Министерство просвещения РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Дагестанский государственный педагогический университет»
Факультет профессионально-педагогического образования
Кафедра информационных технологий и экономики

УТВЕРЖДАЮ
Проректор по УМР
_____
«__» _____ 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.01.01.09 АППАРАТНО-ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

(наименование дисциплины (модуля))

Направление подготовки 44.04.04 Профессиональное обучение (по отраслям)

Профиль подготовки компьютерные образовательные технологии
Квалификация магистр
Формы обучения: очная, заочная
Нормативные сроки обучения: очно 2, заочно 2,5 года

Форма обучения	Семестр	Трудоемкость	Виды учебной работы					
			Лекции	Практ. занятия	Лабор. занятия	Промежуточный контроль	СРС	Форма аттестации
очная	2	72	6	12			54	зачет
заочная	2	72	2	2			68	зачет

МАХАЧКАЛА 2022

Нурмагомедова Н.Х. Рабочая программа дисциплины «Аппаратно-программные средства защиты информации». – Махачкала: ДГПУ, 2022. – 30с.

Рецензенты: Эсетов Ф.А., к.п.н., доцент кафедры информатики и ВТ ДГПУ
Везиров Т.Т., к.п.н., доцент кафедры инф. права и инф. ДГУ

Программа утверждена на заседаниях:

кафедры информационных технологий и экономики (протокол № 10 от «12» мая 2022 г.)

Зав. кафедрой Р.А. Таибова

ученого совета факультета профессионально-педагогического образования (протокол № 9 от «20» мая 2022 г.)

Председатель совета Ф.Н. Алипханова

учебно-методического совета ДГПУ (протокол №4 от «28» июня 2022 г.)

Председатель совета И.А.Дибиров

1. Цель освоения дисциплины (модуля)

Предмет курса «Аппаратно-программные средства защиты информации» - механизмы и практические методы защиты информации в информационных системах.

Цель курса - ознакомление студентов с современными средствами защиты информации в компьютерных системах, овладение методами решения профессиональных задач.

Изучение дисциплины «Аппаратно-программные средства защиты информации» должно способствовать воспитанию у студентов профессиональной компетентности и профессионального кругозора, умению ориентироваться в продуктах и тенденциях развития средств защиты информационных технологий.

2. Место дисциплины в структуре магистерской программы

Для ее освоения необходимы знания, умения и компетенции, приобретенные в результате изучения следующих дисциплин:

- Информационные и коммуникационные технологии в науке и образовании;
- Проектирование информационных систем;
- Программное обеспечение компьютерных сетей;
- Сетевые методы управления учебным процессом;
- Создание педагогических программных средств;
- Динамическое программирование;
- Математическое моделирование в профессиональном образовании.

Знания и умения, полученные в результате освоения данной дисциплины, могут быть использованы при подготовке магистерской диссертации, а также в научной и практической деятельности после окончания университета.

3. *Требования к результатам освоения дисциплины (модуля)* «Аппаратно-программные средства защиты информации»:

В результате освоения дисциплины у магистра формируются компетенции:

ПК-12 «Способен организовать и провести изучение требований рынка труда и обучающихся к качеству СПО и (или) ДПО и (или) профессионального обучения».

ПК-16 – «Способен понимать сущность и значение информации в современном обществе, осознать опасности и угрозы, соблюдать основные требования информационной безопасности»

В результате изучения дисциплины «Аппаратно-программные средства защиты информации» магистрант должен:

Знать:

ПК12.1.

-программы социально-экономического развития и развития профессионального образования РД; тенденции, методику и практику маркетинговых исследований

Основы мониторинга труда и требований к квалификации работников; технологии изучения качественных и количественных потребностей рынка труда; способы определения требований рынка труда и обучаемых к качеству обучения в СПО; методы консультирования специалистов

-требования профессиональных и иных квалификационных требований к специалистам среднего звена, квалифицированным рабочим; методы выявления соответствия выпускников магистратуры требованиям профессиональных стандартов; способы обработки, анализа и интерпретации результатов исследования, их обследования

ПК 16.1.

- базовые принципы выявления информационной опасности и угроз, и способы её обезвреживания

- принципы определения информационной опасности и угроз, и способов её обезвреживания

- методы устранения информационной опасности и угроз, и её обезвреживания

Уметь:
ПК 12.2.
-формулировать и обсуждать задачи и методы изучения требований рынка труда и обучающихся к качеству СПО и (или) профессионального обучения; определять ресурсы и источники их привлечения; разрабатывать с привлечением специалистов инструментарий исследования
-обеспечивать оптимизацию затрат на проведение исследования; обучать работников СПО исследованию инструментария исследования; координировать работу специалистов, привлеченных к исследованию; использовать инструментарий исследования, различные формы и средства взаимодействия с работодателями; проводить первичную обработку результатов их исследований.
-обрабатывать, анализировать и интерпретировать результаты исследований; организовать обсуждение результатов анализа; разрабатывать и представлять предложения и рекомендации по формированию образовательных программ, совершенствованию условий их реализации

ПК 16.2. :

- выявлять базовые принципы информационной опасности и угроз, и способов её обезвреживания

- определять принципы информационной опасности и угроз, и способы её обезвреживания

- устранить информационную опасность и угрозы, и технологии её обезвреживания

Владеть:
ПК12.3. :
методами организации разработок программ и инструментария и проведения маркетинговых исследований методами изучения образовательных запросов обучающихся и их требований к качеству обучения; способностями взаимодействия с работодателями методами разработки предложений и рекомендаций по формированию образовательных программ и условий их реализации

