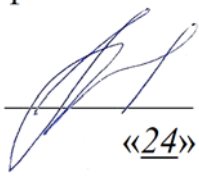
Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)
Липецкий филиал Финуниверситета

УТВЕРЖДАЮ
Заместитель директора
по учебно-методической работе
Липецкого филиала Финуниверситета



О.Н. Левчегов
«*24*» *апреля* 20*24* г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ «ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНЫХ И ПРОГРАММНО-АППАРАТНЫХ (В ТОМ ЧИСЛЕ, КРИПТОГРАФИЧЕСКИХ) СРЕДСТВ ЗАЩИТЫ»

по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

Липецк - 2024

Фонд оценочных средств разработан на основе федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем».

Разработчики:

Черпаков Игорь Владимирович, к.ф.-м.н., доцент кафедры Учет и информационные технологии в бизнесе Липецкого филиала Финуниверситета.

Фонд оценочных средств рассмотрен и рекомендован к утверждению на заседании кафедры Учет и информационные технологии в бизнесе Липецкого филиала Финуниверситета.

Протокол от 23.04.2024 г. №10

Заведующий кафедрой

Учет и информационные технологии в бизнесе _____ Н.С. Морозова

1. Общие положения

Фонды оценочных средств (далее ФОС) предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу профессионального модуля ПМ.02. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты.

ФОС включают контрольные материалы для проведения текущего контроля и итоговой аттестации в форме экзамена по МДК.02.01. «Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты» и зачёта по МДК. 02.02. «Криптографическая защита информации».

ФОС разработаны на основании положений:

– ФГОС по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем;

– Положения о ФОС Липецкого филиала Финуниверситета;

– программы профессионального модуля ПМ.02. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты.

2. Результаты освоения модуля, подлежащие проверке

Уметь	**У1 –** выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах; **У2 –** определять рациональные методы и средства защиты на объектах и оценивать их эффективность; **У3 –** производить установку и настройку типовых программно-аппаратных средств защиты информации; **У4 –** пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации;
Знать	**З1 –** типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах; **З2 –** основные протоколы идентификации и аутентификации в телекоммуникационных системах; **З3 –** состав и возможности типовых конфигураций программно-аппаратных средств защиты информации; **З4 –** особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах; основные способы противодействия; **З5 –** несанкционированному доступу к информационным ресурсам информационно-телекоммуникационной системы; **З6 –** основные понятия криптографии и типовые криптографические методы защиты информации;

3. Распределение оценивания результатов обучения по видам контроля

Наименование элемента умений или знаний	Виды аттестации	
	Текущий контроль	Промежуточная аттестация
У1 – выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах;	+	+
У2 – определять рациональные методы и средства защиты на объектах и оценивать их эффективность;	+	+
У3 – производить установку и настройку типовых программно-аппаратных средств защиты информации;	+	+
У4 – пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации;	+	+
З1 – типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах;	+	+
З2 – основные протоколы идентификации и аутентификации в телекоммуникационных системах;	+	+
З3 – состав и возможности типовых конфигураций программно-аппаратных средств защиты информации;	+	+
З4 – особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах; основные способы противодействия;	+	+
З5 – несанкционированному доступу к информационным ресурсам информационно-телекоммуникационной системы;	+	+
З6 – основные понятия криптографии и типовые криптографические методы защиты информации;	+	+

4. Распределение типов контрольных заданий по элементам знаний и умений

Объекты проверки	МДК.02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты				МДК. 02.02. Криптографическая защита информации		
	Тема 1.1. Обеспечение безопасности операционных систем	Тема1.2. Технологии разграничения доступа	Тема 1.3. Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN	Тема 1.4. Методы управления средствами защиты	Тема 2.1. Основы криптографических методов защиты информации	Тема 2.2. Современные стандарты шифрования	Тема 2.3. Криптографические методы обеспечения безопасности сетевых технологий
У1	Т	Т		Рз		Рз	
У2			Т		Рз		Рз
У3	Л	Л		Т	Пр		Л
У4			Л	Т		Рз	
З1	Т	Т		Рз		Рз	
З2			Т		Рз		Рз
З3	Л	Л		Т	Пр		Л
З4			Л	Т		Рз	
З5					Т	Пр	
З6				Л			

Т – тест
Пр – практические работы
Л – лабораторные работы
Рз – решение задачи

5. Распределение типов и количества контрольных заданий по элементам знаний и умений, контролируемых на промежуточной аттестации

Объекты проверки	МДК.02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты				МДК. 02.02. Криптографическая защита информации		
	Тема 1.1. Обеспечение безопасности операционных систем	Тема1.2. Технологии разграничения доступа	Тема 1.3. Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN	Тема 1.4. Методы управления средствами защиты	Тема 2.1. Основы криптографических методов защиты информации	Тема 2.2. Современные стандарты шифрования	Тема 2.3. Криптографические методы обеспечения безопасности сетевых технологий
У1	Э	Э	Э	Э	З	З	З
У2	Э	Э	Э	Э	З	З	
У3	Э	Э	Э	Э	З		З
У4		Э	Э		З	З	
З1		Э		Э	З		З
З2	Э	Э	Э		З	З	З
З3	Э	Э		Э	З	З	З
З4	Э		Э	Э	З	З	
З5	Э	Э	Э	Э	З		З
З6	Э	Э					

Э - экзамен, З - зачёт

6. Содержание контрольных заданий

Комплект тестов

Критерии оценки:

Количество правильных ответов	Процент выполнения	Оценка
31-35	более 90%	Отлично
27-30	80-90%	Хорошо
20-26	60-79%	Удовлетворительно
менее 20	менее 60%	Неудовлетворительно

Задание № 1. Выберите один из нескольких вариантов ответа:

1. Информация это -

1 сведения, поступающие от СМИ

2 только документированные сведения о лицах, предметах, фактах, событиях

3 сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления

4 только сведения, содержащиеся в электронных базах данных

2. Информация

1 не исчезает при потреблении

2 становится доступной, если она содержится на материальном носителе

3 подвергается только "моральному износу"

4 характеризуется всеми перечисленными свойствами

3. Какими официальными документами информация отнесена к объектам гражданских прав?

1 УК РФ

2 Законом РФ "О праве на информацию"

3 ГК и законом РФ "Об информации, информатизации и защите информации"

4 Конституцией РФ

4. Информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать, называется

1 достоверной

2 конфиденциальной

3 документированной

4 коммерческой тайной

5. Формы защиты интеллектуальной собственности -

1 авторское, патентное право и коммерческая тайна

2 интеллектуальное право и смежные права

3 коммерческая и государственная тайна

4 гражданское и административное право

6. По принадлежности информационные ресурсы подразделяются на

1 государственные, коммерческие и личные

2 государственные, не государственные и информацию о гражданах

3 информацию юридических и физических лиц

4 официальные, гражданские и коммерческие

7. К негосударственным относятся информационные ресурсы

1 созданные, приобретенные за счет негосударственных учреждений и организаций

2 созданные, приобретенные за счет негосударственных предприятий и физических лиц

3 полученные в результате дарения юридическими или физическими лицами

4 указанные в п.1-3

8. По доступности информация классифицируется на

1 открытую информацию и государственную тайну

2 конфиденциальную информацию и информацию свободного доступа

3 информацию с ограниченным доступом и общедоступную информацию
4 виды информации, указанные в остальных пунктах

9. К конфиденциальной информации относятся документы, содержащие

1 государственную тайну
2 законодательные акты
3 "ноу-хау"
4 сведения о золотом запасе страны

10. Запрещено относить к информации ограниченного доступа

1 информацию о чрезвычайных ситуациях
2 информацию о деятельности органов государственной власти
3 документы открытых архивов и библиотек
4 все, перечисленное в остальных пунктах

11. Какие методы обеспечения информационной безопасности Российской Федерации направлены на создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи?

1 правовые
2 организационно-технические
3 экономические
4 стратегические

12. Что использует системы защиты информации Secret Disk для хранения паролей?

1 накопители на магнитных дисках
2 оперативную память компьютера
3 электронные ключи
4 бумажные носители

13. С какой целью используется теория информации при рассмотрении каналов передачи информационных потоков?

1 для повышения эффективности работы каналов связи
2 для анализа качества передаваемой информации
3 для вычисления количества информации в потоке и пропускной способности канала
4 для шифровки передаваемых сообщений

14. Какие преобразования шифра выполняются при операции рассеивания?

1 сжатие шифра
2 передача текста небольшими частями
3 наложение ложных сообщений
4 изменение любого знака открытого текста или ключа

15. Сколько типов архитектуры используется при создании системы сертификации в инфраструктуре с открытыми ключами?

1 один
2 два
3 три
4 четыре

16. Какой уровень контроля достаточен для ПО, используемого при защите информации с грифом «ОВ»?

1 первый
2 второй
3 третий
4 четвертый

17. С какой целью выполняется шифрование кода программ?

1 для противодействия дизассемблированию
2 для ускорения работы программ

3 в целях повышения надежности программного обеспечения
4 для упрощения работы пользователей

18. Какая система обеспечивает защиту информации?

1 система разграничения доступа субъектов к объектам
2 система кодирования информации
3 система управления потоками данных
4 система идентификации

19. Сколько существует классов, на которые подразделяются носители информации на предприятии?

1 два
2 три
3 пять

20. В чем заключается сущность приема "Троянский конь"?

