаний необходимо выполнение условия

а. $= К$;
б. $\beta К < 1$;
в. $\beta К \geq 1$.

19. Какой атом называется возбужденным?

а. атом, поглотивший один квант энергии;
б. атом, поглотивший один или несколько квантов энергии;
в. атом, из которого вырван электрон.

20. Почему с увеличением температуры увеличивается проводимость полупроводникового кристалла?

а. увеличивается количество пар свободных носителей заряда;
б. увеличивается длина свободного пробега электрон;
в. увеличивается ширина запрещенной зоны.

21. Отрицательная обратная связь в усилителе

а. уменьшает динамический диапазон;
б. уменьшает нелинейные искажения;
в. повышает коэффициент усиления.

22. В каком направлении включается эмиттерный и коллекторный p-n-переходы биполярного транзистора?

а. это зависит от типа транзистора (n-p-n или p-n-p);
б. эмиттерный – в обратном, коллекторный – в прямом;
в. эмиттерный – в прямом, коллекторный – в обратном.

23. Каково соотношение величины обратного тока p-n- перехода и прямого тока?

а. Iобр>> Iпр;
б. Iобр << Iпр;
в. Iобр = Iпр.

24. В каких режимах находятся транзисторы VT1 и VT2 в устойчивых состояниях триггера на транзисторах

а. VT1 и VT2 закрыты;
б. VT1 и VT2 открыты;
в. VT1 открыт, VT2 закрыт; VT1 закрыт, VT2 открыт.

25. Как измениться скважность q если увеличить длительность паузы между импульсами

а. q увеличится;
б. q уменьшится;
в. q не изменится.

26. Какие микросхемы могут быть изготовлены без навесных элементов?

а. тонкопленочные;
б. толстопленочные;
в. полупроводниковые.

27. Как включается емкостной фильтр Сф?

а. параллельно нагрузкеRн;
б. последовательно с нагрузкой Rн;
в. параллельно вторичной обмотке трансформатора.

28. Назовите главное достоинство схемы трехфазного выпрямителя

а. малое значение тока диодов;
б. малое обратное напряжение диодов;
в. малая пульсация выпрямленного тока.

29. Определить правильный ответ в логическом выражении $X + \overline{X} =$

а. 0;
б. 1;
в. X .

30. Определите коэффициент усиления по мощности трехкаскадного усилителя в децибелах, если каждый каскад обеспечивает десятикратное усиление по напряжению

а. 60 ;
б. 100;
в. 1000.

Основы алгоритмизации и программирования

1. **Что изменяет операция присваивания?**

а. Значение переменной
б. Имя переменной
в. Тип переменной
г. Тип алгоритма

2. **Свойством алгоритма является…**

а. Цикличность
б. Результативность
в. Возможность изменения последовательности выполнения команд
г. Возможность выполнения алгоритма в обратном порядке

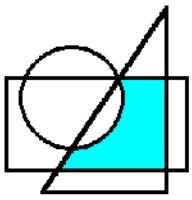
3. **Укажите, какие из перечисленных понятий не относятся к основным группам алгоритмов?**
   а. Линейные
   б. Разветвляющиеся
   в. Структурные
   г. Циклические

4. **Чему равно число 2.731E07**
   а. 2731000
   б. 0,0000002731
   в. 273100000
   г. 27310000

5. **Поменять значения переменных x и y не используя дополнительных переменных:**

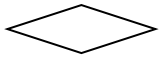
а. x=2y, y=x/2, x=x/2
б. x=x-y, y=y-x, y=y+x
в. x=x+y, y=x-y, x=x-y

6. **Высказывания A, B, C истинны для точек, принадлежащих кругу, треугольнику, прямоугольнику соответственно. Для всех точек выделенной на рисунке области истинно высказывание**



а. (A или B) и B
б. (C и не A) и не B
в. (B или C) и не C
г. (B и C) и не A
д. (A и C) и не B

7. **При графическом способе записи алгоритма блок означает**



а. Проверку условия и выбор направления выполнения алгоритма*
б. Начало или конец обработки данных
в. Начало цикла
г. Конец цикла

8. Свойство алгоритма "Массовость" это:

а. Возможность применения алгоритма множеством пользователей
б. Возможность решения всего класса задач определенного типа без изменения алгоритма
в. Возможность применения алгоритма исполнителями с различной системой команд
г. Возможность одновременного выполнения нескольких копий алгоритма одним исполнителем

9. Чему равны значения переменных x и y после выполнения операторов присваивания x=2; y=5; x=y; y=x?

а. 5; 2
б. 2; 5
в. 5; 5
г. 2; 2

10. Если элементы массива F[1..6] равны соответственно 6, 5, 4, 3, 2, 1, то значение выражения F[F[F[3]]] – F[F[2]-F[4]] равно:

а. – 1;
б. 6;
в. 0;
г. 4;
д. – 3.

11. Укажите последовательность команд, в результате выполнения которых значения переменных X и Y поменяются местами:

а. B=X; X=Y; Y=X;
б. X=Y; Y=X;
в. Y=X; B=X; X=Y;
г. C=X; X=Y; Y=C.

12. Величины в языках программирования характеризуются:

а. элементами, размером, значением;
б. однородностью, предназначением, полезностью;
в. местоположением, принадлежностью, значением;
г. типом, именем, значением*

13. Переменная в программировании считается полностью заданной, если известны ее…

а. Тип, имя
б. Имя, значение
в. Тип, значение
г. Тип, имя, значение

14. Каждое выражение (каждый оператор) в программе отделяется друг от друга ...

а. ;*
б. -
в. .
г. ,
д. :

15. Правильная строковая запись выражения

$$x-\frac{x^3}{|x|}+\sin x$$

а. x-x***3/absx + sin(x)
б. x-x*x*x/abs(x) +sin(x)
в. (x-x*x*x)/abs(x) +sin(x)
г. x-x*x*x/absx +sinx

16. До каких пор будут выполняться операторы в теле цикла while (x < 100)?

а. Пока х строго меньше ста
б. Пока х равен ста
в. Пока х меньше или равен ста
г. Пока х больше ста

17. Укажите объектно-ориентированный язык программирования

а. Java
б. Все варианты ответов
в. C++
г. C#

18. Тело оператора выбора if, будет выполняться. если его условие:

а. истинно (true)
б. ложно (false)

19. Массив - это ...

а. Массив - это упорядоченные в памяти элементы одного и того же типа, имеющие имя. Доступ к отдельным элементам массива осуществляется по имени массива и индексу
б. Массив - это упорядоченные в памяти элементы одного и того же типа, имеющие имя. Доступ к отдельным элементам массива осуществляется по имени массива и адресу

в. Массив - это упорядоченные в памяти элементы одного и того же типа, имеющие общий адрес. Доступ к отдельным элементам массива осуществляется по адресу и индексу

20. Графическое представление алгоритма?

а. Блок - схема;
б. Схема;
в. График;
г. Структура;

21. Что такое условный оператор?

а. Конструкция языка программирования, обеспечивающее выполнение действий только при выполнении некоторого логического выражения*
б. Некоторая часть исходного кода обеспечивающее повторение определенного действия
в. Стандартная библиотека во многих языках программирования

22. Что такое цикл?

а. Имя переменной
б. Оператор присваивания
в. Оператор, предназначенный для многократного использования определенных инструкций

23. Зачем нужен тип данных?

а. Для обеспечения целостности данных
б. Для создания переменных с неизвестным типом
в. Для указания переменной типа ее содержимого

24. Что такое функция?

а. Некоторая часть программы, имеющая собственное имя и которая может вызываться столько раз, сколько это нужно
б. Некоторая часть программы, содержащая вредоносный код, и блокирующая определенные действия системы
в. Некоторая часть программы, в которой происходит начальная инициализация всех полей структур, массивов, переменных и т д.

25. Какие операции допустимы с логическими переменными?