ПК 16.3. :

- принципами выявления базовых информационной опасности и угроз, и способами её обезвреживания

- навыками выявления информационной опасности и угроз, и способами её обезвреживания
- технологиями выявления информационной опасности и угроз, и способами её обезвреживания

Таблица1

Вид учебной работы	Всего часов	
	Очно	Заочно
Общая трудоемкость час	**72**	**72**
Аудиторные занятия (всего)	18	12
Лекции	6	2
Практические работы (ПР)	12	2
Самостоятельная работа (всего)	54	68
Зачетные Единицы Трудоемкости	2	2
Вид промежуточной аттестации (зачет)	зачет	зачет

4. Структура и содержание дисциплины (модуля)

№ п/п	Наименование раздела дисциплины	Количество часов						Формируемые компетенции
		Очно			Заочно			
		Лек/из них пр. под.	ПР/ из них пр. под.	СРС	Лек/ из них пр. под.	ПР/ из них пр. под.	СРС	
Модуль 1								
1.	Предмет и задачи аппаратно- программных средств защиты информации	1/-	2/-	10	1/-	1/-	15	ПК-12; ПК-16;
2.	Основные понятия	1/-	2/-	15			15	
3,	Понятие уязвимости компьютерных систем	1/-	2/-					
Модуль 2								
4,	Понятие идентификации пользователя	1/-	2/-	15	1/-	1/-	22	ПК-12; ПК-16;
5,	Построение программно-аппаратных комплексов шифрования	2/-	4/-	14			16	ПК-12; ПК-16;
	Всего	**6/-**	**12/-**	**54**	**2/-**	**2/-**	**68**	

Содержание лабораторных занятий

1. Разработка программы разграничения полномочий пользователей на основе парольной аутентификации

2. Разработка и программная реализация криптографических алгоритмов

3. Использование функций криптографического интерфейса Windows для защиты информации

4. Защита программного обеспечения от несанкционированного использования и копирования.

5. Основы использования средств защиты от несанкционированного доступа в операционной системе Linux

6. Основы использования средств защиты от несанкционированного доступа в операционной системе Windows

5. Образовательные технологии

Изучение данной дисциплины предполагает использование коллективных способов обучения, технологий личностно-ориентированного, проблемного, модульного и дифференцированного обучения. Для магистров, проявляющих повышенный интерес к изучению дисциплины, возможно применение технологий проектной деятельности и исследовательского обучения. В рамках изучения дисциплины имеют место также интерактивные формы обучения с применением информационных технологий.

Методы и формы интерактивного обучения при разных формах занятий (в часах)

Самостоятельная работа представляет собой углубленное изучение теории аппаратно программных средств защиты информации в рамках программы дисциплины. Методическим обеспечением для проведения самостоятельной работы является литература, представленная в разделе 7.

По каждой лабораторной работе магистрант готовит отчет. Он выполняется в форме компьютерной презентации, в процессе которой и проверяется правильность выполнения лабораторной работы. Если лабораторная работа выполнена верно, то за ее выполнение ставится отметка «зачтено», в противном случае задание возвращается магистранту на доработку.

Контроль и оценка учебных достижений магистрантов по дисциплине «АППАРАТНО-ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ» проводится по балльно-рейтинговой системе с использованием кредитно-зачетных единиц. Итоговые баллы по результатам изучения дисциплинарных модулей и всего курса основывается на интегральной оценке всех видов учебной (аудиторной, внеаудиторной, самостоятельной). Балльно-рейтинговая система оценки учебной работы магистрантов по дисциплине дисциплине «АППАРАТНО-ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ» опирается на следующие принципы:

- модульность, предполагающая формирование содержания образования в виде модулей;
- мониторинг, означающий непрерывный контроль текущей, аудиторной и самостоятельной работы магистрантов;
- рейтингование педагогических достижений магистрантов по завершению изучения каждого модуля;
- систематичность контроля;
- гласность для всех участников образовательного процесса результатов оценки учебной деятельности магистрантов;

- комулятивность (накопительность) оценок при выполнении различных видов учебной деятельности, предусмотренных образовательной программой дисциплины.

Для решения задач дисциплины все участники образовательного процесса должны быть ознакомлены с порядком и правилами использования балльно-рейтинговой системы оценки учебной работы магистрантов.

Для реализации идей балльно-рейтинговой системы оценки учебных достижений магистрантов содержание образовательной программы разбито на 3 дисциплинарных модуля. В каждом дисциплинарном модуле предусмотрено проведение лекционных и лабораторных занятий, самостоятельное выполнение заданий, написание рефератов и выступление с докладами. Изучение дисциплинарного модуля завершается итоговым контролем. В конце изучения курса (всех дисциплинарных модулей) по желанию студентов проводится итоговое тестирование.

Балльно-рейтинговая система оценки является составной частью организации учебного процесса с использованием зачетных единиц. Рейтинговая оценка по учебному модулю складывается из количества баллов, набранных студентом за текущую, самостоятельную, учебную работу и баллов, полученных при промежуточном контроле по итогам изучения данного модуля.

