МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования
«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФГБОУ ВО «ИГУ»

Факультет бизнес-коммуникаций и информатики
Кафедра прикладной информатики и документоведения

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине Б1.О.22 Информационная безопасность

направление подготовки 09.03.03 Прикладная информатика

направленность (профиль) Прикладная информатика в управлении

Иркутск – 2023

Одобрен
УМК факультета бизнес-коммуникаций
и информатики

Разработан в соответствии с ФГОС ВО

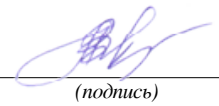
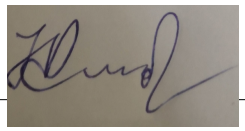
_____

с учетом требований проф. стандарта

_____

Председатель УМК — В.К. Карнаухова (*ФИО, должность, ученая степень, звание*) — _____ (*подпись, печать*)

Разработчики:

	профессор	А.В. Рохин
(подпись)	*(занимаемая должность)*	*(инициалы, фамилия)*
	профессор	Н.В. Амбросов
	(занимаемая должность)	*(инициалы, фамилия)*

Цель фонда оценочных средств. Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «Б1.О.22 Информационная безопасность». Перечень видов оценочных средств соответствует рабочей программе дисциплины.

Фонд оценочных средств включает контрольные материалы для проведения текущего контроля (в следующих формах: тест, устный опрос, практическое задание) и промежуточной аттестации в форме вопросов и заданий к экзамену.

Структура и содержание заданий – задания разработаны в соответствии с рабочей программой дисциплины «Б1.О.22 Информационная безопасность».

1. Паспорт фонда оценочных средств

Компетенция	**Индикаторы компетенций**	**Результаты обучения**
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1	Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
	ОПК-3.2	Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
	ОПК-3.3	Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

Компетенция	Индикаторы компетенций	Результаты обучения
ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.1	Знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы
	ОПК-4.2	Умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы
	ОПК-4.3	Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы
УК-10 Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	УК-10.1	Понимает действующие правовые нормы, обеспечивающие борьбу с коррупцией в различных областях жизнедеятельности; способы профилактики коррупции и формирования нетерпимого отношения к ней
	УК-10.2	Взаимодействует в обществе на основе нетерпимого отношения к коррупции
	УК-10.3	Планирует, организовывает и проводит мероприятия, обеспечивающие формирование гражданской позиции и предотвращение коррупции в профессиональной деятельности, в социуме

2. Показатели и критерии оценивания компетенций, шкалы оценивания

2.1. Показатели и критерии оценивания компетенций

№ п\п	Раздел, тема	Код индикатора компетенции	Наименование ОС	
			ТК	ПА
1	Раздел 1. Введение в безопасность информационных систем.	ОПК-3.1	Тест, УО	Тест
2	Раздел 2. Угрозы безопасности информационных систем и их реализация	ОПК-3.1, ОПК-4.1, УК-10.1, ОПК-3.2, ОПК-3.3, ОПК-4.2, УК-10.2, ОПК-4.3, УК-10.3	Тест, УО	Тест

№ п\п	Раздел, тема	Код индикатора компетенции	Наименование ОС	
			ТК	ПА
3	Раздел 3. Криптографические системы защиты информации	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3	Тест, Пз, УО	Тест
4	Раздел 4. Программно-технические средства защиты информации	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3	Тест, УО, Пз	Тест

2.2. Критерии оценивания результатов обучения для текущего контроля успеваемости и промежуточной аттестации

Оценочное средство	Критерии оценивания	Шкала оценивания
Тест	Студентом даны правильные ответы на 91-100% заданий	Отлично
	Студентом даны правильные ответы на 81-90% заданий	Хорошо
	Студентом даны правильные ответы на 71-80% заданий	Удовлетворительно
	Студентом даны правильные ответы менее чем на 70% заданий	Неудовлетворительно

Оценочное средство	Критерии оценивания	Шкала оценивания
Устный опрос	Ответ соответствует поставленной теме и содержит ответы на поставленные задачи, имеет четкую структуру, логически сопоставляемую с поставленными вопросами. Ответ демонстрирует способность анализировать и обобщать информацию, опираясь на знания, полученные в ходе изучения темы, а также демонстрировать самостоятельность автора в решении поставленных задач. Ответ содержит качественную речь и аргументацию, которая убедительно подтверждает выводы и ответы на поставленные вопросы	Отлично
	Ответ должен быть направлен на ответ на поставленные вопросы и соответствовать поставленной теме, иметь логическую цепочку рассуждений и четко демонстрировать связь между поставленными вопросами. Ответ выдержан в четкой форме, быть грамотно и без ошибок озвучен, выделены ключевые термины. Ответ должен демонстрировать способность анализировать и критически оценивать информацию, выбирая ключевые аспекты и выделяя главные выводы	Хорошо
	Ответ должен соответствовать поставленной теме и содержать ответы на поставленные вопросы, должен содержать существенную информацию, ясно передавать ответы и идеи. Ответ должен содержать достаточное количество аргументов и примеров, связанных с темой работы и позволяющих изложить свою точку зрения. Ответ должен быть грамотно сформулирован	Удовлетворительно
	Ответ не соответствует поставленной теме или не содержит ответов на поставленные задачи, содержит недостаточно аргументации и примеров, которые подтверждают высказанные в ответе идеи и выводы. Ответ не соответствует логической цепочке рассуждений и не выполняет требования логической последовательности высказывания, затрудняющей понимание ответа. Ответ содержит грубые ошибки, что затрудняет понимание высказывания	Неудовлетворительно

Оценочное средство	Критерии оценивания	Шкала оценивания
Практическое задание	Задание выполнено верно. Выбран оптимальный путь решения. Присутсвует развернутое описание алгоритма решения	Отлично
	Задание выполнено верно. Допущены негрубые логические ошибки при описании алгоритма решения. Отсутствуют пояснения к решению задания	Хорошо
	Ход решения задания верный, но допущены ошибки приведшие к неправильному ответу	Удовлетворительно
	В работе получен неверный ответ, связанный с грубыми ошибками допущенными в ходе решения, либо решение отсутсвует полностью	Неудовлетворительно

2.3. Оценочные средства для текущего контроля (примеры)