1 это тайное введение в чужую программу команд, которые позволяют ей осуществлять новые, не планировавшиеся владельцем функции, но одновременно сохранять и прежнюю работоспособность
2 это тайное введение в чужую программу команд, которые позволяют ей осуществлять новые, не планировавшиеся владельцем функции
3 это тайное проникновение в чужую программу

21. RAID-массив это

1 набор жестких дисков, подключенных особым образом
2 антивирусная программа
3 вид хакерской утилиты
4 база защищенных данных

22. Вирус внедряется в исполняемые файлы и при их запуске активируется. Это…

1 загрузочный вирус
2 макровирус
3 файловый вирус
4 сетевой червь

23. В каких основных форматах существует симметричный алгоритм?

1 блока и строки
2 потока и блока
3 потока и данных
4 данных и блока

24. Шифр, который заключается в перестановках структурных элементов шифруемого блока данных – битов, символов, цифр – это:

1 шифр функциональных преобразований
2 шифр замен
3 шифр перестановок

25. Возможно ли, вычислить закрытый ключ ассиметричного алгоритма, зная открытый?

1 нет
2 да
3 в редких случаях

26. Условие, при котором в распоряжении аналитика находится возможность получить результат зашифровки для произвольно выбранного им массива открытых данных размера n используется в анализе:

1 на основе произвольно выбранного шифротекста
2 на основе произвольно выбранного открытого текста
3 правильного ответа нет

Задание № 2. Выберите несколько вариантов ответа:

27. Отметьте составные части современного антивируса

1 модем
2 принтер
3 сканер
4 межсетевой экран
5 монитор

28. К вредоносным программам относятся:

1 потенциально опасные программы
2 вирусы, черви, трояны
3 шпионские и рекламные программы
4 вирусы, программы-шутки, антивирусное программное обеспечение
5 межсетевой экран, брандмауэр

29. К биометрической системе защиты относятся:

1 защита паролем
2 физическая защита данных
3 антивирусная защита
4 идентификация по радужной оболочке глаз
5 идентификация по отпечаткам пальцев

30. Компьютерные вирусы – это:

1) Вредоносные программы, наносящие вред данным.
2) Программы, уничтожающие данные на жестком диске
3) Программы, которые могут размножаться и скрыто внедрять свои копии в файлы, загрузочные сектора дисков, документы.
4) Программы, заражающие загрузочный сектор дисков и препятствующие загрузке компьютера
5) Это скрипты, помещенные на зараженных интернет-страничках

Задание № 3. Укажите соответствие для всех 6 вариантов ответа

31. Сопоставьте названия программ и изображений.

1) 	а) Antivir
2) 	б) DrWeb
3) 	в) Nod 32
4) 	г) Antivirus Kaspersky
5) 	д) Avast
6) 	е) Antivirus Panda

Задание № 4. Укажите истинность или ложность вариантов ответа, поставив «да» или «нет»

32. Выразите свое согласие или несогласие.

___ Почтовый червь активируется в тот момент, когда к вам поступает электронная почта.
___ Если компьютер не подключен к сети Интернет, в него не проникнут вирусы.
___ Файловые вирусы заражают файлы с расширениями *.doc, *.ppt, *.xls.
___ Чтобы защитить компьютер недостаточно только установить антивирусную программу.
___ На Web-страницах могут находиться сетевые черви.

Задание № 5. Запишите ответ

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

Ответ: _____

34. Процесс преобразования информации, хранящейся в файле к виду, при котором уменьшается избыточность в ее представлении и соответственно требуется меньший объем памяти для ее хранения.

Ответ: _____

Задание № 6. Укажите порядок следования всех 3 вариантов ответа

35. Укажите порядок действий при наличии признаков заражения компьютера.

__ Сохранить результаты работы на внешнем носителе.
__ Запустить антивирусную программу.
__ Отключиться от глобальной или локальной сети.

Вариант № 2

1. К конфиденциальной информации не относится

1 коммерческая тайна
2 персональные данные о гражданах
3 государственная тайна
4 "ноу-хау"

2. Вопросы информационного обмена регулируются (...) правом

1 гражданским
2 информационным
3 конституционным
4 уголовным

3. Согласно ст.138 ГК РФ интеллектуальная собственность это

1 информация, полученная в результате интеллектуальной деятельности индивида
2 литературные, художественные и научные произведения
3 изобретения, открытия, промышленные образцы и товарные знаки
4 исключительное право гражданина или юридического лица на результаты интеллектуальной деятельности

4. Интеллектуальная собственность включает права, относящиеся к

1 литературным, художественным и научным произведениям, изобретениям и открытиям
2 исполнительской деятельности артиста, звукозаписи, радио- и телепередачам
3 промышленным образцам, товарным знакам, знакам обслуживания, фирменным наименованиям и коммерческим обозначениям
4 всему, указанному в остальных пунктах

5. Конфиденциальная информация это

1 сведения, составляющие государственную тайну
2 сведения о состоянии здоровья высших должностных лиц
3 документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ
4 данные о состоянии преступности в стране

6. Какая информация подлежит защите?

1 информация, циркулирующая в системах и сетях связи
2 зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать
3 только информация, составляющая государственные информационные ресурсы
4 любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу

7. Система защиты государственных секретов определяется Законом
1 "Об информации, информатизации и защите информации"
2 "Об органах ФСБ"
3 "О государственной тайне"
4 "О безопасности"

8. Государственные информационные ресурсы не могут принадлежать
1 физическим лицам
2 коммерческим предприятиям
3 негосударственным учреждениям
4 всем перечисленным субъектам

9. Из нижеперечисленных законодательных актов наибольшей юридической силой в вопросах информационного права обладает
1 Указ Президента "Об утверждении перечня сведений, относящихся к государственной тайне"
2 ГК РФ
3 Закон "Об информации, информатизации и защите информации"
4 Конституция

10. Классификация и виды информационных ресурсов определены
1 Законом "Об информации, информатизации и защите информации"
2 Гражданским кодексом
3 Конституцией
4 всеми документами, перечисленными в остальных пунктах

11. Какие действия квалифицируются как компьютерное пиратство?
1 незаконное тиражирование лазерных дисков
2 распространение незаконно полученной информации по компьютерным сетям
3 попытка получить санкционированный доступ к компьютерной системе или вычислительной сети
4 попытка получить несанкционированный доступ к компьютерной системе или вычислительной сети

12. Какую задачу решает сертификация средств защиты информации?
1 обеспечения требуемого качества защиты информации
2 повышения квалификации разработчиков средств защиты информации
3 создания надежных средств защиты информации
4 защиты отечественных производителей средств защиты информации

13. Какие задачи решает система антивирусной защиты?
1 предотвращения проникновения вирусов к персональным ресурсам
2 повышения надежности работы программного обеспечения
3 предотвращения поломок технических средств
4 повышения эффективности работы программных средств

14. Что служит мерой опасности незаконного канала передачи информации?
1 пропускная способность незаконного канала
2 количество информации, передаваемой по незаконному каналу
3 время существования незаконного канала
4 число лиц, имеющих доступ к незаконному каналу

15. Какие шифры называются послойными?
1 состоящие из слоев шифрования
2 состоящие из цепочки циклов шифрования

3 выполняющие единственное преобразование информационного сообщения
4 обеспечивающие высокоэффективное шифрование

16. Какой цифровой документ подтверждает соответствие между открытым ключом и информацией, идентифицирующей владельца ключа?

1 код пользователя
2 цифровой сертификат
3 доверенность
4 шифр программы

17. Какой уровень контроля достаточен для ПО, используемого при защите информации с грифом «СС»?

1 первый
2 второй
3 третий
4 четвертый

18. Как используются дизассемблеры при взломе программы?

1 с их помощью изучается полученный код программы
2 с их помощью совершенствуется программное обеспечение
3 с их помощью кодируется программное обеспечение
4 они применяются для стыковки отдельных модулей

19. Кем формулируются требования к системе по защите компьютерной информации?

1 разработчиком
2 пользователем
3 заказчиком
4 головной организацией

20. Что принято называть утечкой информации?

1 доступ посторонних лиц к конфиденциальной информации
2 выход информации, составляющей коммерческую тайну, за пределы области ее обращения
3 утрату информации, хранящейся на носителях

21. В чем заключается сущность приема "Асинхронная атака"?

1 это способ смешивания двух или более различных программ, поочередно выполняемых в памяти компьютера, что позволяет достигать любых целей - заложенных преступником
2 это способ размещения памяти компьютера двух или более различных программ, выполняемых одновременно
3 это способ смешивания двух или более различных программ, одновременно выполняемых в памяти компьютера, что позволяет достигать любых целей - заложенных преступником

22. Вредоносные программы - это

1 шпионские программы
2 программы, наносящие вред данным и программам, находящимся на компьютере
3 программы, наносящие вред пользователю, работающему на зараженном компьютере
4 троянские утилиты и сетевые черви

23. Вирус, поражающий документы называется

1 троян
2 файловый вирус
3 макровирус
4 сетевой червь

24. Открытым текстом в криптографии называют:

1 расшифрованный текст
2 любое послание
3 исходное послание

25. Шифрование – это:

1 процесс создания алгоритмов шифрования
2 процесс сжатия информации

3 процесс криптографического преобразования информации к виду, когда ее смысл полностью теряется

26. Аутентификацией называют:

1 процесс регистрации в системе

2 способ защиты системы

3 процесс распознавания и проверки подлинности заявлений о себе пользователей и процессов

Задание № 2. Выберите несколько вариантов ответа:

27. К биометрической системе защиты относятся:

1 защита паролем

2 физическая защита данных

3 антивирусная защита

4 идентификация по радужной оболочке глаз

5 идентификация по отпечаткам пальцев

28. Компьютерные вирусы – это:

1) Вредоносные программы, наносящие вред данным.