Текущий контроль по курсу «АППАРАТНО-ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ» включает:

− *лекционные занятия (2 часа)*: неявка на занятия – 0; посещение занятий – 1 балл; за конспектирование лекции или ее самостоятельное составление – 1 балл (максимальное количество баллов – 9 занятий × 2 балла = 18 баллов);

− *лабораторные занятия (2 часа)*: неявка на занятия – 0; посещение занятий – 1 балл; за работу на занятиях или самостоятельную работу– 1 балл, за защиту лабораторной работы 2 балла (максимальное количество баллов – 9 занятий × 4 балла = 36 баллов).

Максимальное количество баллов по результатам текущей работы и промежуточного контроля по дисциплинарному модулю (без учета бонусов) – 100 баллов (текущая работа – 54 баллов, промежуточный контроль (защита лабораторных работ) – 46 баллов). Промежуточный контроль представляет собой выполнение тестовых заданий.

Дополнительные баллы (бонусы):

− инициативное решение учебных задач на занятиях – 1 балл;
− оригинальное решение задачи – 2 балла;
− решение большего количества задач, чем предусмотрено в модуле – 4 балла;
− доклад на семинарском или практическом занятии – 2 балла.
− Дополнительные баллы по результатам участия студентов в научно-
− исследовательской работе по дисциплине:
− реферат – 1 балл;
− научный доклад – 2 балла;
− публикация в печати – 4 балла;
− участие в работе научного кружка – 4 балла.
− доклады на научно-практической конференции:
− институтской – 2 балла;
− университетской – 3 балла;
− республиканской – 4 балла;
− Российской – 5 баллов;
− международной – 6 баллов.
− участие в олимпиаде:
− институтской – 1 балл;
− университетской – 2 балла;
− республиканской – 4 балла;
− Российской – 6 баллов;
− международной – 8 баллов.

− получение патента, свидетельства на охрану интеллектуальной собственности – 20 баллов.

Минимальное количество баллов, необходимое для получения положительной оценки по данной дисциплине определено – 51 баллов.

После завершения изучения дисциплинарного модуля студенту предоставляется одна неделя для добора баллов.

Экзамены и зачеты как отдельные виды учебной нагрузки не предусматриваются, но проводятся как одна из форм добора баллов.

Шкала диапазонов итоговой оценки определяется в соответствии с таблицей 2.

Тест 1

1. В каком году в России появились первые преступления с использованием компьютерной техники (были похищены 125,5 тыс. долларов США во Внешэкономбанке)?

a) 1988;

b) 1991;

c) 1994;

d) 1997;

c) 2002.

2. Сколько уголовных дела по ст. 272 и 165 УК РФ было возбуждено в 2003 году в России?

a) 6;

b) 60;

c) 160;

d) 600;

c) 1600.

3. Какой общий ущерб по данным Института Компьютерной Безопасности нанесли компьютерные вирусы за последние 5 лет, (млрд. долл. США)?

a) 4;

b) 34;

c) 54;

d) 74;

c) 94.

4. По данным журнала «Security Magazine», средний размер ущерба от компьютерного мошенничества составляет (долл. США):

a) 500 000;

b) 1 000 000;

c) 1 500 000;

d) 2 000 000;

e) 2 500 000.

5. По данным Главного информационного центра МВД России количество компьютерных преступлений ежегодно увеличивается в (раза):

a) 2;

b) 2,5;

c) 3;

d) 3,5;

e) 4.

6. По данным Главного информационного центра МВД России ежегодный размер материального ущерба от компьютерных преступлений составляет около (млн. рублей):

a) 6;

b) 60;

c) 160;

d) 600;

e) 1600.

7. По данным Главного информационного центра МВД России средний ущерб, причиняемый потерпевшему от 1 компьютерного преступления, равен (млн. рублей):

a) 7;

b) 1,7;

c) 2,7;

d) 3,7;

e) 4,7.

8. Сколько процентов электронных писем являются Спамом?

a) 10;

b) 30;

c) 50;

d) 70;

e) 90.

9. К каким ежегодным убыткам приводят спамы (млрд. долл. США)?

a) 20;
b) 40;
c) 60;

d) 80;

e) 100.

10. В 2003 году ФСБ пресечено попыток проникновения в информационные ресурсы органов государственной власти России около (раз):

a) 10;
b) 100;
c) 1 000;

d) 10 000;
e) 100 000.

11. Сколько выделяются основных составляющих национальных интересов Российской Федерации в информационной сфере?

a) 2;
b) 3;
c) 4;
d) 5;
e) 6.

12. Активный перехват информации это перехват, который:

a) заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
b) основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
c) неправомерно использует технологические отходы информационного процесса;
d) осуществляется путем использования оптической техники;
e) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

13. Пассивный перехват информации это перехват, который:

a) заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
b) основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
c) неправомерно использует технологические отходы информационного процесса;
d) осуществляется путем использования оптической техники;
e) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

14. Аудиоперехват перехват информации это перехват, который:

a) заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
b) основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
c) неправомерно использует технологические отходы информационного процесса;
d) осуществляется путем использования оптической техники;
e) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

15. Просмотр мусора это перехват информации, который:

a) заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
b) основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
c) неправомерно использует технологические отходы информационного процесса;
d) осуществляется путем использования оптической техники;

e) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

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

a) активный перехват;
b) пассивный перехват;
c) аудиоперехват;
d) видеоперехват;
e) просмотр мусора

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

a) активный перехват;
b) пассивный перехват;
c) аудиоперехват;
d) видеоперехват;
e) просмотр мусора.