2.3.1. Материалы для компьютерного тестирования обучающихся

Общие критерии оценивания

Процент правильных ответов	Оценка
91% – 100%	5 (отлично)
81% – 90%	4 (хорошо)
71% – 80%	3 (удовлетворительно)
Менее 70%	2 (неудовлетворительно)

Соответствие вопросов теста индикаторам формируемых и оцениваемых компетенций

№ вопроса в тесте	Код индикатора компетенции
1	УК-10.1
2	УК-10.2
3	УК-10.3
4	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3
5	УК-10.2
6	ОПК-3.1
7	УК-10.3
8	ОПК-3.1
9	ОПК-4.3
10	ОПК-3.3
11	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3
12	ОПК-4.2

№ вопроса в тесте	Код индикатора компетенции
13	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3
14	ОПК-3.1
15	ОПК-3.1
16	ОПК-3.1
17	ОПК-3.1
18	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3
19	ОПК-3.3
20	ОПК-3.3
21	УК-10.1
22	ОПК-3.1
23	ОПК-3.2
24	ОПК-3.1
25	ОПК-4.3
26	ОПК-4.3
27	ОПК-3.1
28	УК-10.3
29	ОПК-3.2
30	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3
31	ОПК-4.1
32	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3
33	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3
34	ОПК-3.1
35	ОПК-3.1
36	ОПК-3.1
37	ОПК-3.2
38	ОПК-3.1
39	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3
40	ОПК-4.1
41	ОПК-4.2
42	УК-10.1
43	ОПК-4.1
44	ОПК-3.1

№ вопроса в тесте	Код индикатора компетенции
45	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3
46	ОПК-3.2
47	ОПК-4.2
48	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3
49	ОПК-4.3
50	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3
51	ОПК-4.1
52	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3
53	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3
54	УК-10.2
55	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3
56	ОПК-4.2
57	ОПК-3.2
58	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3
59	ОПК-3.1
60	ОПК-3.3

Ключ ответов

№ вопроса в тесте	Номер ответа (или ответ, или соответствие)
1	b
2	c
3	a, b
4	d
5	a
6	c
7	a
8	b
9	a
10	d
11	a, b
12	b
13	d

№ вопроса в тесте	Номер ответа (или ответ, или соответствие)
14	c
15	d
16	a
17	c
18	d
19	e
20	c
21	a
22	b
23	c
24	b
25	c
26	d
27	a, c, d
28	a
29	d
30	c
31	c
32	f
33	a
34	a
35	a
36	a
37	a
38	b
39	a
40	e
41	b
42	e
43	a
44	a
45	b
46	a
47	b
48	d
49	a
50	b
51	a

№ вопроса в тесте	Номер ответа (или ответ, или соответствие)
52	c
53	b
54	a, c
55	a
56	b
57	a
58	b, d
59	a
60	d

Перечень тестовых вопросов

№ 1. Задание с единичным выбором. Выберите один правильный ответ.

Алгоритм ГОСТ 28147:

a. разбивает блок на фиксированные 16-битные подблоки

b. основан на сети Фейштеля

c. имеет переменную длину ключа

№ 2. Задание с единичным выбором. Выберите один правильный ответ.

Что не может являться источником компьютерных вирусов?

a. Программы, написанные хакерами

b. Всемирно известная сеть Internet

c. Устройства пиратской перезаписи

d. Программы фирмы Касперского

№ 3. Задание с множественным выбором. Выберите 2 правильных ответа.

Виды симметричных криптосистем:

a. поточные шифры

b. блочные шифры

c. ЭЦП

d. криптосистемы с открытым ключом

№ 4. Задание с единичным выбором. Выберите один правильный ответ.

Что не обеспечивает логическое управление доступом?

a. конфиденциальность

b. доступность

c. целостность

d. полезность

№ 5. Задание с единичным выбором. Выберите один правильный ответ.

При дешифровании DES подключи используются

a. в обратном порядке относительно их использования при шифровании

b. в том же порядке, что и при шифровании

c. в произвольном порядке

№ 6. Задание с единичным выбором. Выберите один правильный ответ.

Криптография - это:

a. наука о методах и способах вскрытия шифров

b. наука о способах преобразования информации с целью ее защиты от незаконных пользователей и о методах и способах вскрытия шифров

c. наука о способах преобразования информации с целью ее защиты от незаконных пользователей

№ 7. Задание с единичным выбором. Выберите один правильный ответ.

Последовательность случайных чисел должна быть

a. иметь равномерное распределение

b. монотонно убывающей

c. монотонно возрастающей

№ 8. Задание с единичным выбором. Выберите один правильный ответ.

С увеличением количества раундов стойкость алгоритма:

a. уменьшается

b. увеличивается

c. не изменяется

№ 9. Задание с единичным выбором. Выберите один правильный ответ.

В алгоритмах симметричного шифрования секретным должен быть:

a. ключ

b. отдельные элементы алгоритма симметричного шифрования (такие как S-box)

c. весь алгоритм симметричного шифрования

№ 10. Задание с единичным выбором. Выберите один правильный ответ.

Какой принцип работы симметричных криптосистем?

a. Процесс шифрования выглядит следующим образом: ab...z(ИСХОДНЫЙ ТЕКСТ)z...ba, a,b,...,z-буквы ключа

b. Открытый и шифрованный текст обязательно одинаковой длины (поэтому и название симметричные)

c. Криптографический ключ имеет длину в 2 раза короче, чем текст для шифрования

d. Для шифрования и расшифрования применяется один и тот же криптографический ключ

№ 11. Задание с множественным выбором. Выберите 2 правильных ответа.

Идентификация - это:

a. имя пользователя

b. login

c. проверка подлинности

d. password

№ 12. Задание с единичным выбором. Выберите один правильный ответ.

Что обычно в себя включает схема электронной подписи?

a. функцию проверки подписи

b. всё из вышеперечисленного

c. ничего из вышеперечисленного

d. алгоритм генерации ключевых пар пользователя

e. функцию вычисления подписи

№ 13. Задание с единичным выбором. Выберите один правильный ответ.

Что не может быть использовано при биометрической идентификации клиента?

a. динамика подписи (ручной)

b. стиль работы с клавиатурой

c. анализ особенностей голоса и распознавание речи

d. геометрия и размер ноги

e. особенности отпечатков пальцев

f. геометрия руки и лица

g. сетчатка и роговица глаз

№ 14. Задание с единичным выбором. Выберите один правильный ответ.

