Министерство науки и высшего образования Российской Федерации

Муромский институт (филиал)

федерального государственного бюджетного образовательного учреждения высшего образования

«Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»

(МИ ВлГУ)

Кафедра *ИС*

«УТВЕРЖДАЮ»
Заместитель директора по УР
_____Д.Е. Андрианов
16.06.2020

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность и защита информации

Направление подготовки *09.03.02 Информационные системы и технологии*

Профиль подготовки *Информационные системы и технологии*

Семестр	Трудоемкость, час./зач. ед.	Лекции, час.	Практические занятия, час.	Лабораторные работы, час.	Консультация, час.	Контроль, час.	Всего (контактная работа), час.	СРС, час.	Форма промежуточного контроля (экз., зач., зач. с оц.)
7	**144 / 4**	**16**		**32**	**3,6**	**0,35**	**51,95**	**56,4**	**Экз.(35,65)**
Итого	**144 / 4**	**16**		**32**	**3,6**	**0,35**	**51,95**	**56,4**	**35,65**

Муром, 2020 г.

1. Цель освоения дисциплины

Цель дисциплины: обучить студентов основным принципам защиты информации, дать навыки построения систем защиты.

Задачи дисциплины:

- обеспечить студентами основных задач в рамках общей проблемы обеспечения информационной безопасности в организации, решаемых организационно-правовыми, техническими и программно-аппаратными средствами защиты информации;
- изучить нормативные и методические материалы по методам, способам и средствам обеспечения информационной безопасности телекоммуникационных систем;
- изучить возможности современных технических и программно-аппаратных средств защиты информации;
- научиться использовать современные пакеты прикладных программ для решения типовых задач, связанных с анализом и синтезом элементов защищенных телекоммуникационных систем;
- научиться практически решать задачи защиты программ и данных;
- научиться применять современный подход к обеспечению информационной безопасности телекоммуникационных систем.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Информационная безопасность и защита информации» — наука, изучающая все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчётности, аутентичности и достоверности информации или средств её обработки; обеспечивает понимание основ защиты информации в информационных системах и сетях. Курс базируется на знаниях, полученных студентами в процессе изучения дисциплин «Информационные технологии», «Управление данными», "Основы теории алгоритмов". Углубление и расширение вопросов, изложенных в данном курсе, будет осуществляться при написании студентами бакалаврских работ.

3. Планируемые результаты обучения по дисциплине

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОПОП (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	Планируемые результаты обучения по дисциплине, в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения компетенции	Результаты обучения по дисциплине	
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 Подготавливает обзоры, аннотации, библиографические ссылки, составляет рефераты и подготавливает публикации с использованием библиотечных каталогов и информации из сети Интернет	Знает основы составления рефератов и подготовки публикаций с использованием библиотечных каталогов и информации из сети Интернет (ОПК-3.1)	тест
	ОПК-3.2 Применяет знания приемов безопасной работы в сети Интернет при поиске информации, связанной с профессиональной деятельностью	Умеет применять знания о приемах безопасной работы в сети Интернет при поиске информации, связанной с профессиональной деятельностью (ОПК-3.2)	

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 часа.

4.1. Форма обучения: очная

Уровень базового образования: среднее общее.
Срок обучения 4г.

4.1.1. Структура дисциплины

№ п\п	Раздел (тема) дисциплины	Семестр	Контактная работа обучающихся с педагогическим работником							Самостоятельная работа	Форма текущего контроля успеваемости (по неделям семестра), форма промежуточной аттестации(по семестрам)
			Лекции	Практические занятия	Лабораторные работы	Контрольные работы	КП / КР	Консультация	Контроль		
1	Введение. Основы информационной безопасности	7	2		4					2	тестирование
2	Принципы криптографической защиты информации	7	2		4					4	тестирование
3	Современные симметричные криптосистемы	7	2		4						тестирование
4	Асимметричные криптосистемы	7	2							2	тестирование
5	Идентификация и проверка подлинности	7	2		4					12	тестирование
6	Электронная цифровая подпись	7	2		16					13	тестирование
7	Управление криптографическими ключами	7	2							9	тестирование
8	Резервное хранение информации. RAID-массивы	7	2							14,4	тестирование
Всего за семестр		144	16		32			3,6	0,35	56,4	Экз.(35,65)
Итого		144	16		32			3,6	0,35	56,4	35,65

4.1.2. Содержание дисциплины

4.1.2.1. Перечень лекций

Семестр 7

Раздел 1. Введение. Основы информационной безопасности

Лекция 1.

Традиционные симметричные криптосистемы (2 часа).

Раздел 2. Принципы криптографической защиты информации

Лекция 2.

Шифры простой замены. Шифры сложной замены. Шифрование методом гаммирования (2 часа).

Раздел 3. Современные симметричные криптосистемы

Лекция 3.

Американский стандарт шифрования данных DES (2 часа).

Раздел 4. Асимметричные криптосистемы

Лекция 4.

Алгоритм шифрования данных IDEA. Отечественный стандарт шифрования (2 часа).

Раздел 5. Идентификация и проверка подлинности

Лекция 5.

Асимметричные криптосистемы (2 часа).

Раздел 6. Электронная цифровая подпись

Лекция 6.

Идентификация и проверка подлинности (2 часа).

Раздел 7. Управление криптографическими ключами

Лекция 7.

Электронная цифровая подпись (2 часа).

Раздел 8. Резервное хранение информации. RAID-массивы

Лекция 8.

Резервное хранение информации. RAID-массивы (2 часа).

4.1.2.2. Перечень практических занятий

Не планируется.

4.1.2.3. Перечень лабораторных работ

Семестр 7

Раздел 1. Введение. Основы информационной безопасности

Лабораторная 1.

Реализация дискреционной политики безопасности (4 часа).

Раздел 2. Принципы криптографической защиты информации

Лабораторная 2.

Простейшие методы криптографического преобразования информации (4 часа).

Раздел 3. Современные симметричные криптосистемы

Лабораторная 3.

Аддитивные методы криптографического преобразования информации (4 часа).

Раздел 5. Идентификация и проверка подлинности

Лабораторная 4.

Асимметричные схемы шифрования данных (4 часа).

Раздел 6. Электронная цифровая подпись

Лабораторная 5.

Защита программного комплекса от несанкционированного доступа методом подсчета контрольных сумм (4 часа).

Лабораторная 6.

Определение показателей защищенности информации при несанкционированном доступе (4 часа).

Лабораторная 7.

Цифровая подпись (4 часа).

Лабораторная 8.

Методы определения хэш-функций (4 часа).

4.1.2.4. Перечень тем и учебно-методическое обеспечение самостоятельной работы

Перечень тем, вынесенных на самостоятельное изучение:

1. Виды криптоаналитических атак.
2. Система омофонов.
3. Одноразовая система шифрования.
4. Сравнение симметричных и ассиметричных систем.
5. Взаимная проверка подлинности пользователей. Механизм запроса-ответа.
6. Взаимная проверка подлинности пользователей. Механизм отметки времени.
7. Модель рукопожатия.
8. Отечественный стандарт цифровой подписи.
9. Аутентификация мастер-ключа хост-компьютера.
10. Схема защиты сеансового ключа.
11. Алгоритм Диффи-Хеллмана.
12. Основные схемы сетевой защиты на базе межсетевых экранов. Межсетевой экран - экранированная подсеть.
13. Правовые аспекты компьютерной безопасности.
14. Вредоносные программы.
15. Безопасность платежных систем.
16. Теоретическая оценка безопасности информации.
17. Конституция РФ. Доктрина информационной безопасности России. Кодексы РФ. Законы РФ. ГОСТы. Руководящие документы (РД).

Для самостоятельной работы используются методические указания по освоению дисциплины и издания из списка приведенной ниже основной и дополнительной литературы.

4.1.2.5. Перечень тем контрольных работ, рефератов, ТР, РГР, РПР

Не планируется.

4.1.2.6. Примерный перечень тем курсовых работ (проектов)

Не планируется.

4.2 Форма обучения: заочная

Уровень базового образования: среднее профессиональное.
Срок обучения 3г 6м.

Семестр	Трудоемкость, час./ зач. ед.	Лекции, час.	Практические занятия, час.	Лабораторные работы, час.	Консультация, час.	Контроль,час.	Всего (контактная работа), час.	СРС, час.	Переаттестация	Форма промежуточного контроля (экз., зач., зач. с оц.)
7	**144 / 4**	**10**	**10**	**8**	**5**	**0,6**	**33,6**	**65,75**	**36**	**Экз.(8,65)**
Итого	**144 / 4**	**10**	**10**	**8**	**5**	**0,6**	**33,6**	**65,75**	**36**	**8,65**

4.2.1. Структура дисциплины

№ п\п	Раздел (тема) дисциплины	Семестр	Контактная работа обучающихся с педагогическим работником							Самостоятельная работа	Форма текущего контроля успеваемости (по неделям семестра), форма промежуточной аттестации(по семестрам)
			Лекции	Практические занятия	Лабораторные работы	Контрольные работы	КП / КР	Консультация	Контроль		
1	Введение. Основы информационной безопасности	7	2		4					19	тестирование
2	Принципы криптографической защиты информации	7	2		4					32	тестирование
3	Современные симметричные криптосистемы	7	2	2						0	тестирование
4	Асимметричные криптосистемы	7	2	2						0	тестирование
5	Идентификация и проверка подлинности	7	2	2						0	тестирование
6	Электронная цифровая подпись	7		2						5	тестирование
7	Управление криптографическими ключами	7		2						4	тестирование
8	Резервное хранение	7								5,75	тестирование

	информации. RAID-массивы										
Всего за семестр		108	10	10	8	+		5	0,6	65,75	Экз.(8,65)
Итого		108	10	10	8			5	0,6	65,75	8,65
Итого с переаттестацией		144									

4.2.2. Содержание дисциплины

4.2.2.1. Перечень лекций

Семестр 7

Раздел 1. Введение. Основы информационной безопасности

Лекция 1.