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

a) активный перехват;
b) пассивный перехват;
c) аудиоперехват;
d) видеоперехват;
e) просмотр мусора.

19. Перехват, который осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера называется:

a) активный перехват;
b) пассивный перехват;
c) аудиоперехват;
d) видеоперехват;
e) просмотр мусора.

20. Перехват, который неправомерно использует технологические отходы информационного процесса называется:

a) активный перехват;
b) пассивный перехват;
c) аудиоперехват;
d) видеоперехват;
e) просмотр мусора.

21. Как называется способ несанкционированного доступа к информации, который заключается в несанкционированном доступе в компьютер или компьютерную сеть без права на то?

a) “За дураком”;
b) “Брешь”;
c) “Компьютерный абордаж”;
d) “За хвост”;
e) “Неспешный выбор”.

22. Как называется способ несанкционированного доступа к информации, который заключается в подключении компьютерного терминала к каналу связи в тот момент времени, когда сотрудник, кратковременно покидает свое рабочее место, оставляя терминал в рабочем режиме?

a) “За дураком”;
b) “Брешь”;
c) “Компьютерный абордаж”;
d) “За хвост”;
e) “Неспешный выбор”.

23. Как называется способ несанкционированного доступа к информации, который заключается в подключении злоумышленника к линии связи законного пользователя и после сигнала, обозначающего конец работы, перехватывания его на себя, получая доступ к системе?

a) “За дураком”;
b) “Брешь”;
c) “Компьютерный абордаж”;
d) “За хвост”;
e) “Неспешный выбор”.

24. Как называется способ несанкционированного доступа к информации, который заключается в отыскании участков программ, имеющих ошибку или неудачную логику построения?

a) “За дураком”;
b) “Брешь”;
c) “Компьютерный абордаж”;
d) “За хвост”;
e) “Неспешный выбор”.

25. Как называется способ несанкционированного доступа к информации, который заключается в нахождении злоумышленником уязвимых мест в ее защите?

a) “За дураком”;
b) “Брешь”;
c) “Компьютерный абордаж”;
d) “За хвост”;
e) “Неспешный выбор”.

26. Способ несанкционированного доступа к информации “За дураком” заключается в:

a) отыскании участков программ, имеющих ошибку или неудачную логику построения;
b) подключении злоумышленника к линии связи законного пользователя и после сигнала, обозначающего конец работы, перехватывания его на себя, получая доступ к системе;
c) подключении компьютерного терминала к каналу связи в тот момент времени, когда сотрудник, кратковременно покидает свое рабочее место, оставляя терминал в рабочем режиме;
d) нахождении злоумышленником уязвимых мест в ее защите;
e) несанкционированном доступе в компьютер или компьютерную сеть без права на то.

27. Способ несанкционированного доступа к информации “Брешь” заключается в:

a) отыскании участков программ, имеющих ошибку или неудачную логику построения;
b) подключении злоумышленника к линии связи законного пользователя и после сигнала, обозначающего конец работы, перехватывания его на себя, получая доступ к системе;
c) подключении компьютерного терминала к каналу связи в тот момент времени, когда сотрудник, кратковременно покидает свое рабочее место, оставляя терминал в рабочем режиме;
d) нахождении злоумышленником уязвимых мест в ее защите;
e) несанкционированном доступе в компьютер или компьютерную сеть без права на то.

28. Способ несанкционированного доступа к информации “Компьютерный абордаж” заключается в:

a) отыскании участков программ, имеющих ошибку или неудачную логику построения;
b) подключении злоумышленника к линии связи законного пользователя и после сигнала, обозначающего конец работы, перехватывания его на себя, получая доступ к системе;
c) подключении компьютерного терминала к каналу связи в тот момент времени, когда сотрудник, кратковременно покидает свое рабочее место, оставляя терминал в рабочем режиме;
d) нахождении злоумышленником уязвимых мест в ее защите;
e) несанкционированном доступе в компьютер или компьютерную сеть без права на то.

29. Способ несанкционированного доступа к информации “За хвост” заключается в:

a) отыскании участков программ, имеющих ошибку или неудачную логику построения;
b) подключении злоумышленника к линии связи законного пользователя и после сигнала, обозначающего конец работы, перехватывания его на себя, получая доступ к системе;
c) подключении компьютерного терминала к каналу связи в тот момент времени, когда сотрудник, кратковременно покидает свое рабочее место, оставляя терминал в рабочем режиме;
d) нахождении злоумышленником уязвимых мест в ее защите;
e) несанкционированном доступе в компьютер или компьютерную сеть без права на то.

30. Способ несанкционированного доступа к информации “Неспешный выбор” заключается в:

a) отыскании участков программ, имеющих ошибку или неудачную логику построения;
b) подключении злоумышленника к линии связи законного пользователя и после сигнала, обозначающего конец работы, перехватывания его на себя, получая доступ к системе;
c) подключении компьютерного терминала к каналу связи в тот момент времени, когда сотрудник, кратковременно покидает свое рабочее место, оставляя терминал в рабочем режиме;
d) нахождении злоумышленником уязвимых мест в ее защите;

e) несанкционированном доступе в компьютер или компьютерную сеть без права на то.

