Автономная некоммерческая образовательная организация
высшего образования
«Воронежский экономико-правовой институт»
(АНОО ВО «ВЭПИ»)

АНОО ВО "ВОРОНЕЖСКИЙ ЭКОНОМИКО-ПРАВОВОЙ ИНСТИТУТ", АНОО ВО "ВЭПИ", ВЭПИ

Подписано цифровой подписью: АНОО ВО "ВОРОНЕЖСКИЙ ЭКОНОМИКО-ПРАВОВОЙ ИНСТИТУТ", АНОО ВО "ВЭПИ", ВЭПИ
Дата: 23.04.2024 15:50:35 +03'00'

УТВЕРЖДАЮ
Проректор
по учебно-методической работе
_____ А.Ю. Жильников
«23» апреля 2024 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Б1.О.22 Информационная безопасность
(наименование дисциплины (модуля)

38.05.01 Экономическая безопасность
(код и наименование направления подготовки)

Специализация Экономико-правовое обеспечение экономической безопасности в условиях цифровизации
(наименование направленности (профиля)

Квалификация выпускника Специалист
(наименование квалификации)

Форма обучения Очная, заочная
(очная, очно-заочная, заочная)

Рекомендована к использованию филиалами АНОО ВО «ВЭПИ»

Воронеж 2024

Фонд оценочных средств рассмотрен и одобрен на заседании кафедры прикладной информатики.

Протокол от «15» апреля 2024 г. № 8

Директор ООО «НСКОМ», Петров Р.А. 01.04.2024

(должность, наименование организации, ФИО, подпись, дата, печать)

Директор ООО «Ангелы АйТи», Попов Р.И. 01.04.2024

(должность, наименование организации, ФИО, подпись, дата, печать)

Директор ООО «Стройцех Регион», Белозеров Ф.Ф. 01.04.2024

(должность, наименование организации, ФИО, подпись, дата, печать)

Заведующий кафедрой М.С. Агафонова

Разработчики:

Ст. преподаватель Д.В. Байбеков

1. Перечень компетенций с указанием этапов их формирования в процессе освоения ОП ВО

Целью проведения дисциплины Б1.О.22 Информационная безопасность является достижение следующих результатов обучения:

Код компетенции	Наименование компетенции
ОПК-7	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

В формировании данных компетенций также участвуют следующие дисциплины (модули), практики образовательной программы (по семестрам (курсам) их изучения):

- для очной формы обучения:

Наименование дисциплин (модулей), практик	Этапы формирования компетенций по семестрам изучения									
	1 сем.	2 сем.	3 сем.	4 сем.	5 сем.	6 сем.	7 сем.	8 сем.	9 см.	10 сем.
Информатика и программирование			ОПК-7	ОПК-7						
Информационные технологии в экономике			ОПК-7	ОПК-7						
Введение в системы искусственного интеллекта					ОПК-7					
Информационный менеджмент						ОПК-7				
Цифровая экономика	ОПК-7									
Учебная практика (ознакомительная практика)				ОПК-7						
Подготовка к сдаче и сдача государственного экзамена										ОПК-7
Подготовка к процедуре защиты и защита выпускной квалификационной работы										ОПК-7

- для заочной формы обучения:

Наименование дисциплин (модулей), практик	Этапы формирования компетенций по курсам изучения					
	1 курс	2 курс	3 курс	4 курс	5 курс	6 курс
Информатика и программирование	ОПК-7					
Информационные технологии в экономике			ОПК-7			
Введение в системы искусственного интеллекта			ОПК-7			
Информационный менеджмент			ОПК-7			
Цифровая экономика		ОПК-7				
Учебная практика (ознакомительная практика)			ОПК-7			
Подготовка к сдаче и сдача государственного экзамена						ОПК-7
Подготовка к процедуре защиты и защита выпускной квалификационной работы						ОПК-7

Этап дисциплины (модуля) Б1.О.22 Информационная безопасность соответствует:

- для очной формы обучения – 7 и 8 семестру
- для заочной формы обучения – 5 курсу.

2. Показатели и критерии оценивания компетенций на различных этапах их формирования, шкалы оценивания

Показателями оценивания компетенций являются следующие результаты обучения:

Код компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине (модулю)
ОПК-7. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.	**ИОПК 7.1.** Знает и понимает принципы работы и возможности современных информационных технологий, предназначенных для решения задач обеспечения экономической безопасности	ЗНАТЬ – способы сбора, анализа, систематизации, оценки и интерпретации данных, необходимых для решения профессиональных задач – основные методы, способы и средства получения, хранения, переработки информации, навыки работы с компьютером как средством управления информацией, современные принципы работы с деловой информацией- – основные понятия, свойства, классификацию и этапы развития информационных технологий и систем, современные принципы работы с информационно- коммуникационными технологиями, методы и средства управления информацией и управление с помощью информации в целях обеспечения экономической безопасности; – основные принципы работы информационных технологий и систем для обеспечения экономической безопасности. УМЕТЬ – понимать принципы работы современных информационных технологий и использовать их для решения задач обеспечения информационной безопасности; ВЛАДЕТЬ – принципами работы современных информационных технологий с учетом обеспечения информационной безопасности – навыками работы с современными информационными технологиями для автоматизации процессов обеспечения экономической безопасности.
	ИОПК 7.2 Использует современные информационные технологии для решения задач профессиональной деятельности	ЗНАТЬ – особенности обеспечения информационной безопасности. УМЕТЬ – использовать информационно-коммуникационные технологии в экономической сфере деятельности предприятий или организаций; – использовать современные информационные технологии для решения задач профессиональной деятельности. ВЛАДЕТЬ – принципами работы современных информационных технологий с учетом обеспечения информационной безопасности – навыками работы с современными информационными технологиями для

		автоматизации процессов обеспечения экономической безопасности.