2) Программы, уничтожающие данные на жестком диске

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

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

5) Это скрипты, помещенные на зараженных интернет-страничках

29. Отметьте составные части современного антивируса

1 модем

2 принтер

3 сканер

4 межсетевой экран

5 монитор

30. К вредоносным программам относятся:

1 потенциально опасные программы

2 вирусы, черви, трояны

3 шпионские и рекламные программы

4 вирусы, программы-шутки, антивирусное программное обеспечение

5 межсетевой экран, брандмауэр

Задание № 3. Укажите соответствие для всех 6 вариантов ответа

31. Сопоставьте названия программ и изображений.

1)  а) Antivir

2)  б) DrWeb

3)  в) Nod 32

4)  г) Antivirus Kaspersky

5)  д) Avast

6)  е) Antivirus Panda

Задание № 4. Укажите истинность или ложность вариантов ответа, поставив «да» или «нет»

32. Выразите свое согласие или несогласие.

___ Если компьютер не подключен к сети Интернет, в него не проникнут вирусы.
___ Почтовый червь активируется в тот момент, когда к вам поступает электронная почта.
___ На Web-страницах могут находиться сетевые черви.
___ Чтобы защитить компьютер недостаточно только установить антивирусную программу.
___ Файловые вирусы заражают файлы с расширениями *.doc, *.ppt, *.xls.

Задание № 5. Запишите ответ

33. Применяет метод сжатия отдельных участков файла, при этом длина файла после внедрения вируса может не измениться.

Ответ: _____

34. Процесс, обеспечивающий уменьшение объема данных, выполняется за счет устранения избыточности информации.

Ответ: _____

Задание № 6. Укажите порядок следования всех 3 вариантов ответа

35. Укажите порядок действий при наличии признаков заражения компьютера.

__ Отключиться от глобальной или локальной сети.
__ Сохранить результаты работы на внешнем носителе.
__ Запустить антивирусную программу.

Вариант № 3

1. Определение понятия "конфиденциальная информация" дано в

1 ГК РФ
2 Законе "О государственной тайне"
3 Законе "Об информации, информатизации и защите информации"
4 УК РФ

2. Формой правовой защиты литературных, художественных и научных произведений является (...) право

1 литературное
2 художественное
3 авторское
4 патентное

3. Запрещено относить к информации с ограниченным доступом

1 законодательные акты, информацию о чрезвычайных ситуациях и информацию о деятельности органов государственной власти (кроме государственной тайны)
2 только информацию о чрезвычайных ситуациях
3 только информацию о деятельности органов государственной власти (кроме государственной тайны)
4 документы всех библиотек и архивов

4. Формой правовой защиты изобретений является

1 институт коммерческой тайны
2 патентное право

3 авторское право
4 все, перечисленное в остальных пунктах

5. К коммерческой тайне могут быть отнесены

1 сведения не являющиеся государственными секретами
2 сведения, связанные с производством и технологической информацией
3 сведения, связанные с управлением и финансами
4 сведения, перечисленные в остальных пунктах

6. Является ли авторское право, патентное право и КТ формами защиты интеллектуальной собственности?

1 да
2 нет
3 только авторское и патентное
4 только КТ

7. «Ноу-хау» это -

1 незащищенные новшества
2 защищенные новшества
3 общеизвестные новые технологии
4 опубликованные технические и технологические новинки

8. Каким законом в РФ защищаются права исполнителей и производителей фонограмм?

1 "О правовой охране программ для ЭВМ и баз данных"
2 "Об авторском праве и смежных правах"
3 "Патентный закон РФ"
4 закон еще не принят

9. Закон "Об авторском праве и смежных правах" защищает права

1 исполнителей (актеров, певцов и т.д.)
2 производителей фонограмм
3 организации эфирного и кабельного вещания
4 всех лиц, перечисленных в остальных пунктах

10. Какой законодательный акт содержит сведения по защите коммерческой тайны?

1 Закон "Об авторском праве и смежных правах"
2 Закон "О коммерческой тайне"
3 Патентный закон
4 Закон "О правовой охране программ для ЭВМ и баз данных"

11. На решение каких вопросов направлена система лицензирования деятельности в области защиты государственной тайны?

1 на выполнение требований к организациям и лицам, занимающимся вопросами защиты государственной тайны
2 на повышение экономической эффективности деятельности в области защиты государственной тайны
3 на обеспечение правовых основ деятельности в области защиты государственной тайны
4 на решение проблемы надлежащего финансирования работ в области защиты государственной тайны

12. Как решается проблема защиты каналов передачи данных между головным офисом и филиалами компании?

1 с помощью специального программного обеспечения
2 шифровкой передаваемых сообщений
3 с помощью защищенных виртуальных частных сетей
4 передачей информации специальными курьерами

13. Что можно противопоставить взлому системы защиты информации?

1 систему контроля передаваемых сообщений
2 установку дополнительной системы защиты
3 введение специальных паролей

4 создание защищенного домена для системы защиты

14. В чем сущность идеи многократного шифрования?

1 многократное использование ключей

2 построение стойкой к дешифрованию системы путем последовательного применения относительно простых криптографических преобразований

3 многократное использование паролей

4 многократное шифровка и расшифровка исходного текста

15. Какой стандарт задает формат цифрового сертификата?

1 X.509

2 SP321

3 VGI

4 UPL

16. Какой уровень контроля достаточен для ПО, используемого при защите информации с грифом «С»?

1 первый

2 второй

3 третий

4 четвертый

17. Что представляют собой средства мониторинга?

1 это набор утилит, отслеживающих операции с файлами, реестром, портами и сетью

2 это набор утилит, используемых для вывода на монитор текстовой информации

3 это набор утилит, защищающих информацию от вирусов

4 это набор утилит, позволяющих сократить время выполнения арифметических операций

18. Кто отвечает за разработку комплексной системы защиты информации?

1 заказчик комплексной системы защиты информации

2 главный конструктор комплексной системы защиты информации

3 пользователь комплексной системы защиты информации

4 поставщик комплексной системы защиты информации

19. Каким образом должен быть организован процесс формирования и потребления информации, составляющей коммерческую тайну предприятия?

1 он должен быть организован таким образом, чтобы исключить утечку информации

2 он должен быть организован таким образом, чтобы область обращения информации, была бы минимальна и достаточна

3 он должен быть организован таким образом, чтобы обеспечить сохранность информации

20. Какой из методов защиты информации на персональном компьютере или рабочей станции сети является основным?

1 шифрование с достаточной длиной ключа

2 средства антивирусной защиты

3 системы защиты, блокирующие загрузку компьютера до предъявления электронного идентификатора

21. Сетевые черви – это

1 вредоносные программы, устанавливающие скрытно от пользователя другие вредоносные программы и утилиты

2 вирусы, которые проникнув на компьютер, блокируют работу сети

3 вирусы, которые внедряются в документы под видом макросов

4 вредоносные программы, которые проникают на компьютер, используя сервисы компьютерных сетей

22. Создание помех для нормальной работы канала передачи связи, то есть нарушение работоспособности канала связи возникает:

1 со стороны злоумышленника

2 со стороны законного отправителя сообщения

3 со стороны законного получателя сообщения

4 как со стороны злоумышленника, так и со стороны законного получателя

23. Открытым текстом в криптографии называют:

1 расшифрованный текст
2 любое послание
3 исходное послание

24. Функция, предназначенная для выработки блока данных, используемого для модификации шифруемого блока, из инварианта и ключевого элемента называется:

1 функция шифрования шага преобразования
2 инвариант стандартного шага шифрования

25. Характерная черта алгоритма Эль-Гамаля состоит в:

1 протоколе передачи подписанного сообщения, позволяющего подтверждать подлинность отправителя
2 в точной своевременной передаче сообщения
3 алгоритм не имеет особенностей и идентичен RSA

26. Условие, при котором в распоряжении аналитика находится возможность получить результат зашифровки для произвольно выбранного им массива открытых данных размера n используется в анализе:

1 на основе произвольно выбранного шифротекста
2 на основе произвольно выбранного открытого текста
3 правильного ответа нет

Задание № 2. Выберите несколько вариантов ответа:

27. Компьютерные вирусы – это:

1) Вредоносные программы, наносящие вред данным.
2) Программы, уничтожающие данные на жестком диске
3) Программы, которые могут размножаться и скрыто внедрять свои копии в файлы, загрузочные сектора дисков, документы.
4) Программы, заражающие загрузочный сектор дисков и препятствующие загрузке компьютера
5) Это скрипты, помещенные на зараженных интернет-страничках

27. К вредоносным программам относятся:

1 потенциально опасные программы
2 вирусы, черви, трояны
3 шпионские и рекламные программы
4 вирусы, программы-шутки, антивирусное программное обеспечение
5 межсетевой экран, брандмауэр

29. К биометрической системе защиты относятся:

1 защита паролем
2 физическая защита данных
3 антивирусная защита
4 идентификация по радужной оболочке глаз
5 идентификация по отпечаткам пальцев

30. Отметьте составные части современного антивируса

1 модем
2 принтер
3 сканер
4 межсетевой экран
5 монитор

Задание № 3. Укажите соответствие для всех 6 вариантов ответа

31. Сопоставьте названия программ и изображений.

