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 *ТБ*

«УТВЕРЖДАЮ»
Заместитель директора по УР
_____Д.Е. Андрианов
25.05.2021

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность

Направление подготовки *20.03.01 Техносферная безопасность*

Профиль подготовки *Безопасность жизнедеятельности в техносфере*

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	**108 / 3**	**16**	**32**		**1,6**	**0,25**	**49,85**	**58,15**	**Зач.**
Итого	**108 / 3**	**16**	**32**		**1,6**	**0,25**	**49,85**	**58,15**	

Муром, 2021 г.

1. Цель освоения дисциплины

Цель дисциплины: изучение комплекса проблем информационной безопасности организаций различных типов и направлений деятельности, построения, функционирования и совершенствования правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты ценной и конфиденциальной информации в сферах охраны интеллектуальной собственности и сохранности их информационных ресурсов.

Задачи курса - овладение теоретическими, практическими и методическими вопросами обеспечения информационной безопасности и освоение системных комплексных методов защиты информации от различных видов объективных и субъективных угроз в процессе ее возникновения, обработки, использования и хранения. Изучаемые вопросы рассматриваются в широком диапазоне современных проблем и затрагивают предметные сферы защиты как документированной информации (на бумажных и технических носителях), циркулирующей в традиционном или электронном документообороте, находящейся в компьютерных системах, так и недокументированной информации, распространяемой персоналом в процессе управленческой (деловой) или производственной деятельности.

2. Место дисциплины в структуре ОПОП ВО

Для успешного освоения дисциплины «Информационная безопасность» от обучающегося требуются знании и навыки, полученные в результате изучения курсов «Математика», «Информатика», «Информационные технологии в управлении техносферной безопасностью». Полученные студентами знания и умения могут быть использованы при выполнении бакалаврской работы.

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-4 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-4.1 Обладает знаниями в области современных информационных технологий в профессиональной деятельности	знать основные понятия в области информационной безопасности (ОПК-4.1) знать основные методы обеспечения защиты информации (ОПК-4.1) знать современные тенденции развития техники и технологий в области обеспечения информационной безопасности (ОПК-4.1) уметь осуществлять шифрование данных и осуществлять их передачу с использованием современных средствам телекоммуникаций (ОПК-4.1) уметь использовать электронную подпись в профессиональной деятельности (ОПК-4.1)	тест

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

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	Концепция информационной безопасности	7	4	2						18	тестирование
2	Направления обеспечения информационной безопасности	7	4	16						4	тестирование
3	Способы защиты информации	7	8	14						36,15	тестирование
Всего за семестр		108	16	32				1,6	0,25	58,15	Зач.
Итого		108	16	32				1,6	0,25	58,15	

4.1.2. Содержание дисциплины

4.1.2.1. Перечень лекций

Семестр 7

Раздел 1. Концепция информационной безопасности

Лекция 1.

Основные понятия и определения в сфере информационной безопасности (2 часа).

Лекция 2.

Угрозы информации (2 часа).

Раздел 2. Направления обеспечения информационной безопасности

Лекция 3.

Правовое обеспечение информационной безопасности (2 часа).

Лекция 4.

Организационное и инженерно-техническое обеспечение информационной безопасности (2 часа).

Раздел 3. Способы защиты информации

Лекция 5.

Система защиты информации (2 часа).

Лекция 6.

Криптографические методы защиты компьютерной информации (2 часа).

Лекция 7.

Защита компьютерной информации в компьютерных сетях (2 часа).

Лекция 8.

Компьютерные преступления (2 часа).

4.1.2.2. Перечень практических занятий

Семестр 7

Раздел 1. Концепция информационной безопасности

Практическое занятие 1

Изучение системы отечественных стандартов информационной безопасности (2 часа).

Раздел 2. Направления обеспечения информационной безопасности

Практическое занятие 2

Настройки безопасности операционной системы Windows 7 (2 часа).

Практическое занятие 3

Настройки безопасности приложений Microsoft Office (2 часа).

Практическое занятие 4

Организация консоли администрирования в ОС Windows (2 часа).

Практическое занятие 5

Консоль администрирования в ОС Windows: Работа с пользователями (2 часа).

Практическое занятие 6

Программа «КриптоАРМ»: Работа с сертификатами (2 часа).

Практическое занятие 7

Программа «КриптоАРМ»: Шифрование данных (2 часа).

Практическое занятие 8

Программа «КриптоАРМ»: электронная подпись (2 часа).

Практическое занятие 9

Программа «КриптоАРМ»: настройки программы (2 часа).

Раздел 3. Способы защиты информации

Практическое занятие 10

Настройки безопасности Интернет-обозревателей (2 часа).

Практическое занятие 11

Изучение методов шифрования: простых шифрующих таблиц, магических квадратов, маршрутных перестановок (2 часа).

Практическое занятие 12

Изучение методов шифрования: шифр Цезаря, аффинная система подстановок Цезаря, шифр Плейфера, шифр Трисемуса (2 часа).

Практическое занятие 13

Изучение методов шифрования: шифр Хилла, шифр Атбаш, Тарабарская грамота, шифр Полибия (2 часа).

Практическое занятие 14

Изучение методов шифрования: шифр Гронсфельда, шифр Виженера, шифр Уитстона, шифр Вернама (2 часа).

Практическое занятие 15

Защита данных с помощью шифрования диска BitLocker (2 часа).

Практическое занятие 16

Установка и использование Защитника Windows (2 часа).

4.1.2.3. Перечень лабораторных работ

Не планируется.

4.1.2.4. Перечень тем и учебно-методическое обеспечение самостоятельной работы

Перечень тем, вынесенных на самостоятельное изучение:

1. Угрозы информации: Ознакомление.

2. Угрозы информации: Модификация.
3. Угрозы информации: Уничтожение.
4. Угрозы информации: Блокирование.
5. Угрозы конфиденциальной информации.
6. Основные законы в области информационной безопасности.
7. Организационная защита.
8. Средства инженерно-технической защиты.
9. Аппаратные средства защиты.
10. Программные средства защиты.
11. Криптографические средства защиты.
12. Криптографические методы защиты.
13. Методы шифрования.
14. Защита информации в компьютерных сетях.
15. Основные виды компьютерных преступлений.

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 общее.

Срок обучения 5л.

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.)
9	**108 / 3**	**4**	**6**		**2**	**0,5**	**12,5**	**91,75**	**Зач.(3,75)**
Итого	**108 / 3**	**4**	**6**		**2**	**0,5**	**12,5**	**91,75**	**3,75**

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	Концепция информационной безопасности	9	2	2						30	тестирование
2	Направления обеспечения информационной безопасности	9		2						6	тестирование
3	Способы защиты информации	9	2	2						55,75	тестирование
Всего за семестр		108	4	6		+		2	0,5	91,75	Зач.(3,75)
Итого		108	4	6				2	0,5	91,75	3,75

4.2.2. Содержание дисциплины

4.2.2.1. Перечень лекций

Семестр 9

Раздел 1. Концепция информационной безопасности

Лекция 1.

Основные понятия и определения в сфере информационной безопасности (2 часа).

Раздел 3. Способы защиты информации

Лекция 2.

Система защиты информации (2 часа).

4.2.2.2. Перечень практических занятий

Семестр 9

Раздел 1. Концепция информационной безопасности

Практическое занятие 1.

Изучение системы отечественных стандартов информационной безопасности (2 часа).

Раздел 2. Направления обеспечения информационной безопасности

Практическое занятие 2.