а. логическое сложение
б. логическое умножение
в. отрицание
г. логическое вычитание

26. Данные, значения которых не меняются в процессе выполнения алгоритма.

а. Переменные
б. Константы
в. Исходные данные

27. Тело цикла для вычисления значений функций f(x)=x*4, на отрезке [-5,5] с шагом 0.1 будет иметь вид:

а. f:= x*x*x*x; x:=x+0.5; cout<<f<<x;
б. f:= x*4; x:=0.1; cout<<f<<x;
в. f:= x*4; cout<<f<<x; x:=x+0.1;
г. f:= x*4; x:=x+0.1; cout<<f<<x;

28. Рекурсия – это:

а. Повторение выполнения функции или процедуры внутри себя;
б. Оператор;
в. Цикл;
г. Возвращаемое функцией или процедурой значение.

29. Указать выражение, соответствующее указанному условию: ни одно из чисел x, y и z не является положительным.

а. (x>0) или (y>0) или (z>0)
б. (x<0) и (y<0) и (z<0)
в. (x<0) или (y<0) или (z<0)
г. (x>0) и (y>0) и (z>0)

30. Какой из документов является алгоритмом?

а. Правила техники безопасности
б. Инструкция по получению денег в банкомате
в. Расписание уроков

Базы данных

1. **В базе данных хранятся:**

а. Только данные
б. Данные и описание данных — метаданные
в. Данные, метаданные и программы СУБД
г. Данные, метаданные и пользовательские программы
д. Все ответы неверны

2. Система управления базами данных — это:

а. Программы работы с данными и метаданными
б. Программы работы с данными и метаданными и программы пользовательского интерфейса
в. Программы работы с данными и метаданными и программы решения задач предметной области
г. Данные, метаданные и пользовательские программы
д. Все ответы неверны

3. По отношению к метаданным СУБД выполняет функции:

а. Создания новых объектов
б. Создание и изменение объектов
в. Создание, изменение и удаление объектов
г. Создание, изменение, удаление и выборка объектов

4. По отношению к данным СУБД выполняет функции:

а. Добавление новых данных
б. Добавление и изменение данных
в. Добавление, изменение и удаление данных
г. Добавление, изменение, удаление и выборка данных

5. Произвольные структуры данных позволяют поддерживать модели данных:

а. Только иерархические
б. Сетевые и реляционные
в. Только реляционные
г. Только сетевые
д. Ни одна из перечисленных

6. Метаданные представляют собой:

а. Описание данных, хранящихся в базе данных
б. Данные, хранящиеся в базе данных
в. Ничего из указанного

7. Произвольные запросы к базе данных лучше всего реализуются:

а. В последовательных файлах
б. В иерархических системах
в. В сетевых системах
г. В реляционных системах
д. В сетевых и реляционных базах данных
е. Во всех базах данных

8. Безопасность данных лучше всего может быть реализована:

а. В последовательных файлах
б. В иерархических системах
в. В сетевых системах
г. В реляционных системах
д. В сетевых и реляционных базах данных
е. Во всех базах данных

9. Целостность данных лучше всего может быть реализована:

а. В последовательных файлах
б. В иерархических системах
в. В сетевых системах
г. В реляционных системах
д. В сетевых и реляционных базах данных
е. Во всех базах данных

10. В реляционной базе данных данные хранятся в виде однородных таблиц:

а. Верно
б. Неверно

11. Диаграммы Бахмана позволяют описать:

а. Структуру программы
б. Отношения внутри записи (структуру записи)
в. Отношения в базе данных (отношения между данными в базе данных)
г. Ни одно из указанных

12. Администратор базы данных:

а. Создает базу данных
б. Разрабатывает программы для работы с базой данных
в. Отвечает за обеспечение целостности и безопасности базы данных
г. Работает с программами, использующими базу данных

13. Разработчик базы данных:

а. Создает базу данных
б. Разрабатывает программы для работы с базой данных
в. Отвечает за обеспечение целостности и безопасности базы данных
г. Работает с программами, использующими базу данных

14. Прикладной программист:

а. Создает базу данных
б. Разрабатывает программы для работы с базой данных
в. Отвечает за обеспечение целостности и безопасности базы данных
г. Работает с программами, использующими базу данных

15. Для добавления в базу данных нового объекта используется оператор (набор текста)

16. Для добавления в таблицу базы данных новой строки используется оператор (набор текста)

17. Для удаления из базы данных объекта используется оператор (набор текста)

18. Для удаления строк из таблицы базы данных используется оператор (набор текста)

19. Для изменения характеристик объекта базы данных используется оператор (набор текста)

20. Для изменения данных в базе данных используется оператор (набор текста)

21. Для выборки данных из таблиц базы данных используется оператор (набор текста)

22. Индексы в реляционной базе данных используются:

а. Для ускорения выборки данных
б. Для ускорения упорядочения выбранных данных
в. Для ускорения выборки и упорядочения данных
г. Ни для чего из перечисленного

23. Таблица может иметь несколько первичных ключей:

а. Верно
б. Неверно

24. Таблица может иметь несколько внешних ключей:

а. Верно
б. Неверно

25. Первичный ключ в таблице может быть использован:

а. Для однозначной идентификации строки таблицы
б. В реализации отношения один ко многим
в. Во всех перечисленных случаях
г. Ни в одном из перечисленных случаев

26. Внешний ключ в таблице может быть использован:

а. Для однозначной идентификации строки таблицы
б. В реализации отношения один ко многим
в. Во всех перечисленных случаях
г. Ни в одном из перечисленных случаев

27. Предложение CHECK в таблице задает:

а. Ограничение первичного ключа
б. Ограничение внешнего ключа
в. Ограничение уникального ключа
г. Проверку значения столбца или группы столбцов
д. Значение по умолчанию

28. Предложение DEFAULT в таблице задает:

а. Ограничение первичного ключа
б. Ограничение внешнего ключа
в. Ограничение уникального ключа
г. Проверку значения столбца или группы столбцов
д. Значение по умолчанию

29. К хранимым процедурам в базе данных могут обращаться:

а. Только хранимые процедуры
б. Хранимые процедуры и триггеры
в. Хранимые процедуры, триггеры, программы
г. Ничто из указанного неверно

30. К триггерам в базе данных могут обращаться:

а. Только хранимые процедуры
б. Хранимые процедуры и триггеры
в. Хранимые процедуры, триггеры, программы
г. Ничто из указанного неверно

<u>ПМ.01 Эксплуатация подсистем безопасности автоматизированных систем</u>

1. **Что относятся к активным методам защиты речевой информации?**
   а. создание маскирующих акустических и вибрационных помех;
   б. выявление факта несанкционированного подключения к линии;
   в. создание прицельных электромагнитных помех акустическим закладным устройствам;
   г. выявление излучений акустических закладных устройств;
   д. уничтожение средств несанкционированного подключения к телефонной линии.

2. **К мероприятиям по выявлению технических каналов утечки информации относятся:**
   а. специальная проверка автоматизированной системы;
   б. специальные обследования выделенных помещений;
   в. специальные исследования с использованием контрольно-измерительной аппаратуры;
   г. специальный анализ потенциального злоумышленника.

3. **Закончите фразу: «Период создания и использования АИС, охватывающий ее различные состояния, начиная с момента возникновения необходимости в данной автоматизированной системе и заканчивая моментом ее полного выхода из употребления у пользователей – это ...»**

4. **Восстановите в правильном порядке основные стадии жизненного цикла АИС**
   а. проектная;
   б. функционирование;
   в. внедрение;
   г. предпроектная.
5. **Какая из приведенных моделей не является моделью жизненного цикла АИС**
   а. поэтапная модель с промежуточным контролем;
   б. каскадная;
   в. спиральная;
   г. классическая.
6. **Периодичность проведения контроля эффективности средств защиты:**
   а. раз в 6 месяцев;
   б. раз в год;
   в. раз в 4 месяца;
   г. раз в месяц.