31. Хакер?

a) Это лицо, которое взламывает интрасеть в познавательных целях;
b) Это мошенник, рассылающий свои послания, в надежде обмануть наивных и жадных;
c) Это лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО;
d) Так в XIX веке называли плохого игрока в гольф, дилетанта;
e) Это мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

32. Фракер?

a) Это лицо, которое взламывает интрасеть в познавательных целях;
b) Это мошенник, рассылающий свои послания, в надежде обмануть наивных и жадных;
c) Это лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО;
d) Так в XIX веке называли плохих игроков в гольф, дилетантов;
e) Это мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

33. Кракер?

a) Это лицо, которое взламывает интрасеть в познавательных целях;
b) Это мошенник, рассылающий свои послания, в надежде обмануть наивных и жадных;
c) Это лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО;
d) Так в XIX веке называли плохих игроков в гольф, дилетантов;
e) Это мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

34. Фишер?

a) Это лицо, которое взламывает интрасеть в познавательных целях;
b) Это мошенник, рассылающий свои послания, в надежде обмануть наивных и жадных;
c) Это лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО;
d) Так в XIX веке называли плохих игроков в гольф, дилетантов;
e) Это мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

35. Скамер?

a) Это лицо, которое взламывает интрасеть в познавательных целях;
b) Это мошенник, рассылающий свои послания, в надежде обмануть наивных и жадных;

c) Это лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО;
d) Так в XIX веке называли плохих игроков в гольф, дилетантов;
e) Это мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

36. Спамер?

a) Это лицо, которое взламывает интрасеть в познавательных целях;
b) Это мошенник, рассылающий свои послания, в надежде обмануть наивных и жадных;
c) Это лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО;
d) Это тот, от кого приходят в наши почтовые ящики не запрошенные рассылки;
e) Это мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

37. Лицо, которое взламывает интрасеть в познавательных целях это:

a) скамер;
b) хакер;
c) фишер;
d) фракер;
e) кракер.

38. Мошенник, рассылающий свои послания, в надежде обмануть наивных и жадных это:

a) скамер;
b) хакер;
c) фишер;
d) фракер;
e) кракер.

39. Лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО это:

a) скамер;
b) хакер;
c) фишер;
d) фракер;
e) кракер.

40**. Так в XIX веке называли плохих игроков в гольф, дилетантов это:**

a) скамер;
b) хакер;
c) фишер;
d) фракер;
e) кракер.

41. Мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию это:

a) скамер;

b) хакер;
c) фишер;
d) фракер;
e) кракер.

42. От них приходят в наши почтовые ящики не запрошенные рассылки это:

a) скамер;
b) хакер;
c) спамер;
d) фракер;
e) кракер.

43. Защита информации это:

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

44. Информационные процессы это:

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

45. Шифрование информации это:

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

46. Доступ к информации это:

a) процесс сбора, накопления, обработки, хранения, распределения и поиска информации;

b) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
c) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
d) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
e) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

47. Защита информации от утечки это деятельность по предотвращению:

a) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
b) 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;
c) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
d) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
e) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

48. Защита информации от несанкционированного воздействия это деятельность по предотвращению:

a) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
b) 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;
c) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
d) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
e) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

49. Защита информации от непреднамеренного воздействия это деятельность по предотвращению:

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

b) 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;
c) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
d) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
e) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

50. Защита информации от разглашения это деятельность по предотвращению:

a) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
b) 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;
c) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
d) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
e) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

6.2. Тест 2

1. Защита информации от несанкционированного доступа это деятельность по предотвращению:

a) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
b) 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;
c) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
d) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
e) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

2. Субъект доступа к информации это:

a) физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;
b) субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;
c) субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;
d) субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами;
e) участник правоотношений в информационных процессах.

3. Носитель информации это:

a) физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;
b) субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;
c) субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;
d) субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами;
e) участник правоотношений в информационных процессах.

4. Собственник информации это:

a) физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;
b) субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;
c) субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;
d) субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами;
e) участник правоотношений в информационных процессах.

5. Владелец информации это:

a) физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;
b) субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;
c) субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;

d) субъект, в полном объеме реализующий полномочия, пользования, распоряжения информацией в соответствии с законодательными актами;
e) участник правоотношений в информационных процессах.

6. Пользователь (потребитель) информации это:

a) физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;
b) субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;
c) субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;
d) субъект, в полном объеме реализующий полномочия, пользования, распоряжения информацией в соответствии с законодательными актами;
e) участник правоотношений в информационных процессах.

7. Естественные угрозы безопасности информации вызваны:

a) деятельностью человека;
b) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
c) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
d) корыстными устремлениями злоумышленников;
e) ошибками при действиях персонала.

8. Искусственные угрозы безопасности информации вызваны:

a) деятельностью человека;
b) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
c) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
d) корыстными устремлениями злоумышленников;
e) ошибками при действиях персонала.

9. К основным непреднамеренным искусственным угрозам АСОИ относится:

a) физическое разрушение системы путем взрыва, поджога и т.п.;
b) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
c) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
d) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
e) неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.