Организация консоли администрирования в ОС Windows (2 часа).

Раздел 3. Способы защиты информации

Практическое занятие 3.

Настройки безопасности Интернет-обозревателей (2 часа).

4.2.2.3. Перечень лабораторных работ

Не планируется.

4.2.2.4. Перечень тем и учебно-методическое обеспечение самостоятельной работы

Перечень тем, вынесенных на самостоятельное изучение:

1. Угрозы информации: Ознакомление.
2. Угрозы информации: Модификация.
3. Угрозы информации: Уничтожение.
4. Угрозы информации: Блокирование.
5. Угрозы конфиденциальной информации.
6. Основные законы в области информационной безопасности.
7. Организационная защита.
8. Средства инженерно-технической защиты.
9. Аппаратные средства защиты.
10. Программные средства защиты.
11. Криптографические средства защиты.
12. Криптографические методы защиты.
13. Методы шифрования.
14. Защита информации в компьютерных сетях.
15. Основные виды компьютерных преступлений.

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. Национальные интересы и безопасность России.
2. Методы обеспечения информационной безопасности.
3. Информационные ресурсы.
4. Информационная война. Информационное оружие.
5. Угрозы безопасности России.
6. Интегральная безопасность.
7. Угрозы безопасности АСОД.
8. Стандарты в области ИБ.
9. Показатели защищенности СВТ.
10. Защита Информации в АСОД.
11. Методы и системы защиты информации.
12. Виды доступа. Уровни доступа Контроль доступа.
13. Автоматизированная система, как объект информационной защиты.
14. Основные методы и приемы защиты от несанкционированного доступа.
15. Проблема вирусного заражения программ. Классификация вирусов. Способы заражения программ.
16. Структура современных вирусных программ.

17. Перспективные методы антивирусной защиты. Основные классы антивирусных программ.

18. Криптографические методы защиты информации.

19. Криптология. Этапы развития. Стеганография.

20. Шифрование заменой (подстановка).

21. Шифр Цезаря. Шифр Атбаш.

22. Квадрат Полибия.

23. Афинные криптосистемы.

24. Моноалфавитная подстановка.

25. Полиалфавитная подстановка.

26. Таблица Вижинера.

27. Квадрат Бьюфорта.

28. Монофоническая замена.

29. Система Плейфера.

30. Шифрование методом перестановки.

31. Шифрование с помощью аналитических преобразований.

32. Шифрование методом гаммирования.

33. Система с открытым ключом.

34. Электронно-цифровая подпись и приемы хеширования.

35. Проблемы защиты информации в сетях ЭВМ. Архитектура механизмов защиты в сетях.

36. Цели, функции и задачи защиты информации в сетях ЭВМ.

37. Межсетевые экраны – брандмауэры.. Прокси (Proxy) серверы.

38. Организационно-правовое обеспечение ИБ.

39. Комплексное обеспечение безопасности.

4.2.2.6. Примерный перечень тем курсовых работ (проектов)

Не планируется.

5. Образовательные технологии

В процессе изучения дисциплины применяется контактная технология преподавания (за исключением самостоятельно изучаемых студентами вопросов). При проведении практических 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 практических работ студенты получают индивидуальные занятия, которые самостоятельно выполняются с использованием компьютерной техники.

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. Башлы, П. Н. Информационная безопасность и защита информации : учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. — Москва : Евразийский открытый институт, 2012. — 311 с. - http://www.iprbookshop.ru/10677

2. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере : учебное пособие / А. Е. Фаронов. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 154 с. - http://www.iprbookshop.ru/89453

3. Информационная безопасность: Практикум для студентов образовательной программы 20.03.01 Техносферная безопасность / сост. Шарапов Р.В. [Электронный ресурс]. – Электрон. текстовые дан. (1,7 Мб). – Муром: МИ ВлГУ, 2016. – 1 электрон. опт. диск (CD-R). – Систем. требования: процессор x86 с тактовой частотой 500 МГц и выше; 512 Мб ОЗУ; Windows XP/7/8; видеокарта SVGA 1280x1024 High Color (32 bit); привод CD-ROM. – Загл. с экрана. – № госрегистрации 0321602442. - http://evrika.mivlgu.ru/index.php?mod=view_book&com=read_book&book_id=2838

4. Работа с «КриптоАРМ»: Практикум для студентов образовательной про-граммы 20.03.01 Техносферная безопасность / сост. Шарапов Р.В. [Электронный ресурс]. – Электрон. текстовые дан. (2,47 Мб). – Муром: МИ ВлГУ, 2016. – 1 электрон. опт. диск (CD-R). – Систем. требования: процессор x86 с тактовой частотой 500 МГц и выше; 512 Мб ОЗУ; Windows XP/7/8; видеокарта SVGA 1280x1024 High Color (32 bit); привод CD-ROM. – Загл. с экрана. – № госрегистрации 0321602440. - http://evrika.mivlgu.ru/index.php?mod=view_book&com=read_book&book_id=2836

5. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. - http://www.iprbookshop.ru/97562

6. Артемов, А. В. Информационная безопасность : курс лекций / А. В. Артемов. — Орел : Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. — 256 с. - http://www.iprbookshop.ru/33430

7.2. Дополнительная учебно-методическая литература по дисциплине

1. Формализация подхода к определению актуальности угроз информационной безопасности : монография / О. М. Голембиовская, М. Ю. Рытов, М. М. Голембиовский [и др.]. — Саратов : Вузовское образование, 2022. — 147 с. - https://www.iprbookshop.ru/121143

2. Зенков, А. В. Основы информационной безопасности : учебное пособие / А. В. Зенков. — Москва, Вологда : Инфра-Инженерия, 2022. — 104 с. - https://www.iprbookshop.ru/124242

3. Семенов, Ю. А. Процедуры, диагностики и безопасность в Интернет : учебное пособие / Ю. А. Семенов. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2022. — 581 с. - https://www.iprbookshop.ru/120489

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:

ЦИТфорум http://citforum.ru/

Журнал "Информатика и системы управления" http://ics.khstu.ru/

Программное обеспечение:

LibreOffice (Mozilla Public License v2.0)

Google Chrome (Лицензионное соглашение Google)

Microsoft Windows 10 Professional (Программа Microsoft Azure Dev Tools for Teaching (Order Number: IM126433))

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

iprbookshop.ru
evrika.mivlgu.ru
citforum.ru
ics.khstu.ru
mivlgu.ru/iop

8. Материально-техническое обеспечение дисциплины

Лекционная аудитория
проектор NEC Projector MP40G; ноутбук HP.

Компьютерный класс
10 компьютеров Intel Core i3-2100; 5 компьютеров Pentium CPU G4620, 3.70 GHz.

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.

На практических занятиях пройденный теоретический материал подкрепляется решением задач по основным темам дисциплины. Занятия проводятся в компьютерном классе, используя специальное программное обеспечение. Каждой подгруппе обучающихся преподаватель выдает задачу, связанную с информационной безопасностью. В конце занятия обучающие демонстрируют полученные результаты преподавателю и при необходимости делают работу над ошибками.

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 – зачет. 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 *20.03.01 Техносферная безопасность* и профилю подготовки *Безопасность жизнедеятельности в техносфере*
Рабочую программу составил *к.т.н., доцент Шарапов Р.В.*_____

Программа рассмотрена и одобрена на заседании кафедры *ТБ*

протокол № 16 от 25.05.2021 года.
Заведующий кафедрой *ТБ* _____*Шарапов Р.В.*
(Подпись)

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

протокол № 6 от 25.05.2021 года.
Председатель комиссии МСФ _____ *Калиниченко М.В.*
(Подпись) (Ф.И.О.)