Что из перечисленного относится к числу основных аспектов информационной безопасности:

a. приватность - сокрытие информации о личности пользователя

b. подотчетность - полнота регистрационной информации о действиях субъектов

c. конфиденциальность - защита от несанкционированного ознакомления

№ 15. Задание с единичным выбором. Выберите один правильный ответ.

Внутренними угрозами, не представляющими опасность для объектов обороны, являются:

a. нерешенность вопросов защиты интеллектуальной собственности предприятий оборонного комплекса

b. нерешенность вопросов социальной защиты военнослужащих и членов их семей

c. преднамеренные действия, а также ошибки персонала информационных систем специального назначения;

d. информационные ресурсы, содержащие сведения, отнесенные к государственной тайне

e. диверсионно-подрывная деятельность специальных служб иностранных государств

№ 16. Задание с единичным выбором. Выберите один правильный ответ.

Что из перечисленного не относится к числу основных аспектов информационной безопасности:

a. стерильность - отсутствие недекларированных возможностей

b. целостность - актуальность и непротиворечивость информации, защищенность информации и поддерживающей инфраструктуры от разрушения и несанкционированного изменения

c. подлинность - аутентичность субъектов и объектов

№ 17. Задание с единичным выбором. Выберите один правильный ответ.

Исход, при котором криптоаналитик получает некоторую информацию об открытом тексте или ключе, называется:

a. частичная дедукция

b. полный взлом

c. информационная дедукция

d. глобальная дедукция

№ 18. Задание с единичным выбором. Выберите один правильный ответ.

Какие способы не помогут защите информации в телекоммуникационных каналах

a. Процедура подтверждения характеристик данных

b. Процедуры аутентификации

c. Метод защиты кодов паролей, хранимых в вычислительной системе

d. Управление маршрутом

e. Цифровая подпись передаваемых сообщений

№ 19. Задание с единичным выбором. Выберите один правильный ответ.

Какую информацию можно не защищать?

a. Жизненно важную информацию

b. Полезную информацию

c. Ценную информацию

d. Незаменимую информацию

e. Несущественную информацию

№ 20. Задание с единичным выбором. Выберите один правильный ответ.

Исход, при котором криптоаналитик разрабатывает функциональный эквивалент исследуемого алгоритма, позволяющий зашифровывать и расшифровывать информацию без знания ключа, называется

a. частичная дедукция

b. информационная дедукция

c. глобальная дедукция

d. полный взлом

№ 21. Задание с единичным выбором. Выберите один правильный ответ.

Криптология - это:

a. наука о способах преобразования информации с целью ее защиты от незаконных пользователей и о методах и способах вскрытия шифров

b. наука о методах и способах вскрытия шифров

c. наука о способах преобразования информации с целью ее защиты от незаконных пользователей

№ 22. Задание с единичным выбором. Выберите один правильный ответ.

Средний ущерб от компьютерного преступления в США составляет примерно:

a. десятки тысяч долларов

b. сотни тысяч долларов

c. десятки долларов

d. копейки

№ 23. Задание с единичным выбором. Выберите один правильный ответ.

Алгоритм симметричного шифрования называется блочным, если

a. алгоритм основан на сети Фейстеля

b. в алгоритме используются S-box

c. для шифрования исходный текст разбивается на блоки фиксированной длины

№ 24. Задание с единичным выбором. Выберите один правильный ответ.

Затраты организаций на информационную безопасность:

a. снижаются

b. растут

c. остаются на одном уровне

№ 25. Задание с единичным выбором. Выберите один правильный ответ.

По принципу Керкгоффса криптографическая стойкость шифра целиком определяется ...

a. его сложностью

b. временем шифрования

c. секретностью ключа

d. длиной ключа

№ 26. Задание с единичным выбором. Выберите один правильный ответ.

Такой метод обеспечения безопасности процессов переработки информации не применяется:

a. Побуждение

b. Принуждение

c. Регламентация

d. Опознание

e. Маскировка

№ 27. Задание с множественным выбором. Выберите 3 правильных ответа.

Что из перечисленного относится к числу основных аспектов информационной безопасности:

a. конфиденциальность

b. защита от копирования

c. целостность

d. доступность

№ 28. Задание с единичным выбором. Выберите один правильный ответ.

Такой приём в «азбуке пропаганды» неизвестен:

a. «запугивание» или «красная угроза»

b. «приклеивание или навешивание ярлыков»

c. «свои ребята» или «игра в простонародность»

d. «сияющие обобщения» или «блистательная неопределенность»

e. «перетасовка» или «подтасовка карт»

№ 29. Задание с единичным выбором. Выберите один правильный ответ.

Какой класс нарушителя предполагает низкую квалификацию?

a. класс Н-4

b. класс Н-3

c. класс Н-1

d. класс Н-2

№ 30. Задание с единичным выбором. Выберите один правильный ответ.

Метка безопасности относится к следующему виду управления доступом:

a. дискреционному

b. свободному

c. принудительному

№ 31. Задание с единичным выбором. Выберите один правильный ответ.

Причина использования двух ключей в тройном DES состоит в том, что

a. в этом случае отсутствует атака «встреча посередине»

b. стойкость алгоритма не повышается при использовании трех ключей вместо двух

c. при использовании трех ключей общая длина ключа равна 168 битам, что может потребовать существенно больших вычислений при его распределении

№ 32. Задание с единичным выбором. Выберите один правильный ответ.

Какие не бывают меры защиты парольной аутентификации?

a. ограничение доступа к файлу паролей

b. ограничение числа неудачных попыток входа в систему

c. использование программных генераторов паролей

d. управление сроком действия паролей

e. обучение пользователей

f. наложение семантических ограничений

g. наложение технических ограничений

№ 33. Задание с единичным выбором. Выберите один правильный ответ.

Какого из видов аутентификации не бывает?

a. трехсторонней

b. односторонней

c. двусторонней

№ 34. Задание с единичным выбором. Выберите один правильный ответ.

Как называется преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины? (использует одностороннюю функцию)

a. Хэширование

b. Сжатие

c. Разбиение входного массива

№ 35. Задание с единичным выбором. Выберите один правильный ответ.

Что понимается под информационной безопасностью:

a. защита от нанесения неприемлемого ущерба субъектам информационных отношений

b. защита душевного здоровья телезрителей

c. обеспечение информационной независимости России

№ 36. Задание с единичным выбором. Выберите один правильный ответ.

