МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Дагестанский государственный университет»

Колледж

УТВЕРЖДАЮ
директор Колледжа ДГУ
_____ Д.Ш. Пирбудагова
«30» 04 2022г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по учебной дисциплине

МДК.02.01. ПРОГРАММНЫЕ И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Махачкала - 2022

Составители:

Шахбанова М.И. - преподаватель кафедры естественно-научных и гуманитарных дисциплин Колледжа ФГБОУ ВО «Дагестанский государственный университет»

Шахбанова З.И. - к.э.н., доцент кафедры прикладной информатики в экономике факультета информатики и информационных технологий ФГБОУ ВО «Дагестанский государственный университет»

Фонд оценочных средств дисциплины рассмотрен и рекомендован к утверждению кафедрой специальных дисциплин Колледжа ДГУ.

Протокол №__8__ от «30» 04 2022 г.

Зав.кафедрой специальных дисциплин к.ю.н.,доцент _____/Магомедова К.К./

Утвержден на заседании учебно-методического совета Колледжа ДГУ

Ст. методист _____/Шамсутдинова У.А./
подпись *Фамилия И.О.*

ПАСПОРТ

ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине

МДК.02.01. ПРОГРАММНЫЕ И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

№	Контролируемые разделы, темы, модули	Код контролируемой компетенции	Наименование оценочного средства
1.	**Раздел 1.** Основные принципы программной и программно-аппаратной защиты информации	ОК 1, ОК 2, ОК 3, ОК 5, ОК 6, ОК 9, ОК 10, ПК. 2.1, ПК. 2.4, ПК. 2.5.	Комбинированный метод контроля в форме индивидуального, фронтального опроса и самостоятельной работы тестирование рефераты составление и оформление письменных документов подготовка и защита рефератов экспертная оценка результатов выполнения индивидуальных практических работ по решению ситуационных задач.
2.	**Раздел 2.** Защита информации в локальных сетях	ОК 1, ОК 2, ОК 3, ОК 5, ОК 6, ОК 9, ОК 10, ПК. 2.1, ПК. 2.4, ПК. 2.5.	Комбинированный метод контроля в форме индивидуального, фронтального опроса и самостоятельной работы тестирование рефераты составление и оформление письменных документов подготовка и защита рефератов экспертная оценка результатов выполнения индивидуальных практических работ по решению ситуационных задач.
3.	**Раздел 3.** Мониторинг систем защиты	ОК 1, ОК 2, ОК 3, ОК 5, ОК 6, ОК 9, ОК 10, ПК. 2.1, ПК. 2.4, ПК. 2.5.	Комбинированный метод контроля в форме индивидуального, фронтального опроса и самостоятельной работы тестирование рефераты составление и оформление письменных документов подготовка и защита рефератов экспертная оценка результатов выполнения индивидуальных практических работ по решению ситуационных задач.

Примерный перечень оценочных средств

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1	2	3	4
1.	Деловая и/или ролевая игра	Совместная деятельность группы обучающихся и педагогического работника под управлением педагогического работника с целью решения учебных и профессионально-ориентированных задач путем игрового моделирования реальной проблемной ситуации. Позволяет оценивать умение анализировать и решать типичные профессиональные задачи.	Тема (проблема), концепция, роли и ожидаемый результат по каждой игре
2.	Кейс-задача	Проблемное задание, в котором обучающемуся предлагают осмыслить реальную профессионально-ориентированную ситуацию, необходимую для решения данной проблемы.	Задания для решения кейс-задачи
3.	Коллоквиум	Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования педагогического работника с обучающимися.	Вопросы по темам/разделам дисциплины
4.	Контрольная работа	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу.	Комплект контрольных заданий по вариантам
5.	Круглый стол, дискуссия, полемика, диспут, дебаты	Оценочные средства, позволяющие включить обучающихся в процесс обсуждения спорного вопроса, проблемы и оценить их умение аргументировать собственную точку зрения.	Перечень дискуссионных тем.
6.	Портфолио	Целевая подборка работ студента, раскрывающая его индивидуальные образовательные достижения в одной или	Структура портфолио