Приложение

Фонд оценочных материалов (средств) по дисциплине

Информационная безопасность

1. Оценочные материалы для проведения текущего контроля успеваемости по дисциплине

Тесты:

1. Какие законы существуют в России в области компьютерного права?

Выберите несколько из 6 вариантов ответа:

1) О государственной тайне

2) об авторском праве и смежных правах

3) о гражданском долге

4) о правовой охране программ для ЭВМ и БД

5) о правовой ответственности

6) об информации, информатизации, защищенности информации

2. Какие существуют основные уровни обеспечения защиты информации?

Выберите несколько из 7 вариантов ответа:

1) законодательный

2) административный

3) программно-технический

4) физический

5) вероятностный

6) процедурный

7) распределительный

3. Физические средства защиты информации

1) средства, которые реализуются в виде автономных устройств и систем

2) устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу

3) это программы, предназначенные для выполнения функций, связанных с защитой информации

4) средства, которые реализуются в виде электрических, электромеханических и электронных устройств

4. В чем заключается основная причина потерь информации, связанной с ПК?

1) с глобальным хищением информации

2) с появлением интернета

3) с недостаточной образованностью в области безопасности

5. Технические средства защиты информации

1) средства, которые реализуются в виде автономных устройств и систем

2) устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу

3) это программы, предназначенные для выполнения функций, связанных с защитой информации

4) средства, которые реализуются в виде электрических, электромеханических и электронных устройств

6. К аспектам ИБ относятся

Выберите несколько из 5 вариантов ответа:

1) дискретность

2) целостность

3) конфиденциальность

4) актуальность

5) доступность

7. Что такое криптология?

1) защищенная информация

2) область доступной информации

3) тайная область связи

8. Что такое несанкционированный доступ (нсд)?

1) Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа

2) Создание резервных копий в организации

3) Правила и положения, выработанные в организации для обхода парольной защиты

4) Вход в систему без согласования с руководителем организации

5) Удаление не нужной информации

9. Что является основой для формирования государственной политики в сфере информации? (Ответьте 1 словом)

Запишите ответ:

_____

10. Что такое целостность информации?

1) Свойство информации, заключающееся в возможности ее изменения любым субъектом

2) Свойство информации, заключающееся в возможности изменения только единственным пользователем

3) Свойство информации, заключающееся в ее существовании в виде единого набора файлов

4) Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию)

11.Кто является знаковой фигурой в сфере информационной безопасности

1) Митник

2) Шеннон

3) Паскаль

4) Беббидж

12. В чем состоит задача криптографа?

1) взломать систему защиты

2) обеспечить конфиденциальность и аутентификацию передаваемых сообщений

13. Под ИБ понимают

1) защиту от несанкционированного доступа

2) защиту информации от случайных и преднамеренных воздействий естественного и искуственного характера

3) защиту информации от компьютерных вирусов

14. Что такое аутентификация?

1) Проверка количества переданной и принятой информации

2) Нахождение файлов, которые изменены в информационной системе несанкционированно

3) Проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа).

4) Определение файлов, из которых удалена служебная информация

5) Определение файлов, из которых удалена служебная информация

15. "Маскарад"- это

1) осуществление специально разработанными программами перехвата имени и пароля

2) выполнение каких-либо действий одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями

16. Верификация -

1) это проверка принадлежности субъекту доступа предъявленного им идентификатора.

2) проверка целостности и подлинности инф, программы, документа

3) это присвоение имени субъекту или объекту

17. Кодирование информации -

1) представление информации в виде условных сигналов с целью автоматизации ее хранения, обработки, передачи и т.д.

2) метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом

18. Утечка информации

1) несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу

2) ознакомление постороннего лица с содержанием секретной информации

3) потеря, хищение, разрушение или неполучение переданных данных

19. Под изоляцией и разделением (требование к обеспечению ИБ) понимают

1) разделение информации на группы так, чтобы нарушение одной группы информации не влияло на безопасность других групп информации (документов)

2) разделение объектов защиты на группы так, чтобы нарушение защиты одной группы не влияло на безопасность других групп

20. К аспектам ИБ относятся

Выберите несколько из 5 вариантов ответа:

1) дискретность

2) целостность

3) конфиденциальность

4) актуальность

5) доступность

21. Линейное шифрование -

1) несанкционированное изменение информации, корректное по форме и содержанию, но отличное по смыслу

2) криптографическое преобразование информации при ее передаче по прямым каналам связи от одного элемента ВС к другому

3) криптографическое преобразование информации в целях ее защиты от ознакомления и модификации посторонними лицами

22. Прочность защиты в АС

1) вероятность не преодоления защиты нарушителем за установленный промежуток времени

2) способность системы защиты информации обеспечить достаточный уровень своей безопасности

3) группа показателей защиты, соответствующая определенному классу защиты

23. Уровень секретности - это

1) ответственность за модификацию и НСД информации

2) административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю конкретной секретной информации, регламентируемой специальным документом, с учетом государственных, военно-стратегических, коммерческих, служебных или частных интересов

24. Угроза - это

1) возможное событие, действие, процесс или явление, которое может привести к ущербу чьих-либо интересов

2) событие, действие, процесс или явление, которое приводит к ущербу чьих-либо интересов

25. Под ИБ понимают

1) защиту от несанкционированного доступа

2) защиту информации от случайных и преднамеренных воздействий естественного и искуственного характера

3) защиту информации от компьютерных вирусов

26. Что такое криптография?

1) метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом

2) область доступной информации

3) область тайной связи, с целью защиты от ознакомления и модификации посторонним лицом

27. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, установленными собственником информации называется

1) кодируемой
2) шифруемой
3) недостоверной
4) защищаемой

28. Продолжите фразу: "Административная и законодательная мера, соответствующая мере ответственности лица за потерю конкретной секретной информации, регламентирующаяся специальным документом с учетом государственных и военно-стратегических, коммерческих или частных интересов - это..."

Запишите ответ:

_____

29. Продолжите фразу: " Последовательность символов, недоступная для посторонних, предназначенная для идентификации и аутентификации субъектов и объектов между собой - это..."

Запишите ответ:

_____

30. Способ представления информации в вычислительных системах

Запишите ответ:

_____

31. Вставьте пропущенное слово:

Информация может быть защищена без аппаратных и программных средств защиты с помощью _____ преобразований.

Запишите ответ:

_____

32. Абстрактное содержание какого-либо высказывания, описание, указание, сообщение либо известие - это

1) текст
2) данные
3) информация
4) пароль

33. Какие атаки предпринимают хакеры на программном уровне?

Выберите несколько из 4 вариантов ответа:

1) атаки на уровне ОС
2) атаки на уровне сетевого ПО
3) атаки на уровне пакетов прикладных программ
4) атаки на уровне СУБД

34. Организационные угрозы подразделяются на

Выберите несколько из 4 вариантов ответа:

1) угрозы воздействия на персонал
2) физические угрозы
3) действия персонала
4) несанкционированный доступ

35. Виды технической разведки (по месту размещения аппаратуры)

Выберите несколько из 7 вариантов ответа:

1) космическая
2) оптическая
3) наземная
4) фотографическая
5) морская
6) воздушная
7) магнитометрическая

36. Основные группы технических средств ведения разведки

Выберите несколько из 5 вариантов ответа:

1) радиомикрофоны

2) фотоаппараты

3) электронные "уши"

4) дистанционное прослушивание разговоров

5) системы определения местоположения контролируемого объекта

37. Разновидности угроз безопасности

Выберите несколько из 6 вариантов ответа:

1) техническая разведка

2) программные

3) программно-математичекие

4) организационные

5) технические

6) физические

38. Потенциально возможное событие, действие, процесс или явление, которое может причинить ущерб чьих-нибудь данных, называется

1) угрозой;

2) опасностью;

3) намерением;

4) предостережением.