7. **В результате реализации атаки доступа (прослушивания) по технических каналов утечки информации, возможно возникновение -**
   а. угрозы утечки акустической информации;
   б. угрозы утечки видовой информации;
   в. угроза утечки информации по каналам побочных электромагнитных излучений и наводок.

8. **Закончите фразу: «Любой _____объект содержит информацию о самом себе или о другом объекте»**

9. **Продолжите фразу: «…- продукт абстрактного мышления человека. Она отображает объекты, явления, как материального мира, так и создаваемые им образы и модели с помощью символов на языках общения людей».**
10. **К источникам функциональных сигналов относятся:**
    а. передатчики систем связи;
    б. передатчики радиотехнических систем;
    в. излучатели акустических сигналов гидролокаторов;
    г. условные сигналы;
    д. ничего не относится.
11. **Признаки, позволяющие отличить один объект от другого, называются**
    а. демаскирующими;
    б. отличительными;
    в. опознавательные;
    г. признаки деятельности.

12. **Наиболее характерные уязвимости АС предприятия, на которые следует особо обратить внимание при составлении плана защиты, это:**

а. точки доступа;
б. наличие в АС часто используемых сетевых служб;
в. неправильно сконфигурированные системы;
г. программные ошибки;
д. внутренние враги.

13. Комплексные системы защиты информации в сетях могут включать в себя такие подсистемы, как:

а. подсистема виртуальных частных сетей (VPN);
б. подсистема защиты удалённых и мобильных пользователей;
в. подсистема контроля и разграничения доступа;
г. подсистема аутентификации.

14. Совокупность компонент, которая реализует основные принципы функционирования и управления подсистемой защиты информации, правила взаимодействия ее компонент, позволяет конфигурировать состав средств обеспечения защиты в зависимости от динамично изменяющихся условий эксплуатации и модели угроз в системе это -

а. центр;
б. ядро;
в. главный компонент;
г. ключ.

15. Особенностью этих вирусов является умение изменять собственный код

а. файловые вирусы;
б. трояны;
в. резидентные вирусы;
г. полиморфные вирусы.

16. Активный перехват информации это перехват, который:

а. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
б. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
в. неправомерно использует технологические отходы информационного процесса;
г. осуществляется путем использования оптической техники;
д. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

17. Как называется способ несанкционированного доступа к информации, который заключается в отыскании участков программ, имеющих ошибку или неудачную логику построения?

а. “За дураком”;
б. “Брешь”;
в. “Компьютерный абордаж”;
г. “За хвост”;
д. “Неспешный выбор”.

18. Способ несанкционированного доступа к информации “Компьютерный абордаж” заключается в:

а. отыскании участков программ, имеющих ошибку или неудачную логику построения;
б. подключении злоумышленника к линии связи законного пользователя и после сигнала, обозначающего конец работы, перехватывания его на себя, получая доступ к системе;

в. подключении компьютерного терминала к каналу связи в тот момент времени, когда сотрудник, кратковременно покидает свое рабочее место, оставляя терминал в рабочем режиме;
г. нахождении злоумышленником уязвимых мест в ее защите;
д. несанкционированном доступе в компьютер или компьютерную сеть без права на то.

19. Кого называют «Фишер»?

а. это лицо, которое взламывает интрасеть в познавательных целях;
б. это мошенник, рассылающий свои послания, в надежде обмануть наивных и жадных;
в. это лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО;
г. так в XIX веке называли плохих игроков в гольф, дилетантов;
д. это мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

20. Искусственные угрозы безопасности информации вызваны:

а. деятельностью человека;
б. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
в. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
г. корыстными устремлениями злоумышленников;
д. ошибками при действиях персонала.

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

а. условные и безусловные;
б. атаки с обратной связью и без обратной связи;
в. внутрисегментные и межсегментные;
г. пассивные и активные;
д. атаки, которые могут реализовываться на всех семи уровнях.

22. Атака, которая заключается в запуске на атакуемом компьютере программы "сетевого шпиона":

а. подмена доверенного объекта или субъекта распределенной вычислительной сети;
б. ложный объект распределенной вычислительной сети;
в. анализ сетевого трафика;
г. отказ в обслуживании;
д. удаленный контроль над станцией в сети.

23. По среде обитания классические вирусы разделяются на:

а. паразитические;
б. компаньоны;
в. файловые;
г. ссылки;
д. перезаписывающие.

24. Защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной и муниципальной службой, распространение которой может нанести ущерб правам и законным интересам

другого лица (доверителя), доверившего эти сведения, и не являющаяся государственной или коммерческой тайной.

а. Профессиональная тайна;
б. Коммерческая тайна;
в. Банковская тайна;
г. Врачебная тайна.

25. Метод защиты информации идентификация и установление подлинности заключается в:

а. контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления;
б. создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями;
в. разделении информации, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;
г. том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;
д. проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

26. Замкнутая программная среда — предотвращает запуск _____ _____программного обеспечения (ПО)

а. доступного;
б. неразрешённого;
в. разрешенного;
г. базового.

27. Совместно с ОС Windows модуль входа в систему обеспечивает:

а. обработку выхода пользователя в систему (проверка возможности входа, оповещение остальных модулей о начале или завершении работы пользователя);
б. блокировку работы пользователя;
в. функциональный контроль работоспособности системы;
г. загрузку данных с персональных идентификаторов пользователя;
д. усиленную аутентификацию пользователя при входе в систему.

28. Подсистема обеспечивает взаимодействие с устройствами аппаратной поддержки системы Secret Net и состоит из следующих компонентов:

а. модуль, обеспечивающий единый интерфейс обращения ко всем поддерживаемым устройствам;
б. модули работы с устройствами (каждый модуль обеспечивает работу с конкретным устройством);
в. драйверы устройств аппаратной поддержки (если они необходимы);
г. программные модули.

29. Временное нарушение работоспособности какого – либо элемента АСОД, следствием чего может быть неправильное выполнение им в этот момент своих функций.

а. сбой;
б. отказ;
в. ошибка;
г. стихийное бедствие;
д. побочное явление.

30. **DNS (Domain Name System) – это…**

    а. сетевая служба, производящая преобразование доменных (символьных) имен в IP адреса и обратно;

    б. параметр, обозначающий скорость передачи информации по сети;

    в. главный компьютер (сервер) в сети;

    г. программа на сервере, назначающая каждому компьютеру уникальный IP адрес.

ПМ. 02 Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах

1. **Шифры замены бывают:**
   а. простые одноалфавитные;
   б. одноконтурные полиалфавитные;
   в. многоконтурные полиалфавитные;
   г. монофонические полиалфавитные;
   д. усложненные по маршрутам.
2. **Криптосистемы с секретным ключом называют:**
   а. симметричными криптосистемами;
   б. асимметричными криптосистемами;
   в. одноключевыми криптосистемами;
   г. двуключевыми криптосистемами.

3. **Хэш-функция должна обладать следующими функциями:**
   а. устойчивость к коллизиям;
   б. симметричность;
   в. однонаправленность;
   г. линейность.

4. **Алгоритм RSA основан на использовании**
   а. односторонней функции;
   б. односторонней функции с лазейкой;
   в. надежного простого числа;
   г. составного числа, образованного двумя простыми числами.

5. **Коды аутентичности сообщений позволяют**
   а. шифровать сообщения;
   б. дешифровывать сообщения;
   в. подтверждать целостность сообщения;
   г. подтверждать подлинность отправителя.

6. **К симметричным криптосистемам относятся алгоритмы**
   а. DES
   б. 3DES
   в. AES
   г. RSA
   д. TWOFISH

7. **Устройство «Сцитало» является примером шифрования:**
   а. методом подстановки;

б. методом перестановки;
в. методом гаммирования.

8. Шифры делятся на

а. блоковые и последовательные;
б. блочные и поточные;
в. потоковые и дискретные.