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины (модуля):

№ п/п	Наименование раздела дисциплины, темы (модуля)	Код компетенции, код индикатора достижения компетенции	Критерии оценивания	Оценочные средства текущего контроля успеваемости	Шкала оценивания
1	Тема 1. Проблема обеспечения ИБ. Основные понятия	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	Знать: - Объекты защиты информации Уметь: -Пользоваться основными понятиями Владеть: -Проблемами обеспечения ИБ	Сообщение	«Зачтено» «Не зачтено»
2	Тема 2. Угрозы ИБ	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	Знать: -Угрозы ИБ Уметь: - Классифицировать угрозы безопасности Владеть: - Прямыми и косвенными каналами утечки данных.	Доклад	«Зачтено» «Не зачтено»
3	Тема 3. Основы теории ИБ	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	Знать: - Способы мошенничества в информационных системах Уметь: - применять модель потенциального нарушителя Владеть: - Основными способами реализации угроз ИБ	Опрос	«Зачтено» «Не зачтено»
4	Тема 4. Оценка эффективности систем защиты информации	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	Знать: - Понятие мониторов безопасности Уметь: - использовать физические средства защиты информации Владеть: - Принципами организации	Сообщение	«Зачтено» «Не зачтено»

			систем обеспечения безопасности данных.		
5	Тема 5. Нормативные руководящие документы в сфере обеспечения ИБ	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	Знать: - Понятие политики безопасности Уметь: -применять показатели эффективности систем защиты информации Владеть: - Моделью безопасности информационных потоков	Доклад	«Зачтено» «Не зачтено»
6	Тема 6. Программно-технические средства обеспечения ИБ	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	Знать: -Принципы организации систем обеспечения безопасности данных Уметь: -применять физические средства защиты информации Владеть: - Понятием мониторов безопасности	Опрос	«Зачтено» «Не зачтено»
7	Тема 7. Межсетевые экраны	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	Знать: - Руководящие документы Гостехкомиссии в сфере обеспечения ИБ Уметь: - «Общие критерии» Владеть: - Структурой	Сообщение	«Зачтено» «Не зачтено»
8	Тема 8. Борьба с компьютерными вирусами	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	Знать: - Типы компьютерных вирусов Уметь: -Бороться с компьютерными вирусами Владеть: -Методами борьбы с компьютерными вирусами	Сообщение	«Зачтено» «Не зачтено»
9	Тема 9. Криптографические методы	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	Знать: - Федеральный стандарт США на шифрование данных (стандарт	Доклад	«Зачтено» «Не зачтено»

			DES) Уметь: -Шифровать с открытым ключом Владеть: -Отечественным стандартом на шифрование данных		
10	Тема 10. Построение защищённых виртуальных сетей	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	Знать: - Понятие, назначение и основные функции защищённой виртуальной сети Уметь: -Туннелировать в протоколах различных уровней. Владеть: - Средствами построения защищённой виртуальной сети	Опрос	«Зачтено» «Не зачтено»
ИТОГО			Форма контроля	Оценочные средства промежуточной аттестации	Шкала оценивания
			Зачёт с оценкой	Письменный ответ на билет	«Отлично», «Хорошо», «Удовлетворительно», «Неудовлетворительно»

Критерии оценивания результатов обучения для текущего контроля успеваемости и промежуточной аттестации по дисциплине (модулю)

1. Критерий оценивания опроса:

- зачтено – выставляется обучающемуся, если демонстрирует знание основных разделов программы изучаемого курса: его базовых понятий и фундаментальных проблем; приобрел необходимые умения и навыки; освоил вопросы практического применения полученных знаний, не допустил фактических ошибок при ответе; достаточно последовательно и логично излагает теоретический материал, допуская лишь незначительные нарушения последовательности изложения и некоторые неточности; показывает всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их;

- не зачтено – выставляется обучающемуся, если демонстрирует фрагментарные знания основных разделов программы изучаемого курса: его базовых понятий и фундаментальных проблем; слабо выражена способность к самостоятельному аналитическому мышлению, имеются затруднения в изложении материала, отсутствуют необходимые умения и навыки; допущены грубые ошибки и незнание терминологии, отказ отвечать на дополнительные вопросы, знание которых необходимо для получения

положительной оценки; выставляется обучающемуся, ответ которого содержит существенные пробелы в знаниях основного содержания рабочей программы дисциплины.

2. Критерий доклада:

- зачтено – представленный доклад соответствует тематике, экономически обоснован, выводы по изученной проблеме изложены логически, соблюдены требования, при разработке доклада были использованы современны информационные технологии;
- не зачтено – доклад обучающимся не представлена; материалы доклад не обоснованы или логически не связаны, использованы устаревшие источники информации.

3. Критерий сообщения:

- зачтено – представленный сообщение актуально, экономически обоснован, выводы по изученной представленная информация изложена логически, соблюдены требования, при разработке собщения были использованы современны информационные технологии;
- не зачтено – сообщение обучающимся не представлена; представленная информация не обоснованы или логически не связана, использованы устаревшая информация.

4. Критерии оценивания письменного ответа на билет на зачете с оценкой:

- отлично – выставляется обучающемуся, если: даны исчерпывающие и обоснованные ответы на все поставленные вопросы, правильно и рационально (с использованием рациональных методик) решены соответствующие задачи; в ответах выделялось главное, все теоретические положения умело увязывались с требованиями руководящих документов; ответы были четкими и краткими, а мысли излагались в логической последовательности; показано умение самостоятельно анализировать факты, события, явления, процессы в их взаимосвязи и диалектическом развитии;
- хорошо – выставляется обучающемуся, если: даны полные, достаточно обоснованные ответы на поставленные вопросы, правильно решены практические задания; в ответах не всегда выделялось главное, отдельные положения недостаточно увязывались с требованиями руководящих документов, при решении практических задач не всегда использовались рациональные методики расчётов; ответы в основном были краткими, но не всегда четкими; показано слабое умение самостоятельно анализировать факты, события, явления, процессы в их взаимосвязи и диалектическом развитии;
- удовлетворительно – выставляется обучающемуся, если: даны в основном правильные ответы на все поставленные вопросы, но без должной глубины и обоснования, при решении практических задач обучающийся использовал прежний опыт и не применял новые методики выполнения

расчётов, однако на уточняющие вопросы даны в целом правильные ответы; при ответах не выделялось главное; отдельные положения недостаточно увязывались с требованиями руководящих документов, при решении практических задач не использовались рациональные методики расчётов; ответы были многословными, нечеткими и без должной логической последовательности, на отдельные дополнительные вопросы не даны положительные ответы; показано неумение самостоятельно анализировать факты, события, явления, процессы в их взаимосвязи и диалектическом развитии.

- неудовлетворительно – выставляется обучающемуся, если не выполнены требования, соответствующие оценке “удовлетворительно”.