Традиционные симметричные криптосистемы (2 часа).

Раздел 2. Принципы криптографической защиты информации

Лекция 2.

Шифры простой замены. Шифры сложной замены. Шифрование методом гаммирования (2 часа).

Раздел 3. Современные симметричные криптосистемы

Лекция 3.

Американский стандарт шифрования данных DES (2 часа).

Раздел 4. Асимметричные криптосистемы

Лекция 4.

Алгоритм шифрования данных IDEA. Отечественный стандарт шифрования (2 часа).

Раздел 5. Идентификация и проверка подлинности

Лекция 5.

Асимметричные криптосистемы (2 часа).

4.2.2.2. Перечень практических занятий

Семестр 7

Раздел 3. Современные симметричные криптосистемы

Практическое занятие 1.

Аддитивные методы криптографического преобразования информации (2 часа).

Раздел 4. Асимметричные криптосистемы

Практическое занятие 2.

Асимметричные схемы шифрования данных (2 часа).

Раздел 5. Идентификация и проверка подлинности

Практическое занятие 3.

Защита программного комплекса от несанкционированного доступа методом подсчета контрольных сумм (2 часа).

Раздел 6. Электронная цифровая подпись

Практическое занятие 4.

Определение показателей защищенности информации при несанкционированном доступе (2 часа).

Раздел 7. Управление криптографическими ключами

Практическое занятие 5.

Цифровая подпись (2 часа).

4.2.2.3. Перечень лабораторных работ

Семестр 7

Раздел 1. Введение. Основы информационной безопасности

Лабораторная 1.

Реализация дискреционной политики безопасности (4 часа).

Раздел 2. Принципы криптографической защиты информации

Лабораторная 2.

Простейшие методы криптографического преобразования информации (4 часа).

4.2.2.4. Перечень тем и учебно-методическое обеспечение самостоятельной работы

Перечень тем, вынесенных на самостоятельное изучение:

1. Виды криптоаналитических атак.
2. Система омофонов.
3. Одноразовая система шифрования.
4. Сравнение симметричных и ассиметричных систем.
5. Взаимная проверка подлинности пользователей. Механизм запроса-ответа.
6. Взаимная проверка подлинности пользователей. Механизм отметки времени.
7. Модель рукопожатия.
8. Отечественный стандарт цифровой подписи.
9. Аутентификация мастер-ключа хост-компьютера.
10. Схема защиты сеансового ключа.
11. Алгоритм Диффи-Хеллмана.
12. Основные схемы сетевой защиты на базе межсетевых экранов. Межсетевой экран - экранированная подсеть.
13. Правовые аспекты компьютерной безопасности.
14. Вредоносные программы.
15. Безопасность платежных систем.
16. Теоретическая оценка безопасности информации.
17. Конституция РФ. Доктрина информационной безопасности России. Кодексы РФ. Законы РФ. ГОСТы. Руководящие документы (РД).

Для самостоятельной работы используются методические указания по освоению дисциплины и издания из списка приведенной ниже основной и дополнительной литературы.

4.2.2.5. Перечень тем контрольных работ, рефератов, ТР, РГР, РПР

1. Американский стандарт шифрования данных DES.
2. Алгоритм шифрования данных IDEA. Отечественный стандарт шифрования.
3. Асимметричные криптосистемы.
4. Идентификация и проверка подлинности.
5. Электронная цифровая подпись.
6. Резервное хранение информации. RAID-массивы.
7. Защита программного комплекса от несанкционированного доступа методом подсчета контрольных сумм.
8. Определение показателей защищенности информации при несанкционированном доступе.
9. Цифровая подпись.
10. Методы определения хэш-функций.

4.2.2.6. Примерный перечень тем курсовых работ (проектов)

Не планируется.

5. Образовательные технологии

В процессе изучения дисциплины Информационная безопасность и защита информации применяется контактная технология преподавания (за исключением самостоятельно изучаемых студентами вопросов). При проведении лабораторных работ применяется имитационный или симуляционный подход, когда преподавателем разбирается на конкретном примере проблемная ситуация, все шаги решения задачи студентам демонстрируются при помощи мультимедийной техники. Затем студенты самостоятельно решают аналогичные задания.

Во время выполнения лабораторных работ формируются творческие коллективы из 2-3 студентов, разрабатывающих программы по заданной в лабораторной работе тематике, тем самым формируется способность обучающихся к работе в малых творческих коллективах.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

Фонды оценочных материалов (средств) приведены в приложении.

7. Учебно-методическое и информационное обеспечение дисциплины.

7.1. Основная учебно-методическая литература по дисциплине

1. Зенков, А. В. Основы информационной безопасности : учебное пособие / А. В. Зенков. — Москва, Вологда : Инфра-Инженерия, 2022. — 104 с. — ISBN 978-5-9729-0864-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. - https://www.iprbookshop.ru/124242.html

2. Фомин, Д. В. Информационная безопасность : учебное пособие для СПО / Д. В. Фомин. — Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2022. — 218 с. — ISBN 978-5-4488-1351-1, 978-5-4497-1565-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. - https://www.iprbookshop.ru/118458.html

3. Ревнивых, А. В. Информационная безопасность в организациях : учебное пособие / А. В. Ревнивых. — Москва : Ай Пи Ар Медиа, 2021. — 83 с. — ISBN 978-5-4497-1164-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. - https://www.iprbookshop.ru/108227.html

4. Литвиненко, О. В. Правовые аспекты информационной безопасности : учебное пособие / О. В. Литвиненко. — Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2021. — 63 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. - https://www.iprbookshop.ru/125273.html

5. Фороузан, Б. А. Криптография и безопасность сетей : учебное пособие / Б. А. Фороузан ; под редакцией А. Н. Берлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 776 с. — ISBN 978-5-4497-0946-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. - https://www.iprbookshop.ru/102017.html

7.2. Дополнительная учебно-методическая литература по дисциплине

1. Солонская, О. И. Средства защиты информации : учебное пособие / О. И. Солонская. — Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2021. — 89 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. - https://www.iprbookshop.ru/117115.html

2. Мельников, В.П. Информационная безопасность и защита информации: учеб. пособие / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова. – 2-е изд., стер. – М.: Академия, 2007. – 336 с. - 25 экз.

3. Гультяев, А.К. Восстановление данных. – 2-е изд. – СПб.: Питер, 2006. – 379 с. - 25 экз.

4. Молдовян, Н.А. Практикум по криптосистемам с открытым ключом. – СПб.: БХВ-Петербург, 2007. – 304 с. - 25 экз.

5. Смарт, Н. Криптография / пер. с англ. С.А. Кулешова; под ред. С.К. Ландо. – М.: Техносфера, 2005. – 528 с. - 25 экз.

6. Садердинов, А.А.; Трайнёв, В.А.; Федулов, А.А. Информационная безопасность предприятия: учебное пособие. – 3-е изд. – М.: Дашков и Ко, 2006. – 336 с. - 25 экз.

7.3. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая

перечень программного обеспечения и информационных справочных систем

В образовательном процессе используются информационные технологии, реализованные на основе информационно-образовательного портала института (www.mivlgu.ru/iop), и инфокоммуникационной сети института:

- предоставление учебно-методических материалов в электронном виде;
- взаимодействие участников образовательного процесса через локальную сеть института и Интернет;
- предоставление сведений о результатах учебной деятельности в электронном личном кабинете обучающегося.

Информационные справочные системы:

- электронная библиотечная система "iBooks.ru" (http://www.ibooks.ru/);

Программное обеспечение:

Microsoft Visual Studio (Программа Microsoft Azure Dev Tools for Teaching (Order Number: IM126433))

7.4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

iprbookshop.ru
ibooks.ru
mivlgu.ru/iop

8. Материально-техническое обеспечение дисциплины

Лаборатория ГИС и САПР

Сервер; 12 персональных компьютеров; проектор Sanyo PDG-DSU20; экран настенный Drapper Apex Star

9. Методические указания по освоению дисциплины

Для успешного освоения теоретического материала обучающийся: знакомится со списком рекомендуемой основной и дополнительной литературы; уточняет у преподавателя, каким дополнительным пособиям следует отдать предпочтение; ведет конспект лекций и прорабатывает лекционный материал, пользуясь как конспектом, так и учебными пособиями.

До выполнения лабораторных работ обучающийся изучает соответствующий раздел теории. Перед занятием студент знакомится с описанием заданий для выполнения работы, внимательно изучает содержание и порядок проведения лабораторной работы. Лабораторная работа проводятся в компьютерном классе. Обучающиеся выполняют индивидуальную задачу компьютерного моделирования в соответствии с заданием на лабораторную работу. Полученные результаты исследований сводятся в отчет и защищаются по традиционной методике в классе на следующем лабораторном занятии. Необходимый теоретический материал, индивидуальное задание, шаги выполнения лабораторной работы и требование к отчету приведены в методических указаниях, размещенных на информационно-образовательном портале института.