9. К достоинствам блочных шифров относят

а. высокую скорость шифрования;
б. дешевизну реализации;
в. похожесть процедур шифрования и расшифрования.

10. Стандарт шифрования ГОСТ 28147-89 предусматривает шифрование и расшифровку данных в следующих режимах работа:

а. простая замена;
б. маршрутная перестановка;
в. гаммирование;
г. гаммирование с обратной связью;
д. выработка имитовставки.

11. Режим выработка имитовставки в стандарте шифрования ГОСТ 28147-89 гарантирует:

а. конфиденциальность сообщения;
б. целостность сообщения;
в. аутентификацию сообщения;

12. К методам защиты от НСД относятся:

а. разделение доступа;
б. разграничение доступа;
в. увеличение доступа;
г. ограничение доступа;
д. аутентификация и идентификация.

13. Выделите группы, на которые делятся средства защиты информации:

а. физические, аппаратные, программные, криптографические, комбинированные;
б. химические, аппаратные, программные, криптографические, комбинированные;
в. физические, аппаратные, программные, этнографические, комбинированные.

14. Что такое целостность информации?

а. свойство информации, заключающееся в возможности ее изменения любым субъектом;
б. свойство информации, заключающееся в возможности изменения только единственным пользователем;
в. свойство информации, заключающееся в ее существовании в виде единого набора файлов;

г. свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

15. К аспектам ИБ относятся

а. дискретность;
б. целостность;
в. конфиденциальность;
г. актуальность;
д. доступность.

16. Что такое несанкционированный доступ (нсд)?

а. доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа;
б. создание резервных копий в организации;
в. правила и положения, выработанные в организации для обхода парольной защиты;
г. вход в систему без согласования с руководителем организации;
д. удаление не нужной информации.

17. К видам защиты информации относятся:

а. правовые и законодательные;
б. морально-этические;
в. юридические;
г. административно-организационные;

18. Какие атаки предпринимают хакеры на программном уровне?

а. атаки на уровне ОС;
б. атаки на уровне сетевого ПО;
в. атаки на уровне пакетов прикладных программ;
г. атаки на уровне СУБД.

19. ГПСЧ Fortuna состоит из трех частей:

а. генератора;
б. аккумулятора;
в. трансформатора;
г. системы управления файлом начального числа;
д. файла загрузки.

20. Из каких компонентов состоит программное обеспечение любой универсальной компьютерной системы?

а. операционной системы, сетевого программного обеспечения;
б. операционной системы, сетевого программного обеспечения и системы управления базами данных;
в. операционной системы, системы управления базами данных;
г. сетевого программного обеспечения и системы управления базами данных.

21. Верификация –

а. это проверка принадлежности субъекту доступа предъявленного им идентификатора;
б. проверка целостности и подлинности информации, программы, документа;
в. это присвоение имени субъекту или объекту.

22. Утечка информации

а. несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу;

б. ознакомление постороннего лица с содержанием секретной информации;
в. потеря, хищение, разрушение или неполучение переданных данных.

23. К основным аппаратным средствам защиты информации относятся:
а. устройства для ввода идентифицирующей пользователя информации (магнитных и пластиковых карт, отпечатков пальцев и т. п.);
б. устройства для шифрования информации;
в. устройства для воспрепятствования несанкционированному включению рабочих станций и серверов (электронные замки и блокираторы);
г. нет правильного ответа.

24. Продолжите фразу: «В модели_____ программная закладка внедряется в ПЗУ, системное или программное обеспечение и сохраняет вводимую информацию с внешних устройств или выводимую на эти устройства в скрытой области памяти локальной или удаленной компьютерной системы».

25. Закончите фразу: «Уникальная характеристика компьютера или других устройств системы, которая может быть использована для защиты и проверена программным способом – это...»

26. Укажите исходные данные, по которым производится классификация АС:
а. наличие сети передачи данных АС;
б. перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;
в. условий размещения СВТ АС;
г. исходя из принятой схемы обработки информации в АС.

27. При разработке АС, предназначенной для обработки или хранения конфиденциальной информации, необходимо ориентироваться на классы защищенности АС не ниже:
а. 3А
б. 3Б
в. 2А
г. 2Б
д. 1Г

28. Отметьте соответствующие требованию угрозы. Должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС.
а. возможны действие террористических групп или отдельных лиц с целью завладения секретной информации;
б. возможны хищения СВТ;
в. возможен доступ к СВТ посторонних лиц (посетителей, гостей.);
г. возможны действия диверсионных групп;
д. возможны умышленные действия персонала АС нарушающие установленные правила доступа к объектам доступа.

29. Отметьте правильные варианты ответа. К основным способам НСД относятся:

а. непосредственное обращение к объектам доступа;
б. просмотр информации с экранов мониторов посторонними лицами;
в. создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;
г. разглашение защищаемых сведений сотрудниками организации;
д. применение портативных устройств съема информации.

30. Каким из перечисленных способов не реализуется Распределение ключей между пользователями компьютерной сети:

а. документирование алгоритмов обеспечения защиты информации;
б. использование одного или несколько центров распределения ключей;
в. прямым обменом сеансовыми ключами между пользователями сети;
г. использование одного центра распределения ключей.

3. Профессиональное задание.

Профессиональное задание предусматривает выполнение участниками Всероссийской олимпиады комплексного задания на обеспечение безопасности персональных данных в информационной системе, проведение анализа стойкости алгоритма хеширования MD5.

Участники Всероссийской олимпиады должны продемонстрировать следующие практические навыки при выполнении профессионального задания:

Ситуация 1

- применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами.
- участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации;
- использовать и оформлять техническую документацию в соответствии с действующими нормативными правовыми актами;
- решать частные технические задачи, возникающих при аттестации объектов, помещений, программ, алгоритмов;
- осуществлять комплектование, конфигурирование, настройку подсистем безопасности автоматизированных систем;
- выполнять регламенты техники безопасности;
- применять программно-аппаратные средства обеспечения информационной безопасности;

Ситуация 2

- производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав подсистемы безопасности автоматизированной системы;
- эксплуатировать компоненты подсистем безопасности автоматизированных систем;

- обеспечивать работоспособность, обнаруживать и устранять неисправности подсистем безопасности автоматизированных систем согласно технической документации;
- оценивать эффективность применяемых программно-аппаратных средств обеспечения информационной безопасности;
- диагностировать, устранять отказы и обеспечивать работоспособность программно-аппаратных средств обеспечения информационной безопасности;
- использовать типовые криптографические средства и методы защиты информации, в том числе и электронную цифровую подпись.

Ситуация 1. ***«Обеспечение безопасности персональных данных в информационной системе»***

В ОАО «Газавтоматизация», которое занимается разработкой и производством оборудования для добычи газа, имеется база персональных данных о 1800 сотрудниках. В этой базе содержится информация о паспортных данных работников, их семейном положении, профессиональных навыках (квалификация, разряд), сведения о высшем образовании и национальной принадлежности работников. Для организации контрольно-пропускного режима на предприятии в данной базе также хранится оцифрованная фотография работника.

Информационная система предприятия состоит из локальной вычислительной сети, в состав которой входит 100 единиц персональных компьютеров, и сервера с СУБД, находящегося в отделе кадров, и имеет многоточечный выход в Интернет. Локальная сеть развернута на территории нескольких близко расположенных зданий. Доступ к базе данных имеют ограниченный круг лиц, которые имеют возможность выполнять запись, удаление, сортировку записей БД.

Беспроводные технологии передачи данных и технологии виртуализации в ЛВС не используются. Данные в базе не обезличиваются. Сведения из БД без предварительной обработки сторонним пользователям не предоставляются.

Согласно статьи 19 закона «О персональных данных» требуется обеспечить безопасность персональных данных при их обработке в информационной системе.