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

3.1. Вопросы для проведения опроса:

1. Основные понятия ИБ.
2. Информация, защищаемая информация, ценность информации, уровень секретности.
3. Объекты защиты информации.
4. Угрозы безопасности информации, основные понятия: безопасность, конфиденциальность, целостность, доступность, утечка информации; несанкционированный доступ к информации.
5. Классификация угроз безопасности: каналы утечки, воздействия.
6. Прямые и косвенные каналы утечки данных.
7. Модель потенциального нарушителя.
8. Способы мошенничества в информационных системах.
9. Основные способы реализации угроз ИБ.
10. Основные понятия теории ИБ.
11. Принципы организации систем обеспечения безопасности данных.
12. Требования, предъявляемые к системам обеспечения безопасности данных.
13. Понятие мониторов безопасности.
14. Физические средства защиты информации
15. Понятие политики безопасности.
16. Дискреционные политики безопасности.
17. Мандатные политики безопасности
18. Модель безопасности информационных потоков.
19. Показатели эффективности систем защиты информации.
20. Способы оценки эффективности систем защиты информации.
21. Руководящие документы Гостехкомиссии в сфере обеспечения ИБ.
22. Основные понятия теории ИБ.
23. Принципы организации систем обеспечения безопасности данных.

24. Требования, предъявляемые к системам обеспечения безопасности данных.

25. Понятие мониторов безопасности.

26. Физические средства защиты информации

27. Руководящие документы Гостехкомиссии в сфере обеспечения ИБ.

28. «Общие критерии». Структура. Основные понятия.

29. Программно-технические средства обеспечения ИБ.

30. Межсетевые экраны.

31. Типы компьютерных вирусов.

32. Методы борьбы с компьютерными вирусами.

33. Федеральный стандарт США на шифрование данных (стандарт DES).

34. Отечественный стандарт на шифрование данных.

35. Шифрование с открытым ключом, алгоритм RSA.

36. Понятие, назначение и основные функции защищённой виртуальной сети.

37. Средства построения защищённой виртуальной сети. Туннелирование в протоколах различных уровней.

3.2. Примерный перечень тем докладов и сообщений:

1. Причины, виды и каналы утечки информации.
2. Основные понятия ИБ. Основные составляющие.
3. Распространение объектно-ориентированного подхода на информационную безопасность.
4. Несанкционированный доступ, целостность, доступность и конфиденциальность информации.
5. Основные угрозы ИБ.
6. Классификации угроз по возможным последствиям (угрозы целостности, доступности и конфиденциальности), по непосредственному источнику угроз и его расположению, по расположению информации, подвергаемой угрозе и др.
7. Основные способы реализации угроз.
8. Наиболее распространенные угрозы доступности.
9. Вредоносное программное обеспечение.
10. Основные угрозы целостности.
11. Основные угрозы конфиденциальности.
12. Основные понятия (субъект, объект, информационный поток, монитор безопасности, политика безопасности).
13. Аксиомы и следствия.
14. Основные политики и модели безопасности: дискреционного доступа, мандатного доступа (Белла-Лападула), безопасности информационных потоков.
15. Показатели эффективности систем защиты информации.

16. Способы оценки эффективности (комплексная оценка, агрегирование показателей, использование моделирования).

17. Нормативные руководящие документы в сфере обеспечения ИБ.

18. Обзор российского законодательства в области информационной безопасности.

19. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности

20. Гармонизированные критерии Европейских стран.

21. Интерпретация "Оранжевой книги" для сетевых конфигураций.

22. Штатные средства ОС для обеспечения ИБ.

23. Административные меры. Политика безопасности. Программа безопасности. Синхронизация программы безопасности с жизненным циклом систем.

24. Управление рисками.

25. Процедурные меры. Основные классы мер процедурного уровня. Управление персоналом, физическая защита, поддержание работоспособности, реагирование на нарушения режима безопасности. Планирование восстановительных работ.

26. Программно-технические меры средств обеспечения ИБ. Идентификация и аутентификация, управление доступом, протоколирование и аудит, шифрование, контроль целостности.

27. Защищённые СУБД. Технические средства противодействия утечке информации. Анализ защищенности.

28. Назначение, расположение и основные функции. Требования к различным классам защищённости межсетевых экранов.

29. История проблемы. Классификация и характеристика основных типов вирусов. Способы борьбы. Антивирусные пакеты AVP, Dr.Web, Norton AntiVirus.

30. Виды шифрования в каналах связи. Стандарты шифрования (DES и ГОСТ 28147-89). Шифрование паролей в Unix-системах. Реализации цифровой подписи.

31. Понятие, назначение и основные функции защищённой виртуальной сети. Протоколы реализации. Туннелирование. Средства построения.

3.3. Вопросы для проведения зачета с оценкой:

1. Основные понятия ИБ.
2. Информация, защищаемая информация, ценность информации, уровень секретности.
3. Объекты защиты информации.

4. Угрозы безопасности информации, основные понятия: безопасность, конфиденциальность, целостность, доступность, утечка информации; несанкционированный доступ к информации.
5. Классификация угроз безопасности: каналы утечки, воздействия.
6. Прямые и косвенные каналы утечки данных.
7. Модель потенциального нарушителя.
8. Способы мошенничества в информационных системах.
9. Основные способы реализации угроз ИБ.
10. Основные понятия теории ИБ.
11. Принципы организации систем обеспечения безопасности данных.
12. Требования, предъявляемые к системам обеспечения безопасности данных.
13. Понятие мониторов безопасности.
14. Физические средства защиты информации
15. Понятие политики безопасности.
16. Дискреционные политики безопасности.
17. Мандатные политики безопасности
18. Модель безопасности информационных потоков.
19. Показатели эффективности систем защиты информации.
20. Способы оценки эффективности систем защиты информации.
21. Руководящие документы Гостехкомиссии в сфере обеспечения ИБ
22. Основные понятия теории ИБ.
23. Принципы организации систем обеспечения безопасности данных.
24. Требования, предъявляемые к системам обеспечения безопасности данных.
25. Понятие мониторов безопасности.
26. Физические средства защиты информации
27. Руководящие документы Гостехкомиссии в сфере обеспечения ИБ.
28. «Общие критерии». Структура. Основные понятия.
29. Программно-технические средства обеспечения ИБ.
30. Межсетевые экраны.
31. Типы компьютерных вирусов.
32. Методы борьбы с компьютерными вирусами.
33. Федеральный стандарт США на шифрование данных (стандарт
34. DES).
35. Отечественный стандарт на шифрование данных.
36. Шифрование с открытым ключом, алгоритм RSA.
37. Понятие, назначение и основные функции защищённой виртуальной сети.
38. Средства построения защищённой виртуальной сети. Туннелирование в протоколах различных уровней.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Зачет с оценкой 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.