39. Какая угроза возникает в результате технологической неисправности за пределами информационной системы?

Запишите ответ:

_____

40. Из каких компонентов состоит программное обеспечение любой универсальной компьютерной системы?

1) операционной системы, сетевого программного обеспечения

2) операционной системы, сетевого программного обеспечения и системы управления базами данных;

3) операционной системы, системы управления базами данных;

4) сетевого программного обеспечения и системы управления базами данных.

41. Комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объектам защиты называется

1) системой угроз;

2) системой защиты;

3) системой безопасности;

4) системой уничтожения.

42. К угрозам какого характера относятся действия, направленные на сотрудников компании или осуществляемые сотрудниками компании с целью получения конфиденциальной информации или нарушения функции бизнес-процессов?

Запишите ответ:

_____

43. К видам защиты информации относятся:

Выберите несколько из 4 вариантов ответа:

1) правовые и законодательные:

2) морально-этические;

3) юридические;

4) административно-организационные;

44. Доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации называется

Запишите ответ:

_____

45. К методам защиты от НСД относятся

Выберите несколько из 5 вариантов ответа:

1) разделение доступа;

2) разграничение доступа;

3) увеличение доступа;

4) ограничение доступа.

5) аутентификация и идентификация

46. Метод пароля и его модификация, метод вопрос-ответ, метод секретного алгоритма - это методы

Запишите ответ:

_____

47. Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности называется

1) политикой информации

2) защитой информации

3) политикой безопасности

4) организацией безопасности

48. Выделите группы, на которые делятся средства защиты информации:

1) физические, аппаратные, программные, криптографические, комбинированные;

2) химические, аппаратные, программные, криптографические, комбинированные;

3) физические, аппаратные, программные, этнографические, комбинированные;

49. Техническое, криптографическое, программное и иное средство, предназначенное для защиты информации, средство, в котором оно реализовано, а также средство контроля эффективности защиты информации- все это есть

Запишите ответ:

_____

50. Что такое компьютерный вирус?

1) Разновидность программ, которые способны к размножению

2) Разновидность программ, которые самоуничтожаются

3) Разновидность программ, которые не работают

4) Разновидность программ, которые плохо работают

51. Как подразделяются вирусы в зависимости от деструктивных возможностей?

1) Сетевые, файловые, загрузочные, комбинированные

2) Безвредные, неопасные, опасные, очень опасные

3) Резидентные, нерезидентные

4) Полиморфные, макровирусы, вирусы-невидимки, "паразитические", "студенческие", "черви", компаньон-вирусы

52. Нежелательная цепочка носителей информации, один или несколько из которых являются правонарушителем или его специальной аппаратурой называется

Запишите ответ:

_____

53. Установите соответствие

Укажите соответствие для всех 4 вариантов ответа:

1) это комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны за счет электромагнитных полей побочного характера и наводок

2) это комплекс мероприятий, исключающих или уменьшающих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны в виде производственных или промышленных отходов

3) это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей

4) это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет распространения световой энергии

__ защита информации от утечки по акустическому каналу

__ Защита информации от утечки по визуально-оптическому каналу

__ Защита информации от утечки по электромагнитным каналам

__ Защита информации от утечки по материально-вещественному каналу

54. Надежным средством отвода наведенных сигналов на землю служит

Запишите ответ:

_____

55. Установите соответствие

Укажите соответствие для всех 2 вариантов ответа:

1) наука о скрытой передаче информации путем сохранения в тайне самого факта передачи

2) наука скрывающая содержимое секретного сообщения

__ стеганография

__ криптография

Общее распределение баллов текущего контроля по видам учебных работ для студентов

Рейтинг-контроль 1	5 практических заданий, промежуточный тест	20
Рейтинг-контроль 2	5 практических заданий, промежуточный тест	20
Рейтинг-контроль 3	6 практических заданий, промежуточный тест	24
Посещение занятий студентом		16
Дополнительные баллы (бонусы)		5
Выполнение семестрового плана самостоятельной работы		15

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)

Тесты:

ОПК-4:

Блок 1 (знать).

1. Что означает термин ДОСТУПНОСТЬ ИНФОРМАЦИИ?

- Это свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.

- Это подверженность информации воздействию различных дестабилизирующих факторов, которые могут привести к нарушению её конфиденциальности, целостности, доступности, или неправомерному её тиражированию.

- Это свойство информации, заключающееся в её существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному её состоянию).

2. Что означает термин ЦЕЛОСТНОСТЬ ИНФОРМАЦИИ?

- Это свойство информации, заключающееся в её существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному её состоянию).

- Это свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.

- Это подверженность информации воздействию различных дестабилизирующих факторов, которые могут привести к нарушению её конфиденциальности, целостности, доступности, или неправомерному её тиражированию.

3. Что означает термин УЯЗВИМОСТЬ ИНФОРМАЦИИ?

- Это подверженность информации воздействию различных дестабилизирующих факторов, которые могут привести к нарушению её конфиденциальности, целостности, доступности, или неправомерному её тиражированию.

- Это свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.

- Это свойство информации, заключающееся в её существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному её состоянию)

4. В чем заключается конфиденциальность компонента системы?

- В том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия.

- В том, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права.

- В том, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы.

5. В чем заключается целостность компонента системы?

- В том, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права.

- В том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия.

- В том, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы.

6. В чем заключается доступность компонента системы?

- В том, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы.

- В том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия.

- В том, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права.

7. Что означает термин ПРАВОВЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ?

- Это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения.

- Это традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией.

- Это меры, регламентирующие процессы функционирования системы обработки данных, использования её ресурсов.

8. Что означает термин МОРАЛЬНО-ЭТИЧЕСКИЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ?

- Это традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией.

- Это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения.

- Это меры, регламентирующие процессы функционирования системы обработки данных, использование её ресурсов.

9. Что означает термин ОРГАНИЗАЦИОННЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ?

- Это меры, регламентирующие процессы функционирования системы обработки данных, использование её ресурсов, деятельность персонала, а так же порядок взаимодействия пользователей с системой.

- Это действующие в стране законы, указы и другие нормативные акты.

- Это традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией.

10. Что означает термин ФИЗИЧЕСКИЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ?

- Это разного рода механические или электронно-механические устройства и сооружения, специально предназначенные для создания различных препятствий на возможных путях проникновения доступа потенциальных нарушителей к компонентам защищаемой информации.

- Это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения.

- Это меры, регламентирующие процессы функционирования системы обработки данных, использование её ресурсов.

11. Что означает термин АУТЕНТИФИКАЦИЯ?

- Это проверка подлинности объекта или субъекта

- Это проверка целостности информации, программы, документа

- Это присвоение имени субъекту или объекту

12. Что означает термин ВЕРИФИКАЦИЯ?

- Это проверка целостности информации, программы, документа.

- Это проверка подлинности субъекта или объекта.

- Это присвоение имени субъекту или объекту.

13. Что означает термин ИДЕНТИФИКАЦИЯ?