1)  а) Antivir

2)  б) DrWeb

3)  в) Nod 32

4)  г) Antivirus Kaspersky

5)  д) Avast

6)  е) Antivirus Panda

Задание № 4. Укажите истинность или ложность вариантов ответа, поставив «да» или «нет»

32. Выразите свое согласие или несогласие.

___ На Web-страницах могут находиться сетевые черви.
___ Почтовый червь активируется в тот момент, когда к вам поступает электронная почта.
___ Если компьютер не подключен к сети Интернет, в него не проникнут вирусы.
___ Файловые вирусы заражают файлы с расширениями *.doc, *.ppt, *.xls.
___ Чтобы защитить компьютер недостаточно только установить антивирусную программу.

Задание № 5. Запишите ответ

33. Маскируют свое присутствие в среде обитания путем перехвата обращений операционной системы к пораженным файлам, секторам и переадресуют ОС к незараженным участкам информации.

Ответ: _____

34. Процесс преобразования информации, хранящейся в файле к виду, при котором уменьшается избыточность в ее представлении и соответственно требуется меньший объем памяти для ее хранения.

Ответ: _____

Задание № 6. Укажите порядок следования всех 3 вариантов ответа

35. Укажите порядок действий при наличии признаков заражения компьютера.

__ Запустить антивирусную программу.
__ Отключиться от глобальной или локальной сети.
__ Сохранить результаты работы на внешнем носителе.

Вариант № 4

1. К информации ограниченного доступа не относится

1 государственная тайна
2 размер золотого запаса страны

3 персональные данные
4 коммерческая тайна

2. Система защиты государственных секретов

1 основывается на Уголовном Кодексе РФ
2 регулируется секретными нормативными документами
3 определена Законом РФ "О государственной тайне"
4 осуществляется в соотетствии с п.1-3

3. Действие Закона "О государственной тайне" распространяется

1 на всех граждан и должностных лиц РФ
2 только на должностных лиц
3 на граждан, которые взяли на себя обязательство выполнять требования законодательства о государственной тайне
4 на всех граждан и должностных лиц, если им предоставили для работы закрытые сведения

4. К государственной тайне относится...

1 информация в военной области
2 информация о внешнеполитической и внешнеэкономической деятельности государства
3 информация в области экономики, науки и техники и сведения в области разведывательной и оперативнорозыскной деятельности
4 все выше перечисленное

5. Документы, содержащие государственную тайну снабжаются грифом

1 "секретно"
2 "совершенно секретно"
3 "особой важности"
4 указанным в п.1-3

6. Гриф "ДСП" используется

1 для секретных документов
2 для документов, содержащих коммерческую тайну
3 как промежуточный для несекретных документов
4 в учебных целях

7. Порядок засекречивания состоит в установлении следующих принципов:

1 целесообразности и объективности
2 необходимости и обязательности
3 законности, обоснованности и своевременности
4 всех выше перечисленных

8. Предельный срок пересмотра ранее установленных грифов секретности составляет

1 5 лет
2 1 год
3 10 лет
4 15 лет

9. Срок засекречивания сведений, составляющих государственную тайну

1 составляет 10 лет
2 ограничен 30 годами
3 устанавливается Указом Президента РФ
4 ничем не ограничен

10. За нарушения законодательства РФ о ГТ предусматривается (...) ответственность

1 уголовная и административная
2 гражданско-правовая
3 дисциплинарная
4 указанная в п.1-3

11. Частью какой, более общей системы, является система обеспечения информационной безопасности Российской Федерации?

1 системы защиты национальных интересов страны

2 системы обороны страны
3 системы защиты прав граждан страны
4 системы обеспечения национальной безопасности страны

12. В чем заключается сущность приема, обеспечивающего несанкционированный доступ к конфиденциальной информации и известного как "уборка мусора"?

1 это метод получения информации, хранящейся на жестком диске ПК
2 это метод получения информации, переданной пользователем ПК по модему
3 это метод получения информации, хранящейся на сервере
4 это метод получения информации, оставленной пользователем в памяти ПК после окончания работы

13. Как реализуется мандатный контроль?

1 он реализуется подсистемой защиты на аппаратном уровне
2 он реализуется подсистемой защиты на уровне операционной системы
3 он реализуется подсистемой защиты на программном уровне
4 он реализуется подсистемой защиты на самом низком аппаратно-программном уровне

14. Какой признак присущ активной атаке, при использовании самосинхронизирующихся шифров?

1 изменение знака шифротекста при активной атаке не вызывает ошибок при расшифровании других знаков шифротекста
2 искажение значений ключевого потока
3 изменение знака шифротекста при активной атаке не вызывает ошибок при расшифровании других знаков шифротекста
4 любое изменение знаков шифротекста активным противником приведет к тому, что несколько знаков шифротекста расшифруются неправильно и это с большей (по сравнению с синхронными шифрами) вероятностью будет замечено со стороны получателя, расшифровывающего сообщение

15. Что понимается под термином «иерархия доверия»?

1 система проверки цифровых сертификатов
2 система проверки цифровых подписей
3 система аннулирования сертификатов
4 доверенный центр

16. В чем заключается контроль исходного состояния программного обеспечения?

1 он заключается в регулярной проверке правильности результатов, получаемых при работе программного обеспечения.
2 он заключается в проверке избыточности файлов программного обеспечения.
3 он заключается в проверке полноты программного обеспечения.
4 он заключается в фиксации исходного состояния программного обеспечения и сравнении полученных результатов с приведенными в документации.

17. Как выполняется проверка на отсутствие недекларируемых возможностей программного обеспечения?

1 с помощью анализа программного обеспечения на наличие вирусов
2 с помощью анализа на возможность взлома защищенного программного обеспечения
3 с помощью анализа возможностей удаленного доступа к защищенному программному обеспечению
4 с помощью анализа исходных текстов программного обеспечения на наличие явных и критичных программных конструкций, использование которых может привести к нарушению целостности защиты, либо спровоцировать нештатные действия

18. Какие лица рассматриваются в качестве возможных нарушителей средств защиты информации автоматизированных систем?

1 поставщики программного обеспечения автоматизированных систем.
2 разработчики программного обеспечения автоматизированных систем.
3 хакеры.
4 лица, имеющие доступ к работе со штатными средствами автоматизированных систем.

19. Что представляет собой комплексная система защиты информации предприятия, составляющую коммерческую тайну?
1 совокупность аппаратных средств для защиты информации
2 совокупность программных средств для защиты информации
3 действующие в единой совокупности законодательные, организационные, технические и другие способы и средства, обеспечивающие защиту информации, составляющей коммерческую тайну предприятия, по всем выявленным возможным каналам утечки
20. Что использует система защиты информации Secret Disk для хранения паролей?
1 оперативную память компьютера
2 жесткий диск компьютера
3 электронные ключи
21. Вредоносная программа, которая подменяет собой загрузку некоторых программ при загрузке системы, называется...
1 загрузочный вирус
2 макровирус
3 троян
4 файловый вирус
22. Какие алгоритмы используют один и тот же ключ для шифрования и дешифровки?
1 асимметричный
2 симметричный
3 правильного ответа нет
4 и ассиметричный и симметричный
23. Наука, занимающаяся защитой информации, путем преобразования этой информации это:
1 криптография
2 криптология
3 криптоанализ
24. Можно ли отнести слабую аутентификацию к проблемам безопасности?
1 нет
2 да
3 в редких случаях
25. Аутентификация бывает:
1 статическая
2 устойчивая
3 постоянная
4 все варианты правильные
5 правильного варианта нет
26. Условие, при котором в распоряжении аналитика находиться возможность получить результат зашифровки для произвольно выбранного им зашифрованного сообщения размера n используется в анализе:
1 на основе произвольно выбранного шифротекста
2 на основе произвольно выбранного открытого текста
3 на основе только шифротекста

Задание № 2. Выберите несколько вариантов ответа:
27. К вредоносным программам относятся:
1 потенциально опасные программы
2 вирусы, черви, трояны
3 шпионские и рекламные программы
4 вирусы, программы-шутки, антивирусное программное обеспечение
5 межсетевой экран, брандмауэр
28. Отметьте составные части современного антивируса

1 модем
2 принтер
3 сканер
4 межсетевой экран
5 монитор

29. Компьютерные вирусы – это:

1) Вредоносные программы, наносящие вред данным.
2) Программы, уничтожающие данные на жестком диске
3) Программы, которые могут размножаться и скрыто внедрять свои копии в файлы, загрузочные сектора дисков, документы.
4) Программы, заражающие загрузочный сектор дисков и препятствующие загрузке компьютера
5) Это скрипты, помещенные на зараженных интернет-страничках

30. К биометрической системе защиты относятся:

1 защита паролем
2 физическая защита данных
3 антивирусная защита
4 идентификация по радужной оболочке глаз
5 идентификация по отпечаткам пальцев

Задание № 3. Укажите соответствие для всех 6 вариантов ответа

31. Сопоставьте названия программ и изображений.

1)  а) Antivir
2)  б) DrWeb
3)  в) Nod 32
4)  г) Antivirus Kaspersky
5)  д) Avast
6)  е) Antivirus Panda

Задание № 4. Укажите истинность или ложность вариантов ответа, поставив «да» или «нет»

32. Выразите свое согласие или несогласие.

___ На Web-страницах могут находиться сетевые черви.
___ Чтобы защитить компьютер недостаточно только установить антивирусную программу.
___ Файловые вирусы заражают файлы с расширениями *.doc, *.ppt, *.xls.
___ Если компьютер не подключен к сети Интернет, в него не проникнут вирусы.