Зачет с оценкой проводится по расписанию, сформированному учебно-методическим управлением, в сроки, предусмотренные календарным учебным графиком.

Зачет с оценкой принимается преподавателем, ведущим лекционные занятия.

Зачет с оценкой проводится только при предъявлении обучающимся зачетной книжки и при условии выполнения всех контрольных мероприятий, предусмотренных учебным планом и рабочей программой дисциплины.

Обучающимся на зачете с оценкой представляется право выбрать один из билетов. Время подготовки к ответу составляет 30 минут. По истечении установленного времени обучающийся должен ответить на вопросы билета.

Результаты зачета с оценкой 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 зачет с оценкой, экзамен в зачетно-экзаменационную ведомость делается отметка «неявка».

Обучающиеся, не прошедшие промежуточную аттестацию по дисциплине, должны ликвидировать академическую задолженность в установленном локальными нормативными актами Института порядке.

5. Материалы для компьютерного тестирования обучающихся в рамках проведения контроля наличия у обучающихся сформированных результатов обучения по дисциплине

Общие критерии оценивания

№ п/п	Процент правильных ответов	Оценка
1	86 % – 100 %	5 («отлично»)
2	70 % – 85 %	4 («хорошо»)
3	51 % – 69 %	3 («удовлетворительно»)
4	50 % и менее	2 («неудовлетворительно»)

Вариант 1

Номер вопроса и проверка сформированной компетенции

№	Код компетенции	№	Код компетенции

вопроса		вопроса	
1	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	11	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
2	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	12	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
3	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	13	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
4	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	14	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
5	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	15	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
6	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	16	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
7	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	17	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
8	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	18	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
9	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	19	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
10	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	20	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)

Ключ ответов

№ вопроса	Верный ответ	№ вопроса	Верный ответ
1	2	11	2
2	1	12	2
3	1	13	2
4	2	14	3
5	1	15	1
6	2	16	2
7	1	17	1
8	3	18	1
9	3	19	2
10	2	20	1

Задание № 1.

Программная система защиты информации отвечает за:

Ответ:
1. Сохранность всей введённой в информационную систему информации.
2.Реализацию заданной политики безопасности.
3. Корректное поведение пользователей.

Задание № 2.

Аутентификация это:

Ответ:
1. Подтверждение заявленного идентификатора.
2. Процесс ввода текста без отображения на экране.

3. Ввод сведений личного характера.

Задание № 3.

Политика безопасности это:

Ответ:

1.Правила определения разрешённых и запрещённых операций в информационной системе.

2. Правила поведения пользователей.

3. Инструкция действий администратора по обеспечению информационной безопасности.

Задание № 4.

Монитор безопасности это:

Ответ:

1. Личный терминал системного администратора.

2.Совокупность резидентных программ, реализующих политику безопасности.

3. Программа контроля данных аудита.

Задание № 5.

Дискреционная политика доступа:

Ответ:

1.Определяет права доступа идентифицированных субъектов к объектам на основе заданных внешних правил (матрицы доступа).

2. Определяет права доступа субъектов к объектам или разрешает информационные потоки между объектами на основе изменяемых меток прав доступа или конфиденциальности.

3. Является алгоритмом формирования матрицы доступа.

4. Содержит инструкцию для системного администратора по предоставлению прав доступа различным пользователям.

Задание № 6.

Мандатная политика доступа:

Ответ:

1. Определяет права доступа идентифицированных субъектов к объектам на основе заданных внешних правил (матрицы доступа).

2.Определяет права доступа субъектов к объектам или разрешает информационные потоки между объектами на основе изменяемых меток прав доступа субъектов и меток конфиденциальности объектов.

3. Является алгоритмом формирования матрицы доступа.

4. Содержит инструкцию для системного администратора по предоставлению прав доступа различным пользователям.

Задание № 7.

Компьютерным вирусом называется:

Ответ:
1.Программа, способная внедряться в другие программы, с возможностью самовоспроизводства.
2. Вид бактерий, разрушающий микросхемы.
3. Процесс разрушения информации на неисправном жёстком диске.

Задание № 8.

Что здесь не относится к антивирусным программам:

Ответ:
1. Dr. Web
2. AVP
3. Norton DiskDoktor

Задание № 9.

В системе стандартов «Общие критерии» требования не объединяются в:

Ответ:
1. Классы
2. Семейства
3.Группы

Задание № 10.

В документах Гостехкомиссии под показателями защищённости понимается:

Ответ:
1. Экспертная оценка системы защиты информации по пятибалльной шкале.
2.Перечень группы требований, необходимых для выполнения в информационных системах заданного класса защищённости.
3. Временные характеристики реакции системы безопасности на обнаружение несанкционированного доступа.

Задание № 11.

Качество системы информационной безопасности может быть оценено:

Ответ:
1. Запуском специальной тестовой программы.

2.На основе экспертного анализа различных показателей эффективности.
3. Количеством реализованных защитных функций, декларированных в документации.

Задание № 12.

Какое утверждение верно:

Ответ:
1. Последние версии антивирусных программ и регулярное обновление ОС гарантируют защиту от вирусов.
2.ОС с грамотно реализованной системой защиты от несанкционированного доступа лучше защищена от вирусных атак.
3. Защиту от вирусов гарантирует использование только лицензионного программного обеспечения.

Задание № 13.

Брандмауэр это:

Ответ:
1. Источник бесперебойного питания.
2.Межсетевой фильтр.
3. Программа просмотра Web-страниц.

Задание № 14.

Цифровая подпись это:

Ответ:
1. Ключевое слово или набор цифр в конце электронного документа, известное только отправителю и получателю.
2. Цифровое представление графического изображения персональной подписи человека.
3.Результат применения специальной функции к содержимому документа с ключом, известным только отправителю, и который можно проверить с помощью ключа, известного всем получателям.

Задание № 15.

Виртуальный защищённый канал строится:

Ответ:
1.Путём шифрации информации, проходящей через открытые глобальные сети.
2. Для передачи видео и аудио информации в привилегированном, защищённом от задержек и прерываний режиме.
3. Для имитации использования системы защиты информации с целью ввести в заблуждение возможного злоумышленника.

Задание № 16.

Программная система защиты информации отвечает за:

Ответ:
1. Сохранность всей введённой в информационную систему информации.
2.Реализацию заданной политики безопасности.
3. Корректное поведение пользователей.