Самостоятельная работа оказывает важное влияние на формирование личности будущего специалиста, она планируется обучающимся самостоятельно. Каждый обучающийся самостоятельно определяет режим своей работы и меру труда, затрачиваемого на овладение учебным содержанием дисциплины. Он выполняет внеаудиторную работу и изучение разделов, выносимых на самостоятельную работу, по личному индивидуальному плану, в зависимости от его подготовки, времени и других условий.

Форма заключительного контроля при промежуточной аттестации – экзамен. Для проведения промежуточной аттестации по дисциплине разработаны фонд оценочных средств и балльно-рейтинговая система оценки учебной деятельности студентов. Оценка по дисциплине выставляется в информационной системе и носит интегрированный характер,

учитывающий результаты оценивания участия студентов в аудиторных занятиях, качества и своевременности выполнения заданий в ходе изучения дисциплины и промежуточной аттестации.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению *09.03.02 Информационные системы и технологии* и профилю подготовки *Информационные системы и технологии*
Рабочую программу составил *к.т.н., доцент Комкова С.В.*_____

Программа рассмотрена и одобрена на заседании кафедры *ИС*

протокол № 18 от 02.06.2020 года.
Заведующий кафедрой *ИС* _____*Андрианов Д.Е.*
(Подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии факультета

протокол № 10 от 10.06.2020 года.
Председатель комиссии ФИТР _____ *Рыжкова М.Н.*
(Подпись) (Ф.И.О.)

Приложение

Фонд оценочных материалов (средств) по дисциплине

Информационная безопасность и защита информации

1. Оценочные материалы для проведения текущего контроля успеваемости по дисциплине

Рейтинг-контроль №1.

Блок ЗНАТЬ

1. Кто является основным ответственным за определение уровня классификации информации?

- Руководитель среднего звена
- Высшее руководство
- Владелец
- Пользователь

2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

-Сотрудники
- Хакеры
- Атакующие
-Контрагенты (лица, работающие по договору)

3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

- Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
- Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
- Улучшить контроль за безопасностью этой информации
- Снизить уровень классификации этой информации

4. Что самое главное должно продумать руководство при классификации данных?

A. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным

B. Необходимый уровень доступности, целостности и конфиденциальности

C. Оценить уровень риска и отменить контрмеры

D. Управление доступом, которое должно защищать данные

5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

A. Владельцы данных

B. Пользователи

C. Администраторы

D. Руководство

6. Что такое процедура?

A. Правила использования программного и аппаратного обеспечения в компании

B. Пошаговая инструкция по выполнению задачи

C. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

D. Обязательные действия

7. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

A. Поддержка высшего руководства

B. Эффективные защитные меры и методы их внедрения

C. Актуальные и адекватные политики и процедуры безопасности

D. Проведение тренингов по безопасности для всех сотрудников

8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

A. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски

B. Когда риски не могут быть приняты во внимание по политическим соображениям

C. Когда необходимые защитные меры слишком сложны

D. Когда стоимость контрмер превышает ценность актива и потенциальные потери

9. Что такое политики безопасности?

A. Пошаговые инструкции по выполнению задач безопасности

B. Общие руководящие требования по достижению определенного уровня безопасности

C. Широкие, высокоуровневые заявления руководства

D. Детализированные документы по обработке инцидентов безопасности

10. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

A. Анализ рисков

B. Анализ затрат / выгоды

C. Результаты ALE

D. Выявление уязвимостей и угроз, являющихся причиной риска

11. Что лучше всего описывает цель расчета ALE?

A. Количественно оценить уровень безопасности среды

B. Оценить возможные потери для каждой контрмеры

C. Количественно оценить затраты / выгоды

D. Оценить потенциальные потери от угрозы в год

12. Тактическое планирование – это:

A. Среднесрочное планирование

B. Долгосрочное планирование

C. Ежедневное планирование

D. Планирование на 6 месяцев

13. Что является определением воздействия (exposure) на безопасность?

A. Нечто, приводящее к ущербу от угрозы

B. Любая потенциальная опасность для информации или систем

C. Любой недостаток или отсутствие информационной безопасности

D. Потенциальные потери от угрозы

14. Эффективная программа безопасности требует сбалансированного применения:

A. Технических и нетехнических методов

B. Контрмер и защитных механизмов

C. Физической безопасности и технических средств защиты

D. Процедур безопасности и шифрования

15. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

A. Внедрение управления механизмами безопасности

B. Классификацию данных после внедрения механизмов безопасности

C. Уровень доверия, обеспечиваемый механизмом безопасности

D. Соотношение затрат / выгод

16. Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?

A. Только военные имеют настоящую безопасность

B. Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности

C. Военным требуется больший уровень безопасности, т.к. их риски существенно выше

D. Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

17. Как рассчитать остаточный риск?

A. Угрозы х Риски х Ценность актива

B. (Угрозы х Ценность актива х Уязвимости) х Риски

C. SLE x Частоту = ALE

D. (Угрозы x Уязвимости x Ценность актива) x Недостаток контроля

18. Что из перечисленного не является целью проведения анализа рисков?

A. Делегирование полномочий

B. Количественная оценка воздействия потенциальных угроз

C. Выявление рисков

D. Определение баланса между воздействием риска и стоимостью необходимых контрмер

19. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?

A. Поддержка

B. Выполнение анализа рисков

C. Определение цели и границ

D. Делегирование полномочий

20. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

A. Чтобы убедиться, что проводится справедливая оценка

B. Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ

C. Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа

D. Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

21. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод:

1. гаммирования;
2. подстановки;
3. кодирования;
4. перестановки;
5. аналитических преобразований.

22. Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов, это метод:

1. гаммирования;
2. подстановки;
3. кодирования;
4. перестановки;
5. аналитических преобразований.

23. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:

1. гаммирования;
2. подстановки;
3. кодирования;
4. перестановки;
5. аналитических преобразований.

24. Защита информации от утечки это деятельность по предотвращению:

1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;

2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;

3. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;

4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;

5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

25 Защита информации это:

1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;

2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;

3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;

4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;

5. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

26 Естественные угрозы безопасности информации вызваны:

1. деятельностью человека;

2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;

3. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;

4. корыстными устремлениями злоумышленников;

5. ошибками при действиях персонала.

27 Искусственные угрозы безопасности информации вызваны:

1. деятельностью человека;

2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;

3. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;

4. корыстными устремлениями злоумышленников;

5. ошибками при действиях персонала.

28 К основным непреднамеренным искусственным угрозам АСОИ относится:

1. физическое разрушение системы путем взрыва, поджога и т.п.;

2. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;

3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;

4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

5. неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.

29. К посторонним лицам нарушителям информационной безопасности относится:

1. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;

2. персонал, обслуживающий технические средства;

3. технический персонал, обслуживающий здание;

4. пользователи;

5. сотрудники службы безопасности.

6. представители конкурирующих организаций.

7. лица, нарушившие пропускной режим;

Блок (УМЕТЬ):

1. Что понимают под набором норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации?

А Политика безопасности

Б Законная политика

В Свод правил

Г Стратегия предприятия

2. В каких шифрах в качестве ключа используют таблицы?

А Шифрующие таблицы

Б метод Цезаря

В Магические квадраты

Г Полибианский квадрат

3. Самый первый шифр перестановки?

А Метод скитала

Б метод Цезаря

В Магические квадраты

Г Полибианский квадрат

4. В каком шифре каждая буква заменялась на другую букву того же алфавита по следующему правилу: заменяющая буква определялась путем смещения по алфавиту от исходной буквы на К букв.?

А шифрующие таблицы

Б метод Цезаря

В Магические квадраты

Г Полибианский квадрат

5. Какой шифр основан на подсчете частот появления букв в шифртексте..?

А шифр Трисемуса

Б система омофонов

В алгоритм Вернама

Г гаммирование

6. Какой шифр сложной замены представляет собой модификацию шифра Цезаря числовым ключом?

А Шифр Гронсфельда

Б система омофонов

В алгоритм Вернама

Г гаммирование

7. Какой шифр сложной замены описывается таблицей шифрования, и где ключ шифрования меняется от буквы к букве.?

А шифр Трисемуса

Б система Вижинера

В алгоритм Вернама

Г гаммирование

8. Какой шифр является абсолютно надежным?

А шифр Трисемуса

Б одноразовая система шифрования

В алгоритм Вернама

Г гаммирование

9. Какой шифр является в сущности частным случаем системы шифрования Вижинера при значении модуля m = 2.?

А шифр Трисемуса

Б одноразовая система шифрования

В алгоритм Вернама

Г гаммирование

10. Псевдослучайная последовательность, выработанная по заданному алгоритму для зашифрования открытых данных и расшифрования зашифрованных данных это?

А альфа шифра
Б бета шифра
В гамма шифра
Г лямбда шифра

11. Псевдослучайная последовательность, выработанная по заданному алгоритму для зашифрования открытых данных и расшифрования зашифрованных данных это?

А альфа шифра
Б бета шифра
В гамма шифра
Г лямбда шифра

Рейтинг-контроль №2. Блок ЗНАТЬ

1. К посторонним лицам нарушителям информационной безопасности относится:

- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
-персонал, обслуживающий технические средства;
-технический персонал, обслуживающий здание;
-пользователи;
-сотрудники службы безопасности.
- представители конкурирующих организаций.
- лица, нарушившие пропускной режим;

2. Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п:

1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

3. Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:

1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

4. Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

5. Антивирус не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

6. Антивирус запоминает исходное состояние программ, каталогов и системных областей диска когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным:

1. детектор;
2. доктор;

3. сканер;
4. ревизор;
5. сторож.