___ Почтовый червь активируется в тот момент, когда к вам поступает электронная почта.

Задание № 5. Запишите ответ

33. Программы, которые создаются авторами, которые не ставят перед собой цель нанести какой-либо ущерб ресурсам компьютерной сети.

Ответ: _____

34. Процесс, обеспечивающий уменьшение объема данных, выполняется за счет устранения избыточности информации.

Ответ: _____

Задание № 6. Укажите порядок следования всех 3 вариантов ответа

35. Укажите порядок действий при наличии признаков заражения компьютера.

__ Сохранить результаты работы на внешнем носителе.
__ Отключиться от глобальной или локальной сети.
__ Запустить антивирусную программу.

Ключ к тестам

№ вопроса	№ варианта			
	Вариант 1	Вариант 2	Вариант 3	Вариант 4
1.	3	4	3	2
2.	4	4	3	3
3.	3	4	2	4
4.	3	3	2	4
5.	1	3	4	4
6.	2	4	3	3
7.	4	3	2	4
8.	3	4	2	1
9.	1	3	4	2
10.	1	3	2	1
11.	2	4	1	4
12.	3	1	3	4
13.	3	1	4	4
14.	4	2	2	4
15.	2	2	1	1
16.	1	2	3	4
17.	1	2	1	4
18.	1	4	2	4
19.	1	3	1	3
20.	1	2	2	2
21.	1	3	4	1
22.	3	2	1	2
23.	2	3	3	2
24.	3	3	1	2
25.	1	3	1	4
26.	2	3	2	1
27.	345	45	3	123
28.	123	3	123	345
29.	45	345	45	3
30.	3	123	345	45
31.	3а, 4б, 1в, 6г, 2д, 5е	6а, 2б, 3в, 1г, 5д, 4е	4а, 5б, 3в, 2г, 6д, 1е	6а, 1б, 4в, 5г, 3д, 2е
32.	нет, нет, нет, да, да	нет, нет, да, да, нет	да, нет, нет, нет, да	да, да, нет, нет, нет
33.	Троян	Mutant	«Стелс»-вирусы	Безвредные вирусы
34.	Архивация файла	Сжатие (архивация)	Архивация файла	Сжатие (архивация)

35.	231	123	312	231

Перечень вопросов для устного ответа

1. В чем заключается проблема информационной безопасности?
2. Дайте определение понятию "информационная безопасность".
3. Какие определения информационной безопасности приводятся в "Концепции информационной безопасности сетей связи общего пользования Российской Федерации"?
4. Что понимается под "компьютерной безопасностью"?
5. Перечислите составляющие информационной безопасности.
6. Приведите определение доступности информации.
7. Приведите определение целостности информации.
8. Приведите определение конфиденциальности информации.
9. Каким образом взаимосвязаны между собой составляющие информационной безопасности? Приведите собственные примеры.
10. Перечислите задачи информационной безопасности общества.
11. Перечислите уровни формирования режима информационной безопасности.
12. Дайте краткую характеристику законодательно-правового уровня.
13. Какие подуровни включает программно-технический уровень?
14. Что включает административный уровень?
15. В чем особенность морально-этического подуровня?
16. Перечислите основополагающие документы по информационной безопасности.
17. Понятие государственной тайны.
18. Что понимается под средствами защиты государственной тайны?
19. Основные задачи информационной безопасности в соответствии с Концепцией национальной безопасности РФ.
20. Какие категории государственных информационных ресурсов определены в Законе "Об информации, информатизации и защите информации"?
21. Какая ответственность в Уголовном кодексе РФ предусмотрена за создание, использование и распространение вредоносных программ для ЭВМ?
22. Какие виды требований включает стандарт ISO/IEC 15408?
23. Чем отличаются функциональные требования от требований доверия?
24. В чем заключается иерархический принцип "класс – семейство – компонент – элемент"?
25. Какова цель требований по отказоустойчивости информационных систем?
26. Сколько классов функциональных требований?
27. Сколько классов защищенности СВТ от НСД к информации устанавливает РД "СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации"?
28. Дайте характеристику уровням защиты СВТ от НСД к информации по РД "СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации"?
29. Классы защищенности АС от НСД по РД "АС. Защита от НСД к информации. Классификация АС и требования по защите информации".
30. Какие классы защищенных АС от НСД должны обеспечивать идентификацию, проверку подлинности и контроль доступа субъектов в систему?
31. Показатели защищенности межсетевых экранов.
32. Классы защищенности межсетевых экранов.
33. Цели и задачи административного уровня обеспечения информационной безопасности.
34. Содержание административного уровня.
35. Дайте определение политики безопасности.
36. Направления разработки политики безопасности.
37. Перечислите составные элементы автоматизированных систем.
38. Субъекты информационных отношений и их роли при обеспечении информационной безопасности.
39. Перечислите классы угроз информационной безопасности.

40. Назовите причины и источники случайных воздействий на информационные системы.
41. Дайте характеристику преднамеренным угрозам.
42. Перечислите каналы несанкционированного доступа.
43. В чем особенность "упреждающей" защиты в информационных системах.
44. Характерные черты компьютерных вирусов.
45. Дайте определение программного вируса.
46. Какие трудности возникают при определении компьютерного вируса?
47. Когда появился первый вирус, который самостоятельно дописывал себя в файлы?
48. В чем особенность компьютерного вируса "Чернобыль"?
49. Какой вид вирусов наиболее распространяемый в распределенных вычислительных сетях? Почему?
50. Перечислите классификационные признаки компьютерных вирусов.
51. Охарактеризуйте файловый и загрузочный вирусы.
52. В чем особенности резидентных вирусов?
53. Сформулируйте признаки стелс-вирусов.
54. Перечислите деструктивные возможности компьютерных вирусов.
55. Поясните самошифрование и полиморфичность как свойства компьютерных вирусов.
56. Перечислите виды "вирусоподобных" программ.
57. Поясните механизм функционирования "троянской программы" (логической бомбы).
58. В чем заключаются деструктивные свойства логических бомб?
59. Как используются утилиты скрытого администрирования и их деструктивные возможности?
60. Охарактеризуйте "intended"-вирусы и причины их появления.
61. Для чего используются конструкторы вирусов?
62. Для создания каких вирусов используются полиморфик-генераторы?
63. Поясните понятия "сканирование налету" и "сканирование по запросу".
64. Перечислите виды антивирусных программ.
65. Охарактеризуйте антивирусные сканеры.
66. Принципы функционирования блокировщиков и иммунизаторов.
67. Особенности CRC-сканеров.
68. В чем состоят особенности эвристических сканеров?
69. Какие факторы определяют качество антивирусной программы?
70. Перечислите наиболее распространенные пути заражения компьютеров вирусами.
71. Какие особенности заражения вирусами при использовании электронной почты?
72. Особенности заражения компьютеров локальных сетей.
73. Перечислите основные правила защиты от компьютерных вирусов, получаемых не из вычислительных сетей.
74. Как ограничить заражение макровирусом при работе с офисными приложениями?
75. Как обнаружить загрузочный вирус?
76. Как обнаружить резидентный вирус?
77. Характерные черты макровируса.
78. Как проверить систему на наличие макровируса?
79. Является ли наличие скрытых листов в Excel признаком заражения макровирусом?
80. Перечислите основные этапы алгоритма обнаружения вируса.
81. Особенности обеспечения информационной безопасности компьютерных сетей.
82. Дайте определение понятия "удаленная угроза".
83. Основные цели информационной безопасности компьютерных сетях.
84. В чем заключается специфика методов и средств защиты компьютерных сетей?
85. Поясните понятие "глобальная сетевая атака", приведите примеры.
86. Что понимается под протоколом передачи данных?
87. Охарактеризуйте сети с коммутацией сообщений и коммутацией пакетов.
88. Чем отличается соединение по виртуальному каналу от передачи датаграмм?
89. Какие протоколы образуют модель TCP/IP?