10. К основным непреднамеренным искусственным угрозам АСОИ относится:

a) физическое разрушение системы путем взрыва, поджога и т.п.;
b) неправомерное отключение оборудования или изменение режимов работы устройств и программ;

c) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
d) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
e) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

11. К основным непреднамеренным искусственным угрозам АСОИ относится:

a) физическое разрушение системы путем взрыва, поджога и т.п.;
b) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
c) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
d) неумышленная порча носителей информации;
e) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

12. К основным непреднамеренным искусственным угрозам АСОИ относится:

a) запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы;
b) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
c) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
d) физическое разрушение системы путем взрыва, поджога и т.п.;
e) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

13. К основным непреднамеренным искусственным угрозам АСОИ относится:

a) физическое разрушение системы путем взрыва, поджога и т.п.;
b) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
c) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
d) нелегальное внедрение и использование неучтенных программ игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения служебных обязанностей;
e) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

14. К основным непреднамеренным искусственным угрозам АСОИ относится:

a) физическое разрушение системы путем взрыва, поджога и т.п.;
b) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
c) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
d) неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной;
e) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

15. К основным непреднамеренным искусственным угрозам АСОИ относится:

a) физическое разрушение системы путем взрыва, поджога и т.п.;
b) разглашение, передача или утрата атрибутов разграничения доступа;
c) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
d) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
e) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

16. К основным непреднамеренным искусственным угрозам АСОИ относится:

a) физическое разрушение системы путем взрыва, поджога и т.п.;
b) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
c) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
d) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
e) проектирование архитектуры системы, с возможностями, представляющими опасность для работоспособности системы и безопасности информации.

17. К основным непреднамеренным искусственным угрозам АСОИ относится:

a) игнорирование организационных ограничений при работе в системе;
b) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
c) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
d) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
e) физическое разрушение системы путем взрыва, поджога и т.п..

18. К основным непреднамеренным искусственным угрозам АСОИ относится:

a) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
b) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
c) вход в систему в обход средств защиты;
d) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
e) физическое разрушение системы путем взрыва, поджога и т.п.

19. К основным непреднамеренным искусственным угрозам АСОИ относится:

a) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
b) некомпетентное использование, настройка или отключение средств защиты;
c) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
d) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
e) физическое разрушение системы путем взрыва, поджога и т.п..

20. К основным непреднамеренным искусственным угрозам АСОИ относится:

a) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
b) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
c) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
d) пересылка данных по ошибочному адресу абонента;
e) физическое разрушение системы путем взрыва, поджога и т.п..

21. К основным непреднамеренным искусственным угрозам АСОИ относится:

a) ввод ошибочных данных;
b) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
c) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
d) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
e) физическое разрушение системы путем взрыва, поджога и т.п..

22. К основным непреднамеренным искусственным угрозам АСОИ относится:

a) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
b) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
c) неумышленное повреждение каналов связи;
d) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
e) физическое разрушение системы путем взрыва, поджога и т.п.

23. К основным преднамеренным искусственным угрозам АСОИ относится:

a) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
b) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
c) физическое разрушение системы путем взрыва, поджога и т.п.;
d) игнорирование организационных ограничений (установленных правил) при работе в системе;
e) пересылка данных по ошибочному адресу абонента.

24. К основным преднамеренным искусственным угрозам АСОИ относится:

a) отключение или вывод из строя систем электропитания, охлаждения и вентиляции, линий связи и т.п.;
b) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
c) неправомерное отключение оборудования или изменение режимов работы устройств и программ;

d) игнорирование организационных ограничений (установленных правил) при работе в системе;
e) пересылка данных по ошибочному адресу абонента.

25. К основным преднамеренным искусственным угрозам АСОИ относится:

a) пересылка данных по ошибочному адресу абонента;
b) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
c) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
d) игнорирование организационных ограничений (установленных правил) при работе в системе;
e) действия по дезорганизации функционирования системы (изменение режимов работы, забастовка, саботаж персонала, и т.п.).

26. К основным преднамеренным искусственным угрозам АСОИ относится:

a) пересылка данных по ошибочному адресу абонента;
b) внедрение агентов в число персонала системы, в том числе в административную группу, отвечающую за безопасность;
c) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
d) игнорирование организационных ограничений (установленных правил) при работе в системе;
e) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

27. К основным преднамеренным искусственным угрозам АСОИ относится:

a) пересылка данных по ошибочному адресу абонента;
b) игнорирование организационных ограничений (установленных правил) при работе в системе;
c) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
d) вербовка персонала или отдельных пользователей, имеющих необходимые полномочия;
e) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

28. К основным преднамеренным искусственным угрозам АСОИ относится:

a) пересылка данных по ошибочному адресу абонента;
b) игнорирование организационных ограничений (установленных правил) при работе в системе;
c) применение подслушивающих устройств, дистанционная фото- и видеосъемка и т.п.;
d) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
e) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

29. К основным преднамеренным искусственным угрозам АСОИ относится:

a) пересылка данных по ошибочному адресу абонента;
b) игнорирование организационных ограничений (установленных правил) при работе в системе;
c) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
d) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
e) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

30. К основным преднамеренным искусственным угрозам АСОИ относится:

a) перехват данных, передаваемых по каналам связи;
b) игнорирование организационных ограничений (установленных правил) при работе в системе;
c) пересылка данных по ошибочному адресу абонента;
d) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
e) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

31. К основным преднамеренным искусственным угрозам АСОИ относится:

a) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
b) игнорирование организационных ограничений (установленных правил) при работе в системе;
c) пересылка данных по ошибочному адресу абонента;
d) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
e) хищение носителей информации.

32. К основным преднамеренным искусственным угрозам АСОИ относится:

a) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
b) игнорирование организационных ограничений (установленных правил) при работе в системе;
c) несанкционированное копирование носителей информации;
d) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
e) пересылка данных по ошибочному адресу абонента.