Задание

1. Определить уровень защищенности персональных данных, учитывая, что угрозы, связанные с наличием не декларированных возможностей в системном и прикладном программном обеспечении, неактуальны для данной информационной системы (на основании постановления Правительства РФ от 1 ноября 2012 г. № 1119)
2. Определить требования, которые необходимо выполнить для обеспечения определенного в п.1 уровня защищенности персональных данных (на основании постановления Правительства РФ от 1 ноября 2012 г. № 1119 и приказа ФСБ РФ № 378 от 10.07.2014)
3. Определить (предварительно) угрозы безопасности, связанные с несанкционированным доступом к персональным данным в данной информационной системе, реализуемых с использованием протоколов межсетевого взаимодействия (на основе базовой модели угроз безопасности ПДн ФСТЭК).

4. Определить актуальность угроз безопасности из предварительного списка (с помощью методики определения актуальных угроз безопасности ПДн ФСТЭК). Показатель опасности угроз, связанных с несанкционированным доступом, считать высоким.
5. Определить базовый набор мер защиты информации для определенного в п.1 уровня защищенности персональных данных (на основании приказа ФСТЭК России от 18.02.2013 №21).
6. Выполнить адаптацию базового набора мер с учетом структурно-функциональных характеристик и особенностей функционирования информационной системы.
7. Перечислить организационно-распорядительные документы, которые потребуется разработать в организации для выполнения требований статьи 19 закона «О персональных данных».

Указания к выполнению заданий.

При выполнении заданий Ситуации 1 необходимо использовать следующие нормативно-правовые документы:

1. Федеральный закон от 27 июля 2006 № 152-ФЗ «О персональных данных».
2. Базовая модель угроз безопасности персональных данных при их обработке в ИСПДн, утверждена ФСТЭК 15.02.2008 г.
3. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена ФСТЭК 14.02.08 г.
4. Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных».
5. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
6. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
7. Методический документ ФСТЭК России от 11 февраля 2014 «Меры защиты информации в государственных информационных системах».
8. Приказ ФСБ РФ № 378 от 10.07.2014 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных правительством РФ требований к защите персональных данных для каждого из уровней защищенности".
9. Постановление Правительства № 911 от 6 сентября 2014 г. «О внесении изменений в перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

Ситуация 2. «Анализ стойкости алгоритма хеширования MD5»

Одно из требований ФСТЭК – анализ (контроль) защищенности информационной системы – подразумевает поиск слабых мест в системе защиты (в том числе простых паролей). Перед техником по защите информации службы безопасности ОАО «Газавтоматизация» была поставлена задача осуществления периодической проверки стойкости используемых паролей, чтобы не допустить подбора пароля полным перебором (так называемые bruteforce-атаки - «метод грубой силы») и исключить использование сотрудниками компании словарных паролей.

Задание. Для полученного перечня хешей определить исходный пароль, по которому они были сгенерированы с помощью алгоритма MD5.

1) a94dc7d578c98d16eb719dbeefc705c3
2) 7c9e992c6d845e5e4f64ace8c2ed0370
3) 89c4678fa511408d6a6727f253ed0237
4) 89e43eff6445f9bec8818f775ed441d9
5) bead7bdeaa8f66c33d5a189523a91150
6) 2c24186321ae66ce71b48986078ba736
7) 02c59a059e8efa079426f6988b40d2d1
8) e702e0046f7f6b1cd3d0ed0bb0ff8f9c
9) 097604892aa91447fe9d4aa12b3525e9
10) bae1ad7cad92a10d740742690b3b8fe0

Длина исходного пароля – до 8 символов включительно. Символы русского алфавита не используются.

Указания к выполнению заданий.

При выполнении заданий Ситуации 2 необходимо соблюдать следующую последовательность действий:

1. Распаковать программу John The Ripper (*http://www.openwall.com/john/g/john179j5w.zip*).
2. Сохранить хеши в текстовый файл.
3. Сформировать команду для запуска программы John The Ripper в режиме полного перебора (brute-force).
4. Все найденные пароли записать на листе ответов с указанием соответствующего номера хеша.

4. Перечень используемого оборудования, технических средств и программных продуктов.

Для выполнения заданий используется компьютерные классы, оборудованные ПЭВМ в конфигурации не менее, чем: процессор Pentium IV 3 ГГц, ОЗУ 2 Гбайта, НЖМД 200 Гбайт.

Используются программные продукты:

1. Операционные системы: Ubuntu Linux, Windows XP, Windows 7.
2. Пакеты программ Microsoft Office 2010, OpenOffice.
3. Информационные системы «Гарант», «Консультант+».
4. Средства построения виртуальных машин VMWare Player.
5. Свободно распространяемое средство анализа защищенности John The Ripper (http://www.openwall.com/john/g/john179j5w.zip).

5. Рекомендуемая литература

Основная литература

1. Бойкова О. Персональные данные. Обработка, использование и защита. М.: Пашков дом, 2012. – 120 с.
2. Голицына О.Л.., Партыка Т.Л., Попов И.И. Программное обеспечение: Учеб. пособие.- 4-е изд., перераб. и доп.- М.: Форум: ИНФРА-М, 2013.- 448 с.
3. Голицына О.Л.., Попов И.И. Основы алгоритмизации и программирования: Учеб. пособие.- 5-е изд., перераб. и доп.- М.: Форум: ИНФРА-М, 2013.- 432 с.
4. Голицына О.Л.., Попов И.И. Программирование на языках высокого уровня: Учеб. пособие.- М.: Форум: ИНФРА-М, 2013.- 496 с.
5. Гребенюк, Е. И. Технические средства информатизации: Учебник /Е. И. Гребенюк, Н. А. Гребенюк. – 6-е изд. – М.: Академия, 2011. – 352 с.
6. Губенков А.А. Информационная безопасность вычислительных сетей: учеб. пособие / А. А. Губенков. - Саратов: СГТУ, 2009. - 88 с.
7. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности.- 2-е изд.- М.: Горячая линия-Телеком, 2014.- 244 с.
8. Максимов Н.В. Технические средства информатизации.- М.: Форум: ИНФРА-М, 2015.-608 с.
9. Максимов, Н. В. Архитектура ЭВМ и вычислительные системы : Учебник / Н. В. Максимов, И. И. Попов, Т. П. Партыка. – 4-е изд. – М.: ФОРУМ, 2012. – 512 с.
10. Мельников Д. Информационная безопасность открытых систем.- М.: Форум, 2013.- 441 с.
11. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность: Учеб. Пособие для сред. проф. образ.- М.: Академия, 2012.- 336 с.
12. Олифер, В. Г. Компьютерные сети: Принципы, технологии, протоколы /В. Г. Олифер, Н. А. Олифер. – 4-е изд. – СПб. : Питер, 2010. – 180 с.
13. Партыка, Т. Л. Операционные системы, среды и оболочки : учеб. пособие / Т. Л. Партыка, И. И. Попов. – М. : ФОРУМ, 2013. - 560 с.
14. Северин В. Правовая защита информации в коммерческих организациях. М.: Academia, 2009. – 224 с.
15. Синатаров С.В. Пакеты прикладных программ: Учебное пособие.- М.: Альфа-М, 2012.- 256 с.
16. Таненбаум, Э. С. Компьютерные сети / Э. С. Таненбаум, Д. Уэзеролл. – 5-е изд. – СПб. : Питер, 2012. – 230 с.