Что из перечисленного не относится к числу основных аспектов информационной безопасности:

a. масштабируемость

b. доступность

c. целостность

d. конфиденциальность

№ 37. Задание с единичным выбором. Выберите один правильный ответ.

Как называется наука о математических методах обеспечения конфиденциальности и аутентичности (целостности и подлинности авторства) информации?

a. криптография

b. защита информации

c. математический анализ

d. авторское право

e. криптоанализ

№ 38. Задание с единичным выбором. Выберите один правильный ответ.

Сложность обеспечения информационной безопасности является следствием:

a. все большей зависимости общества от информационных систем

b. быстрого прогресса информационных технологий, ведущего к постоянному изменению информационных систем и требований к ним

c. невнимания широкой общественности к данной проблематике

№ 39. Задание с единичным выбором. Выберите один правильный ответ.

Для чего нужна электронно-цифровая подпись?

a. для подтверждения правильности содержания сообщения

b. для засекречивания данных

c. для шифрования данных

№ 40. Задание с единичным выбором. Выберите один правильный ответ.

Информационным оружием нельзя назвать следующие средства:

a. уничтожения, искажения или хищения информационных массивов

b. преодоления систем защиты

c. ограничения допуска законных пользователей;

d. дезорганизации работы технических средств, компьютерных систем.

e. фальсификация информации в каналах государственного и военного управления

№ 41. Задание с единичным выбором. Выберите один правильный ответ.

Криптоанализ - это:

a. наука о способах преобразования информации с целью ее защиты от незаконных пользователей

b. наука о методах и способах вскрытия шифров

c. наука о способах преобразования информации с целью ее защиты от незаконных пользователей и о методах и способах вскрытия шифров

№ 42. Задание с единичным выбором. Выберите один правильный ответ.

К основным задачам в сфере обеспечения и регулирования информационной безопасности РФ не относятся:

a. защита государственных информационных ресурсов,

b. координация деятельности органов государственной власти по обеспечению информационной безопасности;

c. совершенствование и защита отечественной информационной инфраструктуры;

d. пропаганда средствами массовой информации элементов национальных культур народов России

e. доктрина информационной безопасности Российской Федерации;

№ 43. Задание с единичным выбором. Выберите один правильный ответ.

В алгоритмах симметричного шифрования секретным должен быть:

a. ключ

b. отдельные элементы алгоритма симметричного шифрования (такие как S-box)

c. весь алгоритм симметричного шифрования

№ 44. Задание с единичным выбором. Выберите один правильный ответ.

Меры информационной безопасности направлены на защиту от:

a. нанесения неприемлемого ущерба

b. нанесения любого ущерба

c. подглядывания в замочную скважину

№ 45. Задание с единичным выбором. Выберите один правильный ответ.

Зачем на смарт-картах с магнитной полосой выполняется рельефная печать?

a. Чтобы слепые имели возможность использовать карты без посторонней помощи

b. Чтобы карта могла читаться на ручных обрабатывающих машинах

c. Выполнение продумано дизайнерским решением

d. Чтобы банкомат считывал номер карты и фамилию владельца

e. Подделка таких карт значительно осуществляется труднее

№ 46. Задание с единичным выбором. Выберите один правильный ответ.

Исход, при котором криптоаналитик извлекает секретный ключ, называется

a. полный взлом

b. частичная дедукция

c. информационная дедукция

d. глобальная дедукция

№ 47. Задание с единичным выбором. Выберите один правильный ответ.

Какой класс нарушителя предполагает высокую квалификацию?

a. класс Н-1

b. класс Н-4

c. класс Н-2

d. класс Н-3

№ 48. Задание с единичным выбором. Выберите один правильный ответ.

На этапе эксплуатации КС целостность и доступность информации в системе не обеспечивается:

a. использованием строго определенного множества программ

b. дублированием информации

c. повышением отказоустойчивости КС (компьютерной системы)

d. перемещением по локально-вычислительным сетям.

e. противодействием перегрузкам и «зависаниям» системы

№ 49. Задание с единичным выбором. Выберите один правильный ответ.

Какая длина ключа в ГОСТ 28147-89? (ответ в битах)

a. 256

b. 56

c. 64

d. 32

e. 128

№ 50. Задание с единичным выбором. Выберите один правильный ответ.

Какое из мероприятий не поможет при организации парольной защиты

a. Пароль не выдается при вводе на экран монитора.

b. Пароль не должен легко запоминаться

c. Длина пароля должна исключать возможность его раскрытия путем подбора

d. Пароли должны периодически меняться.

e. Запись пароля значительно повышает вероятность его компрометации

№ 51. Задание с единичным выбором. Выберите один правильный ответ.

Какой ключ доступен всем для проверки цифровой подписи под документом?

a. открытый

b. приватный

c. внутренний

d. закрытый

№ 52. Задание с единичным выбором. Выберите один правильный ответ.

Какие права системный администратор не может предоставить при работе с файлами и устройствами?

a. удаление

b. запись

c. слушание

d. добавление

e. выполнение

f. чтение

№ 53. Задание с единичным выбором. Выберите один правильный ответ.

Что из перечисленного не относится к подтверждению подлинности субъекта?

a. нечто, чем он владеет

b. нечто, чем владеет его системный администратор

c. нечто, что он знает

d. нечто, что есть часть его самого

№ 54. Задание с множественным выбором. Выберите 2 правильных ответа.

Какая информация шифруется при использовании программы BitLocker?

a. том данных

b. поврежденные сектора

c. код операционной системы

d. метаданные тома

e. загрузочный сектор

№ 55. Задание с единичным выбором. Выберите один правильный ответ.

Роли могут быть приписаны:

a. многим пользователям

b. двум пользователям

c. трем пользователям

d. одному пользователю

№ 56. Задание с единичным выбором. Выберите один правильный ответ.

Исход, при котором криптоаналитику удается расшифровать некоторые сообщения, называется:

a. полный взлом

b. частичная дедукция

c. глобальная дедукция

d. информационная дедукция

№ 57. Задание с единичным выбором. Выберите один правильный ответ.

Какой класс нарушителя предполагает среднюю квалификацию?

a. класс Н-3

b. класс Н-4

c. класс Н-1

d. класс Н-2

№ 58. Задание с множественным выбором. Выберите 2 правильных ответа.