33. К основным преднамеренным искусственным угрозам АСОИ относится:

a) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
b) хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);
c) игнорирование организационных ограничений (установленных правил) при работе в системе;

d) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
e) пересылка данных по ошибочному адресу абонента.

34. К основным преднамеренным искусственным угрозам АСОИ относится:

a) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
b) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
c) игнорирование организационных ограничений (установленных правил) при работе в системе;
d) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
e) пересылка данных по ошибочному адресу абонента.

35. К основным преднамеренным искусственным угрозам АСОИ относится:

a) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
b) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
c) игнорирование организационных ограничений (установленных правил) при работе в системе;
d) незаконное получение паролей и других реквизитов разграничения доступа;
e) пересылка данных по ошибочному адресу абонента.

36. К основным преднамеренным искусственным угрозам АСОИ относится:

a) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
b) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
c) игнорирование организационных ограничений (установленных правил) при работе в системе;
d) пересылка данных по ошибочному адресу абонента;
e) несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики.

37. К основным преднамеренным искусственным угрозам АСОИ относится:

a) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
b) вскрытие шифров криптозащиты информации;
c) игнорирование организационных ограничений (установленных правил) при работе в системе;
d) пересылка данных по ошибочному адресу абонента;
e) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

38. К основным преднамеренным искусственным угрозам АСОИ относится:

a) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
b) пересылка данных по ошибочному адресу абонента;
c) игнорирование организационных ограничений (установленных правил) при работе в системе;
d) внедрение аппаратных спецвложений, программных "закладок" и "вирусов";
e) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

39. К основным преднамеренным искусственным угрозам АСОИ относится:

a) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
b) незаконное подключение к линиям связи с целью работы "между строк";
c) игнорирование организационных ограничений (установленных правил) при работе в системе;
d) пересылка данных по ошибочному адресу абонента;
e) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

40. К основным преднамеренным искусственным угрозам АСОИ относится:

a) неправомерное отключение оборудования или изменение режимов работы устройств и программ;
b) игнорирование организационных ограничений (установленных правил) при работе в системе;
c) незаконное подключение к линиям связи с целью подмены законного пользователя путем его отключения после входа в систему;
d) пересылка данных по ошибочному адресу абонента;
e) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

41. К внутренним нарушителям информационной безопасности относится:

a) клиенты;
b) пользователи системы;
c) посетители;
d) любые лица, находящиеся внутри контролируемой территории;
e) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации.

42. К внутренним нарушителям информационной безопасности относится:

a) клиенты;
b) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
c) посетители;
d) любые лица, находящиеся внутри контролируемой территории;
e) персонал, обслуживающий технические средства.

43. К внутренним нарушителям информационной безопасности относится:

a) сотрудники отделов разработки и сопровождения ПО;

b) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
c) посетители;
d) любые лица, находящиеся внутри контролируемой территории;
e) клиенты.

44. К внутренним нарушителям информационной безопасности относится:

a) посетители;
b) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
c) технический персонал, обслуживающий здание;
d) любые лица, находящиеся внутри контролируемой территории;
e) клиенты.

45. К внутренним нарушителям информационной безопасности относится:

a) посетители;
b) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
c) любые лица, находящиеся внутри контролируемой территории;
d) сотрудники службы безопасности;
e) клиенты.

46. К внутренним нарушителям информационной безопасности относится:

a) посетители;
b) руководители различных уровней;
c) любые лица, находящиеся внутри контролируемой территории;
d) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
e) клиенты.

47. К посторонним лицам нарушителям информационной безопасности относится:

a) пользователи;
b) персонал, обслуживающий технические средства;
c) клиенты;
d) технический персонал, обслуживающий здание;
e) сотрудники службы безопасности.

48. К посторонним лицам нарушителям информационной безопасности относится:

a) пользователи;
b) персонал, обслуживающий технические средства;
c) технический персонал, обслуживающий здание;
d) посетители;
e) сотрудники службы безопасности.

49. К посторонним лицам нарушителям информационной безопасности относится:

a) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
b) персонал, обслуживающий технические средства;
c) технический персонал, обслуживающий здание;
d) пользователи;
e) сотрудники службы безопасности.

50. К посторонним лицам нарушителям информационной безопасности относится:

a) сотрудники службы безопасности;
b) персонал, обслуживающий технические средства;
c) технический персонал, обслуживающий здание;
d) пользователи;
e) представители конкурирующих организаций.