Дополнительная литература

1. Алгоритмы категорирования персональных данных для систем автоматизированного проектирования баз данных информационных систем / Благодаров А. и др. М.: Горячая Линия - Телеком, 2013. – 116 с.
2. Безбогов А.А., Яковлев А.В., Мартемьянов Ю.Ф. Безопасность операционных систем. М.: Гелиос АРВ, 2008.
3. Борисов М.А. Особенности защиты персональных данных в трудовых отношениях. (Гриф УМО по дополнительному профессиональному образованию). М.: Либроком, 2012. – 224 с.
4. Бэндл Д. Защита и безопасность в сетях Linux. –СПб.: Питер-пресс, 2001. – 480с.
5. Галицкий А.В. Защита информации в сети – анализ технологий и синтез решений. – М.: ДМК Пресс, 2004. – 616 с.
6. Губенков А.А., Байбурин В.Б. Информационная безопасность: Учеб. пособие. – М.: ЗАО «Новый издательский дом», 2005. – 128 с.
7. Граннеман С. Linux. Карманный справочник. М: Вильямс, 2010. – 416 с.
8. Девякин П.Н. Модели безопасности компьютерных систем: Учеб. Пособие для вузов.- М.: Академия, 2005.- 144 с.
9. Дейтел Х.М., Дейтел П.Дж., Чофнес Д.Р. Операционные системы. Основы и принципы: Третье издание. М.: ООО «Бином-Пресс», 2006 г., 1024 с.
10. Защита персональных данных в организациях здравоохранения / Сабанов А. и др. М.: Горячая Линия - Телеком, 2012. – 206 с.
11. Калабеков Б.А. Цифровые устройства и микропроцессорные системы: Учебник для техникумов связи.- 2-е изд., перераб. и доп.- М.: Горячая линия- Телеком, 2007.- 336 с.
12. Колисниченко Д.Н. Linux. Полное руководство. М.: Изд-во "Наука и технологии", 2006. – 777с.
13. Корт С.С. Теоретические основы защиты информации: Учеб. Пособие.- М.: Гелиос АРВ, 2004.- 240 с.
14. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: Учебное пособие.- 2-е изд., испр.- М.: Интернет-Университет Информационных технологий; БИНОМ. Лаборатория знаний, 2007.- 531 с.
15. Мак-Клар С., Скембрей Дж., Куртц Д. Секреты хакеров. Безопасность сетей – готовые решения, 4-е изд. – М.: Вильямс, 2004. – 656 с.
16. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учеб. Пособие для вузов.- 3-е изд., стер. М.: Горячая линия, 2005.- 147 с.
17. Мельников, В. П. Информационная безопасность и защита информации: Учебник для студ. высш. учеб. заведений / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под. ред. С. А. Клейменова. – 4-е изд., стер. – М.: Академия, 2008. – 336 с.
18. Мышляева И.М. Цифровая схемотехника: Учеб. Пособие для сред. Проф. образования.- М.: Академия, 2005.- 400 с.
19. Норткатт С. Защита сетевого периметра: наиболее полное руководство. – М.: DiaSoft, 2004. – 672с.

20. Платонов, В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : Учеб. пособие для студ. высш. учеб. заведений / В. В. Платонов. – М.: Академия, 2006. – 240 с.
21. Романец Ю., Тимофеев П., Шаньгин В. Защита информации в компьютерных системах и сетях. –М.: Радио и связь, 2001. – 376с.
22. Северин В. Комплексная защита информации на предприятии. М.: Городец, 2008. – 368 с.
23. Смирнов Ю.А., Соколов С.В., Титов Е.В. Основы микроэлектроники и микропроцессорной техники: Учебное пособие.- 2-е изд., испр.- СПб.: Лань, 2013.- 496 с.
24. Скляров И.С. Головоломки для хакера: - СПб.:БХВ-Петербург, 2008.- 320 с.
25. Хатч Б., Ли Дж., Курц Дж. Секреты хакеров. Безопасность Linux — готовые решения. – М.: Вильямс, 2004. – 704 с.
26. Шагигин В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие.- М.: Форум: ИНФРА-М, 2008.-416 с.
27. Шумский А.А., Шелупанов А.А. Системный анализ в защите информации: Учеб. Пособие для вузов.- М.: Гелиос АРВ, 2005.- 224 с.

Председатель экспертной комиссии

Заведующий кафедрой
«Информационная безопасность
автоматизированных систем» ИнЭТМ
СГТУ имени Гагарина Ю.А. _____ В.Б. Байбурин

Члены экспертной комиссии:

Доцент кафедры «Информационная безопасность
автоматизированных систем» ИнЭТМ
СГТУ имени Гагарина Ю.А. _____ Н.Ю. Хороводова
Доцент кафедры «Информационная безопасность
автоматизированных систем» ИнЭТМ
СГТУ имени Гагарина Ю.А. _____ А.А. Губенков
Доцент кафедры «Информационная безопасность
автоматизированных систем» ИнЭТМ
СГТУ имени Гагарина Ю.А. _____ А.О. Мантуров
Доцент кафедры «Информационная безопасность
автоматизированных систем» ИнЭТМ
СГТУ имени Гагарина Ю.А. _____ А.С. Ершов
Заведующая отделением «Информационные технологии»
ППК СГТУ имени Гагарина Ю.А. _____ Ю.А. Хлебникова
Председатель МК отделения «Информационные
технологии» ППК СГТУ имени Гагарина Ю.А. _____ Ю.В. Таланова

Формы для фиксации ответов при выполнении пунктов заданий Ситуации 1.

Задание 1	Приложение 1 – заполняется таблица
Задание 2	Приложение 2 – заполняется таблица
Задание 3	Приложение 3 – заполняется таблица
Задание 4	Приложение 4 – заполняется таблица
Задание 5	Приложение 5 – заполняется таблица
Задание 6	Приложение 6 – заполняется таблица
Задание 7	Приложение 7 - выполняется в свободной форме

Приложение 1

Уровень защищенности персональных данных

Тип ИСПДн	
Категория субъектов	
Количество субъектов	
Тип актуальных угроз	
Уровень защищенности	

Приложение 2

Перечень требований, которые необходимо выполнить для обеспечения определенного в п.1 уровня защищенности персональных данных

пп.	Требование	Основание - документ
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		

Правильных ответов 16.

Приложение 3

Угрозы безопасности, связанные с НСД к персональным данным в данной информационной системе (на основе базовой модели угроз безопасности ПДн ФСТЭК)

№ п/п	Угроза
1.	
2.	
3.	
4.	
5.	
6.	
7.	

Правильных ответов 7.

Данные из таблицы будут использоваться для решения Задания 4.

Приложение 4

Определить актуальность угроз безопасности из предварительного списка (с помощью методики определения актуальных угроз безопасности ПДн ФСТЭК). Показатель опасности угроз, связанных с несанкционированным доступом, считать высоким.

№ п/п	Угроза	Возможность реализации угрозы	Показатель опасности угрозы	Актуальность угрозы
1.				
2.				
3.				
4.				
5.				
6.				
7.				

Правильных ответов 7.

Вывод: Так как показатель опасности угроз высокий, то все угрозы из предварительного списка являются _____

Приложение 5

Базовый набор мер защиты информации для определенного в п.1 уровня защищенности персональных данных (на основании *п*риказа ФСТЭК России от 18.02.2013 №21).

№ п/п	Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		
21.		
22.		
23.		
24.		
25.		
26.		
27.		
28.		
29.		
30.		
31.		
32.		
33.		
34.		
35.		
36.		
37.		
38.		
39.		
40.		
41.		
42.		

Правильных ответов 42.

Приложение 6

Адаптация базового набора мер с учетом структурно-функциональных характеристик и особенностей функционирования информационной системы.

№ п/п	Условное обозначение и номер меры	Меры по обеспечению безопасности персональных данных исключенные из базового набора
1.		
2.		
3.		
4.		
5.		
6.		
7.		

Правильных ответов 7.