		нескольких учебных дисциплинах.	
7.	Рабочая тетрадь	Дидактический комплекс, предназначенный для самостоятельной работы обучающегося и позволяющий оценивать уровень усвоения им учебного материала.	Образец рабочей тетради
8.	Проект	Конечный продукт, получаемый в результате планирования и выполнения комплекса учебных и исследовательских заданий. Позволяет оценить умение обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве и уровень сформированное аналитических, исследовательских навыков, навыков практического и творческого мышления. Может выполняться в индивидуальном порядке или группой обучающихся.	Темы групповых и/или индивидуальных проектов
9.	Разно-уровневые задачи и задания	*Различают задачи и задания:* – репродуктивного уровня, позволяющие оценивать и диагностировать знание фактического материала (базовые понятия, алгоритмы, факты) и умение правильно использовать специальные термины и понятия, узнавание объектов изучения в рамках определенного раздела дисциплины – реконструктивного уровня, позволяющие оценивать и диагностировать умения синтезировать, анализировать, обобщать фактический и теоретический материал с формулированием конкретных выводов, установлением причинно-следственных связей – творческого уровня, позволяющие оценивать и диагностировать умения, интегрировать знания различных областей, аргументировать собственную точку зрения.	Комплект разно-уровневых задач и заданий
10.	Расчетно-графическая работа	Средство проверки умений применять полученные знания по заранее определенной методике для решения задач или заданий по модулю или дисциплине в целом.	Комплект заданий для выполнения расчетно-графической работы

11.	Реферат	Продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее.	Темы рефератов

КРИТЕРИИ ОЦЕНКИ
по дисциплине
МДК.02.01. ПРОГРАММНЫЕ И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Критерии оценки:

Оценка «отлично»: студент владеет знаниями предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, в логической последовательности и исчерпывающе отвечает на все вопросы, подчеркивал при этом самое существенное, умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделять в нем главное: устанавливать причинно-следственные связи. Четко формирует ответы, решает ситуационные задачи повышенной сложности, хорошо знаком с основной литературой, увязывает теоретические аспекты предмета с задачами практического характера.

Оценка «хорошо»: студент владеет знаниями дисциплины почти в полном объеме программы (имеются пробелы знаний только в некоторых, особенно сложных разделах). Самостоятельно и отчасти при наводящих вопросах дает полноценные ответы, не всегда выделяет наиболее существенное, не допускает вместе с тем серьезных ошибок в ответах, умеет решать легкие и средней тяжести ситуационные задачи.

Оценка «удовлетворительно»: студент владеет основным объемом знаний по дисциплине проявляет затруднения в самостоятельных ответах, оперирует неточными формулировками. В процессе ответов допускаются ошибки по существу вопросов. Студент способен решать лишь наиболее легкие задачи, владеет только обязательным минимумом методов исследований.

Оценка «неудовлетворительно»: студент обнаруживает незнание ответа на соответствующее задание, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал, отмечаются такие недостатки в подготовке студента, которые являются серьезным препятствием к успешному овладению последующим материалом.

Вопросы к экзамену:

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. 16 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.

Примерные задачи:

Дано: описание алгоритма хэширования паролей в базах данных аутентификации

Windows NT/2000 (Lan manager):

Для формирования хэша пароля все буквенные символы исходной строки пользовательского пароля приводятся к верхнему регистру, и если пароль содержит меньше 14 символов, то он дополняется нулями. Из каждой 7-байтовой половины преобразованного таким образом пароля пользователя (длина пароля в Windows NT/2000/XP ограничена 14 символами), отдельно формируется ключ для шифрования некоторой фиксированной 8-байтовой последовательности по DES-алгоритму с ключом 64(56)бит. При этом в качестве ключа используется PID (персональный идентификатор) пользователя). Полученные в результате две 8- байтовые половины хешированного пароля Lan Manager еще раз шифруются по DESалгоритму и помещаются в базу данных SAM.

Проанализируйте уровень защищенности баз данных аутентификации операционных систем, связанную с описанным алгоритмом.

1. Дано: имеется сервер, работающий под управлением ОС Windows Server 2003. На сервере запущена СУБД Oracle 9i.

   С помощью каких программных средств можно составить список возможных уязвимостей и определить уровень угроз? Опишите известные Вам виды уязвимостей, присущие предложенной конфигурации сервера и способы защиты от них.

2. Дано: Имеется процедура добавления (регистрации) нового покупателя на PL/SQL следующего содержания:

```
Create procedure NewCustomer(CName varchar2,CPassword varchar2,CInfo varchar2) as
Begin
Insert into CustomersTable (Name,Password,Info) values('||CName||' ,*||CPassword||'
,'||CInfo||');
End;
```

Какой способ SQL Injection необходимо применить, чтобы в поле CInfo занести пароль

пользователя «Иванов» из этой же таблицы. Как обнаружить и предотвратить попытку

SQL Injection

3. Дано: имеется функция проверки аутентификации покупателя по имени пользователя и

паролю на PL/SQL следующего содержания:

Create function GetCustomerInfo(CName varchar2,CPassword varchar2) return varchar2 as

CInfo varchar2(200);

Begin

Select Info into CInfo from CustomersTable where

Name='||CName||' and Password='||CPassword||';

Return CInfo;

End;

17

Какой способ SQL Injection необходимо применить, чтобы злоумышленник зарегистрировался под пользователем «Иванов» из этой же таблицы без знания пароля. Как обнаружить и предотвратить попытку SQL Injection

Дано: Как известно, мера информационной энтропии измеряется по формуле Шэннона:

n

H = -^p(i)log2p(i).. В то же время, по формуле Хартли, на один символ алфавита

источника сообщений (со стандартным объемом в 256 символов) приходится

H=log2256=8bit.