6.3. ВОПРОСЫ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

1) Каковы методы изучения курса «Программно-аппаратная защита информации»?
2) Каково содержание курса «Программно-аппаратная защита информации»?
3) Что такое идентификация?
4) В чем отличия между идентификацией и аутентификацией?
5) Какие существуют методы ограничения доступа к файлам?
6) В чем отличия механизмов доступа к файлам в операционных системах Linux и Windows?
7) Какие алгоритмы шифрования используются в программно-аппаратных средствах шифрования?
8) Чем обусловлена стойкость современных средств шифрования?
9) Какие существуют методы и средства ограничения доступа к компонентам ЭВМ?
10) Какие методы можно использовать, чтобы защитить программу от несанкционированного копирования?
11) Какая информация относится к ключевой?
12) Как организованы ключевые системы?
13) Технология построения защищенных компьютерных систем. Бизнес процессы и информационная поддержка. Противники, ущербы, угрозы, уязвимости. Политика безопасности. Риски. Аксиома безопасности как защиты доступа.
14) Классификация (категорирование) информации. Доказательство непротиворечивости, полноты. Задание функций автоматического категорирования.
15) Дискреционная политика безопасности. Неустойчивость к атакам с помощью «троянского коня». Сложность задачи контроля распространения прав в дискреционной политике. Модель take-grant.
16) Ролевая модель политики безопасности. Теорема о связи ролевой модели и дискреционной политики.
17) Простейшие информационные потоки. Многоуровневая политика безопасности (MLS). Устойчивость MLS к атакам с помощью троянского коня. Условия сохранение безопасного состояния при функционировании системы с многоуровневой политикой безопасности. Модель Белла-Лападулла. BST теорема. Модель LOW WATER MARK.
18) Сложные информационные потоки. Скрытые каналы. Примеры выполнения политики безопасности и нарушения безопасности с помощью скрытых каналов. Невидимость нарушения системой защиты.
19) Модель невлияния. Теоремы о сохранении безопасного состояния в автоматной модели невлияния. Невидимость верхнего уровня относительно нижнего уровня. Примеры.
20) Пример нарушения невидимости при выполнении условий невлияния.
21) Модель изолированной программной среды.
22) Распределенные системы. Критические системы. Обоснование нового базового набора требований по безопасности для больших распределенных систем. Угрозы в распределенных системах. Простейшие модели безопасных распределенных систем (с доказательством)

23) Механизмы защиты.

24) Архитектурная реализация многоуровневой политики безопасности. Доказательство безопасности для потоков в общем виде.

7. Учебно-методическое и информационное обеспечение учебной дисциплины:

7.1. Литература

1. Закон РФ "О государственной тайне" 2008 г. 32 стр.
2. Закон РФ "Об информации, информатизации и защите информации" 2006г. 24стр.
3. Доктрина информационной безопасности Российской Федерации от 09.09.2000 № ПР 1895. 2004г. 48стр.
4. Словарь терминов Гостехкомиссии при президенте РФ
5. http://prikladnayainformatika.ru/keywords
6. Носов В.А. Вводный курс по дисциплине “Информационная безопасность” 2004г. 50стр.
7. Соколов А.В. «Методы информационной защиты объектов и компьютерных сетей». 2000г. 272стр.
8. Б. Анин «Защита компьютерной информации». 2000г. 384стр.
9. Малюк «Информационная безопасность: концептуальные и методологические основы защиты информации». 2004г. 280стр.
10. Галатенко В.А. «Стандарты информационной безопасности». 2004г. 328стр.
11. П. Ю. Белкин, О. О. Михальский, А. С. Першаков, Д. И. Правиков, В. Г. Проскурин, Г. В. Фоменков «Защита программ и данных». 1999г.
12. http://www.jetinfo.ru/2002/7/1/article1.7.200231.html - Нормативная база анализа защищенности
13. http://www.sbcinfo.ru/articles/doc/gtc_doc/contents.htm
14. http://counter-terrorism.narod.ru/magazine1/kotenko-8-1.htm - Вопросы ИБ и терроризма
15. http://snoopy.falkor.gen.nz/~rae/des.html - описание алгоритма DES
16. http://markova-ne.narod.ru/infbezop.html - Вопросы ИБ и СМИ
17. http://www.ctta.ru/ - Некоторые проблемы ИБ
18. http://st.ess.ru/steganos.htm - Вопросы стеганографии
19. http://www.infosecurity.ru/_site/problems.shtml - Суть проблемы Информационной Безопасности
20. http://www.jetinfo.ru/2004/11/3/article3.11.2004.html - Федеральный стандарт США FIPS 140-2**7.**

7.2. Программное обеспечение и Интернет-ресурсы

Антивирусные программы

8. Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий (проводятся в форме компьютерных презентаций) по учебной дисциплине необходима аудитория, рассчитанная на группу магистрантов, оборудованная интерактивной доской и компьютером. На компьютере должно быть установлено программное обеспечение, включающее операционную систему MS Windows 7 (или 8) и редактор презентаций MS Power Point (версии 2007 или более поздней).

Для лабораторных занятий требуется аудитория из 12-15 персональных компьютеров (IBM PC или совместимой с ней), объединенные в локальную сеть с возможностью доступа к ресурсам сети Internet и с периферийным оборудованием.

Каждый компьютер должен иметь:

- 4-ядерный процессор семейства Intel Pentium или более производительный;
- оперативную память объемом не менее 4 Гб;

- жесткий диск объемом не менее 500 Гб;
- дисковод оптических дисков класса DVD-RW;
- монитор с диагональю не менее 17";
- стандартную клавиатуру (102 клавиши или более);
- манипулятор «мышь» оптического типа с тремя кнопками и колесом прокрутки;
-коврик для манипулятора «мышь» оптического типа.

На каждом компьютере должно быть установлено следующее программное обеспечение:

- сетевая операционная система семейства Microsoft Windows (Windows 7 или более поздняя);

Программа составлена в соответствии с требованиями ФГОС ВПО с учетом рекомендаций и ПООП ВПО по направлению 051000 – Профессиональное образование (магистратура)

Авторы (разработчики): к.т.н., профессор Г.П. Раджабалиев; ст.пр-ль Нурмагомедова Н.Х.

кафедра информационных технологий

Рецензенты (эксперты): Нажмудинов А.М. к. ф.-м.н., доцент, зав каф. ТФиТД, ДГПУ

Программа одобрена на заседании _____

(*уполномоченный орган вуза (УМК, НМС, Ученый совет)*