90. Какие уровни входят в сетевую модель TCP/IP?
91. Дайте характеристику всех уровней модели TCP/IP и укажите соответствующие этим уровням протоколы.
92. Соотнесите по уровням модели TCP/IP понятия "пакет" и "кадр". Чем они отличаются?
93. Какой протокол обеспечивает преобразование логических сетевых адресов в аппаратные?
94. Проведите сравнительную характеристику моделей передачи данных TCP/IP и OSI/ISO.
95. Перечислите уровни модели OSI/ISO.
96. Назначение прикладного и представительного уровней модели OSI/ISO.
97. Какие функции выполняет транспортный уровень?
98. Назначение сетевого уровня и его характеристика.
99. Какие физические устройства реализуют функции канального уровня?
100. В чем особенности физического уровня модели OSI/ISO?
101. На каких уровнях модели OSI/ISO должна обеспечиваться аутентификация?
102. На каком уровне модели OSI/ISO реализуется сервис безопасности "неотказуемость" (согласно "Общим критериям")?
103. Как рассматривается сеть в концепции протокола IP?
104. Что такое IP-адрес?
105. Преобразуйте IP-адрес "11110011 10100101 00001110 11000001" в десятичную форму.
106. Сколько классов сетей определяет IP протокол?
107. Из каких частей состоит IP-адрес?
108. К какому классу относится следующий адрес: 199.226.33.168?
109. Какой из этих адресов не может существовать: 109.256.33.18 или 111.223.44.1?
110. Поясните понятие домена.
111. В чем заключается иерархический принцип системы доменных имен?
112. Для чего предназначен DNS-сервер?
113. Приведите примеры доменов верхнего уровня по географическому признаку
114. Перечислите классы удаленных угроз.
115. Как классифицируются удаленные угрозы "по характеру воздействия"?
116. Охарактеризуйте удаленные угрозы "по цели воздействия".
117. Как классифицируются удаленные угрозы "по расположению субъекта и объекта угрозы"?
118. Дайте определение маршрутизатора.
119. Что такое подсеть и сегмент сети? Чем они отличаются?
120. Может ли пассивная угроза привести к нарушению целостности информации?
121. Дайте определение типовой удаленной атаки.
122. Механизм реализации удаленной атаки "анализ сетевого трафика".
123. Что является целью злоумышленников при "анализе сетевого трафика"?
124. Назовите причины успеха удаленной атаки "ложный объект".
125. Охарактеризуйте удаленную атаку "подмена доверенного объекта" по классам угроз.
126. Поясните возможные механизмы реализации удаленной атаки "отказ в обслуживании".
127. Какие составляющие "информационной безопасности" могут быть нарушены при реализации каждой из типовых удаленных атак?
128. Перечислите основные причины успешной реализации удаленных угроз информационной безопасности в вычислительных сетях.
129. Почему виртуальное соединение не обеспечивает требуемого уровня защиты вычислительных сетей?
130. Какая из причин приводит к успеху удаленной угрозы "анализ сетевого трафика"?
131. Что является следствием недостаточной аутентификации субъектов и объектов вычислительных сетей?
132. К чему приводит недостаточность информации об объектах вычислительной сети? Приведите пример.
133. Может ли быть нарушена целостность информации при отсутствии в распределенных вычислительных сетях возможности контроля за маршрутом сообщений? Почему?

134. В чем заключаются преимущества сети с выделенными каналами?
135. Какие алгоритмы удаленного поиска Вам известны?
136. Какой из алгоритмов поиска более безопасный?
137. Как повысить защищенность вычислительных сетей при установлении виртуального соединения?
138. Как можно защитить сеть от реализации атаки "отказ в обслуживании"?
139. Как можно контролировать маршрут сообщения в сети?
140. Что понимается под идентификацией пользователя?
141. Что понимается под аутентификацией пользователей?
142. Применим ли механизм идентификации к процессам? Почему?
143. Перечислите возможные идентификаторы при реализации механизма идентификации.
144. Перечислите возможные идентификаторы при реализации механизма аутентификации.
145. Какой из механизмов (аутентификация или идентификация) более надежный? Почему?
146. В чем особенности динамической аутентификации?
147. Опишите механизм аутентификации пользователя.
148. Что такое "электронный ключ"?
149. Перечислите виды аутентификации по уровню информационной безопасности.
150. Какой из видов аутентификации (устойчивая аутентификация или постоянная аутентификация) более надежный?
151. Что входит в состав криптосистемы?
152. Какие составляющие информационной безопасности могут обеспечить криптосистемы?
153. Назовите классификационные признаки методов шифрования данных.
154. Поясните механизм шифрования "налету".
155. Как реализуется симметричный метод шифрования?
156. Как реализуется асимметричный метод шифрования?
157. Что понимается под ключом криптосистемы?
158. Какие методы шифрования используются в вычислительных сетях?
159. Что такое электронная цифровая подпись?
160. Какой метод шифрования используется в электронной цифровой подписи?
161. Чем определяется надежность криптосистемы?
162. Перечислите известные методы разграничения доступа.
163. В чем заключается разграничение доступа по спискам?
164. Как используется матрица разграничения доступа?
165. Опишите механизм разграничения доступа по уровням секретности и категориям.
166. Какие методы управления доступа предусмотрены в руководящих документах Гостехкомиссии?
167. Поясните механизм дискретного управления доступом?
168. Сравните дискретное и мандатное управление доступом.
169. На чем основан механизм регистрации?
170. Какие события, связанные с безопасностью, подлежат регистрации?
171. Чем отличаются механизмы регистрации и аудита?
172. Дайте определение аудита событий информационной системы.
173. Что относится к средствам регистрации и аудита?
174. Что такое регистрационный журнал? Его форма.
175. Что понимается под подозрительной активностью?
176. Какие этапы предусматривают механизмы регистрации и аудита?
177. Охарактеризуйте известные методы аудита безопасности информационных систем.
178. В чем заключается механизм межсетевого экранирования?
179. Дайте определение межсетевого экрана.
180. Принцип функционирования межсетевых экранов с фильтрацией пакетов.
181. На уровне каких протоколов работает шлюз сеансового уровня?
182. В чем особенность межсетевых экранов экспертного уровня?

183. Какие сервисы безопасности включает технология виртуальных частных сетей?
184. Назовите функции VPN-агента.
185. Каким образом технология VPN обеспечивает конфиденциальность данных?
186. Каким образом технология VPN обеспечивает целостность данных?
187. Почему при использовании технологии VPN IP-адреса внутренней сети недоступны внешней сети?
188. Что такое "туннель" и технология его создания?
189. Чем определяется политика безопасности виртуальной частной сети?

Перечень практических занятий и лабораторных работ

Практическое занятие №1. Анализ бизнес-требований к информационной безопасности
Практическое занятие №2. Анализ бизнес-требований к информационной безопасности (продолжение)
Практическое занятие №3. Разработка концептуального плана защиты.
Практическое занятие №4. Разработка концептуального плана защиты. (продолжение)
Практическое занятие №5. Анализ технических ограничений плана защиты
Практическое занятие №6. Анализ технических ограничений плана защиты (продолжение)
Практическое занятие №7. Применение сертификатов для аутентификации и авторизации
Практическое занятие №8. Применение сертификатов для аутентификации и авторизации (продолжение)
Практическое занятие №9. Проектирование иерархии ЦС.
Практическое занятие №10. Проектирование иерархии ЦС. (продолжение)
Практическое занятие №11. Проектирование административных ролей ЦС
Практическое занятие №12. Проектирование административных ролей ЦС (продолжение)
Практическое занятие №13. Проектирование политики подачи заявок на сертификаты.
Практическое занятие №14. Проектирование политики подачи заявок на сертификаты. (продолжение)
Практическое занятие №15. Проектирование размещения CRL и интервала публикации.
Практическое занятие №16. Проектирование размещения CRL и интервала публикации. (продолжение)
Практическое занятие №17. Проектирование защиты границ сети.
Практическое занятие №18. Проектирование защиты границ сети. (продолжение)
Практическое занятие №19. Зашита DNS. Проектирование политики IPSec.
Практическое занятие №20. Зашита DNS. Проектирование политики IPSec. (продолжение)
Практическое занятие №21. Сервисы безопасности в вычислительных сетях
Практическое занятие №22. Сервисы безопасности в вычислительных сетях (продолжение)
Практическое занятие №23. Администрирование средств безопасности
Практическое занятие №24. Администрирование средств безопасности (продолжение)
Практическое занятие №25. Разработка политики информационной безопасности
Практическое занятие №26. Разработка политики информационной безопасности (продолжение)
Практическое занятие №27. Каналы несанкционированного доступа к информации
Практическое занятие №28. Каналы несанкционированного доступа к информации (продолжение)
Практическое занятие №29. Борьба с компьютерными вирусами
Практическое занятие №30. Борьба с компьютерными вирусами (продолжение)
Практическое занятие №31. Обнаружение загрузочного вируса
Практическое занятие №32. Обнаружение резидентного вируса
Практическое занятие №33. Обнаружение макровируса
Практическое занятие №34. Изучение протоколов TCP и UDP
Практическое занятие №35. Сравнение сетевых моделей передачи данных TCP/IP и OSI/ISO
Практическое занятие №36. Сравнение сетевых моделей передачи данных TCP/IP и OSI/ISO (продолжение)
Практическое занятие №37. Защита распределенных вычислительных сетей
Практическое занятие №38. Защита распределенных вычислительных сетей (продолжение)
Практическое занятие №39. Построение защищенной вычислительной сети
Практическое занятие №40. Построение защищенной вычислительной сети (продолжение)