- Это присвоение имени субъекту или объекту.

- Это проверка подлинности субъекта или объекта.

- Это проверка целостности информации, программы, документа.

14. Что означает термин КРИПТОГРАФИЯ?

- Это метод специального преобразования информации с целью сокрытия от посторонних лиц

- Это преобразование информации в виде условных сигналов с целью автоматизации её хранения, обработки, передачи и ввода-вывода

- Это преобразование информации при её передаче по каналам связи от одного элемента вычислительной сети к другому

15. Что означает термин КОДИРОВАНИЕ ИНФОРМАЦИИ?

- Это преобразование информации в виде условных сигналов с целью автоматизации её хранения, обработки, передачи и ввода-вывода.

- Это метод специального преобразования информации с целью сокрытия от посторонних лиц.

- Это криптографическое преобразование информации при её передаче по каналам связи от одного элемента в вычислительной сети к другому.

16. Что означает термин ЛИНЕЙНОЕ ШИФРОВАНИЕ?

- Это криптографическое преобразование информации при её передаче по каналам связи от одного элемента вычислительной сети к другому.

- Это метод специального преобразования информации с целью сокрытия от посторонних лиц.

- Это преобразование информации в виде условных сигналов с целью автоматизации её хранения, обработки, передачи и ввода-вывода.

17. Как классифицируются виды угроз информации по природе возникновения?

- Стихийные бедствия, несчастные случаи, ошибки обслуживающего персонала и пользователей, злоупотребления обслуживающего персонала и пользователей, злоумышленные действия нарушителей, сбои и отказы оборудования.

- Угрозы персоналу, информации, информационным системам, материальным, финансовым, информационным данным.

- Угрозы информационным системам, материальным, финансовым, информационным данным, злоумышленные действия нарушителей, сбои и отказы оборудования.

18. Как классифицируются виды угроз информации по ориентации на ресурсы?

- Угрозы персоналу, информации, информационным системам, материальным, финансовым, информационным данным.

- Стихийные бедствия, несчастные случаи, ошибки обслуживающего персонала и пользователей, злоупотребления обслуживающего персонала и пользователей, злоумышленные действия нарушителей, сбои и отказы оборудования.

- Угрозы информационным системам, материальным, финансовым, информационным данным, злоумышленные действия нарушителей, сбои и отказы оборудования.

19. Какие угрозы относятся к естественным?

- Отказы и сбои аппаратуры; Помехи на линиях связи от воздействий внешней среды; аварийные ситуации; стихийные бедствия.

- Ошибки человека как звена системы; схемные и системотехнические ошибки разработчиков структурные, алгоритмические и программные ошибки; действия

- человека, направленные на несанкционированные воздействия на информацию.

- Аварийные ситуации; стихийные бедствия; ошибки человека как звена системы; схемные и системотехнические ошибки разработчиков

20. Какие угрозы информации относятся к искусственным?

- Ошибки человека как звена системы; схемные и системотехнические ошибки разработчиков; структурные, алгоритмические и программные ошибки; действия человека, направленные на несанкционированные воздействия на информацию

- Отказы и сбои аппаратуры; помехи на линиях связи от воздействий внешней среды; аварийные ситуации; стихийные бедствия

- Аварийные ситуации; стихийные бедствия; ошибки человека как звена системы; схемные и системотехнические ошибки разработчиков

21. Какие угрозы информации относятся к случайным?

- Проявление ошибок программно-аппаратных средств АС; некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности; неумышленная порча носителей информации.

- Несанкционированное чтение информации; несанкционированное изменение информации; несанкционированное уничтожение информации; полное или частичное разрушение операционной системы.

- Пересылка данных по ошибочному адресу абонента; ввод ошибочных данных; несанкционированное уничтожение информации; полное или частичное разрушение операционной системы.

22. Какие угрозы информации относятся к преднамеренным?

- Несанкционированное чтение информации; несанкционированное изменение информации; несанкционированное уничтожение информации; полное или частичное разрушение операционной системы.

- Проявление ошибок программно-аппаратных средств АС; некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности; неправомерное включение оборудования или изменение режимов работы устройств и программ.

- Пересылка данных по ошибочному адресу абонента; ввод ошибочных данных; несанкционированное уничтожение информации; полное или частичное разрушение операционной системы

23. В чем заключается метод защиты - ограничение доступа?

- В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям

- В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями

- В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы

- В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. приведении её к неявному виду

24. В чем заключается метод защиты информации - разграничение доступа?

- В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями

- В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям

- В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы

- В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении её к неявному виду

25. В чем заключается метод защиты информации - разделение доступа (привелегий)

- В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы

- В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям

- В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями

- В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении её к неявному виду

26. В чем заключается криптографическое преобразование информации?

- В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении её к неявному виду

- В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям

- В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями

- В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы

27. Что означает термин БЕЗОПАСНОСТЬ ИНФОРМАЦИИ

- Потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному её тиражированию.

- Свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.

- Защищенность информации от нежелательного её разглашения, искажения, утраты или снижения степени доступности информации, а также незаконного её тиражирования

28. Какие законы существуют в России в области компьютерного права?

- О государственной тайне

- об авторском праве и смежных правах

- о гражданском долге

- о правовой охране программ для ЭВМ и БД
- о правовой ответственности
- об информации, информатизации, защищенности информации

29. Утечка информации

- несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу
- ознакомление постороннего лица с содержанием секретной информации
- потеря, хищение, разрушение или неполучение переданных данных

30. Виды технической разведки (по месту размещения аппаратуры)

- космическая
- оптическая
- наземная
- фотографическая
- морская
- воздушная
- магнитометрическая

31. Какими основными свойствами обладает компьютерный вирус?

- Способностью к созданию собственных копий; наличием механизма, обеспечивающего внедрение создаваемых копий в исполняемые объекты вычислительной системы.
- Способностью к созданию собственных копий; способностью уничтожать информацию на дисках; способностью создавать всевозможные видео и звуковые эффекты.
- Наличием механизма, обеспечивающего внедрение создаваемых копий в исполняемые объекты вычислительной системы; способностью оставлять в оперативной памяти свою резидентную часть; способностью вируса полностью или частично скрыть себя в системе.

32. Как классифицируются вирусы в зависимости от среды обитания?

- Файловые; загрузочные; макровирусы; сетевые.
- Заражающие DOS, Windows, Win95/NT, OS/2, Word, Excel,Office 97.
- Безвредные; неопасные; опасные.
- Очень опасные.

33. Как классифицируются вирусы в зависимости от заражаемой ОС?

- Заражающие DOS, Windows, Win95/NT, OS/2, Word, Excel, Office 97.2
- Файловые; загрузочные; макровирусы; сетевые.
- Безвредные; неопасные; опасные; очень опасные.
- Использование резидентности, использование "стелс"-алгоритмов;
- Использование самошифрование и полиморфичность; использование нестандартных приемов

34. Как классифицируются вирусы в зависимости от особенностей алгоритма работы?

- Использование резидентность; использование "стелс"-алгоритмов; использование самошифрование и полиморфичность; использование нестандартных приемов.
- Файловые; загрузочные; макровирусы; сетевые
- Заражающие DOS, Windows, Win95/NT,OS/2,Word, Excel, Office 97
- Безвредные; неопасные; опасные; очень опасные

35. Как классифицируются вирусы в зависимости от деструктивных возможностей?