Эталонный вариант решения профессионального задания

1. **Определите уровень защищенности персональных данных, учитывая, что угрозы, связанные с наличием недекларированных возможностей в системном и прикладном программном обеспечении, неактуальны для данной информационной системы (на основании постановления Правительства РФ от 1 ноября 2012 г. № 1119).**

Тип ИСПДн	Специальная (т.к. есть сведения о национальной принадлежности)
Категория субъектов	сотрудники
Количество субъектов	менее чем 100 000 (1800)
Тип актуальных угроз	3 тип (угрозы, связанные с наличием недекларированных возможностей в системном и прикладном программном обеспечении, неактуальны)
Уровень защищенности	**3**

2. **Перечислите требования, которые необходимо выполнить для обеспечения определенного в п.1 уровня защищенности персональных данных (на основании постановления Правительства РФ от 1 ноября 2012 г. № 1119 и приказа ФСБ РФ № 378 от 10.07.2014)**

Уровень защищенности персональных данных – 3
Тип актуальных угроз НДВ - 3

пп.	Требование	Основание - документ
1.	**1.Назначение должностного лица** (работника), **ответственного за обеспечение безопасности** персональных данных в информационной системе	постановление Правительства РФ от 1 ноября 2012 г. № 1119
2.	1.1.Назначение обладающего достаточными навыками должностного лица (работника) оператора ответственным за обеспечение безопасности персональных данных в информационной системе	приказ ФСБ РФ № 378 от 10.07.2014
3.	**2.Организация режима обеспечения безопасности помещений**, в которых размещена ИСПДн, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения	постановление Правительства РФ от 1 ноября 2012 г. № 1119
4.	2.1.Оснащение помещений входными дверьми с замками, обеспечение постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода, а также опечатывание помещений по окончании рабочего дня или оборудование помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений	приказ ФСБ РФ № 378 от 10.07.2014
5.	2.2.Утверждение правил доступа в помещения в рабочее и нерабочее время, а также в нештатных ситуациях	приказ ФСБ РФ № 378 от 10.07.2014
6.	2.3.Утверждение перечня лиц, имеющих право доступа в помещения	приказ ФСБ РФ № 378 от 10.07.2014
7.	**3.Обеспечение сохранности носителей персональных данных**	постановление Правительства РФ

		от 1 ноября 2012 г. № 1119
8.	3.1.Хранение съемных машинных носителей персональных данных в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками. В случае если на съемном машинном носителе персональных данных хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов (металлических шкафов)	приказ ФСБ РФ № 378 от 10.07.2014
9.	3.2.Поэкземплярный учет машинных носителей персональных данных, который достигается путем ведения журнала учета носителей персональных данных с использованием регистрационных (заводских) номеров	приказ ФСБ РФ № 378 от 10.07.2014
10.	4.Утверждение руководителем оператора документа, определяющего **перечень лиц**, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей	постановление Правительства РФ от 1 ноября 2012 г. № 1119 приказ ФСБ РФ № 378 от 10.07.2014
11.	4.1.Поддержание в актуальном состоянии документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей	приказ ФСБ РФ № 378 от 10.07.2014
12.	**5.Использование средств защиты информации, прошедших процедуру оценки соответствия** требованиям законодательства РФ в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз	постановление Правительства РФ от 1 ноября 2012 г. № 1119
13.	5.1.Получение исходных данных для формирования совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак	приказ ФСБ РФ № 378 от 10.07.2014
14.	5.2.Формирование и утверждение руководителем оператора совокупности предположений о	приказ ФСБ РФ № 378 от 10.07.2014

	возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, и определение на этой основе и с учетом типа актуальных угроз требуемого класса СКЗИ	
15.	5.3.Использование для обеспечения требуемого уровня защищенности персональных данных при их обработке в информационной системе СКЗИ класса КС1 и выше (сертифицированных)	приказ ФСБ РФ № 378 от 10.07.2014
16.	**6.Контроль за выполнением требований** организуется и проводится оператором самостоятельно и/или с привлечением на договорной основе лицензиатов ФСТЭК. Контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором.	постановление Правительства РФ от 1 ноября 2012 г. № 1119

3. Определите (предварительные) угрозы безопасности, связанные с НСД к персональным данным в данной информационной системе (на основе базовой модели угроз безопасности ПДн ФСТЭК).

Список угроз:

1. угрозы «Анализа сетевого трафика» с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации;
2. угрозы сканирования, направленные на выявление типа операционной системы ИСПДн, сетевых адресов рабочих станций, открытых портов и служб, открытых соединений и др.;
3. угрозы выявления паролей;
4. угрозы получения НСД путем подмены доверенного объекта;
5. угрозы типа «Отказ в обслуживании»;
6. угрозы удаленного запуска приложений;
7. угрозы внедрения по сети вредоносных программ.

4. **Определите актуальность угроз безопасности из предварительного списка (с помощью методики определения актуальных угроз безопасности ПДн ФСТЭК).**
Показатель опасности угроз, связанных с несанкционированным доступом, считать низким.

Оценка актуальности угроз безопасности персональных данных при их обработке в ИСПДн проводится с использованием «Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной ФСТЭК 14.02.08 г.

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для ПДн.

Для оценки возможности реализации угрозы применяются два показателя: уровень исходной защищенности ИСПДн и вероятность реализации *каждой* рассматриваемой угрозы.

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн, который имеет три уровня: низкий, средний и высокий. Исходная степень защищенности определяется путем оценки показателей защищенности информационной системы по таблице, приведенной в Методике ФСТЭК. Затем каждой степени исходной защищенности ставится в соответствие числовой коэффициент Y_1, а именно:

- 0 – для высокой степени исходной защищенности;
- 5 – для средней степени исходной защищенности;
- 10 – для низкой степени исходной защищенности.

Определим показатель исходной защищенности для информационной системы ОАО «Газавтоматизация»:

1.Локальная сеть в пределах близкорасположенных зданий	средний
2. Имеет многоточечный выход в глобальную сеть общего пользования	низкий
3. Возможные операции: запись, удаление, сортировка	средний
4. Доступ к ИСПДн имеют ограниченный круг лиц	высокий
5. ИСПДн принадлежит одному организации-владельцу	высокий
6. Данные в ИСПДн не обезличиваются	низкий
7. ИСПДн не предоставляет ПДн сторонним пользователям	высокий

Так как 71% ответов выше или равны оценке “средний”, а остальные – оценке “низкий”, то коэффициент степени исходной защищенности ИСПДн $Y_1 = 5$.

Вероятность реализации угрозы определяет, насколько вероятной является реализация конкретной угрозы для данной ИСПДн. Этот показатель **определяется экспертным путем**. Вводятся четыре градации этого показателя:

- маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими права доступа в помещение);
- низкая вероятность – существуют объективные предпосылки для реализации угрозы, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты);
- средняя вероятность – существуют объективные предпосылки для реализации угрозы, но принятые меры обеспечения безопасности недостаточны;
- высокая вероятность – существуют объективные предпосылки для реализации угрозы, и не приняты меры по обеспечению безопасности ПДн.

Каждой градации вероятности реализации угрозы ставится в соответствие числовой коэффициент Y_2, а именно:

- 0 – для маловероятной угрозы;
- 2 – для низкой вероятности угрозы;
- 5 – для средней вероятности угрозы;
- 10 – для высокой вероятности угрозы.

Коэффициент (возможность) реализуемости угрозы Y равен сумме коэффициента степени исходной защищенности ИСПДн и коэффициента вероятности реализации угрозы, разделенной на 20:

$$Y = (Y_1 + Y_2) / 20.$$

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация возможности реализуемости угрозы следующим образом:

- если $0 \le Y \le 0{,}3$, то возможность реализации угрозы признается низкой;
- если $0{,}3 < Y \le 0{,}6$, то возможность реализации угрозы признается средней;
- если $0{,}6 < Y \le 0{,}8$, то возможность реализации угрозы признается высокой;
- если $Y > 0{,}8$, то возможность реализации угрозы признается очень высокой.

Определим возможность реализации для каждой угрозы безопасности из предварительного перечня угроз для рассматриваемой ИСПДн.