Итоговое тестирование

1. Под СВТ понимается:
а) совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем
б) электронные компоненты, из которых строятся вычислительные системы
в) совокупность программных и технических элементов систем передачи информации, используемая для построения компьютерных систем
2. Под АС понимается:
а) система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций
б) локальная ПЭВМ или компьютерная сеть с установленным системным программным обеспечением и средствами коммуникации
в) автоматизированная система управления обработкой информации с целью выполнения производственных функций организации
3. Под несанкционированным доступом в компьютерной системе понимается:
а) доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС
б) доступ к информации с преодолением парольной защиты, фальсификации аутентификационной информации с использованием штатных средств, предоставляемых СВТ или АС
в) реализация угроз безопасности информации с целью ознакомления и/или уничтожения информации с использованием штатных или специальных СВТ
4. К основным функциям СРД относятся:
а) регистрация действий субъекта и активизированного им приложения
б) контроль целостности программной и аппаратной части СРД
в) реакция на попытки НСД
г) управление потоками информации в целях предотвращения записи её н носители несоответствующего уровня конфиденциальности.
5. К основным функциям СРД не относятся:
а) реализация правил разграничения доступа субъектов и их процессов к информации и устройствам создания ее твердых копий б) изоляция процесса, выполняемого в интересах субъекта доступа, от других субъектов
в) идентификация и аутентификация субъектов, и поддержание привязки субъекта к процессу, выполняемому для него
6. К функциям обеспечивающих средств для СРД не относятся:
а) учет выходных печатных и графических форм и твердых копий в КС
б) очистка оперативной памяти после завершения работы пользователя с защищаемыми данными
в) реализация правил обмена информацией между субъектами в компьютерных сетях.
7. Идентификация это:
а) однозначное определение уникального имени, под которым пользователь зарегистрирован в КС
б) генерация уникального имени, под которым пользователь будет зарегистрирован в КС
в) проверка уникальности имени зарегистрированного в КС пользователя при запросе доступа к ресурсам КС
8. Аутентификация это:
а) подтверждение подлинности имени, предъявленного пользователем
б) подтверждение заявленных пользователем прав доступа к ресурсам КС
в) проверка наличия введенного имени пользователя в регистрационной базе КС.
9. Авторизация это:
а) процесс наделения пользователя индивидуальным набором привилегий в системе и определение его прав доступа к объектам КС
б) процесс определения набора информационных ресурсов, доступ к которым разрешен пользователю
в) проверка соответствия введенного пользователем пароля его идентификатору.
10. Аудит безопасности КС это:
а) учет возникающих при работе системы событий, связанных с безопасностью информации в ней, и регистрация этих событий в системном журнале
б) учет попыток НСД и регистрация их в системном журнале
в) проверка соответствия защитных функций установленных в АС СЗИ требованиям, предъявляемым к СЗИ в АС

г) учет неудачных попыток ввода пароля и регистрация этих попыток в системном журнале.

11. Укажите наиболее правильную формулировку требований к «идеальной» системе защиты информации (СЗИ).

а) СЗИ должна быть прозрачна для легальных пользователей и создавать непреодолимые трудности для реализации НСД.

б) СЗИ должна обеспечивать уровень защищенности информации, соответствующий требованиям для данного класса АС.

в) СЗИ должна обеспечивать защищенность информации на программном и аппаратном уровне, включать в себя подсистемы, использующие разные технологии ЗИ.

12. Выберите наиболее полное правило, которым следует руководствоваться при выборе паролей:

а) пароли должны трудно подбираться и легко запоминаться

б) в паролях следует использовать буквы и цифры, причем длина пароля должна быть не менее 4 символов

в) в качестве паролей не следует использовать простые слова, имена собственные и т.п.

13. Выберите наиболее правильное описание начального этапа модели «рукопожатия».

а) система генерирует случайное значение, вычисляет и сообщает пользователю.

б) пользователь генерирует случайное значение, вычисляет и вводит в ответ на запрос системы.

в) система генерирует случайное значение, вычисляет и сообщает пользователю.

г) система генерирует случайное значение, вычисляет и сообщает и пользователю.

14. К пассивным устройствам аутентификации не относятся:

а) пластиковые карты с магнитной полоской

б) элементы Touch Memory

в) USB-ключи

15.Уязвимость информационной системы это:

а) любая характеристика, использование которой нарушителем может привести к реализации угрозы

б) ошибки в программном обеспечении, возникновение которых может привести к реализации угрозы

в) количественная и качественная недостаточность средств ЗИ, которая может привести к реализации угрозы.

16.Угрозой информационной системе называется:

а) потенциально возможное событие, действие, процесс или явление, которое может вызвать нанесение ущерба ресурсам системы

б) совокупность программно-аппаратных средств осуществления НСД при наличии методов их использования для нанесения ущерба ресурсам системы

в) возможность использования информации, штатных и нештатных технических средств АС для нанесения ущерба ресурсам системы.

17. Под информационной безопасностью понимается:

а) защищенность информации и поддерживающей инфраструктуры
от случайных и преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры

б) комплекс программно-аппаратных средств, направленных на защиту от случайных и преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры

в) совокупность мер организационно-технического характера, направленных на защиту от случайных и преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры

18. Сущность комплексного подхода к ЗИ заключается в:

а) сочетании различных мер обеспечения безопасности на законодательном, административном, процедурном и программно-техническом уровнях

б) сочетании различных мер обеспечения безопасности на законодательном и программно-техническом уровнях

в) сочетании различных программно-аппаратных средств защиты АС от НСД.

19.Аспекты обеспечения ИБ:

а) формальный и практический

б) общий и частный

в) программный и аппаратный.

20. Укажите, что не является контекстом ЗИ и соответствующих бизнес- процессов:

а) конфиденциальность
б) целостность
в) доступность
г) достоверность.
21. Основная цель сетевой ПБ:
а) контроль сетевого трафика и его использования
б) противодействие попыткам НСД с использованием сетевой инфраструктуры
в) установка и правильная настройка программно-аппаратных СЗИ.
22. Под доверенными понимаются сети, ...
а) ...над которыми специалисты организации имеют полный административный контроль
б) ...на компьютерах которых установлены средства удаленного администрирования
в) ...оснащенные программно-аппаратными СЗИ и проходящие регулярные проверки на предмет вирусной активности.
23. Ресурсы (в контексте задачи управления рисками) это:
а) то, что организация ценит и хочет защитить
б) финансовые и информационные активы организации
в) файлы и бумажные документы.
24. Политика информационной безопасности определяет:
а) способы развертывания систем безопасности и поведение пользователей при использовании КС
б) способы настройки межсетевых экранов и антивирусных средств
в) порядок получения доступа пользователей к ресурсам КС организации.
25.Основная цель сетевой ПБ:
а) описание топологии ЛВС и определение мест установки МЭ
б) контроль сетевого трафика и его использования
в) формирование требований к настройке МЭ и антивирусных систем
г) разрешить то, что явно не запрещено д) запретить то, что явно не разрешено.
26. Выберите пункт из перечисленного ниже, который не относится к службам безопасности:
а) аутентификация
б) целостность
в) информированность.
27. Под доверенными понимаются сети, ...
а) ...на компьютерах которых установлены средства удаленного администрирования
б) ...над которыми специалисты организации имеют полный административный контроль
в) оснащенные программно-аппаратными СЗИ и проходящие регулярные проверки на предмет вирусной активности.
29. Ресурсы (в контексте задачи управления рисками) это:
а) информация и поддерживающие средства для ведения бизнеса
б) базы данных корпоративных информационных систем (бухгалтерских, аналитических и т.п.)
в) файлы и бумажные документы
г) описания устройств и технологических процессов, являющиеся «ноу-хау» организации.
30. Угроза – это ...
а) ...потенциальная причина нежелательного события, которое может нанести ущерб организации и ее объектам
б) ...сетевая атака, влекущая нарушение работоспособности КС организации
в) ...потенциальная возможность НСД к конфиденциальной информации организации
г) ...совокупность вредоносного ПО, распространяющаяся по компьютерным сетям.
31. По характеру воздействия угрозы могут быть...
а) ...против доступности, целостности, конфиденциальности
б) ...внутренними, внешними
в) ...преднамеренными, случайными.
32. Риск безопасности это ...
а) ...возможность реализации сетевой атаки на ресурсы КС
б) вероятность преодоления системы защиты за произвольный период времени
в) ...возможность данной угрозы реализовать уязвимости для нанесения ущерба организации
г) ...вероятность начала вредоносного воздействия на ресурсы КС злоумышленником.
33. Классы межсетевых экранов по функционированию на уровнях модели OSI:
а) пакетный фильтр, программно-аппаратный, программный.
б) пакетный фильтр, экранирующий транспорт, прикладной шлюз
в) контроллер состояния протокола, экранирующий транспорт, прикладной шлюз.
34. Список доступа маршрутизатора – это...
а) ...набор строк, описывающих доверенные адреса хостов

б) ...набор строк, определяющих некие образцы, на соответствие которым проверяются пакеты IP

в) ...набор строк, описывающих конфигурацию интерфейсов маршрутизатора.

35. Выберите наиболее правильное утверждение.

а) стандартный ACL может проверять адреса отправителей, получателей и ряд параметров

б) нумерация стандартных ACL выполняется в диапазоне от 100 до 199

в) стандартный ACL может выполнять контроль состояния соединения

г) стандартный ACL может проверять только адреса отправителей.

36. Выберите наиболее правильное утверждение.

а) ключевое слово host означает любой IP-адрес хоста

б) обратная маска 255.255.255.255 определяет единственный IP-адрес

в) обратная маска 0.0.0.0 определяет единственный IP-адрес

г) ключевое слово any соответствует WildCard-маске 0.0.0.0.

37.В чем заключается смысл следующего списка доступа?

а) access-list 45 permit 192.168.20.0 0.0.0.255

б) access-list 45 deny host 192.168.20.13

в) трафику сети 192.168.20.0 разрешено проходить через маршрутизатор, за исключением хоста192.168.20.13

г) трафику сети 192.168.20.0 разрешено проходить через маршрутизатор

д) трафику сети 192.168.20.0 запрещено проходить через маршрутизатор, за исключением хоста 192.168.20.13

е) трафику хоста 192.168.20.13 запрещено проходить через маршрутизатор, а остальным хостам сети 192.168.20.0 – разрешено.

38. Выберите наиболее правильное утверждение.

а) расширенный ACL может проверять адреса источников, получателей, тип протокола и порты.

б) расширенный ACL обеспечивает более быструю проверку пакетов, чем стандартный ACL.

в) допускается размещать более 1 расширенного ACL на интерфейс, на протокол, на направление.

г) расширенный ACL не может проверить состояние соединения TCP.

39.В чем заключается смысл следующего выражения?