- Безвредные; неопасные; опасные; очень опасные.
- Файловые; загрузочные; макровирусы; сетевые.
- Заражающие DOS, Windows, Win95/NT,OS/2, Word, Excel, Office 97.4.
- Использование резидентность; использование "стелс"-алгоритмов.
- Использование самошифрование и полиморфичность; использование нестандартных приемов

36. В чем заключается принцип работы файлового вируса?

- Вирусы либо различными способами внедряются в выполняемые файлы, либо создают файлы-двойники, либо используют особенности организации файловой системы.

- Записывают себя либо в загрузочный сектор диска, либо в сектор, содержащий системный загрузчик винчестера, либо меняют указатель на активный boot-сектор.

- Вирусы заражают файлы-документы и электронные таблицы популярных редакторов.

- Вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

37. В чем заключается принцип работы загрузочного вируса?

- Вирусы записывают себя либо в загрузочный сектор диска, либо в сектор, содержащий системный загрузчик винчестера, либо меняет указатель на активный boot-сектор

- Вирусы либо различными способами внедряются в выполняемые файлы, либо создают файлы-двойники, либо используют особенности организации файловой системы

- Вирусы заражают файлы-документы и электронные таблицы популярных редакторов

- Вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты

38. Какие программы относятся к программам Конструкторы вирусов?

- Это утилита, предназначенная для изготовления новых компьютерных вирусов. Они позволяют генерировать исходные тексты вирусов (ASM-файлы), объектные модули и/или непосредственно зараженные файлы.

- Это программы, наносящие какие-либо разрушительные действия, т.е. в зависимости от определенных условий или при каждом запуске уничтожающие информацию на дисках, приводящие систему к зависанию и т.п.

- Это программы, которые на первый взгляд являются стопроценными вирусами, но неспособны размножаться по причине ошибок. Например, вирус, который при заражении "забывает" поместить в начало файлов команду передачи управления на код вируса.

- Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика

39. Какие программы относятся к программам полиморфик-генераторы?

- Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика.

- Это программы, наносящие какие-либо разрушительные действия, т.е. в зависимости от определенных условий или при каждом запуске уничтожающие информацию на дисках, приводящие систему к зависанию и т.п.

- Это программы, которые на первый взгляд являются стопроцентными вирусами, но неспособны размножаться по причине ошибок. Например, вирус, который при заражении "забывает" поместить в начало файлов команду передачи управления на код вируса.

- Это утилита, предназначенная для изготовления новых компьютерных вирусов. Они позволяют генерировать исходные тексты вирусов (ASM-файлы), объектные модули и/или непосредственно зараженные файлы

40. В чем заключается принцип работы макровируса?

- Вирусы заражают файлы-документы и электронные таблицы популярных редакторов.

- Вирусы либо различными способами внедряются в выполняемые файлы, либо создают файлы-двойники, либо используют особенности организации файловой системы.

- Вирусы записывают себя либо в загрузочный сектор диска, либо в сектор, содержащий системный загрузчик винчестера, либо меняют указатель на активный boot-сектор.

41. В чем заключается принцип работы сетевого вируса?

- Вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

- Вирусы либо различными способами внедряются в выполняемые файлы, либо создают файлы-двойники, либо используют особенности организации файловой системы.

- Вирусы записывают себя либо в загрузочний сектор диска, либо в сектор, содержащий системный загрузчик винчестера, либо меняют указатель на активный boot-сектор.

42. На чем основан алгоритм работы резедентного вируса?

- Вирус при инфицировании компьютера оставляет в оперативной памяти свою часть, которая затем перехватывает обращения ОС к объектам заражения и внедряется в них. Эти вирусы находятся в памяти и являются активными вплоть до выключения компьютера.

- Использование этих алгоритмов позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным алгоритмом является перехват запросов ОС на чтение-запись зараженных объектов и затем вирусы временно лечат их.

- Используются для того, чтобы максимально усложнить процедуру обнаружения вируса. Эти вирусы трудно поддаются обнаружению. Два образца не будут иметь ни одного совпадения

43. На чем основан алгоритм работы вируса с использованием "стелс"-алгоритмов?

- Использование этих алгоритмов позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным алгоритмом является перехват запросов ОС на чтение-запись зараженных объектов, затем вирусы временно лечат их.

- Вирус при инфицировании оставляет в оперативной памяти свою часть, которая затем перехватывает обращения ОС к объектам заражения и внедряется в них. Эти вирусы находятся в памяти вплоть до выключения компьютера.

- Используются для того, чтобы максимально усложнить процедуру обнаружения вируса. Эти вирусы достаточно трудно поддаются обнаружению, они не содержат ни одного постоянного участка кода.

44. На чем основан алгоритм работы вируса с использованием самошифрования и полиморфичности?

- Эти вирусы достаточно трудно поддаются обнаружению, они не содержат ни одного постоянного участка кода. В большинстве случаев два образца одного итого же вируса не будут иметь ни одного совпадения.

- Вирус оставляет в оперативной памяти свою часть, которая затем перехватывает обращения ОС к объектам заражения и внедряется в них. Эти вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки ОС.

- Использование этих алгоритмов позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным является перехват запросов ОС на чтение-запись зараженных объектов, затем вирусы временно лечат их.

45. По деструктивным возможностям, как влияют на работу компьютера безвредные вирусы?

- Никак не влияющие на работу компьютера, кроме уменьшения свободной памяти на диске в результате своего распространения.

- Влияние ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и прочими эффектами.

- Могут привести к серьезным сбоям в работе компьютера.

- В алгоритм работы заведомо заложены процедуры, которые могут вызвать потерю программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти.

46. По деструктивным возможностям, как влияют на работу компьютера не опасные вирусы?

- Влияние ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и прочими эффектами.

- Никак не влияющие на работу компьютера, кроме уменьшения свободной памяти на диске в результате своего распространения.

- Могут привести к серьезным сбоям в работе компьютера.

- В алгоритм работы заведомо заложены процедуры, которые могут вызвать потерю программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти

47. По дистуктивным возможностям, как влияют на работу компьютера опасные вирусы?

- Могут привести к серьезным сбоям в работе компьютера.

- Никак не влияющие на работу компьютера, кроме уменьшения свободной памяти на диске в результате своего распространения.

- Влияние ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и прочими эффектами.

- В алгоритме работы заведомо заложены процедуры, которые могут вызвать потерю программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти.

48. По деструктивным возможностям, как влияют на работу компьютера очень опасные вирусы?

- В алгоритм работы заведомо заложены процедуры, которые могут вызвать потерю программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти.

- Никак не влияющие на работу компьютера кроме уменьшения свободной памяти на диске в результате своего распространения.

- Влияние ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и прочими эффектами.

49. По способу заражения файловых вирусов, как работают overwriting-вирусы?

- Вирус не изменяет заражаемых файлов. Алгоритм работы состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т. е. вирус.

- При запуске зараженного файла заставляют ОС выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы.

- Вирусы никоим образом не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они всего лишь копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем.

- Вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое.

50. По способу заражения файловых вирусов, как работают parasitic-вирусы?

- Вирус при распространении своих копий обязательно изменяет содержимое файлов, оставляя сами файлы при этом полностью или частично работоспособными.

- Вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое.

- Вирус не изменяет заражаемых файлов. Алгоритм работы состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т.е. вирус в надежде, что эти новые копии будут когда-либо запущены пользователем

51. По способу заражения файловых вирусов, как работают companion-вирусы?

- Вирус не изменяет заражаемых файлов. Алгоритм работы состоим в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т.е. вирус.

- Вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое.

- Вирус при распространении своих копий обязательно изменяет содержимое файлов, оставляя сами файлы при этом полностью или частично работоспособными.

- Вирусы не изменяют физического содержимого файлов, однако при запуске зараженного файла заставляют ОС выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы.

52. По способу заражения файловых вирусов, как работают link-вирусы?

- Вирусы не изменяют физического содержимого файлов, однако при запуске заражаемого файла заставляет ОС выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы.

- Вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое.

- Вирус при распространении своих копий обязательно изменяет содержимое файлов, оставляя сами файлы при этом полностью или частично работоспособными.

- Вирус не изменяет заражаемых файлов. Алгоритм работы состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т.е. вирус.

53. По способу заражения файловых вирусов, как работают файловые черви?

- Вирус при распространении своих копий обязательно изменяет содержимое файлов, оставляя сами файлы при этом полностью или частично работоспособными.

- Вирус не изменяет заражаемых файлов. Алгоритм работы состоит в том, что для заражаемого файла управление получает именно этот двойник, т.е. вирус.

- Вирусы не изменяют физического содержимого файлов, однако при запуске зараженного файла заставляют ОС выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы.

- Вирусы никоим образом не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они всего лишь копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем.

- Вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое.

54. Какие программы относятся к программам "Троянские кони" (логические бомбы)

- Это программы, наносящие какие-либо разрушительные действия, т.е. в зависимости от определенных условий или при каждом запуске уничтожающие информацию на дисках, приводящие систему к зависанию и т.п.

- Это программы, которые на первый взгляд являются стопроцентными вирусами, но не способны размножаться по причине ошибок. Например, вирус, который при заражении "забывает" поместить в начало файлов команду передачи управления на код вируса.

- Это утилита, предназначенная для изготовления новых компьютерных вирусов. Они позволяют генерировать исходные тексты вирусов (ASM-файлы), объектные модули и/или непосредственно зараженные файлы.

- Главной функцией подобного рада программ является шифрование тела вируса и генерация соответствующего расшифровщика.

55. Какие программы относятся к программам Intended-вирусы?

- Это программы, которые на первый взгляд являются стопроцентными вирусами, но не способны размножаться по причине ошибок. Например, вирус, который при заражении "забывает" поместить в начало файлов команду передачи управления на код вируса.

- Это программы, наносящие какие-либо разрушительные действия, т.е. в зависимости от определенных условий или при каждом запуске уничтожающие информацию на дисках, приводящие систему к зависанию и т.п.

- Это утилита, предназначенная для изготовления новых компьютерных вирусов. Они позволяют генерировать исходные тексты вирусов (ASM-файлы), объектные модули и/или непосредственно зараженные файлы.

- Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика.

56. Основные группы технических средств ведения разведки

- радиомикрофоны
- фотоаппараты
- электронные "уши"
- дистанционное прослушивание разговоров
- системы определения местоположения контролируемого объекта

Блок 2 (уметь).

1. Нежелательная цепочка носителей информации, один или несколько из которых являются правонарушителем или его специальной аппаратурой называется

_____

2. Укажите соответствие для всех 4 вариантов ответа:

- это комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны за счет электромагнитных полей побочного характера и наводок

- это комплекс мероприятий, исключающих или уменьшающих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны в виде производственных или промышленных отходов

- это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей

- это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет распространения световой энергии

__ защита информации от утечки по акустическому каналу

__ Защита информации от утечки по визуально-оптическому каналу

__ Защита информации от утечки по электромагнитным каналам

__ Защита информации от утечки по материально-вещественному каналу

3. Надежным средством отвода наведенных сигналов на землю служит

_____

4. Укажите соответствие для всех 2 вариантов ответа:

- наука о скрытой передаче информации путем сохранения в тайне самого факта передачи

- наука скрывающая содержимое секретного сообщения

__ стеганография

__ криптография

5. К аспектам ИБ относятся

Выберите несколько из 5 вариантов ответа:

- дискретность
- целостность
- конфиденциальность
- актуальность
- доступность

6. Какие действия являются реагированием на нарушение режима информационной безопасности организации?

- Локализация и уменьшение вреда
- Выявление нарушителя
- Предупреждение повторных нарушений
- Судебное рассмотрение
- Проведение общего собрания организации

7. Что относится к основным организационным мероприятиям, направленным на поддержание работоспособности информационных систем?

- Резервное копирование
- Поддержка программного обеспечения
- Документирование
- Регламентные работы
- Усложнение управления техническими средствами
- Выполнение нескольких операций одним оперативно-техническим персоналом

8. Какие меры позволяют повысить надежность парольной защиты?

- Наложение технических ограничений (пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знакипунктуации и т.п.)

- Управление сроком действия паролей, их периодическая смена

- Ограничение доступа к файлу паролей

- Ограничение числа неудачных попыток входа в систему (это затруднит применение "метода грубой силы") обучениепользователей

- Выбор простого пароля (имя подруги, название спортивной команды)

9. Что относится к идентификации и/или аутентификации людей на основе их физиологических характеристик?

- Анализ особенностей голоса
- Распознавание речи
- Отпечатки пальцев
- Сканирование радужной оболочки глаза
- Анализ знаний по информационной безопасности

10. Что относится к идентификации и/или аутентификации людей на основе их поведенческих характеристик?

- Анализ динамики подписи (ручной)
- Анализ стиля работы с клавиатурой
- Анализ отпечатков пальцев
- Анализ административных указаний по информационной безопасности
- Отпечатки пальцев

11. Какими способами обеспечиваются основные уровни антивирусной защиты?

- Поиск и уничтожение известных вирусов
- Поиск и уничтожение неизвестных вирусов
- Блокировка проявления вирусов
- Определения адреса отправителя вирусов
- Выявление создателей вирусов

12. На чем основан принцип работы антивирусных мониторов?

- На перехватывании вирусоопасных ситуаций и сообщении об этом пользователю
- На проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются маски
- На подсчете контрольных сумм для присутствующих на диске файлов или системных секторов. Эти суммы затем сохраняются в базе данных антивируса, а также другая информация: длина файлов, дата их последней модификации и т.д.
- На защите системы от поражения вирусом какого-то определенного вида. Файлы на дисках модифицируются таким образом, что вирус принимает их за уже зараженные

13. На чем основан принцип работы антивирусных иммунизаторов?

- На защите системы от поражения вирусом какого-то определенного вида. Файлы на дисках модифицируются таким образом, что вирус принимает их за уже зараженные
- На проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются маски
- На подсчете контрольных сумм для присутствующих на диске файлов или системных секторов. Эти суммы затем сохраняются в базе данных антивируса, а также другая информация: длина файлов, дата их последней модификации и т.д.
- На перехватывании вирусоопасных ситуаций и сообщении об этом пользователю

14. Что необходимо сделать при обнаружении файлового вируса?

- Компьютер необходимо отключить от сети и проинформировать системного администратора
- Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются
- Вместо отключения компьютера от сети достаточно на период лечения убедиться в том, что соответствующий редактор неактивен

15. Что необходимо сделать при обнаружении загрузочного вируса?

- Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются
- Компьютер необходимо отключить от сети и проинформировать системного администратора
- Вместо отключения компьютера от сети достаточно на период лечения убедиться в том, что соответствующий редактор неактивен

16. Что необходимо сделать при обнаружении макровируса?