Угрозы сетевых атак	**Y_1**	**Y_2**	**Y**
угрозы «Анализа сетевого трафика» с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации;	5	10	0,75
угрозы сканирования, направленные на выявление типа операционной системы ИСПДн, сетевых адресов рабочих станций, открытых портов и служб, открытых соединений и др.;	5	10	0,75
угрозы выявления паролей;	5	0	0,25
угрозы получения НСД путем подмены доверенного объекта;	5	10	0,75
угрозы внедрения по сети вредоносных программ.	5	10	0,75
угрозы типа «Отказ в обслуживании»;	5	5	0,5
угрозы удаленного запуска приложений;	5	10	0,75

Показатель опасности каждой угрозы для рассматриваемой ИСПДн определен **на основе опроса экспертов**.

Тип угроз	Показатель опасности угроз
Угрозы, связанные с НСД (сетевые атаки)	Высокий

Выбор актуальных для данной ИСПДн угроз безопасности из общего (предварительного) перечня угроз, осуществляется в соответствии с таблицей:

Таблица. Правила отнесения угрозы безопасности ПДн к актуальным угрозам

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	Неактуальная	Неактуальная	Актуальная
Средняя	Неактуальная	Актуальная	Актуальная
Высокая	Актуальная	Актуальная	Актуальная
Очень высокая	Актуальная	Актуальная	Актуальная

Определим актуальные угрозы безопасности для рассматриваемой ИСПДн:

Угрозы сетевых атак	**Возможность реализации угрозы**	**Показатель опасности угрозы**	**Актуальность угрозы**
угрозы «Анализа сетевого трафика» с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации;	высокая	высокая	**актуальна**
угрозы сканирования, направленные на выявление типа операционной системы ИСПДн, сетевых адресов рабочих станций, открытых портов и служб, открытых соединений и др.;	высокая	высокая	**актуальна**
угрозы выявления паролей;	низкая	высокая	**актуальна**
угрозы получения НСД путем подмены доверенного объекта;	высокая	высокая	**актуальна**
угрозы внедрения по сети вредоносных программ.	высокая	высокая	**актуальна**
угрозы типа «Отказ в обслуживании»;	средняя	высокая	**актуальна**
угрозы удаленного запуска приложений;	высокая	высокая	**актуальна**

Т.к. показатель опасности угроз высокий, то все угрозы из предварительного списка являются актуальными.

5. Определите базовый набор мер защиты информации для определенного в п.1 уровня защищенности персональных данных (на основании приказа ФСТЭК России от 18.02.2013 №21).

БАЗОВЫЙ НАБОР МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, НЕОБХОДИМЫХ ДЛЯ ОБЕСПЕЧЕНИЯ 3 УРОВНЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)
II. Управление доступом субъектов доступа к объектам доступа (УПД)	
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
УПД.6	Ограничение неуспешных попыток входа в

	информационную систему (доступа к информационной системе)
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
IV. Защита машинных носителей персональных данных (ЗНИ)	
ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания
V. Регистрация событий безопасности (РСБ)	
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ.7	Защита информации о событиях безопасности
VI. Антивирусная защита (АВЗ)	
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)	
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации
XI. Защита среды виртуализации (ЗСВ)	
ЗСВ.1	Идентификация и аутентификация субъектов доступа и

	объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей
XII. Защита технических средств (ЗТС)	
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе
XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)	
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных
УКФ.4	Документирование информации (данных) об изменениях

	в конфигурации информационной системы и системы защиты персональных данных

6**. Выполните адаптацию базового набора мер с учетом структурно-функциональных характеристик и особенностей функционирования информационной системы.**

Из базового набора исключены меры:

- ЗСВ.1 ЗСВ.2 ЗСВ.3 ЗСВ.9 ЗСВ.10 , т.к. не используются технологии виртуализации
- УПД.14, ЗИС.20, т.к. не используются беспроводные технологии.

Условное обозначение и номер меры	Меры по обеспечению безопасности персональных данных исключенные из базового набора
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа

7. Перечислите организационно-распорядительных документы, которые потребуется разработать в организации для выполнения требований статьи 19 закона «О персональных данных».

1. перечень обрабатываемых оператором персональных данных;
2. перечень информационных систем персональных данных;
3. приказ об утверждении «Положения об обработке и защите персональных данных»,

4. перечень лиц, осуществляющих обработку персональных данных,
5. приказ о назначении должностного лица, ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн;
6. должностные обязанности лица, ответственного за обеспечение безопасности персональных данных (пп-1119, уз-2, уз-3).
7. описание помещений, в которых осуществляется обработка персональных данных (расположение, номера помещений, наличие охраны, режима обеспечения безопасности, оборудование помещений, общее количество рабочих мест, количество рабочих мест, на которых обрабатываются персональные данные),
8. приказ о выделении помещений для обработки персональных данных
9. документ, устанавливающий требования к помещениям, в которых эксплуатируются криптосредства (приказ 378)
10. правила доступа в помещения в рабочее и нерабочее время, а также в нештатных ситуациях (приказ 378)
11. перечень лиц, имеющих право доступа в помещения, где производится обработка ПДн (приказ 378);
12. перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей (приказ 378);
13. разрешительные документы о допуске конкретных сотрудников к обработке персональных данных
14. приказ о возложении персональной ответственности за защиту персональных данных
15. должностные инструкции сотрудников, имеющих отношение к автоматизированной и/или неавтоматизированной обработке персональных данных;
16. инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные
17. приказ об утверждении мест хранения персональных данных,
18. перечень мер, необходимых для обеспечения сохранности персональных данных и исключающего несанкционированный доступ к ним (правила обработки персональных данных без использования средств автоматизации),
19. журнал учета машинных носителей персональных данных с использованием регистрационных (заводских) номеров (приказ 378)
20. план мероприятий по обеспечению безопасности персональных данных;
21. протокол оценки возможного вреда субъектам персональных данных;

22. модель угроз безопасности персональных данных;
23. приказ о создании комиссии по определению уровня защищенности ИСПДн;
24. акт определения уровня защищенности персональных данных;
25. положение о применимости базовых мер по обеспечению безопасности персональных данных
26. журналы учёта средств защиты информации (наименование, заводской, инвентарный номер);
27. журнал поэкземплярного учёта криптографических средств, эксплуатационной и технической документации к ним, ключевых документов;
28. журнал учета работы с ключевыми средствами;
29. Приказ о назначении пользователей криптосредств;
30. Лицевые счета на пользователей криптосредств;
31. Приказ о назначении ответственного пользователя криптосредств
32. Функциональные обязанности ответственного пользователя криптосредств.
33. сертификаты средств защиты информации;
34. положение о разграничении прав доступа к обрабатываемым персональным данным;
35. инструкция администратора информационной безопасности;
36. инструкция по организации парольной защиты;
37. инструкция по антивирусной защите;
38. инструкция пользователя при обработке персональных данных на объектах вычислительной техники;
39. инструкция пользователю по обеспечению безопасности при возникновении внештатных ситуаций;
40. журнал проведения инструктажа по информационной безопасности,
41. инструкции о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации;
42. план внутренних проверок состояния защиты персональных данных;
43. журнал периодического тестирования средств защиты информации;
44. документ, устанавливающий порядок организации контроля за соблюдением условий использования криптосредств;
45. приказы об организации режима обеспечения безопасности (охраны);

46. локальные акты, устанавливающие порядок уничтожения персональных данных (приказ о назначении комиссии по уничтожению персональных данных, акты об уничтожении материальных носителей персональных данных) (приказ 21).
47. приказ по границе контролируемой зоны, схема контролируемой зоны (СТР-К).
48. приказ о вводе в эксплуатацию информационной системы персональных данных и назначении ответственного лица.
49. приказ о вводе в эксплуатацию средств вычислительной техники, обрабатывающих персональные данные и назначении ответственных лиц.
50. акт оценки эффективности мер защиты персональных данных.

8. Ответы к заданию ситуации 2: Для полученного перечня хешей определить исходный пароль, по которому они были сгенерированы с помощью алгоритма MD5.

1) monkeys
2) bi0br0
3) 00ger2
4) ralphzz
5) pin77ky
6) l-312
7) ipugyhy
8) vnbp4a1
9) s0ghj3
10) 1magie5