Задание № 17.

Аутентификация это:

Ответ:
1.Подтверждение заявленного идентификатора.
2. Процесс ввода текста без отображения на экране.
3. Ввод сведений личного характера.

Задание № 18.

Политика безопасности это:

Ответ:
1.Правила определения разрешённых и запрещённых операций в информационной системе.
2. Правила поведения пользователей.
3. Инструкция действий администратора по обеспечению информационной безопасности.

Задание № 19.

Монитор безопасности это:

Ответ:
1. Личный терминал системного администратора.
2.Совокупность резидентных программ, реализующих политику безопасности.
3. Программа контроля данных аудита.

Задание № 20.

Дискреционная политика доступа:

Ответ:
1.Определяет права доступа идентифицированных субъектов к объектам на основе заданных внешних правил (матрицы доступа).

2. Определяет права доступа субъектов к объектам или разрешает информационные потоки между объектами на основе изменяемых меток прав доступа или конфиденциальности.
3. Является алгоритмом формирования матрицы доступа.
4. Содержит инструкцию для системного администратора по предоставлению прав доступа различным пользователям.

Вариант 2

Номер вопроса и проверка сформированной компетенции

№ вопроса	Код компетенции	№ вопроса	Код компетенции
1	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	11	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
2	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	12	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
3	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	13	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
4	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	14	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
5	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	15	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
6	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	16	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
7	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	17	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
8	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	18	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
9	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	19	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
10	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	20	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)

Ключ ответов

№ вопроса	Верный ответ	№ вопроса	Верный ответ
1	2	11	2
2	1	12	2
3	2	13	1
4	2	14	1
5	2	15	2
6	1	16	1
7	3	17	2
8	3	18	2
9	2	19	3
10	2	20	1

Задание № 1.

Мандатная политика доступа:

Ответ:
1. Определяет права доступа идентифицированных субъектов к объектам на основе заданных внешних правил (матрицы доступа).
2. Определяет права доступа субъектов к объектам или разрешает информационные потоки между объектами на основе изменяемых меток прав доступа субъектов и меток конфиденциальности объектов.
3. Является алгоритмом формирования матрицы доступа.
4. Содержит инструкцию для системного администратора по предоставлению прав доступа различным пользователям.

Задание № 2.

Компьютерным вирусом называется:

Ответ:
1.Программа, способная внедряться в другие программы, с возможностью самовоспроизводства.
2. Вид бактерий, разрушающий микросхемы.
3. Процесс разрушения информации на неисправном жёстком диске.

Задание № 3.

В документах Гостехкомиссии под показателями защищённости понимается:

Ответ:
1. Экспертная оценка системы защиты информации по пятибалльной шкале.
2.Перечень группы требований, необходимых для выполнения в информационных системах заданного класса защищённости.
3. Временные характеристики реакции системы безопасности на обнаружение несанкционированного доступа.

Задание № 4.

Качество системы информационной безопасности может быть оценено:

Ответ:
1. Запуском специальной тестовой программы.
2.На основе экспертного анализа различных показателей эффективности.
3. Количеством реализованных защитных функций, декларированных в документации.

Задание № 5.

Какое утверждение верно:

Ответ:
1. Последние версии антивирусных программ и регулярное обновление ОС гарантируют защиту от вирусов.
2.ОС с грамотно реализованной системой защиты от несанкционированного доступа лучше защищена от вирусных атак.
3. Защиту от вирусов гарантирует использование только лицензионного программного обеспечения.

Задание № 6.

Компьютерным вирусом называется:

Ответ:
1.Программа, способная внедряться в другие программы, с возможностью самовоспроизводства.
2. Вид бактерий, разрушающий микросхемы.
3. Процесс разрушения информации на неисправном жёстком диске.

Задание № 7.

Что здесь не относится к антивирусным программам:

Ответ:
1. Dr. Web
2. AVP
3.Norton DiskDoktor

Задание № 8.

В системе стандартов «Общие критерии» требования не объединяются в:

Ответ:
1. Классы
2. Семейства
3.Группы

Задание № 9.

В документах Гостехкомиссии под показателями защищённости понимается:

Ответ:
1. Экспертная оценка системы защиты информации по пятибалльной шкале.
2.Перечень группы требований, необходимых для выполнения в информационных системах заданного класса защищённости.
3. Временные характеристики реакции системы безопасности на обнаружение несанкционированного доступа.

Задание № 10.

Качество системы информационной безопасности может быть оценено:

Ответ:
1. Запуском специальной тестовой программы.
2.На основе экспертного анализа различных показателей эффективности.
3. Количеством реализованных защитных функций, декларированных в документации.

Задание № 11.

Какое утверждение верно:

Ответ:
1. Последние версии антивирусных программ и регулярное обновление ОС гарантируют защиту от вирусов.
2.ОС с грамотно реализованной системой защиты от несанкционированного доступа лучше защищена от вирусных атак.
3. Защиту от вирусов гарантирует использование только лицензионного программного обеспечения.

Задание № 12.

Программная система защиты информации отвечает за:

Ответ:
1. Сохранность всей введённой в информационную систему информации.
2.Реализацию заданной политики безопасности.
3. Корректное поведение пользователей.

Задание № 13.

Аутентификация это:

Ответ:
1.Подтверждение заявленного идентификатора.
2. Процесс ввода текста без отображения на экране.
3. Ввод сведений личного характера.

Задание № 14.

Политика безопасности это:

Ответ:
1.Правила определения разрешённых и запрещённых операций в информационной системе.
2. Правила поведения пользователей.
3. Инструкция действий администратора по обеспечению информационной безопасности.

Задание № 15.
Монитор безопасности это:

Ответ:
1. Личный терминал системного администратора.
2.Совокупность резидентных программ, реализующих политику безопасности.
3. Программа контроля данных аудита.

Задание № 16.
Дискреционная политика доступа:

Ответ:
1.Определяет права доступа идентифицированных субъектов к объектам на основе заданных внешних правил (матрицы доступа).
2. Определяет права доступа субъектов к объектам или разрешает информационные потоки между объектами на основе изменяемых меток прав доступа или конфиденциальности.
3. Является алгоритмом формирования матрицы доступа.
4. Содержит инструкцию для системного администратора по предоставлению прав доступа различным пользователям.