7 . Антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

8. Активный перехват информации это перехват, который:

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

9. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

10. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;

5.просмотр мусора.

11 . Перехват, который осуществляется путем использования оптической техники называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

12. К внутренним нарушителям информационной безопасности относится:

1. клиенты;
2. пользователи системы;
3. посетители;
4. любые лица, находящиеся внутри контролируемой территории;
5. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации.
6. персонал, обслуживающий технические средства.
7. сотрудники отделов разработки и сопровождения ПО;
8. технический персонал, обслуживающий здание

12. Как называется умышленно искаженная информация?

- Дезинформация

- Информативный поток
- Достоверная информация
- Перестает быть информацией

13. Как называется информация, к которой ограничен доступ?

- Конфиденциальная
- Противозаконная
- Открытая
- Недоступная

14. Какими путями может быть получена информация?

-проведением, покупкой и противоправным добыванием информации научных исследований

- захватом и взломом ПК информации научных исследований
- добыванием информации из внешних источников и скремблированием информации научных исследовании
- захватом и взломом защитной системы для информации научных исследований

15. Как называются компьютерные системы, в которых обеспечивается безопасность информации?

- защищенные КС
- небезопасные КС
- Само достаточные КС
- Саморегулирующиеся КС

16. Основной документ, на основе которого проводится политика информационной безопасности?

- программа информационной безопасности
- регламент информационной безопасности
- политическая информационная безопасность
- Протекторат

17. В зависимости от формы представления информация может быть разделена на?

- Речевую, документированную и телекоммуникационную
- Мысль, слово и речь
- цифровая, звуковая и тайная
- цифровая, звуковая

18. К каким процессам относят процессы сбора, обработки, накопления, хранения, поиска и распространения информации

- Информационным процессам
- Мыслительным процессам
- Машинным процессам
- Микропроцессам

19. Что называют защитой информации?

- Все ответы верны
- Называют деятельность по предотвращению утечки защищаемой информации
- Называют деятельность по предотвращению несанкционированных воздействий на защищаемую информацию
- Называют деятельность по предотвращению непреднамеренных воздействий на защищаемую информацию

20. Под непреднамеренным воздействием на защищаемую информацию понимают?

- Воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств и воздействие природных явлений
- Процесс ее преобразования, при котором содержание информации изменяется на ложную
- Возможности ее преобразования, при котором содержание информации изменяется на ложную информацию
- Не ограничения доступа в отдельные отрасли экономики или на конкретные производства

21. Шифрование информации это

- Процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов

- Процесс преобразования, при котором информация удаляется

- Процесс ее преобразования, при котором содержание информации изменяется на ложную

- Процесс преобразования информации в машинный код

22. Основные предметные направления Защиты Информации?

- охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности

- Охрана золотого фонда страны

- Определение ценности информации

- Усовершенствование скорости передачи информации

23. Государственная тайна это

- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны

- ограничения доступа в отдельные отрасли экономики или на конкретные производства

- защищаемые банками и иными кредитными организациями сведения о банковских операциях

- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

24. Коммерческая тайна это….

- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны

- ограничения доступа в отдельные отрасли экономики или на конкретные производства

- защищаемые банками и иными кредитными организациями сведения о банковских операциях

- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

25. Банковская тайна это….

- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны

- ограничения доступа в отдельные отрасли экономики или на конкретные производства

- защищаемые банками и иными кредитными организациями сведения о банковских операциях

- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

26. Профессиональная тайна

- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны

- ограничения доступа в отдельные отрасли экономики или на конкретные производства

- защищаемые банками и иными кредитными организациями сведения о банковских операциях

- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

27. К основным объектам банковской тайны относятся следующие:

- Все ответы верны
- Тайна банковского счета
- Тайна операций по банковскому счету
- Тайна банковского вклада

28. Как называется тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений?

- Тайна связи
- Нотариальная тайна
- Адвокатская тайна
- Тайна страхования

29. Как называются сведения, доверенные нотариусу в связи с совершением нотариальных действий?

- Нотариальная тайна
- Общедоступные сведения
- Нотариальный секрет
- Нотариальное вето

30. Элемент аппаратной защиты, где используется установка источников бесперебойного питания (UPS)?

- защита от сбоев в электропитании
- защита от сбоев серверов, рабочих станций и локальных компьютеров
- защита от сбоев устройств для хранения информации
- защита от утечек информации электромагнитных излучений

31.Функция защиты информационной системы, гарантирующая то, что доступ к информации, хранящейся в системе может быть осуществлен только тем лицам, которые на это имеют право

- управление доступом
- конфиденциальность
- аутентичность
- целостность
- доступность

Блок УМЕТЬ:

1. По мнению К. Шеннона, в практических шифрах необходимо использовать два общих принципа:

- рассеивание
- перемешивание
- встряска
- перестановка

2. Ключ какой длины используется в алгоритме DES:

- 56 бит
- 64 бит
- 128 бит
- 32 бит

3. Блок какой длины обрабатывается в алгоритме DES:

- 64 бит
- 56 бит
- 128 бит
- 32 бит

4. Сколько основных итераций в алгоритме DES:

- 16
- 14
- 20
- 8

5. Первым этапом алгоритма DES является:

- начальная перестановка битов исходного блока
- конечная перестановка битов исходного блока
- начальное рассеивание битов исходного блока
- начальная замена битов исходного блока

6. Какая операция используется в алгоритме DES:
- сложение по модулю два
- сложение
- битовая инверсия
- битовое умножение

7. Какая операция используется в алгоритме DES при вычислении ключей:
- сдвиг влево
- сдвиг вправо
- битовая инверсия
- битовое умножение

8. Сколько ключей используется в алгоритме DES:
- 16
- 12
- 20
- 32

9. При каком режиме DES длинный файл разбивают на 64-битовые отрезки (блоки) по 8 байтов. Каждый из этих блоков шифруют независимо с ис¬пользованием одного и того же ключа шифрования?
- электронная кодовая книга ECB (Electronic Code Book);
- сцепление блоков шифра CBC (Cipher Block Chaining);
- обратная связь по шифртексту CFB (Cipher Feed Back);
- обратная связь по выходу OFB (Output Feed Back).

10. При каком режиме DES исходный файл M разбивается на 64-битовые блоки: M = M(1)M(2)...M(n). Первый блок M(1) складывается по модулю 2 с 64-битовым начальным вектором IV, который меняется ежедневно и держится в секрете. Полученная сумма затем шифруется с использованием ключа DES, известного и отправителю, и получателю информации. Полученный 64-битовый блок шифртекста C(1) складывается по модулю 2 со вторым блоком исходного текста, результат шифруется и получается второй 64-битовый блок шифртекста C(2) и т.д.

-электронная кодовая книга ECB (Electronic Code Book);
-сцепление блоков шифра CBC (Cipher Block Chaining);
-обратная связь по шифртексту CFB (Cipher Feed Back);
-обратная связь по выходу OFB (Output Feed Back).

11. При каком режиме DES размер блока может отличаться от 64. Исходный файл M считывается последовательными t-битовыми блоками (t <= 64): M = M(1)M(2)...M(n) (остаток дописывается нулями или пробелами).

-электронная кодовая книга ECB (Electronic Code Book);
- сцепление блоков шифра CBC (Cipher Block Chaining);
- обратная связь по шифртексту CFB (Cipher Feed Back);
- обратная связь по выходу OFB (Output Feed Back).

Рейтинг-контроль №3. Блок ЗНАТЬ

1. Элемент аппаратной защиты, где используется резервирование особо важных компьютерных подсистем
- защита от сбоев в электропитании

защита от сбоев серверов, рабочих станций и локальных компьютеров
- защита от сбоев устройств для хранения информации
- защита от утечек информации электромагнитных излучений

2. Элемент аппаратной защиты, где используется организация надежной и эффективной системы резервного копирования и дублирования данных

- защита от сбоев в электропитании
- защита от сбоев серверов, рабочих станций и локальных компьютеров
-защита от сбоев устройств для хранения информации
- защита от утечек информации электромагнитных излучений

3. Элемент аппаратной защиты, где используется экранирование, фильтрацию, заземление, электромагнитное зашумление, а также средства ослабления уровней нежелательных электромагнитных излучений.

- защита от сбоев в электропитании
- защита от сбоев серверов, рабочих станций и локальных компьютеров
- защита от сбоев устройств для хранения информации
-защита от утечек информации электромагнитных излучений

4. Какая из перечисленных атак на поток информации является пассивной:

- перехват.
- имитация.
- модификация.
- фальсификация.
- прерывание.

5. К открытым источникам информация относятся.

-Газеты, Радио, Новости
- Информация украденная у спецслужб
- Из вскрытого сейфа
- Украденная из правительственной организации

6. Технические каналы утечки информации делятся на…

- Все перечисленное
- Акустические и виброакустические
- Электрические
- Оптические

7. Какой технический канал утечки отвечает за распространение звуковых колебаний в любом звукопроводящем материале или среде?

- Акустические и виброакустические
- Электрические
- Оптические
- Радиоканалы

8. Какой технический канал утечки отвечает за напряжение и токи в различных токопроводящих коммуникациях?