Проанализируйте применимость формул для случая парольной защиты с паролем, запоминаемым пользователем, и для случая парольной защиты с паролем, запоминаемым в аппаратном устройстве хранения паролей. В каких случаях формула Шэннона будет давать такой же результат, что и формула Хартли.

Критерии оценки эссе (рефератов, докладов, сообщений)

Оценка «отлично»: выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована ее актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объем, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.

Оценка «хорошо»: основные требования к реферату и его защите выполнены, но при этом допущены недочеты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объем реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.

Оценка «удовлетворительно»: имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы.

Оценка «неудовлетворительно»: тема освоена лишь частично; допущены грубые ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод. Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы.

Темы для эссе (рефератов, докладов, сообщений):

1. Анализ российского рынка средств обеспечения информационной безопасности беспроводных сетей.
2. Анализ зарубежного рынка средств обеспечения информационной безопасности беспроводных сетей.
3. Анализ методов и средств анализа защищенности беспроводных сетей.
4. Средства защиты акустической информации, современные проблемы и возможные (перспективные) пути их решения.
5. Виброакустические средства современных систем обеспечения информационной безопасности.
6. Средства защиты от ПЭМИН, современное состояние, проблемы и решения.
7. Средства обеспечения информационной безопасности проводных сетей общего доступа, методология и анализ применяемых решений.
8. Средства обеспечения информационной безопасности банков данных.
9. Разработка программы автоматизированного анализа результатов опросного метода оценки показателей обеспечения информационной безопасности деятельности организации, полученных методом сбора информации анкет (опроса).
10. Анализ критических характеристик линий связи с точки зрения обеспечения защиты информации.
11. Использование ЭЦП для обеспечения защиты информации при использовании системы электронного документооборота.

12. Обеспечение защиты конфиденциальной информации в распределённых системах разграничения доступа.
13. Анализ существующих методик оценки экономического ущерба от разглашения (утраты) конфиденциальной информации.
14. Информационная система мониторинга и координации деятельности сотрудников информационно-технического отдела.
15. Инструментальные средства анализа рисков информационной безопасности.
16. Сравнительный и оценочный анализ международных стандартов в области информационной безопасности и управления рисками.
17. Оценочный анализ методов и средств тестирования системы защиты вычислительных сетей (аудита информационной безопасности).
18. Контроль работы и регистрации пользователей и технических средств
19. Идентификация имеющихся технических средств, пользователей и файлов
20. Защита операционных ресурсов ЭВМ и пользовательских программ
21. Обслуживания различных режимов обработки данных
22. Уничтожение данных после ее использования в элементах системы
23. Сигнализирование при нарушениях
24. Анализ аппаратных средств защиты ПК
25. Разработка ПС на основе асимметричного шифрования для защиты ОС.
26. Разработка ПС для защиты ОС с помощью цветовой схемы.
27. Разработка программно-аппаратного комплекса для защиты ОС.
28. Разработка электронного ключа для защиты от несанкционированного доступа к ПК.
29. Разработка ПС для защиты от спама.
30. Разработка ПС для защиты ПК от несанкционированного сканирования портов.
31. Анализ существующих методов защиты ОС.
32. Разработка ПС для защиты от фишинговых атак.
33. Разработка ПС для защиты ПК от несанкционированного сканирования портов.
34. Разработка электронного ключа для доступа к ПК.
35. Разработка межсетевого экрана.
36. Создание системы защиты локальной сети от несанкционированного доступа.
37. Разработка системы управления сайтом с дополнительной аутентификацией пользователя.
38. Разработка ПС для аутентификации пользователя с помощью графического изображения.
39. Разработка аппаратно-программного комплекса защиты ПК.
40. Анализ существующих ПС по защите локальных сетей от внешних атак.

СТРУКТУРА ИТОГОВОГО ТЕСТА:

Тест содержит 20 вопросов случайным образом выбранных их списка. Тест проводиться на персональном компьютере в оболочке для тестирования

MyTest. Результат выдается сразу после тестирования и формируется отчет протестированных студентов на сервере.