Аутентификация - это:

a. имя пользователя

b. проверка подлинности

c. login

d. password

№ 59. Задание с единичным выбором. Выберите один правильный ответ.

Что из перечисленного не относится к числу основных аспектов информационной безопасности:

a. защита от копирования

b. целостность

c. конфиденциальность

d. доступность

№ 60. Задание с единичным выбором. Выберите один правильный ответ.

Какая схема лежит в основе DES и ГОСТ 28147-89?

a. Цезаря

b. Пратта

c. Вижинера

d. Фейштеля

e. Кантора

2.3.2. Вопросы для коллоквиумов, собеседования для оценки компенетции «ОПК-3.1»

№ 1. Подходы к моделированию угроз безопасности.

Описать следующие подходы к моделированию угроз безопасности:

CIA

Гексада Паркера

5A

STRIDE

№ 2. Классические методы шифрования информации.

Подготовить разбор методов шифрования и кратко описать историю методов:Шифрование методом Цезарь и Цезарь с ключевым словом

Шифрование методом магических квадратов.

Метод двойных квадратов Уитсона

Шифр Плейфера

Шифр Виженера

Шифр Вернама (XOR-шифр)

2.3.3. Вопросы для коллоквиумов, собеседования для оценки компенетции «ОПК-4.1»

№ 3. Классификация и характеристика угроз информационной безопасности.

Вопросы:

При каком уровне вероятности атаки, скорее всего не будет, а при каком скорее всего будет проведена?

Что такое угроза и какие классификации Вы знаете?

Какой вред может нанести персонал?

2.3.4. Вопросы для коллоквиумов, собеседования для оценки компенетции «ОПК-3.2»

№ 4. Классические методы шифрования информации.

Подготовить разбор методов шифрования и кратко описать историю методов:Шифрование методом Цезарь и Цезарь с ключевым словом

Шифрование методом магических квадратов.

Метод двойных квадратов Уитсона

Шифр Плейфера

Шифр Виженера

Шифр Вернама (XOR-шифр)

2.3.5. Вопросы для коллоквиумов, собеседования для оценки компенетции «ОПК-3.3»

№ 5. Классические методы шифрования информации.

Подготовить разбор методов шифрования и кратко описать историю методов:Шифрование методом Цезарь и Цезарь с ключевым словом

Шифрование методом магических квадратов.

Метод двойных квадратов Уитсона

Шифр Плейфера

Шифр Виженера

Шифр Вернама (XOR-шифр)

2.3.6. Вопросы для коллоквиумов, собеседования для оценки компенетции «УК-10.1»

№ 6. Управление доступом.

Управление доступом

2.3.7. Вопросы для коллоквиумов, собеседования для оценки компенетции «УК-10.2»

№ 7. Управление доступом.

Управление доступом

2.3.8. Вопросы для коллоквиумов, собеседования для оценки компенетции «УК-10.3»

№ 8. Управление доступом.

Управление доступом

3. Промежуточная аттестация

3.1. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и опыта деятельности

Экзамен является заключительным этапом процесса формирования компетенций обучающегося при изучении дисциплины и имеет целью проверку и оценку знаний обучающегося по теории, и применению полученных знаний, умений и навыков при решении практических задач.

Экзамен проводится по расписанию, сформированному учебно-методическим управлением, в сроки, предусмотренные календарным учебным графиком. Экзамен принимается преподавателем, ведущим лекционные занятия.

Экзамен проводится только при предъявлении обучающимся зачетной книжки и при условии выполнения всех контрольных мероприятий, предусмотренных учебным планом и рабочей программой дисциплины. Обучающимся на экзамене представляется право выбрать один из билетов. Время подготовки к ответу составляет 30 минут. По истечении установленного времени обучающийся должен ответить на вопросы экзаменационного билета. Результаты экзамена оцениваются по четырехбалльной системе и заносятся в зачетно-экзаменационную ведомость и зачетную книжку. В зачетную книжку заносятся только положительные оценки. Подписанный преподавателем экземпляр ведомости сдаётся не позднее следующего дня в деканат.

В случае неявки обучающегося на экзамен в зачетно-экзаменационную ведомость делается отметка «не явка». Обучающиеся, не прошедшие промежуточную аттестацию по дисциплине, должны ликвидировать академическую задолженность в установленном локальными нормативными актами порядке.

3.2. Вопросы к экзамену

№	Вопрос	Код компетенции
1.	Основные понятия информационной безопасности. Основные направления информационной безопасности.	ОПК-3.1
2.	Основные подходы к моделированию угроз безопасности	ОПК-3.1
3.	Определение угрозы безопасности информации. Принципы, методы и средства защиты информации.	ОПК-4.1, ОПК-4.2, ОПК-4.3
4.	Основные понятия криптографии. Алгоритм DES и его развитие. Российские алгоритмы шифрования информации. Стандарт криптографической защиты США. Двухключевые криптографические системы. Сравнение симметричных и несимметричных алгоритмов шифрования. Хэш-функция. Цифровая подпись. Квантовое и постквантовое шифрование.	ОПК-3.1, ОПК-3.2, ОПК-3.3
5.	Определение технического канала утечки информации. Методы и средства защиты программ и данных в ЭВМ. Классификация вредоносных программ.	ОПК-3.1, ОПК-3.2, ОПК-3.3
6.	Определение технического канала утечки информации. Методы и средства защиты программ и данных в ЭВМ. Классификация вредоносных программ.	ОПК-3.1, ОПК-3.2, ОПК-3.3
7.	Определение несанкционированного доступа к информации. Методы и средств защиты информации от утечки по техническим каналам.	ОПК-4.1, ОПК-4.2, ОПК-4.3

3.3. Тематика курсовых работ

По данной дисциплине выполнение курсовых проектов (работ) не предусматривается.