- Акустические и виброакустические
- Электрические
- Оптические
- Радиоканалы

9. Какой технический канал утечки отвечает за электромагнитные излучения радиодиапазона?

- Акустические и виброакустические
- Электрические
- Оптические
-Радиоканалы

10. Какой технический канал утечки отвечает за электромагнитные излучения в видимой, инфракрасной и ультрафиолетовой частях спектра?

- Акустические и виброакустические
- Электрические
- Оптические
- Радиоканалы

11. Учет всех возможных коммуникационных каналов, обеспечения физической безопасности, шифрования резервных копий и информации, покидающей корпоративный периметр, и других организационных мероприятий это?

- Индивидуальный подход к защите
- Комплексный подход к защите
- Смешанный подход к защите
- Рациональный подход к защите

12. Меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе

- Информационная безопасность
- Защитные технологии
- Заземление
- Конфиденциальность

13. Можно выделить следующие направления мер информационной безопасности

- Правовые
- Организационные
- Все ответы верны
- Технические

14. Что можно отнести к правовым мерам информационной безопасности?

- Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства
- охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра итд
- Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установку оборудования обнаружения и тушения пожара, оборудования обнаружения воды, принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое
- охрану вычислительного центра, установку сигнализации и многое другое

15. Что можно отнести к организационным мерам ИБ?

- Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства.
- Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.
- Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем.
- Охрану работоспособности отдельных звеньев и организацию вычислительных сетей с возможностью перераспределения ресурсов.
- Принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

16. Что можно отнести к техническим мерам ИБ?

- Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства
- Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.

- Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев и многое другое

- Простые и доступные меры защиты от хищений, саботажа, диверсий, взрывов

- В административных местах установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

17. Потенциальные угрозы, против которых направлены технические меры защиты информации

- Потери информации из-за сбоев оборудования, некорректной работы программ и ошибки обслуживающего персонала и пользователей

- Потери информации из-за халатности обслуживающего персонала и не ведения системы наблюдения

- Потери информации из-за не достаточной установки резервных систем электропитании и оснащение помещений замками.

- Потери информации из-за не достаточной установки сигнализации в помещении.

- Процессы преобразования, при котором информация удаляется

Блок УМЕТЬ

1. Блоками какого размера оперирует алгоритм шифрования IDEA?
- 64 бит
- 56 бит
- 128 бит
- 32 бит

2. Сколько итераций цикла использует алгоритм шифрования IDEA?
- 8
- 16
- 5
- 24

3. Ключ какого размера использует алгоритм шифрования IDEA?
- 128 бит
- 56 бит
- 64 бита
- 32 бит

4. Какие режимы использует отечественный стандарт шифрования?
- простая замена;
- гаммирование;
- гаммирование с обратной связью;
- выработка имитовставки.
- Все перечисленные

5. Чем отличаются ассиметричные шифры от симметричных?
- Простотой реализации;
- наличием постоянного ключа
- наличием трех секретных ключей;
- Наличием двух ключей

6. Какая процедура устанавливает, является ли данный объект именно таким, каким он себя объявляет.

- авторизация
- идентификация
-коммутация
-аутентификация

7. Какая процедура устанавливает сферу действия объекта и доступ¬ные ему ресурсы сети?

- авторизация
- идентификация
-коммутация
-аутентификация

8. Для проверки подлинности применяют:
-механизм запроса-ответа;
-механизм отметки времени.
-Механизм ответа-ответа
-Механизм запроса-запроса

9. Какую процедуру используют для взаимной проверки подлинности ?
- «рукопожатия»
-механизм отметки времени.
-Механизм ответа-ответа
-Механизм запроса-запроса

18. Какие сбои оборудования бывают?
- потери при заражении системы компьютерными вирусами
- несанкционированное копирование, уничтожение или подделка информации
- сбои работы серверов, рабочих станций, сетевых карт и тд - ознакомление с конфиденциальной информацией

19.Какие сбои оборудования, при которых теряется информация, бывают?
- случайное уничтожение или изменение данных
- перебои электропитания
- некорректное использование программного и аппаратного обеспечения, ведущее к уничтожению или изменению данных
- несанкционированное копирование, уничтожение или подделка информации

20. Какие потери информации бывают из-за некорректной работы программ?
- сбои работы серверов, рабочих станций, сетевых карт и тд
- перебои электропитания
-потеря или изменение данных при ошибках ПО
- ознакомление с конфиденциальной информацией

21. Какие потери информации бывают из-за некорректной работы программ?
- потери при заражении системы компьютерными вирусами
- сбои дисковых систем
- перебои электропитания
- сбои работы серверов, рабочих станций, сетевых карт и тд

22. Какие потери информации, связанные с несанкционированным доступом, бывают?
- несанкционированное копирование, уничтожение или подделка информации
- потери при заражении системы компьютерными вирусами
- случайное уничтожение или изменение данных
- сбои дисковых систем

23. Потери из-за ошибки персонала и пользователей бывают?
- несанкционированное копирование, уничтожение или подделка информации
- потери при заражении системы компьютерными вирусами
- случайное уничтожение или изменение данных
- сбои дисковых систем

24. Наиболее надежным средством предотвращения потерь информации при кратковременном отключении электроэнергии?
- установка источников бесперебойного питания (UPS)
- Такого средства не существует
- Каждую минуту сохранять данные
- Перекидывать информацию на носитель, который не зависит от энергии

25. Способ защиты от сбоев процессора?
- установка источников бесперебойного питания (UPS)
- симметричное мультипроцессирование

- Каждую минуту сохранять данные
- Перекидывать информацию на носитель, который не зависит от энергии

Общее распределение баллов текущего контроля по видам учебных работ для студентов

Рейтинг-контроль 1	тесты	До 10 баллов
Рейтинг-контроль 2	тесты	До 10 баллов
Рейтинг-контроль 3	тесты	До 10 баллов
Посещение занятий студентом	Отметка в журнале посещений	До 10 баллов
Дополнительные баллы (бонусы)		0
Выполнение семестрового плана самостоятельной работы	Защита лабораторных работ	до 20 баллов

2. Промежуточная аттестация по дисциплине

Перечень вопросов к экзамену / зачету / зачету с оценкой.
Перечень практических задач / заданий к экзамену / зачету / зачету с оценкой (при наличии)

ОПК-3

Блок ЗНАТЬ

1. Кто является основным ответственным за определение уровня классификации информации?

- Руководитель среднего звена
- Высшее руководство
- Владелец
- Пользователь

2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

-Сотрудники
- Хакеры
- Атакующие
-Контрагенты (лица, работающие по договору)

3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

- Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
- Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
- Улучшить контроль за безопасностью этой информации
- Снизить уровень классификации этой информации

4. Что самое главное должно продумать руководство при классификации данных?

A. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
B. Необходимый уровень доступности, целостности и конфиденциальности
C. Оценить уровень риска и отменить контрмеры
D. Управление доступом, которое должно защищать данные

5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

A. Владельцы данных

B. Пользователи

C. Администраторы

D. Руководство

6. Что такое процедура?

A. Правила использования программного и аппаратного обеспечения в компании

B. Пошаговая инструкция по выполнению задачи

C. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

D. Обязательные действия

7. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

A. Поддержка высшего руководства

B. Эффективные защитные меры и методы их внедрения

C. Актуальные и адекватные политики и процедуры безопасности

D. Проведение тренингов по безопасности для всех сотрудников

8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

A. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски

B. Когда риски не могут быть приняты во внимание по политическим соображениям

C. Когда необходимые защитные меры слишком сложны

D. Когда стоимость контрмер превышает ценность актива и потенциальные потери

9. Что такое политики безопасности?

A. Пошаговые инструкции по выполнению задач безопасности

B. Общие руководящие требования по достижению определенного уровня безопасности

C. Широкие, высокоуровневые заявления руководства

D. Детализированные документы по обработке инцидентов безопасности

10. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

A. Анализ рисков

B. Анализ затрат / выгоды

C. Результаты ALE

D. Выявление уязвимостей и угроз, являющихся причиной риска

11. Что лучше всего описывает цель расчета ALE?

A. Количественно оценить уровень безопасности среды

B. Оценить возможные потери для каждой контрмеры

C. Количественно оценить затраты / выгоды

D. Оценить потенциальные потери от угрозы в год

12. Тактическое планирование – это:

A. Среднесрочное планирование

B. Долгосрочное планирование

C. Ежедневное планирование

D. Планирование на 6 месяцев

13. Что является определением воздействия (exposure) на безопасность?

A. Нечто, приводящее к ущербу от угрозы

B. Любая потенциальная опасность для информации или систем

C. Любой недостаток или отсутствие информационной безопасности

D. Потенциальные потери от угрозы

14. Эффективная программа безопасности требует сбалансированного применения:

A. Технических и нетехнических методов

B. Контрмер и защитных механизмов

C. Физической безопасности и технических средств защиты

D. Процедур безопасности и шифрования

15. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

A. Внедрение управления механизмами безопасности

B. Классификацию данных после внедрения механизмов безопасности

C. Уровень доверия, обеспечиваемый механизмом безопасности

D. Соотношение затрат / выгод

16. Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?

A. Только военные имеют настоящую безопасность

B. Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности

C. Военным требуется больший уровень безопасности, т.к. их риски существенно выше

D. Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

17. Как рассчитать остаточный риск?

A. Угрозы х Риски х Ценность актива

B. (Угрозы х Ценность актива х Уязвимости) х Риски

C. SLE х Частоту = ALE

D. (Угрозы х Уязвимости х Ценность актива) х Недостаток контроля

18. Что из перечисленного не является целью проведения анализа рисков?