Время на подготовку и выполнение:

Выполнение – 20 минут. За правильный ответ выставляется по 1 баллу, затем результаты суммируются, и выставляется оценка. За неправильный ответ 0 баллов.

Критерии оценки промежуточной аттестации:

Оценка «отлично» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «отлично», средний балл по аттестациям не ниже 4,5.

Оценка «хорошо» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «хорошо», средний балл по аттестациям не ниже 3,5.

Оценка «удовлетворительно» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «удовлетворительно», средний балл по аттестациям не ниже 2,5.

Оценка «неудовлетворительно» выставляется, если имеются все конспекты лекции обучающимися выполнено менее 100% практических работ, оценка за итоговое тестирование – «неудовлетворительно», средний балл по аттестациям ниже 2,5.

Цель итогового тестирования:

Тестирование по учебной дисциплине **«Программные и программно-аппаратные средства обеспечения информационной безопасности»** предназначено для проверки теоретических знаний и понятийного аппарата, которые лежат в основе профессионального образования и найдут самое широкое применение в будущей профессиональной деятельности учащихся по специальности 10.02.05.Обеспечение информационной безопасности автоматизированных систем.

Критерии оценки знаний:

Процент правильных ответов, %	Оценка знаний
90-100	5 «отлично»
75-89	4 «хорошо»

60-74	3 «удовлетворительно»
Менее 60	2 «неудовлетворительно»

Список теоретических заданий для подготовки к итоговому тестированию (ТЗ)

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 её 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
    б) организации и её объектам
    в) …сетевая атака, влекущая нарушение работоспособности КС организации

г) …потенциальная возможность НСД к конфиденциальной информации организации
д) …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

Основная литература:

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2022. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497433 .
2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/476997

3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/449548

Дополнительная литература:

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2019. — 312 с. — (Специалист). — ISBN 978-5-9916-9043-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/.
2. Долозов Н. Л., Гультяева Т. А. Программные средства защиты информации: конспект лекций Новосибирск: Новосибирский государственный технический университет, 2015. – 63 с. https://biblioclub.ru/index.php?page=book_red&id=438307&sr=1
3. Ю.Ю. Громов, О.Г. Иванова, К.В. Стародубов, А.А. Кадыков Программно-аппаратные средства защиты информационных систем: учебное пособие Тамбов: Издательство ФГБОУ ВПО «ТГТУ», 2017. – 194 с. https://biblioclub.ru/index.php?page=book_red&id=499013&sr=1
4. Рецензируемый научный журнал «Проблемы информационной безопасности».
5. Научный журнал «Прикладная дискретная математика»
6. Научный журнал «Информатика и ее применение»
7. Журнал о компьютерах и цифровой технике «ComputerBild»
8. Рецензируемый научный журнал «Информатика и система управления»
9. Рецензируемый научный журнал «Проблемы информационной безопасности»
10. Рецензируемый научный журнал «Прикладная информатика»
11. ГОСТ 34.320-96.Информационные технологии. Система стандартов по базам данных. Концепции и терминология для концептуальной схемы и информационной базы. 2001 г.www.standartgost.ru
12. ГОСТ Р ИСО/МЭК ТО 12182-2002. Информационная технология. Классификация программных средств. 2002 г.www.standartgost.ru
13. ГОСТ Р ИСО/МЭК 15288-2005. Информационная технология. Системная инженерия. Процессы жизненного цикла систем. 2006 г.www.standartgost.ru
14. ГОСТ Р ИСО/МЭК 12119-2000. Информационная технология. Пакеты программ. Требования к качеству и тестирование. 2005 г.www.standartgost.ru
15. ГОСТ 34.601-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания. 2009 г.www.standartgost.ru
16. ГОСТ 28195-89. Оценка качества программных средств. Общие положения. 2001 г.www.standartgost.ru

17. ГОСТ 34.602-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.www.standartgost.ru

Интернет-ресурсы:

1. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс]. URL: http://elibrary.ru
2. Национальная электронная библиотека [Электронный ресурс]. URL: https://нэб.рф/.
3. Электронно-библиотечная система «Университетская библиотека онлайн» [Электронный ресурс]. URL: http://biblioclub.ru
4. Официальный сайт компании «Консультант Плюс» URL: http://www.consultant.ru
5. Справочная правовая система «Гарант». URL: http://www.garant.ru
6. Информационные ресурсы научной библиотеки Даггосуниверситета [Электронный ресурс]. URL: http://elib.dgu.ru.
7. Юридический вестник ДГУ. URL: www.jurvestnik.dgu.ru
8. Федеральный портал «Российское образование» [Электронный ресурс]. URL: http://www.edu.ru
9. Электронно-библиотечная система Юрайт [Электронный ресурс]. URL: https://urait.ru/.