3.4. Материалы для компьютерного тестирования обучающихся

Общие критерии оценивания

Процент правильных ответов	Оценка
91% – 100%	5 (отлично)
81% – 90%	4 (хорошо)
71% – 80%	3 (удовлетворительно)
Менее 70%	2 (неудовлетворительно)

Соответствие вопросов теста индикаторам формируемых и оцениваемых компетенций

№ вопроса в тесте	Код индикатора компетенции
1	УК-10.1
2	УК-10.2
3	УК-10.3
4	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3
5	УК-10.2

№ вопроса в тесте	Код индикатора компетенции
6	ОПК-3.1
7	УК-10.3
8	ОПК-3.1
9	ОПК-4.3
10	ОПК-3.3
11	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3
12	ОПК-4.2
13	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3
14	ОПК-3.1
15	ОПК-3.1
16	ОПК-3.1
17	ОПК-3.1
18	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3
19	ОПК-3.3
20	ОПК-3.3
21	УК-10.1
22	ОПК-3.1
23	ОПК-3.2
24	ОПК-3.1
25	ОПК-4.3
26	ОПК-4.3
27	ОПК-3.1
28	УК-10.3
29	ОПК-3.2
30	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3
31	ОПК-4.1
32	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3
33	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3
34	ОПК-3.1
35	ОПК-3.1
36	ОПК-3.1
37	ОПК-3.2

№ вопроса в тесте	Код индикатора компетенции
38	ОПК-3.1
39	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3
40	ОПК-4.1
41	ОПК-4.2
42	УК-10.1
43	ОПК-4.1
44	ОПК-3.1
45	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3
46	ОПК-3.2
47	ОПК-4.2
48	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3
49	ОПК-4.3
50	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3
51	ОПК-4.1
52	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3
53	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3
54	УК-10.2
55	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3
56	ОПК-4.2
57	ОПК-3.2
58	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3, УК-10.1, УК-10.2, УК-10.3
59	ОПК-3.1
60	ОПК-3.3

Ключ ответов

№ вопроса в тесте	Номер ответа (или ответ, или соответствие)
1	b
2	c
3	a, b
4	d
5	a

№ вопроса в тесте	Номер ответа (или ответ, или соответствие)
6	c
7	a
8	b
9	a
10	d
11	a, b
12	b
13	d
14	c
15	d
16	a
17	c
18	d
19	e
20	c
21	a
22	b
23	c
24	b
25	c
26	d
27	a, c, d
28	a
29	d
30	c
31	c
32	f
33	a
34	a
35	a
36	a
37	a
38	b
39	a
40	e
41	b
42	e
43	a

№ вопроса в тесте	Номер ответа (или ответ, или соответствие)
44	a
45	b
46	a
47	b
48	d
49	a
50	b
51	a
52	c
53	b
54	a, c
55	a
56	b
57	a
58	b, d
59	a
60	d

Перечень тестовых вопросов

№ 1. Задание с единичным выбором. Выберите один правильный ответ.

Алгоритм ГОСТ 28147:

a. разбивает блок на фиксированные 16-битные подблоки

b. основан на сети Фейштеля

c. имеет переменную длину ключа

№ 2. Задание с единичным выбором. Выберите один правильный ответ.

Что не может являться источником компьютерных вирусов?

a. Программы, написанные хакерами

b. Всемирно известная сеть Internet

c. Устройства пиратской перезаписи

d. Программы фирмы Касперского

№ 3. Задание с множественным выбором. Выберите 2 правильных ответа.

Виды симметричных криптосистем:

a. поточные шифры

b. блочные шифры

c. ЭЦП

d. криптосистемы с открытым ключом

№ 4. Задание с единичным выбором. Выберите один правильный ответ.

Что не обеспечивает логическое управление доступом?

a. конфиденциальность

b. доступность

c. целостность

d. полезность

№ 5. Задание с единичным выбором. Выберите один правильный ответ.

При дешифровании DES подключи используются

a. в обратном порядке относительно их использования при шифровании

b. в том же порядке, что и при шифровании

c. в произвольном порядке

№ 6. Задание с единичным выбором. Выберите один правильный ответ.

Криптография - это:

a. наука о методах и способах вскрытия шифров

b. наука о способах преобразования информации с целью ее защиты от незаконных пользователей и о методах и способах вскрытия шифров

c. наука о способах преобразования информации с целью ее защиты от незаконных пользователей

№ 7. Задание с единичным выбором. Выберите один правильный ответ.

Последовательность случайных чисел должна быть

a. иметь равномерное распределение

b. монотонно убывающей

c. монотонно возрастающей

№ 8. Задание с единичным выбором. Выберите один правильный ответ.

С увеличением количества раундов стойкость алгоритма:

a. уменьшается

b. увеличивается

c. не изменяется

№ 9. Задание с единичным выбором. Выберите один правильный ответ.

В алгоритмах симметричного шифрования секретным должен быть:

a. ключ

b. отдельные элементы алгоритма симметричного шифрования (такие как S-box)

c. весь алгоритм симметричного шифрования

№ 10. Задание с единичным выбором. Выберите один правильный ответ.

Какой принцип работы симметричных криптосистем?

a. Процесс шифрования выглядит следующим образом: ab…z(ИСХОДНЫЙ ТЕКСТ)z...ba, a,b,...,z-буквы ключа

b. Открытый и шифрованный текст обязательно одинаковой длины (поэтому и название симметричные)

c. Криптографический ключ имеет длину в 2 раза короче, чем текст для шифрования

d. Для шифрования и расшифрования применяется один и тот же криптографический ключ

№ 11. Задание с множественным выбором. Выберите 2 правильных ответа.

Идентификация - это:

a. имя пользователя

b. login

c. проверка подлинности

d. password

№ 12. Задание с единичным выбором. Выберите один правильный ответ.

Что обычно в себя включает схема электронной подписи?

a. функцию проверки подписи

b. всё из вышеперечисленного

c. ничего из вышеперечисленного

d. алгоритм генерации ключевых пар пользователя

e. функцию вычисления подписи

№ 13. Задание с единичным выбором. Выберите один правильный ответ.

Что не может быть использовано при биометрической идентификации клиента?

a. динамика подписи (ручной)

b. стиль работы с клавиатурой

c. анализ особенностей голоса и распознавание речи

d. геометрия и размер ноги

e. особенности отпечатков пальцев

f. геометрия руки и лица

g. сетчатка и роговица глаз

№ 14. Задание с единичным выбором. Выберите один правильный ответ.

Что из перечисленного относится к числу основных аспектов информационной безопасности:

a. приватность - сокрытие информации о личности пользователя

b. подотчетность - полнота регистрационной информации о действиях субъектов

c. конфиденциальность - защита от несанкционированного ознакомления

№ 15. Задание с единичным выбором. Выберите один правильный ответ.