A. Делегирование полномочий

B. Количественная оценка воздействия потенциальных угроз

C. Выявление рисков

D. Определение баланса между воздействием риска и стоимостью необходимых контрмер

19. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?

A. Поддержка

B. Выполнение анализа рисков

C. Определение цели и границ

D. Делегирование полномочий

20. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

A. Чтобы убедиться, что проводится справедливая оценка

B. Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ

C. Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа

D. Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

21. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод:

1.гаммирования;

2.подстановки;

3.кодирования;

4.перестановки;

5.аналитических преобразований.

22. Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов, это метод:

1.гаммирования;

2. подстановки;

3. кодирования;
4. перестановки;
5. аналитических преобразований.

23. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:

1. гаммирования;
2. подстановки;
3. кодирования;
4. перестановки;
5. аналитических преобразований.

24. Защита информации от утечки это деятельность по предотвращению:

1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
3. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

25 Защита информации это:

1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
5. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

26 Естественные угрозы безопасности информации вызваны:

1. деятельностью человека;
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
3. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
4. корыстными устремлениями злоумышленников;
5. ошибками при действиях персонала.

27 Искусственные угрозы безопасности информации вызваны:

1. деятельностью человека;
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
3. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
4. корыстными устремлениями злоумышленников;
5. ошибками при действиях персонала.

28 К основным непреднамеренным искусственным угрозам АСОИ относится:

1. физическое разрушение системы путем взрыва, поджога и т.п.;

2. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;

3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;

4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

5. неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.

29. К посторонним лицам нарушителям информационной безопасности относится:

1. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;

2. персонал, обслуживающий технические средства;

3. технический персонал, обслуживающий здание;

4. пользователи;

5. сотрудники службы безопасности.

6. представители конкурирующих организаций.

7. лица, нарушившие пропускной режим;

30. К посторонним лицам нарушителям информационной безопасности относится:

- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;

-персонал, обслуживающий технические средства;

-технический персонал, обслуживающий здание;

-пользователи;

-сотрудники службы безопасности.

- представители конкурирующих организаций.

- лица, нарушившие пропускной режим;

31. Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п:

1. черный пиар;

2. фишинг;

3. нигерийские письма;

4. источник слухов;

5. пустые письма.

32. Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:

1. черный пиар;

2. фишинг;

3. нигерийские письма;

4. источник слухов;

5. пустые письма.

33 Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы:

1. детектор;

2. доктор;

3. сканер;

4. ревизор;

5. сторож.

34 Антивирус не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние:

1. детектор;

2. доктор;

3. сканер;

4. ревизор;

5. сторож.

35 Антивирус запоминает исходное состояние программ, каталогов и системных областей диска когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

36 Антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

37 Активный перехват информации это перехват, который:

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

38 Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

39 Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;

5.просмотр мусора

40 Перехват, который осуществляется путем использования оптической техники называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

41. К внутренним нарушителям информационной безопасности относится:

1. клиенты;
2. пользователи системы;
3. посетители;
4. любые лица, находящиеся внутри контролируемой территории;
5. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации.

6. персонал, обслуживающий технические средства.
7. сотрудники отделов разработки и сопровождения ПО;
8. технический персонал, обслуживающий здание

42. Как называется умышленно искаженная информация?

- Дезинформация
- Информативный поток
- Достоверная информация
- Перестает быть информацией

43. Как называется информация, к которой ограничен доступ?

- Конфиденциальная
- Противозаконная
- Открытая
- Недоступная

44. Какими путями может быть получена информация?

-проведением, покупкой и противоправным добыванием информации научных исследований

- захватом и взломом ПК информации научных исследований
- добыванием информации из внешних источников и скремблированием информации научных исследовании
- захватом и взломом защитной системы для информации научных исследований

45. Как называются компьютерные системы, в которых обеспечивается безопасность информации?

- защищенные КС
- небезопасные КС
- Само достаточные КС
- Саморегулирующиеся КС

46. Основной документ, на основе которого проводится политика информационной безопасности?

- программа информационной безопасности
- регламент информационной безопасности
- политическая информационная безопасность
- Протекторат

47. В зависимости от формы представления информация может быть разделена на?

- Речевую, документированную и телекоммуникационную
- Мысль, слово и речь
- цифровая, звуковая и тайная
- цифровая, звуковая

48. К каким процессам относят процессы сбора, обработки, накопления, хранения, поиска и распространения информации

- Информационным процессам
- Мыслительным процессам
- Машинным процессам
- Микропроцессам

49. Что называют защитой информации?

- Все ответы верны
- Называют деятельность по предотвращению утечки защищаемой информации
- Называют деятельность по предотвращению несанкционированных воздействий на защищаемую информацию
- Называют деятельность по предотвращению непреднамеренных воздействий на защищаемую информацию

50. Под непреднамеренным воздействием на защищаемую информацию понимают?

- Воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств и воздействие природных явлений

- Процесс ее преобразования, при котором содержание информации изменяется на ложную

- Возможности ее преобразования, при котором содержание информации изменяется на ложную информацию

- Не ограничения доступа в отдельные отрасли экономики или на конкретные производства

51. Шифрование информации это

- Процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов

- Процесс преобразования, при котором информация удаляется

- Процесс ее преобразования, при котором содержание информации изменяется на ложную

- Процесс преобразования информации в машинный код

52. Основные предметные направления Защиты Информации?

- охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности

- Охрана золотого фонда страны

- Определение ценности информации

- Усовершенствование скорости передачи информации

53. Государственная тайна это

- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны

- ограничения доступа в отдельные отрасли экономики или на конкретные производства

- защищаемые банками и иными кредитными организациями сведения о банковских операциях

- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

54. Коммерческая тайна это….

- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны

- ограничения доступа в отдельные отрасли экономики или на конкретные производства

- защищаемые банками и иными кредитными организациями сведения о банковских операциях

- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

55. Банковская тайна это….

- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны

- ограничения доступа в отдельные отрасли экономики или на конкретные производства

- защищаемые банками и иными кредитными организациями сведения о банковских операциях

- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

56. Профессиональная тайна

- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны

- ограничения доступа в отдельные отрасли экономики или на конкретные производства

- защищаемые банками и иными кредитными организациями сведения о банковских операциях

- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

57. К основным объектам банковской тайны относятся следующие:

- Все ответы верны
- Тайна банковского счета
- Тайна операций по банковскому счету
- Тайна банковского вклада

58. Как называется тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений?

- Тайна связи
- Нотариальная тайна
- Адвокатская тайна
- Тайна страхования

59. Как называются сведения, доверенные нотариусу в связи с совершением нотариальных действий?

- Нотариальная тайна
- Общедоступные сведения
- Нотариальный секрет
- Нотариальное вето

60. Элемент аппаратной защиты, где используется установка источников бесперебойного питания (UPS)?

- защита от сбоев в электропитании
- защита от сбоев серверов, рабочих станций и локальных компьютеров
- защита от сбоев устройств для хранения информации
- защита от утечек информации электромагнитных излучений

61.Функция защиты информационной системы, гарантирующая то, что доступ к информации, хранящейся в системе может быть осуществлен только тем лицам, которые на это имеют право

- управление доступом
- конфиденциальность
- аутентичность
- целостность
- доступность

62. Элемент аппаратной защиты, где используется резервирование особо важных компьютерных подсистем

- защита от сбоев в электропитании

защита от сбоев серверов, рабочих станций и локальных компьютеров

- защита от сбоев устройств для хранения информации
- защита от утечек информации электромагнитных излучений

63. Элемент аппаратной защиты, где используется организация надежной и эффективной системы резервного копирования и дублирования данных

- защита от сбоев в электропитании
- защита от сбоев серверов, рабочих станций и локальных компьютеров

-защита от сбоев устройств для хранения информации

- защита от утечек информации электромагнитных излучений

64. Элемент аппаратной защиты, где используется экранирование, фильтрацию, заземление, электромагнитное зашумление, а также средства ослабления уровней нежелательных электромагнитных излучений.

- защита от сбоев в электропитании
- защита от сбоев серверов, рабочих станций и локальных компьютеров

- защита от сбоев устройств для хранения информации
-защита от утечек информации электромагнитных излучений

65. Какая из перечисленных атак на поток информации является пассивной:
- перехват.
- имитация.
- модификация.
- фальсификация.
- прерывание.

66. К открытым источникам информация относятся.
-Газеты, Радио, Новости
- Информация украденная у спецслужб
- Из вскрытого сейфа
- Украденная из правительственной организации

67. Технические каналы утечки информации делятся на…
- Все перечисленное
- Акустические и виброакустические
- Электрические
- Оптические

68. Какой технический канал утечки отвечает за распространение звуковых колебаний в любом звукопроводящем материале или среде?
- Акустические и виброакустические
- Электрические
- Оптические
- Радиоканалы

69. Какой технический канал утечки отвечает за напряжение и токи в различных токопроводящих коммуникациях?
- Акустические и виброакустические
- Электрические
- Оптические
- Радиоканалы

70. Какой технический канал утечки отвечает за электромагнитные излучения радиодиапазона?
- Акустические и виброакустические
- Электрические
- Оптические
-Радиоканалы

71. Какой технический канал утечки отвечает за электромагнитные излучения в видимой, инфракрасной и ультрафиолетовой частях спектра?
- Акустические и виброакустические
- Электрические
- Оптические
- Радиоканалы

72. Учет всех возможных коммуникационных каналов, обеспечения физической безопасности, шифрования резервных копий и информации, покидающей корпоративный периметр, и других организационных мероприятий это?
- Индивидуальный подход к защите
- Комплексный подход к защите
- Смешанный подход к защите
- Рациональный подход к защите

73. Меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе
- Информационная безопасность
- Защитные технологии
- Заземление

- Конфиденциальность

74. Можно выделить следующие направления мер информационной безопасности

- Правовые
- Организационные
- Все ответы верны
- Технические

75. Что можно отнести к правовым мерам информационной безопасности?

- Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства
- охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра итд
- Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установку оборудования обнаружения и тушения пожара, оборудования обнаружения воды, принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое
- охрану вычислительного центра, установку сигнализации и многое другое

76. Что можно отнести к организационным мерам ИБ?

- Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства.
- Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.
- Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем.
- Охрану работоспособности отдельных звеньев и организацию вычислительных сетей с возможностью перераспределения ресурсов.
- Принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

77. Что можно отнести к техническим мерам ИБ?

- Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства
- Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.
- Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев и многое другое
- Простые и доступные меры защиты от хищений, саботажа, диверсий, взрывов
- В административных местах установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

ОПК-3

Блок УМЕТЬ

1. Что понимают под набором норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации?

А Политика безопасности
Б Законная политика
В Свод правил
Г Стратегия предприятия

2. В каких шифрах в качестве ключа используют таблицы?
А Шифрующие таблицы
Б метод Цезаря
В Магические квадраты
Г Полибианский квадрат

3. Самый первый шифр перестановки?
А Метод скитала
Б метод Цезаря
В Магические квадраты
Г Полибианский квадрат

4. В каком шифре каждая буква заменялась на другую букву того же алфавита по следующему правилу: заменяющая буква определялась путем смещения по алфавиту от исходной буквы на К букв.?
А шифрующие таблицы
Б метод Цезаря
В Магические квадраты
Г Полибианский квадрат

5. Какой шифр основан на подсчете частот появления букв в шифртексте..?
А шифр Трисемуса
Б система омофонов
В алгоритм Вернама
Г гаммирование

6. Какой шифр сложной замены представляет собой модификацию шифра Цезаря числовым ключом?
А Шифр Гронсфельда
Б система омофонов
В алгоритм Вернама
Г гаммирование

7. Какой шифр сложной замены описывается таблицей шифрования, и где ключ шифрования меняется от буквы к букве.?
А шифр Трисемуса
Б система Вижинера
В алгоритм Вернама
Г гаммирование

8. Какой шифр является абсолютно надежным?
А шифр Трисемуса
Б одноразовая система шифрования
В алгоритм Вернама
Г гаммирование

9. Какой шифр является в сущности частным случаем системы шифрования Вижинера при значении модуля m = 2.?
А шифр Трисемуса
Б одноразовая система шифрования
В алгоритм Вернама
Г гаммирование

10. Псевдослучайная последовательность, выработанная по заданному алгоритму для зашифрования открытых данных и расшифрования зашифрованных данных это?
А альфа шифра
Б бета шифра
В гамма шифра

Г лямбда шифра

11. Псевдослучайная последовательность, выработанная по заданному алгоритму для зашифрования открытых данных и расшифрования зашифрованных данных это?

А альфа шифра

Б бета шифра

В гамма шифра

Г лямбда шифра

12 По мнению К. Шеннона, в практических шифрах необходимо использовать два общих принципа:

- рассеивание
- перемешивание
- встряска
- переставка

13 Ключ какой длины используется в алгоритме DES:

- 56 бит
- 64 бит
- 128 бит
- 32 бит

14.Блок какой длины обрабатывается в алгоритме DES:

- 64 бит
- 56 бит
- 128 бит
- 32 бит

15.Сколько основных итераций в алгоритме DES:

- 16
- 14
- 20
- 8

16.Первым этапом алгоритма DES является:

- начальная перестановка битов исходного блока
- конечная перестановка битов исходного блока
- начальное рассеивание битов исходного блока
- начальная замена битов исходного блока

17.Какая операция используется в алгоритме DES:

- сложение по модулю два
- сложение
- битовая инверсия
- битовое умножение

18.Какая операция используется в алгоритме DES при вычислении ключей:

- сдвиг влево
- сдвиг вправо
- битовая инверсия
- битовое умножение

19.Сколько ключей используется в алгоритме DES:

- 16
- 12
- 20
- 32

20. При каком режиме DES длинный файл разбивают на 64-битовые отрезки (блоки) по 8 байтов. Каждый из этих блоков шифруют независимо с ис¬пользованием одного и того же ключа шифрования?

- электронная кодовая книга ECB (Electronic Code Book);
- сцепление блоков шифра CBC (Cipher Block Chaining);
- обратная связь по шифртексту CFB (Cipher Feed Back);

- обратная связь по выходу OFB (Output Feed Back).

21.При каком режиме DES исходный файл M разбивается на 64-битовые блоки: M = M(1)M(2)...M(n). Первый блок M(1) складывается по модулю 2 с 64-битовым начальным вектором IV, который меняется ежедневно и держится в секрете. Полученная сумма затем шифруется с использованием ключа DES, известного и отправителю, и получателю информации. Полученный 64-битовый блок шифртекста C(1) складывается по модулю 2 со вторым блоком исходного текста, результат шифруется и получается второй 64-битовый блок шифртекста C(2) и т.д.

-электронная кодовая книга ECB (Electronic Code Book);

-сцепление блоков шифра CBC (Cipher Block Chaining);

-обратная связь по шифртексту CFB (Cipher Feed Back);

-обратная связь по выходу OFB (Output Feed Back).

22 При каком режиме DES размер блока может отличаться от 64. Исходный файл M считывается последовательными t-битовыми блоками (t <= 64): M = M(1)M(2)...M(n) (остаток дописывается нулями или пробелами).

-электронная кодовая книга ECB (Electronic Code Book);

- сцепление блоков шифра CBC (Cipher Block Chaining);
- обратная связь по шифртексту CFB (Cipher Feed Back);
- обратная связь по выходу OFB (Output Feed Back).

23.Блоками какого размера оперирует алгоритм шифрования IDEA?

- 64 бит
- 56 бит
- 128 бит
- 32 бит

24.Сколько итераций цикла использует алгоритм шифрования IDEA?

- 8
- 16
- 5
- 24

25.Ключ какого размера использует алгоритм шифрования IDEA?

- 128 бит
- 56 бит
- 64 бита
- 32 бит

26.Какие режимы использует отечественный стандарт шифрования?

- простая замена;
- гаммирование;
- гаммирование с обратной связью;
- выработка имитовставки.
- Все перечисленные

27.Чем отличаются ассиметричные шифры от симметричных?

- Простотой реализации;
- наличием постоянного ключа
- наличием трех секретных ключей;
- Наличием двух ключей

28.Какая процедура устанавливает, является ли данный объект именно таким, каким он себя объявляет.

- авторизация
- идентификация

-коммутация

-аутентификация

29.Какая процедура устанавливает сферу действия объекта и доступ¬ные ему ресурсы сети?

- авторизация

- идентификация
-коммутация
-аутентификация
30.Для проверки подлинности применяют:
-механизм запроса-ответа;
-механизм отметки времени.
-Механизм ответа-ответа
-Механизм запроса-запроса
31.Какую процедуру используют для взаимной проверки подлинности ?
- «рукопожатия»
-механизм отметки времени.
-Механизм ответа-ответа
-Механизм запроса-запроса
32. Какие сбои оборудования бывают?
- потери при заражении системы компьютерными вирусами
- несанкционированное копирование, уничтожение или подделка информации
- сбои работы серверов, рабочих станций, сетевых карт и тд - ознакомление с конфиденциальной информацией
33.Какие сбои оборудования, при которых теряется информация, бывают?
- случайное уничтожение или изменение данных
- перебои электропитания
- некорректное использование программного и аппаратного обеспечения, ведущее к уничтожению или изменению данных
- несанкционированное копирование, уничтожение или подделка информации
34 Какие потери информации бывают из-за некорректной работы программ?
- сбои работы серверов, рабочих станций, сетевых карт и тд
- перебои электропитания
-потеря или изменение данных при ошибках ПО
- ознакомление с конфиденциальной информацией
35. Какие потери информации бывают из-за некорректной работы программ?
- потери при заражении системы компьютерными вирусами
- сбои дисковых систем
- перебои электропитания
- сбои работы серверов, рабочих станций, сетевых карт и тд
36. Какие потери информации, связанные с несанкционированным доступом, бывают?
- несанкционированное копирование, уничтожение или подделка информации
- потери при заражении системы компьютерными вирусами
- случайное уничтожение или изменение данных
- сбои дисковых систем
37. Потери из-за ошибки персонала и пользователей бывают?
- несанкционированное копирование, уничтожение или подделка информации
- потери при заражении системы компьютерными вирусами
- случайное уничтожение или изменение данных
- сбои дисковых систем
38. Наиболее надежным средством предотвращения потерь информации при кратковременном отключении электроэнергии?
- установка источников бесперебойного питания (UPS)
- Такого средства не существует
- Каждую минуту сохранять данные
- Перекидывать информацию на носитель, который не зависит от энергии
39. Способ защиты от сбоев процессора?
- установка источников бесперебойного питания (UPS)
- симметричное мультипроцессирование
- Каждую минуту сохранять данные

- Перекидывать информацию на носитель, который не зависит от энергии

Методические материалы, характеризующие процедуры оценивания

На основе типовых заданий из предыдущего раздела программным комплексом информационно-образовательного портала МИ ВлГУ формируются в автоматическом режиме тестовые задания для студентов: 15 вопросов в тесте (8 вопросов Блока 1, 7 вопросов Блока 2). Программный комплекс формирует индивидуальные задания для каждого зарегистрированного в системе студента и устанавливает время прохождения тестирования. Результатом тестирования является процент правильных ответов, с учетом индивидуального семестрового рейтинга студента проставляется экзаменационная оценка за семестр 7.