Задание № 17.
Мандатная политика доступа:

Ответ:
1. Определяет права доступа идентифицированных субъектов к объектам на основе заданных внешних правил (матрицы доступа).
2.Определяет права доступа субъектов к объектам или разрешает информационные потоки между объектами на основе изменяемых меток прав доступа субъектов и меток конфиденциальности объектов.
3. Является алгоритмом формирования матрицы доступа.
4. Содержит инструкцию для системного администратора по предоставлению прав доступа различным пользователям.

Задание № 18.
Брандмауэр это:

Ответ:
1. Источник бесперебойного питания.
2.Межсетевой фильтр.
3. Программа просмотра Web-страниц.

Задание № 19.

Цифровая подпись это:

Ответ:
1. Ключевое слово или набор цифр в конце электронного документа, известное только отправителю и получателю.
2. Цифровое представление графического изображения персональной подписи человека.
3.Результат применения специальной функции к содержимому документа с ключом, известным только отправителю, и который можно проверить с помощью ключа, известного всем получателям.

Задание № 20.

Виртуальный защищённый канал строится:

Ответ:
1.Путём шифрации информации, проходящей через открытые глобальные сети.
2. Для передачи видео и аудио информации в привилегированном, защищённом от задержек и прерываний режиме.
3. Для имитации использования системы защиты информации с целью ввести в заблуждение возможного злоумышленника.

Вариант 3

Номер вопроса и проверка сформированной компетенции

№ вопроса	Код компетенции	№ вопроса	Код компетенции
1	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	11	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
2	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	12	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
3	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	13	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
4	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	14	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
5	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	15	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
6	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	16	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
7	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	17	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
8	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	18	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
9	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	19	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
10	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	20	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)

Ключ ответов

№ вопроса	Верный ответ	№ вопроса	Верный ответ
1	2	11	2
2	1	12	2
3	1	13	2
4	2	14	2
5	1	15	1
6	2	16	1
7	1	17	2
8	2	18	1
9	2	19	2
10	2	20	2

Задание № 1.

Программная система защиты информации отвечает за:

Ответ:
1. Сохранность всей введённой в информационную систему информации.
2.Реализацию заданной политики безопасности.
3. Корректное поведение пользователей.

Задание № 2.

Аутентификация это:

Ответ:
1.Подтверждение заявленного идентификатора.
2. Процесс ввода текста без отображения на экране.
3. Ввод сведений личного характера.

Задание № 3.

Политика безопасности это:

Ответ:
1.Правила определения разрешённых и запрещённых операций в информационной системе.
2. Правила поведения пользователей.
3. Инструкция действий администратора по обеспечению информационной безопасности.

Задание № 4.

Монитор безопасности это:

Ответ:
1. Личный терминал системного администратора.
2.Совокупность резидентных программ, реализующих политику безопасности.
3. Программа контроля данных аудита.

Задание № 5.

Дискреционная политика доступа:

Ответ:
1.Определяет права доступа идентифицированных субъектов к объектам на основе заданных внешних правил (матрицы доступа).
2. Определяет права доступа субъектов к объектам или разрешает информационные потоки между объектами на основе изменяемых меток прав доступа или конфиденциальности.
3. Является алгоритмом формирования матрицы доступа.
4. Содержит инструкцию для системного администратора по предоставлению прав доступа различным пользователям.

Задание № 6.

Мандатная политика доступа:

Ответ:
1. Определяет права доступа идентифицированных субъектов к объектам на основе заданных внешних правил (матрицы доступа).
2.Определяет права доступа субъектов к объектам или разрешает информационные потоки между объектами на основе изменяемых меток прав доступа субъектов и меток конфиденциальности объектов.
3. Является алгоритмом формирования матрицы доступа.
4. Содержит инструкцию для системного администратора по предоставлению прав доступа различным пользователям.

Задание № 7.

Компьютерным вирусом называется:

Ответ:
1.Программа, способная внедряться в другие программы, с возможностью самовоспроизводства.
2. Вид бактерий, разрушающий микросхемы.
3. Процесс разрушения информации на неисправном жёстком диске.

Задание № 8.

В документах Гостехкомиссии под показателями защищённости понимается:

Ответ:
1. Экспертная оценка системы защиты информации по пятибалльной шкале.
2.Перечень группы требований, необходимых для выполнения в информационных системах заданного класса защищённости.
3. Временные характеристики реакции системы безопасности на обнаружение несанкционированного доступа.

Задание № 9.

Качество системы информационной безопасности может быть оценено:

Ответ:
1. Запуском специальной тестовой программы.
2.На основе экспертного анализа различных показателей эффективности.
3. Количеством реализованных защитных функций, декларированных в документации.

Задание № 10.

Какое утверждение верно:

Ответ:
1. Последние версии антивирусных программ и регулярное обновление ОС гарантируют защиту от вирусов.
2.ОС с грамотно реализованной системой защиты от несанкционированного доступа лучше защищена от вирусных атак.
3. Защиту от вирусов гарантирует использование только лицензионного программного обеспечения.

Задание № 11.

В документах Гостехкомиссии под показателями защищённости понимается:

Ответ:
1. Экспертная оценка системы защиты информации по пятибалльной шкале.
2.Перечень группы требований, необходимых для выполнения в информационных системах заданного класса защищённости.
3. Временные характеристики реакции системы безопасности на обнаружение несанкционированного доступа.

Задание № 12.

Качество системы информационной безопасности может быть оценено:

Ответ:
1. Запуском специальной тестовой программы.
2.На основе экспертного анализа различных показателей эффективности.
3. Количеством реализованных защитных функций, декларированных в документации.

Задание № 13.

Какое утверждение верно:

Ответ:
1. Последние версии антивирусных программ и регулярное обновление ОС гарантируют защиту от вирусов.
2.ОС с грамотно реализованной системой защиты от несанкционированного доступа лучше защищена от вирусных атак.
3. Защиту от вирусов гарантирует использование только лицензионного программного обеспечения.

Задание № 14.

Программная система защиты информации отвечает за:

Ответ:
1. Сохранность всей введённой в информационную систему информации.
2.Реализацию заданной политики безопасности.
3. Корректное поведение пользователей.

Задание № 15.

Аутентификация это:

Ответ:
1.Подтверждение заявленного идентификатора.
2. Процесс ввода текста без отображения на экране.
3. Ввод сведений личного характера.

Задание № 16.

Политика безопасности это:

Ответ:
1.Правила определения разрешённых и запрещённых операций в информационной системе.
2. Правила поведения пользователей.
3. Инструкция действий администратора по обеспечению информационной безопасности.

Задание № 17.