Внутренними угрозами, не представляющими опасность для объектов обороны, являются:

a. нерешенность вопросов защиты интеллектуальной собственности предприятий оборонного комплекса

b. нерешенность вопросов социальной защиты военнослужащих и членов их семей

c. преднамеренные действия, а также ошибки персонала информационных систем специального назначения;

d. информационные ресурсы, содержащие сведения, отнесенные к государственной тайне

e. диверсионно-подрывная деятельность специальных служб иностранных государств

№ 16. Задание с единичным выбором. Выберите один правильный ответ.

Что из перечисленного не относится к числу основных аспектов информационной безопасности:

a. стерильность - отсутствие недекларированных возможностей

b. целостность - актуальность и непротиворечивость информации, защищенность информации и поддерживающей инфраструктуры от разрушения и несанкционированного изменения

c. подлинность - аутентичность субъектов и объектов

№ 17. Задание с единичным выбором. Выберите один правильный ответ.

Исход, при котором криптоаналитик получает некоторую информацию об открытом тексте или ключе, называется:

a. частичная дедукция

b. полный взлом

c. информационная дедукция

d. глобальная дедукция

№ 18. Задание с единичным выбором. Выберите один правильный ответ.

Какие способы не помогут защите информации в телекоммуникационных каналах

a. Процедура подтверждения характеристик данных

b. Процедуры аутентификации

c. Метод защиты кодов паролей, хранимых в вычислительной системе

d. Управление маршрутом

e. Цифровая подпись передаваемых сообщений

№ 19. Задание с единичным выбором. Выберите один правильный ответ.

Какую информацию можно не защищать?

a. Жизненно важную информацию

b. Полезную информацию

c. Ценную информацию

d. Незаменимую информацию

e. Несущественную информацию

№ 20. Задание с единичным выбором. Выберите один правильный ответ.

Исход, при котором криптоаналитик разрабатывает функциональный эквивалент исследуемого алгоритма, позволяющий зашифровывать и расшифровывать информацию без знания ключа, называется

a. частичная дедукция

b. информационная дедукция

c. глобальная дедукция

d. полный взлом

№ 21. Задание с единичным выбором. Выберите один правильный ответ.

Криптология - это:

a. наука о способах преобразования информации с целью ее защиты от незаконных пользователей и о методах и способах вскрытия шифров

b. наука о методах и способах вскрытия шифров

c. наука о способах преобразования информации с целью ее защиты от незаконных пользователей

№ 22. Задание с единичным выбором. Выберите один правильный ответ.

Средний ущерб от компьютерного преступления в США составляет примерно:

a. десятки тысяч долларов

b. сотни тысяч долларов

c. десятки долларов

d. копейки

№ 23. Задание с единичным выбором. Выберите один правильный ответ.

Алгоритм симметричного шифрования называется блочным, если

a. алгоритм основан на сети Фейстеля

b. в алгоритме используются S-box

c. для шифрования исходный текст разбивается на блоки фиксированной длины

№ 24. Задание с единичным выбором. Выберите один правильный ответ.

Затраты организаций на информационную безопасность:

a. снижаются

b. растут

c. остаются на одном уровне

№ 25. Задание с единичным выбором. Выберите один правильный ответ.

По принципу Керкгоффса криптографическая стойкость шифра целиком определяется ...

a. его сложностью

b. временем шифрования

c. секретностью ключа

d. длиной ключа

№ 26. Задание с единичным выбором. Выберите один правильный ответ.

Такой метод обеспечения безопасности процессов переработки информации не применяется:

a. Побуждение

b. Принуждение

c. Регламентация

d. Опознание

e. Маскировка

№ 27. Задание с множественным выбором. Выберите 3 правильных ответа.

Что из перечисленного относится к числу основных аспектов информационной безопасности:

a. конфиденциальность

b. защита от копирования

c. целостность

d. доступность

№ 28. Задание с единичным выбором. Выберите один правильный ответ.

Такой приём в «азбуке пропаганды» неизвестен:

a. «запугивание» или «красная угроза»

b. «приклеивание или навешивание ярлыков»

c. «свои ребята» или «игра в простонародность»

d. «сияющие обобщения» или «блистательная неопределенность»

e. «перетасовка» или «подтасовка карт»

№ 29. Задание с единичным выбором. Выберите один правильный ответ.

Какой класс нарушителя предполагает низкую квалификацию?

a. класс Н-4

b. класс Н-3

c. класс Н-1

d. класс Н-2

№ 30. Задание с единичным выбором. Выберите один правильный ответ.

Метка безопасности относится к следующему виду управления доступом:

a. дискреционному

b. свободному

c. принудительному

№ 31. Задание с единичным выбором. Выберите один правильный ответ.

Причина использования двух ключей в тройном DES состоит в том, что

a. в этом случае отсутствует атака «встреча посередине»

b. стойкость алгоритма не повышается при использовании трех ключей вместо двух

c. при использовании трех ключей общая длина ключа равна 168 битам, что может потребовать существенно больших вычислений при его распределении

№ 32. Задание с единичным выбором. Выберите один правильный ответ.

Какие не бывают меры защиты парольной аутентификации?

a. ограничение доступа к файлу паролей

b. ограничение числа неудачных попыток входа в систему

c. использование программных генераторов паролей

d. управление сроком действия паролей

e. обучение пользователей

f. наложение семантических ограничений

g. наложение технических ограничений

№ 33. Задание с единичным выбором. Выберите один правильный ответ.

Какого из видов аутентификации не бывает?

a. трехсторонней

b. односторонней

c. двусторонней

№ 34. Задание с единичным выбором. Выберите один правильный ответ.

Как называется преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины? (использует одностороннюю функцию)

a. Хэширование

b. Сжатие

c. Разбиение входного массива

№ 35. Задание с единичным выбором. Выберите один правильный ответ.

Что понимается под информационной безопасностью:

a. защита от нанесения неприемлемого ущерба субъектам информационных отношений

b. защита душевного здоровья телезрителей

c. обеспечение информационной независимости России

№ 36. Задание с единичным выбором. Выберите один правильный ответ.

Что из перечисленного не относится к числу основных аспектов информационной безопасности:

a. масштабируемость

b. доступность

c. целостность

d. конфиденциальность

№ 37. Задание с единичным выбором. Выберите один правильный ответ.

Как называется наука о математических методах обеспечения конфиденциальности и аутентичности (целостности и подлинности авторства) информации?

a. криптография

b. защита информации

c. математический анализ

d. авторское право

e. криптоанализ

№ 38. Задание с единичным выбором. Выберите один правильный ответ.