а) запрещение доступа к хосту с IP-адресом 130.120.110.100

б) разрешение доступа к хосту с IP-адресом 130.120.110.100

в) запрещение доступа к подсети 130.120.110.0 0.0.0.255.

г) access-list 101 deny ip 0.0.0.0 255.255.255.255 130.120.110.100 0.0.0.0

40.Межсетевой экран (Брандмауэр, firewall) – это...

а) Комплекс аппаратных средств

б) Комплекс программных средств

в) Комплекс аппаратных или программных средств

г) Комплекс аппаратных и программных средств

Вопросы для промежуточной аттестации

1. Цели, задачи и содержание курса. Основные понятия.
2. Предмет и задачи программно-аппаратной защиты информации.
3. Автоматизированная система.
4. Структура и компоненты АС. Сети ЭВМ.
5. Способы защиты конфиденциальности.
6. Проблема защиты программного обеспечения информационных систем.
7. Объекты защиты.
8. Жизненный цикл программного обеспечения информационных систем.
9. Технологическая и эксплуатационная безопасность программного обеспечения.
10. Основные принципы обеспечения безопасности программного обеспечения.
11. Защита программного обеспечения как система научных дисциплин.
12. Уязвимости программного обеспечения.
13. Угрозы безопасности программного обеспечения.
14. Вредоносные программы.
15. Несанкционированные исследование
16. Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.
17. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты).
18. Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.
19. Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно- аппаратными средствами.
20. Работа с содержанием нормативных правовых актов.
21. Автоматизация процесса обработки информации. Понятие автоматизированной системы.
22. Особенности автоматизированных систем в защищенном исполнении.
23. Основные виды АС в защищенном исполнении. Методы создания безопасных систем.
24. Методология проектирования гарантированно защищенных КС. Дискреционные модели Мандатные модели.
25. Учет, обработка, хранение и передача информации в АИС
26. Ограничение доступа на вход в систему.
27. Идентификация и аутентификация пользователей
28. Разграничение доступа. Регистрация событий (аудит).
29. Контроль целостности данных. Уничтожение остаточной информации.
30. Управление политикой безопасности. Шаблоны безопасности
31. Криптографическая защита. Обзор программ шифрования данных.
32. Управление политикой безопасности. Шаблоны безопасности
33. Организация доступа к файлам. Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД.
34. Понятие несанкционированного доступа к информации.
35. Основные подходы к защите информации от НСД.
36. Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам.
37. Доступ к данным со стороны процесса Особенности защиты данных от изменения. Шифрование. Сети, работающие по технологии коммутации пакетов.
38. Стек протоколов TCP/IP. Особенности маршрутизации.
39. Штатные средства защиты информации стека протоколов TCP/IP.

40. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.
41. Виртуальная частная сеть. Функции, назначение, принцип построения.
42. Виртуальная частная сеть. Функции, назначение, принцип построения.
43. Криптографические и некриптографические средства организации VPN.
44. Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр.
45. Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки.
46. Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки.
47. Методы защиты информации при работе в сетях общего доступа. Межсетевые экраны типа firewall.
48. Достоинства, недостатки, реализуемые политики безопасности Основные типы firewall.
49. Симметричные и несимметричные firewall. Уровень 1. Пакетные фильтры Уровень 2.
50. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне. Уровень 3.
51. Proxy-сервера прикладного уровня.
52. Однохостовые и мультихостовые firewall.
53. Основные типы архитектур мультихостовых firewall.
54. Требования к каждому хосту исходя из архитектуры и выполняемых функций.
55. Требования по сертификации межсетевых экранов.
56. Сертификация средств защиты информации по требованиям безопасности информации.
57. Проверка соответствия реальных и декларируемых функциональных возможностей. Проверка отсутствия недекларируемых возможностей.
58. Методы проведения испытаний. Документация, представляемая на испытания.
59. Статический анализ исходных текстов и исполняемых модулей ПО.
60. Контроль полноты и отсутствия избыточности исходных текстов на уровне файлов.
61. Контроль соответствия исходных текстов ПО его объектному (загрузочному) коду.
62. Контроль связей функциональных объектов по управлению и информации.
63. Синтаксический контроль наличия заданных конструкций.
64. Формирование и анализ маршрутов выполнения функциональных объектов.
65. Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации.
66. Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25.
67. Классификация отслеживаемых событий.
68. Особенности построения систем мониторинга.
69. Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования.
70. Классификация сетевых мониторов.
71. Системы управления событиями информационной безопасности (SIEM).
72. Обзор SIEM-систем на мировом и российском рынке.
73. Изучение требований о защите информации, не составляющей государственную тайну.
74. Изучение методических документов ФСТЭК по применению мер защиты.
75. Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов
76. Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol или других аналогов.
77. Изучение типовых решений для построения VPN на примере VipNet или других аналогов.
78. Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов.
79. Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов.
80. Классификация вредоносных программ.

81. Защита от вредоносных программ.
82. Методы тестирования программного обеспечения на его защищенность.
83. Методы тестирования программ.
84. Фаззинг программ.
85. Методы защиты программ от несанкционированного исследования.
86. Классификация средств несанкционированного исследования программ.
87. Способы защиты программ от несанкционированного исследования.
88. Обфускация программ. Способы встраивания защитных механизмов в программное обеспечение.
89. Методы защиты программ от несанкционированного копирования. Криптографические методы защиты от копирования.
90. Метод привязки к идентификатору. Методы, основанные на работе с переходами и стеком.
91. Манипуляции с кодом программы.
92. Методы противодействия динамическим способам снятия защиты программ от копирования.

Практические задания

1. Анализ бизнес-требований к информационной безопасности
2. Разработка концептуального плана защиты.
3. Анализ технических ограничений плана защиты
4. Применение сертификатов для аутентификации и авторизации
5. Проектирование иерархии ЦС.
6. Проектирование административных ролей ЦС
7. Проектирование политики подачи заявок на сертификаты.
8. Проектирование размещения CRL и интервала публикации.
9. Проектирование защиты границ сети.
10. Зашита DNS. Проектирование политики IPSec.

ПАКЕТ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ		
Код и наименование профессиональных и общих компетенции, формируемых в рамках модуля	**Критерии оценки**	**Отметка о выполнении**
ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей	- выявлять и оценивать угрозы безопасности информации в ИТКС; - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; - проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации; - проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	
ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно- телекоммуникационных системах и сетях	- выявлять и оценивать угрозы безопасности информации в ИТКС; - проводить контроль показателей и процесса функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; - проводить восстановление процесса и параметров функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; - проводить техническое обслуживание и ремонт программно-аппаратных (в том числе криптографических) средств защиты информации;	
ПК 2.3. Осуществлять защиту информации от несанкционированного доступа и специальных воздействий в оборудование информационно- телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты информации	- выявлять и оценивать угрозы безопасности информации в ИТКС; - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; - проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	- обоснованность постановки цели, выбора и применения методов и способов решения профессиональных	

	задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач;	
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач;	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие..	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы;	
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных);	
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	

Список литературы

Печатные издания:

1. Сети и телекоммуникации: учебник и практикум для вузов / К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2024. — 464 с. — ISBN 978-5-534-17315-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://ezpro.fa.ru:2058/bcode/536089 (дата обращения: 28.03.2024)
2. Олифер Н.А, Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание. – Спб.: Питер, 2022. – 1008 с.
3. Белов Е.Б. Организационно-правовое обеспечение информационной безопасности: учебное издание / Белов Е.Б., Пржегорлинский В. Н. - Москва : Академия, 2021. - 336 с. (Специальности среднего профессионального образования). - URL: https://academia-moscow.ru - Режим доступа: Электронная библиотека «Academia-moscow». - Текст : электронный
4. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях : учебное пособие / В. Ф. Шаньгин. - 2-е изд. - Москва : ДМК Пресс, 2023. - 594 с. - ISBN 978-5-89818-506-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/2107178 (дата обращения: 28.03.2024).

Электронные издания (электронные ресурсы):

5. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru.
6. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru.
7. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/.
8. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru.
9. http://www.morion.ru/.
10. http://www.nateks.ru/.
11. http://www.iskratel.com/
12. http://www.ps-ufa.ru/.
13. http://3m.com/.
14. http://www.rusgates.ru/index/php - Материалы сайта завода «Ферроприбор».

Дополнительные источники:

15. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
16. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
17. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
18. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
19. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
20. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

21. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

22. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

23. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

24. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.

25. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25 ноября 1994 г.

26. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

27. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

28. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

29. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

30. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России

31. от 30 августа 2002 г. № 282.

32. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

33. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России

34. от 31 августа 2010 г. № 416/489.

35. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

36. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

37. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

38. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

39. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

40. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий

41. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер

42. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

43. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью

44. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

45. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

46. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

47. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

48. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"

49. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

50. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

51. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

52. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

53. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.

54. Номенклатура показателей качества. Ростехрегулирование, 2005.

55. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.

56. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.

57. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.

58. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.

59. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

60. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

61. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

62. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

63. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

64. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

Отечественные журналы:

65. "InformationSecurity/ Информационная безопасность"

66. Системный администратор

67. Компьютер ПРЕСС

68. Системы безопасности. Журнал для руководителей и специалистов в области

69. безопасности

70. Сети и системы связи

71. Защита информации. Инсайд: Информационно-методический журнал

72. Информационная безопасность регионов: Научно-практический журнал

Интернет ресурсы:

73. http://cryptogrof.ru/