Монитор безопасности это:

Ответ:
1. Личный терминал системного администратора.
2.Совокупность резидентных программ, реализующих политику безопасности.
3. Программа контроля данных аудита.

Задание № 18.

Дискреционная политика доступа:

Ответ:
1.Определяет права доступа идентифицированных субъектов к объектам на основе заданных внешних правил (матрицы доступа).
2. Определяет права доступа субъектов к объектам или разрешает информационные потоки между объектами на основе изменяемых меток прав доступа или конфиденциальности.

3. Является алгоритмом формирования матрицы доступа.
4. Содержит инструкцию для системного администратора по предоставлению прав доступа различным пользователям.

Задание № 19.

Мандатная политика доступа:

Ответ:
1. Определяет права доступа идентифицированных субъектов к объектам на основе заданных внешних правил (матрицы доступа).
2.Определяет права доступа субъектов к объектам или разрешает информационные потоки между объектами на основе изменяемых меток прав доступа субъектов и меток конфиденциальности объектов.
3. Является алгоритмом формирования матрицы доступа.
4. Содержит инструкцию для системного администратора по предоставлению прав доступа различным пользователям.

Задание № 20.

Брандмауэр это:

Ответ:
1. Источник бесперебойного питания.
2.Межсетевой фильтр.
3. Программа просмотра Web-страниц.

Вариант 4

Номер вопроса и проверка сформированной компетенции

№ вопроса	Код компетенции	№ вопроса	Код компетенции
1	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	11	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
2	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	12	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
3	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	13	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
4	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	14	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
5	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	15	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
6	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	16	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
7	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	17	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
8	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	18	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)
9	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	19	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)

10	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)	20	ОПК-7 (ИОПК 7.1 ИОПК 7.2.)

Ключ ответов

№ вопроса	Верный ответ	№ вопроса	Верный ответ
1	3	11	2
2	1	12	2
3	2	13	1
4	1	14	3
5	1	15	3
6	2	16	1
7	1	17	2
8	2	18	1
9	1	19	2
10	2	20	2

Задание № 1.

Цифровая подпись это:

Ответ:
1. Ключевое слово или набор цифр в конце электронного документа, известное только отправителю и получателю.
2. Цифровое представление графического изображения персональной подписи человека.
3.Результат применения специальной функции к содержимому документа с ключом, известным только отправителю, и который можно проверить с помощью ключа, известного всем получателям.

Задание № 2.

Виртуальный защищённый канал строится:

Ответ:
1.Путём шифрации информации, проходящей через открытые глобальные сети.
2. Для передачи видео и аудио информации в привилегированном, защищённом от задержек и прерываний режиме.
3. Для имитации использования системы защиты информации с целью ввести в заблуждение возможного злоумышленника.

Задание № 3.

Программная система защиты информации отвечает за:

Ответ:
1. Сохранность всей введённой в информационную систему информации.
2.Реализацию заданной политики безопасности.
3. Корректное поведение пользователей.

Задание № 4.
Аутентификация это:

Ответ:
1.Подтверждение заявленного идентификатора.
2. Процесс ввода текста без отображения на экране.
3. Ввод сведений личного характера.

Задание № 5.
Политика безопасности это:

Ответ:
1.Правила определения разрешённых и запрещённых операций в информационной системе.
2. Правила поведения пользователей.
3. Инструкция действий администратора по обеспечению информационной безопасности.

Задание № 6.
Монитор безопасности это:

Ответ:
1. Личный терминал системного администратора.
2.Совокупность резидентных программ, реализующих политику безопасности.
3. Программа контроля данных аудита.

Задание № 7.
Дискреционная политика доступа:

Ответ:
1.Определяет права доступа идентифицированных субъектов к объектам на основе заданных внешних правил (матрицы доступа).
2. Определяет права доступа субъектов к объектам или разрешает информационные потоки между объектами на основе изменяемых меток прав доступа или конфиденциальности.
3. Является алгоритмом формирования матрицы доступа.
4. Содержит инструкцию для системного администратора по предоставлению прав доступа различным пользователям.

Задание № 8.

Мандатная политика доступа:

Ответ:
1. Определяет права доступа идентифицированных субъектов к объектам на основе заданных внешних правил (матрицы доступа).
2.Определяет права доступа субъектов к объектам или разрешает информационные потоки между объектами на основе изменяемых меток прав доступа субъектов и меток конфиденциальности объектов.
3. Является алгоритмом формирования матрицы доступа.
4. Содержит инструкцию для системного администратора по предоставлению прав доступа различным пользователям.

Задание № 9.

Компьютерным вирусом называется:

Ответ:
1.Программа, способная внедряться в другие программы, с возможностью самовоспроизводства.
2. Вид бактерий, разрушающий микросхемы.
3. Процесс разрушения информации на неисправном жёстком диске.

Задание № 10.

В документах Гостехкомиссии под показателями защищённости понимается:

Ответ:
1. Экспертная оценка системы защиты информации по пятибалльной шкале.
2.Перечень группы требований, необходимых для выполнения в информационных системах заданного класса защищённости.
3. Временные характеристики реакции системы безопасности на обнаружение несанкционированного доступа.

Задание № 11.

Качество системы информационной безопасности может быть оценено:

Ответ:
1. Запуском специальной тестовой программы.
2.На основе экспертного анализа различных показателей эффективности.
3. Количеством реализованных защитных функций, декларированных в документации.

Задание № 12.

Какое утверждение верно:

Ответ:
1. Последние версии антивирусных программ и регулярное обновление ОС гарантируют защиту от вирусов.
2.ОС с грамотно реализованной системой защиты от несанкционированного доступа лучше защищена от вирусных атак.
3. Защиту от вирусов гарантирует использование только лицензионного программного обеспечения.

Задание № 13.

Компьютерным вирусом называется:

Ответ:
1.Программа, способная внедряться в другие программы, с возможностью самовоспроизводства.
2. Вид бактерий, разрушающий микросхемы.
3. Процесс разрушения информации на неисправном жёстком диске.

Задание № 14.

Что здесь не относится к антивирусным программам:

Ответ:
1. Dr. Web
2. AVP
3.Norton DiskDoktor

Задание № 15.

В системе стандартов «Общие критерии» требования не объединяются в:

Ответ:
1. Классы
2. Семейства
3.Группы

Задание № 16.

Политика безопасности это:

Ответ:
1.Правила определения разрешённых и запрещённых операций в информационной системе.
2. Правила поведения пользователей.
3. Инструкция действий администратора по обеспечению информационной безопасности.