Максимальная сумма баллов, набираемая студентом по дисциплине равна 100.

Оценка в баллах	Оценка по шкале	Обоснование	***Уровень сформированности компетенций***
Более 80	«Отлично»	Содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному	***Высокий уровень***
66-80	«Хорошо»	Содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками	***Продвинутый уровень***

50-65	«Удовлетворительно»	Содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий, возможно, содержат ошибки	***Пороговый уровень***
Менее 50	«Неудовлетворительно»	Содержание курса не освоено, необходимые практические навыки работы не сформированы, выполненные учебные задания содержат грубые ошибки	***Компетенции не сформированы***

3. Задания в тестовой форме по дисциплине

Примеры заданий:

Информационная безопасность и защита информации

Вопросы открытого типа

1. Виды информационной безопасности...

A) Персональная, корпоративная, государственная

B) Клиентская, серверная, сетевая

C) Локальная, глобальная, смешанная

ANSWER: C

2. Вредоносная программа - это...

A) программа, специально разработанная для нарушения нормального функционирования систем

B) упорядочение абстракций, расположение их по уровням

C) процесс разделения элементов абстракции, которые образуют ее структуру и поведение

ANSWER: A

3. Где применяются средства контроля динамической целостности?

A) анализе потока финансовых сообщений

B) обработке данных

C) при выявлении кражи, дублирования отдельных сообщений

ANSWER: C

4. Действие Закона "О государственной тайне" распространяется_

A) на всех граждан и должностных лиц РФ

B) только на должностных лиц

C) на граждан, которые взяли на себя обязательство выполнять требования законодательства о государственной тайне

D) на всех граждан и должностных лиц, если им предоставили для работы закрытые сведения

ANSWER: D

5. Для чего создаются информационные системы?

A) получения определенных информационных услуг

B) обработки информации

C) все ответы правильные

ANSWER: A

6. Информацию с ограниченным доступом делят

A) государственную тайну

B) конфиденциальную информацию
C) достоверную информацию
ANSWER: B
7. Информация, которую следует защищать (по нормативам, правилам сети, системы) называется...
A) Регламентированной
B) Правовой
C) Защищаемой
ANSWER: C
8. Источник угрозы - это..
A) потенциальный злоумышленник
B) злоумышленник
C) нет правильного ответа
ANSWER: A
9. Какие средства используется на инженерных и технических мероприятиях в защите информации:
A) Аппаратные
B) Криптографические
C) Физические
D) Все верно
ANSWER: D
10. Какие существуют грани вредоносного П.О.?
A) вредоносная функция
B) внешнее представление
C) способ распространения
D) все верно
ANSWER: D
11. Какие трудности возникают в информационных системах при конфиденциальности?
A) сведения о технических каналах утечки информации являются закрытыми
B) на пути пользовательской криптографии стоят многочисленные технические проблемы
C) все ответы правильные
ANSWER: C
12. К информации ограниченного доступа не относится
A) Государственная тайна
B) Размер золотого запаса страны
C) Персональные данные
D) Коммерческая тайна
ANSWER: C
13. К какому виду угроз относится присвоение чужого права?
A) нарушение права собственности
B) нарушение содержания
C) внешняя среда
ANSWER: A
14. Когда получен спам по e-mail с приложенным файлом, следует...
A) Прочитать приложение, если оно не содержит ничего ценного - удалить
B) Сохранить приложение в парке "Спам", выяснить затем IP-адрес генератора спама
C) Удалить письмо с приложением, не раскрывая (не читая) его
ANSWER: C
15. Конфиденциальную информацию можно разделить:
A) Предметную
B) Служебную
C) Глобальную

ANSWER: B

16. К организационно - административному обеспечению информации относится:

A) взаимоотношения исполнителей

B) подбор персонала

C) регламентация производственной деятельности

D) все верно

ANSWER: D

17. К основным принципам обеспечения информационной безопасности относится...

A) Экономической эффективности системы безопасности

B) Многоплатформенной реализации системы

C) Усиления защищенности всех звеньев системы

ANSWER: A

18. К основным типам средств воздействия на компьютерную сеть относится...

A) Компьютерный сбой

B) Логические закладки ("мины")

C) Аварийное отключение питания

ANSWER: B

19. К основным функциям системы безопасности можно отнести все перечисленное...

A) Установление регламента, аудит системы, выявление рисков

B) Установка новых офисных приложений, смена хостинг-компании

C) Внедрение аутентификации, проверки контактных данных пользователей

ANSWER: A

20. К правовым методам, обеспечивающим информационную безопасность, относятся...

A) Разработка аппаратных средств обеспечения правовых данных

B) Разработка и установка во всех компьютерных правовых сетях журналов учета действий

C) Разработка и конкретизация правовых нормативных актов обеспечения безопасности

ANSWER: C

21. Криптографические средства - это...

A) средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования

B) специальные программы и системы защиты информации в информационных системах различного назначения

C) механизм, позволяющий получить новый класс на основе существующего

ANSWER: A

22. Наиболее важным при реализации защитных мер политики безопасности является...

A) Аудит, анализ затрат на проведение защитных мер

B) Аудит, анализ безопасности

C) Аудит, анализ уязвимостей, риск-ситуаций

ANSWER: C

23. Наиболее распространены средства воздействия на сеть офиса...

A) Слабый трафик, информационный обман, вирусы в интернет

B) Вирусы в сети, логические мины (закладки), информационный перехват

C) Компьютерные сбои, изменение администрирования, топологии

ANSWER: B

24. Наиболее распространены угрозы информационной безопасности корпоративной системы...

A) Покупка нелицензионного ПО

B) Ошибки эксплуатации и неумышленного изменения режима работы системы

C) Сознательного внедрения сетевых вирусов

ANSWER: B

25. Наиболее распространены угрозы информационной безопасности сети...

A) Распределенный доступ клиент, отказ оборудования

B) Моральный износ сети, инсайдерство

C) Сбой (отказ) оборудования, нелегальное копирование данных

ANSWER: C

26. Окно опасности - это...

A) промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется

B) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области

C) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере

ANSWER: A

Вопросы закрытого типа

1. Попытка реализации угрозы – это..

(атака)

2. Код, обладающий способностью к распространению путем внедрения в другие программы – это…

(вирус)

3. Возможность за приемлемое время получить требуемую информационную услугу – это

(доступность)

4. Комплекс мероприятий, направленных на обеспечение информационной безопасности – это…информации.

(защита)

5. Защита от несанкционированного доступа к информации – это

(конфиденциальность)

6. Нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций – это ..

(отказ)

7. Неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния – это…

(ошибка)

8. Защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре – это

(информационная безопасность)

9. Комплекс руководств, требований обеспечения необходимого уровня безопасности – это

(политика безопасности)

10. Нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент – это..

(сбой)

11. Потенциальная возможность определенным образом нарушить информационную безопасность – это..

(угроза)

12. Ситуация, характеризуемая потерей данных в системе – это ..

(утечка)

13. Код способный самостоятельно, то есть без внедрения в другие программы, вызывать распространения своих копий по ИС и их выполнять.

(вирус)

14. Сведения, защищаемые государством в области военной, экономической и прочей деятельности – это

(государственная тайна)

15. Активный компонент системы, который может стать причиной потока информации от объекта к субъекту или изменения состояния системы – это …

(субъект)

16. Пассивный компонент системы, хранящий, принимающий или передающий информацию – это..

(объект)

17. Какой подход направлен на противодействие четко определенным угрозам в заданных условиях

(фрагментарный)

18. Какой подход ориентирован на создание защищенной среды обработки информации в АСОИ, объединяющей в единый комплекс разнородные меры противодействия угрозам.

(комплексный)

19. Матрица, в которой столбец соответствует объекту системы, а строка – субъекту называется матрицей…

(доступа)

20. Совокупность методов преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для противника – это

(криптография)

21. Наука о раскрытии исходного текста зашифрованного сообщения без доступа к ключу.

(криптоанализ)

22. конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма

(ключ)

23. Шифрование …. заключается в том, что символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста.

(перестановкой)

24. Шифрование …… заключается в том, что символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены.

(заменой (подстановкой))

25. Зашифруйте слово «информатика» шифром Цезаря со сдвигом равным 3.

(прчсупгхлнр)

26. Расшифруйте слово «гжйрсвупруфю» при условии, что оно зашифровано шифром Цезаря со сдвигом равным 2.

(безопасность)

Полный перечень тестовых заданий с указанием правильных ответов, размещен в банке вопросов на информационно-образовательном портале института по ссылке https://www.mivlgu.ru/iop/question/edit.php?cmid=56738

Оценка рассчитывается как процент правильно выполненных тестовых заданий из их общего числа.