- Вместо отключения компьютера от сети достаточно на период лечения убедиться в том, что соответствующий редактор неактивен

- Компьютер необходимо отключить от сети и проинформировать системного администратора

- Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются

Блок 3 (владеть).

1. Какие основные свойства информации и систем обработки информации необходимо поддерживать, обеспечивая информационную безопасность?

- Доступность
- Целостность
- Конфиденциальность
- Управляемость
- Сложность

2. Выберите правильные утверждения

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

3. Отметьте составные части современного антивируса

- Межсетевой экран
- Сканер
- Монитор
- Модем
- Принтер

4. Компьютерные вирусы - это...

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

5. Вредоносные программы - это...

- программы, наносящие вред пользователю, работающему на зараженном компьютере
- шпионские программы
- антивирусные программы
- программы, наносящие вред данным и программам, находящимся на компьютере
- троянские утилиты и сетевые черви

6. К вредоносным программам относятся:

- Межсетевой экран, брандмауэр
- Потенциально опасные программы
- Программы-шутки, антивирусное программное обеспечение
- Шпионские и рекламные программы
- Вирусы, черви, трояны

7. Какая программа не является антивирусной?

- Norton Antivirus
- Dr Web
- Defrag
- AVP

8. Как вирус может появиться в компьютере?

- при работе с макросами
- самопроизвольно
- при работе компьютера в сети
- при решении математической задачи

9. Какие правовые документы решают вопросы информационной безопасности?
- Уголовный кодекс РФ
- Конституция РФ
- Закон "Об информации, информатизации и защите информации"
- Закон РФ "О государственной тайне"
- Закон РФ "О коммерческой тайне"
- Закон РФ "О лицензировании отдельных видов деятельности"
- Закон РФ "Об образовании"
- Закон РФ " Об электронной цифровой подписи "

10. Какие угрозы безопасности информации являются преднамеренными?
- Взрыв в результате теракта
- Поджог
- Забастовка
- Ошибки персонала
- Неумышленное повреждение каналов связи
- Некомпетентное использование средств защиты
- Утрата паролей, ключей, пропусков
- Хищение носителей информации
- Незаконное получение паролей

11. Какие угрозы безопасности информации являются непреднамеренными?
- Взрыв в результате теракта
- Поджог
- Забастовка
- Ошибки персонала
- Неумышленное повреждение каналов связи
- Некомпетентное использование средств защиты
- Утрата паролей, ключей, пропусков
- Хищение носителей информации

12. Что относится к угрозам информационной безопасности?

- Потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному ее тиражированию
- Классификация информации
- Стихийные бедствия и аварии (наводнение, ураган,землетрясение, пожар и т.п.)
- Сбои и отказы оборудования (технических средств) АС
- Ошибки эксплуатации (пользователей, операторов и другого персонала)
- Преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов,диверсантов)
- Последствия ошибок проектирования и разработки компонентов АС (аппаратных средств, технологии обработки информации, программ, структур данных и т.п.)
- Иерархическое расположение данных

13. Какие существуют основные уровни обеспечения защиты информации?
- Законодательный
- Организационно-административный
- Программно-технический (аппаратный)
- Физический
- Вероятностный
- Распределительный

14. Что понимается под средством физического управления доступом?

- Механические, электронно-механические устройства и сооружения, специально предназначенные для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к защищаемой информации

- Силовые действия охраны организации против потенциальных нарушителей

- Указания в инструкциях на мероприятия по подержанию физической формы сотрудников

- Программные меры защиты, предназначенные для создания препятствий потенциальным нарушителям

- Информационное обеспечение секретных задач

15. Каковы основные принципы построения систем физической защиты?

- Принцип системности
- Принцип непрерывности защиты
- Принцип разумной достаточности
- Гибкость управления и применения
- Простота применения защитных мер и средств
- Установка препятствий по мере сложности преодоления
- Установка обязательной связи звуковой и телевизионной сигнализации

16. Что относится к средствам физической защиты информации?

- Пропускная система на предприятиях
- Ограждения на предприятиях
- Документирование
- Системы видео наблюдения на предприятиях
- Резервное копирование
- Средства защиты от пожаров
- Средства защиты от жары, холода, влаги, магнетизма
- Индивидуальные средства защиты
- Противорадиационные средства защиты
- Анализ требований к защищаемому сервису
- Информатизация защищаемого сервиса, установленного на предприятии

17. Какие имеются основные направления обеспечения информационной безопасности, связанные с человеческим фактором?

- Разделение обязанностей
- Минимизация привилегий
- Описание должности (должностные инструкции)
- Обучение персонала информационной безопасности
- Планирование требований к защищаемому серверу
- Информатизация защищаемого сервиса, установленного на предприятии
- Противорадиационные средства защиты
- Индивидуальные средства защиты

18. Какие методы применяются в криптографических методах защиты информации?

- Подстановка
- Перестановка
- Аналитическое преобразование
- Комбинированное преобразование
- Замена контрольными суммами
- Замена только цифр

19. Что входит в задачи службы безопасности организации?

- Выявление лиц, проявляющих интерес к коммерческой тайне предприятия
- Разработка системы защиты секретных документов

- Определение уязвимых участков на предприятии, аварии или сбои в работе которых могут нанести урон предприятию

- Планирование, обоснование и организация мероприятий по защите информации
- Взаимодействие с Управлением внутренних дел
- Определение сведений, составляющих коммерческую тайну

- Арест нарушителей информационной безопасности

20. Каковы меры управления персоналом для обеспечения информационной безопасности?

- Описание должности (должностных обязанностей)
- Разделение обязанностей
- Минимизация привилегий
- Обучение
- Подбор кадров
- Подбор программно-технических средств
- Аттестация персонала

21. Что относится к основным способам физической защиты?

- Физическое управление доступом
- Противопожарные меры
- Защита поддерживающей инфраструктуры
- Защита от перехвата данных
- Защита мобильных систем
- Проведение производственной зарядки
- Проведение соревнований по профессиональному мастерству

Методические материалы, характеризующие процедуры оценивания

Индивидуальный семестровый рейтинг студента формируется на основе действующего в ВУЗе Положения "О проведении текущего контроля успеваемости и промежуточной аттестации обучающихся".

В течение семестра студент получает баллы успеваемости за выполнение всех видов учебных поручений: посещение лекций, выполнение практических работ. Зачет выставляется в случае, если итоговая оценка студента составляет не менее 50 баллов.

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:

Какие имеются основные направления обеспечения информационной безопасности, связанные с человеческим фактором

- Описание должности (должностные инструкции)
- Индивидуальные средства защиты
- Информатизация защищаемого сервиса, установленного на предприятии
- Планирование требований к защищаемому серверу
- Обучение персонала информационной безопасности

- Противорадиационные средства защиты
- Минимизация привилегий
- Разделение обязанностей

Каковы основные принципы построения систем физической защиты
- Установка препятствий по мере сложности преодоления
- Принцип непрерывности защиты
- Установка обязательной связи звуковой и телевизионной сигнализации
- Принцип системности
- Простота применения защитных мер и средств
- Гибкость управления и применения
- Принцип разумной достаточности

В чем заключается криптографическое преобразование информации
- В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям
- В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы
- В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении её к неявному виду
- В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями

Наука о методах защиты информации на основе ее преобразования с помощью различных шифров и сохранением достоверности семантического содержания - ...

Организация ложной работы технических средств связи и обработки информации; изменение режимов использования частот и регламентов связи; показ ложных демаскирующие признаков деятельности и опознавания - ...

Свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия - ...

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?courseid=247

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