Задание № 17.

Монитор безопасности это:

Ответ:
1. Личный терминал системного администратора.
2.Совокупность резидентных программ, реализующих политику безопасности.
3. Программа контроля данных аудита.

Задание № 18.

Дискреционная политика доступа:

Ответ:
1.Определяет права доступа идентифицированных субъектов к объектам на основе заданных внешних правил (матрицы доступа).
2. Определяет права доступа субъектов к объектам или разрешает информационные потоки между объектами на основе изменяемых меток прав доступа или конфиденциальности.
3. Является алгоритмом формирования матрицы доступа.
4. Содержит инструкцию для системного администратора по предоставлению прав доступа различным пользователям.

Задание № 19.

Мандатная политика доступа:

Ответ:
1. Определяет права доступа идентифицированных субъектов к объектам на основе заданных внешних правил (матрицы доступа).
2.Определяет права доступа субъектов к объектам или разрешает информационные потоки между объектами на основе изменяемых меток прав доступа субъектов и меток конфиденциальности объектов.
3. Является алгоритмом формирования матрицы доступа.
4. Содержит инструкцию для системного администратора по предоставлению прав доступа различным пользователям.

Задание № 20.

В документах Гостехкомиссии под показателями защищённости понимается:

Ответ:
1. Экспертная оценка системы защиты информации по пятибалльной шкале.
2.Перечень группы требований, необходимых для выполнения в информационных системах заданного класса защищённости.

3. Временные характеристики реакции системы безопасности на обнаружение несанкционированного доступа.

6. Практические задачи.

Задача 1.

Решение вспомогательных задач для усвоения теоретических основ ИБ. Диагностика и настройка персонального компьютера

Задания:

1. Настройка средств ввода-вывода операционной системы Windows.
2. Настройка элементов управления Windows.
3. Резервное копирование данных.
4. Проверка жесткого диска.

Задача 2.

Формирование требований к системам защиты информации в виде профилей защиты в рамках идеологии «Общих критериев».

Задания

1. Сформулируйте интересы государства, общества и личности в информационной сфере
2. Чем определяется ценность информации для владельца ?
3. В чем заключается комплексное обеспечение ИБ РФ?
4. Каковы основные методы и средства защиты процессов переработки информации в защищенных КС?
5. Назовите основные принципы процессов переработки информации.
6. Назовите основные виды угроз.

Задача 3.

Ознакомление со штатными средствами ОС по обеспечению информационной безопасности на примере WINDOWS NT(XP).

Задания:

1. Создание и установка прав доступа пользователей.
2. Установка прав доступа к объектам

Задача 4.

Защита документа в Microsoft Word. Восстановление текста поврежденного документ. Изучить возможности ограничения изменений в документе:

Задания:

1. Установить в документе пароль для открытия документа, руководствуясь правилами, описанными в работе.

2. Установить в документе пароль разрешения записи.

3. Установить режим: Рекомендовать доступ только для чтения.

4 .Проверить не содержит ли документ скрытых данных.

5. Изменить интервал времени автоматического сохранения документов.

6. Установить режим сохранения резервной копии документа.

Задача 5.

Защита документа в Microsoft Excel. Изучить возможности ограничения просмотра и изменения пользователями данных в электронных таблицах.

Задания:

1. Установить пароль для открытия книги.

2. Установить пароль для разрешения записи.

3. Установить защиту ячеек.

3. Открыть несколько книг, скрыть одну из них.

4. Отобразить скрытую книгу

3. Скрыть лист.

4. Скрыть изображение столбца.

5. Отобразить скрытый столбец.

5. Скрыть изображение строки.

6. Отобразить скрытую строку.

Задача 6.

Работа с реестром ОС. Изучить основные принципы работы с реестром, освоить редактор реестра, научиться создавать резервные копии как реестра целиком, так и его отдельных ключей

Задания:

1. Сохранить значение всей ветви HKEY_CLASSES_ROOT.

2. В ключе HKEY_CLASSES_ROOT найти ветвь lnkfile. Одним из ее параметров является IsShortcut. Удалите его. Аналогичную процедуру повторите с ветвью piffile. Перезагрузите компьютер. Обратите внимание, что исчезли все стрелки с ярлыков программ.

3. Восстановить значение ветви HKEY_CLASSES_ROOT.

4. Создать резервную копию файла реестра.

5. Откройте ключ реестра HKEY_CURRENT_USER, а затем его подключите \ControlPanel\Desktop. Добавьте к открытому ключу новое строковое значение с именем MenuShowDelay. Дважды щелкните мышью, указав на это значение и введите число 1. Затем перезагрузите систему. Теперь меню, запрашиваемые с панели задач, будут появляться гораздо быстрее.

6. Восстановите реестр с резервной копии.

7. С помощью программы Microsoft Backup создать копию реестра, а затем по этой копии восстановить реестр.

8. Перезагрузите систему и убедитесь, что она функционирует нормально.

Задача 7.

Использование архиваторов для защиты информации.

Задания:

1. Выделить группы архивируемых файлов в WinRAR.
2. Создать различных типов архивов в WinRAR и работа с ними.
3. Выполнить шифрование информации в WinRAR.

Задача 8.

Изучение основных принципов уничтожения и восстановления информации на магнитных дисках, знакомство с используемыми утилитами , входящими в пакет Norton Utilities.

Задания:

1. Написать командный файл, при запуске которого произойдет затирание файлов с расширением BAK на жестком диске C. Использовать программу WipeInfo.
2. Удалить на жестком диске несколько файлов, а затем попытаться с помощью программы UnErase восстановить их. Поэкспериментировать для случая, когда файлы удаляются вместе с подкаталогами, содержащими их.
3. Проверить жесткий диск и дискету на наличие сбоев с помощью программы Norton Disk Doctor. Создать ситуацию, когда на дискете могут появиться потерянные кластеры и исправить их.

Задача 9.

Защита информации с помощью антивирусных програмных средств. Использование электронной цифровой подписи.

Задания:

1. Изучить настройки программы Doctor Web.
2. Провести тестирование системных областей жесткого диска и нескольких подкаталогов.
3. Проверить дискету на наличие вирусов.

Задача 10.

Защита информации с помощью шифрования данных, программы PGP (создание электронной цифровой подписи). Освоение работы с механизмами шифрования данных и электронной подписи

Задания:

Шифрование информационных массивов методами битовых манипуляций, подстановки, перестановки, замены.