Сложность обеспечения информационной безопасности является следствием:

a. все большей зависимости общества от информационных систем

b. быстрого прогресса информационных технологий, ведущего к постоянному изменению информационных систем и требований к ним

c. невнимания широкой общественности к данной проблематике

№ 39. Задание с единичным выбором. Выберите один правильный ответ.

Для чего нужна электронно-цифровая подпись?

a. для подтверждения правильности содержания сообщения

b. для засекречивания данных

c. для шифрования данных

№ 40. Задание с единичным выбором. Выберите один правильный ответ.

Информационным оружием нельзя назвать следующие средства:

a. уничтожения, искажения или хищения информационных массивов

b. преодоления систем защиты

c. ограничения допуска законных пользователей;

d. дезорганизации работы технических средств, компьютерных систем.

e. фальсификация информации в каналах государственного и военного управления

№ 41. Задание с единичным выбором. Выберите один правильный ответ.

Криптоанализ - это:

a. наука о способах преобразования информации с целью ее защиты от незаконных пользователей

b. наука о методах и способах вскрытия шифров

c. наука о способах преобразования информации с целью ее защиты от незаконных пользователей и о методах и способах вскрытия шифров

№ 42. Задание с единичным выбором. Выберите один правильный ответ.

К основным задачам в сфере обеспечения и регулирования информационной безопасности РФ не относятся:

a. защита государственных информационных ресурсов,

b. координация деятельности органов государственной власти по обеспечению информационной безопасности;

c. совершенствование и защита отечественной информационной инфраструктуры;

d. пропаганда средствами массовой информации элементов национальных культур народов России

e. доктрина информационной безопасности Российской Федерации;

№ 43. Задание с единичным выбором. Выберите один правильный ответ.

В алгоритмах симметричного шифрования секретным должен быть:

a. ключ

b. отдельные элементы алгоритма симметричного шифрования (такие как S-box)

c. весь алгоритм симметричного шифрования

№ 44. Задание с единичным выбором. Выберите один правильный ответ.

Меры информационной безопасности направлены на защиту от:

a. нанесения неприемлемого ущерба

b. нанесения любого ущерба

c. подглядывания в замочную скважину

№ 45. Задание с единичным выбором. Выберите один правильный ответ.

Зачем на смарт-картах с магнитной полосой выполняется рельефная печать?

a. Чтобы слепые имели возможность использовать карты без посторонней помощи

b. Чтобы карта могла читаться на ручных обрабатывающих машинах

c. Выполнение продумано дизайнерским решением

d. Чтобы банкомат считывал номер карты и фамилию владельца

e. Подделка таких карт значительно осуществляется труднее

№ 46. Задание с единичным выбором. Выберите один правильный ответ.

Исход, при котором криптоаналитик извлекает секретный ключ, называется

a. полный взлом

b. частичная дедукция

c. информационная дедукция

d. глобальная дедукция

№ 47. Задание с единичным выбором. Выберите один правильный ответ.

Какой класс нарушителя предполагает высокую квалификацию?

a. класс Н-1

b. класс Н-4

c. класс Н-2

d. класс Н-3

№ 48. Задание с единичным выбором. Выберите один правильный ответ.

На этапе эксплуатации КС целостность и доступность информации в системе не обеспечивается:

a. использованием строго определенного множества программ

b. дублированием информации

c. повышением отказоустойчивости КС (компьютерной системы)

d. перемещением по локально-вычислительным сетям.

e. противодействием перегрузкам и «зависаниям» системы

№ 49. Задание с единичным выбором. Выберите один правильный ответ.

Какая длина ключа в ГОСТ 28147-89? (ответ в битах)

a. 256

b. 56

c. 64

d. 32

e. 128

№ 50. Задание с единичным выбором. Выберите один правильный ответ.

Какое из мероприятий не поможет при организации парольной защиты

a. Пароль не выдается при вводе на экран монитора.

b. Пароль не должен легко запоминаться

c. Длина пароля должна исключать возможность его раскрытия путем подбора

d. Пароли должны периодически меняться.

e. Запись пароля значительно повышает вероятность его компрометации

№ 51. Задание с единичным выбором. Выберите один правильный ответ.

Какой ключ доступен всем для проверки цифровой подписи под документом?

a. открытый

b. приватный

c. внутренний

d. закрытый

№ 52. Задание с единичным выбором. Выберите один правильный ответ.

Какие права системный администратор не может предоставить при работе с файлами и устройствами?

a. удаление

b. запись

c. слушание

d. добавление

e. выполнение

f. чтение

№ 53. Задание с единичным выбором. Выберите один правильный ответ.

Что из перечисленного не относится к подтверждению подлинности субъекта?

a. нечто, чем он владеет

b. нечто, чем владеет его системный администратор

c. нечто, что он знает

d. нечто, что есть часть его самого

№ 54. Задание с множественным выбором. Выберите 2 правильных ответа.

Какая информация шифруется при использовании программы BitLocker?

a. том данных

b. поврежденные сектора

c. код операционной системы

d. метаданные тома

e. загрузочный сектор

№ 55. Задание с единичным выбором. Выберите один правильный ответ.

Роли могут быть приписаны:

a. многим пользователям

b. двум пользователям

c. трем пользователям

d. одному пользователю

№ 56. Задание с единичным выбором. Выберите один правильный ответ.

Исход, при котором криптоаналитику удается расшифровать некоторые сообщения, называется:

a. полный взлом

b. частичная дедукция

c. глобальная дедукция

d. информационная дедукция

№ 57. Задание с единичным выбором. Выберите один правильный ответ.

Какой класс нарушителя предполагает среднюю квалификацию?

a. класс Н-3

b. класс Н-4

c. класс Н-1

d. класс Н-2

№ 58. Задание с множественным выбором. Выберите 2 правильных ответа.

Аутентификация - это:

a. имя пользователя

b. проверка подлинности

c. login

d. password

№ 59. Задание с единичным выбором. Выберите один правильный ответ.

Что из перечисленного не относится к числу основных аспектов информационной безопасности:

a. защита от копирования

b. целостность

c. конфиденциальность

d. доступность

№ 60. Задание с единичным выбором. Выберите один правильный ответ.

Какая схема лежит в основе DES и ГОСТ 28147-89?

a. Цезаря

b. Пратта

c. Вижинера

d. Фейштеля

e. Кантора