МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет физико-технический

УТВЕРЖДАЮ
Проректор по учебной работе,
качеству образования – первый
проректор
_____ Т.А. Хагуров
подпись
«31» мая 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
ФТД.02 современная криптография

Направление подготовки/специальность 09.04.02 Информационные системы и технологии

Направленность (профиль) / специализация Системы и сети доставки цифрового контента

Форма обучения очная

Квалификация магистр

Краснодар 2024

Рабочая программа дисциплины ФТД.02 Современная криптография составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки/ специальности 09.04.02 Информационные системы и технологии (Системы и сети доставки цифрового контента)

Программу составил (и):
О.М. Жаркова, доцент кафедры теор. физики и комп. технологий, кандидат физ.- мат. наук 
подпись

Рабочая программа дисциплины ФТД.02 Современная криптография утверждена на заседании кафедры теоретической физики и компьютерных технологий
протокол № 8 от «16» апреля 2024 г.
Заведующий кафедрой (выпускающей) Лебедев К.А. 
подпись

Утверждена на заседании учебно-методической комиссии физико-технического факультета
протокол № 5 от «18» апреля 2024 г.
Председатель УМК факультета Богатов Н.М. 
подпись

Рецензенты:

М.С. Коваленко, кандидат физико-математических наук, доцент кафедры физики и информационных систем

Л.Р. Григорян, генеральный директор ООО НПФ «Мезон»
кандидат физико-математических наук

1 Цели и задачи изучения дисциплины (модуля).

1.1 Цель освоения дисциплины.

Формирование у студентов компетенций в области основных принципов, методов, способов и средств защиты информации, а также их применения в корпоративных информационно-технологических системах.

1.2 Задачи дисциплины.

1) изучение и классификация причин нарушений безопасности, методов и средств защиты информации;

2) рассмотрение области применения и тенденций развития средств защиты информации;

3) приобретение практических навыков работы с современными сетевыми фильтрами и средствами криптографического преобразования информации, проектирование мониторов безопасности субъектов и объектов.

1.3 Место дисциплины (модуля) в структуре образовательной программы.

Дисциплина «Современная криптография» относится к дисциплинам по выбору вариативной части Блока 1 "Дисциплины (модули)" учебного плана.

Для освоения дисциплины «Современная криптография» студенты должны обладать базовыми знаниями и умениями по дисциплинам «Теория информационных процессов и систем», «Корпоративные информационные системы», «Информационная безопасность и защита информации» (в соответствии с Рабочим учебным планом Направления 09.03.02 Информационные системы и технологии - Направленность (профиль) "Информационные системы и технологии"), «Модели и методы доступа к информационной среде».

Полученные в рамках дисциплины «Современная криптография» знания инструментальных средств защиты информации и приобретенные навыки построения современных защищенных информационных систем найдут практическое применение при изучении таких дисциплин как «Современные проблемы науки и производства», «Анализ и синтез информационных систем», «Модели и методы проектирования информационных систем».

1.4 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы.

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1.	ПК-2	способность анализировать системные проблемы обработки информации и содержания в современной криптографии	логику рассуждений и высказываний, основанных на интерпретации данных, интегрированных их разных областей науки и техники	проводить разработку и исследование теоретических и экспериментальных моделей, объектов профессиональной деятельности в различных областях; сбор, анализ научно-технической	навыками профессиональной эксплуатации современного оборудования и приборов

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
				информации, отечественного и зарубежного опыта по тематике исследования; выносить суждения на основании неполных данных	

2. Структура и содержание дисциплины.

2.1 Распределение трудоёмкости дисциплины по видам работ.

Общая трудоёмкость дисциплины составляет 1 зач.ед. (36 часов), их распределение по видам работ представлено в таблице

Вид учебной работы		Всего часов	Семестры (часы)			
				10		
Контактная работа, в том числе:		**22,2**		**22,2**		
Аудиторные занятия (всего):		**22**		**22**		
Занятия лекционного типа		10		10		
Лабораторные занятия		-		-		
Занятия семинарского типа (семинары, практические занятия)		12		12		
Иная контактная работа:		**0,2**		**0,2**		
Контроль самостоятельной работы (КСР)		-		-		
Промежуточная аттестация (ИКР)		0,2		0,2		
Самостоятельная работа, в том числе:		**13,8**		13,8		
Проработка учебного (теоретического) материала		6,9		6,9		
Тест		6,9		6,9		
Контроль:						
Подготовка к экзамену		-	-			
Общая трудоемкость	**час.**	**36**		**36**		
	в том числе контактная работа	**22,2**		**22,2**		
	зач. ед	**1**		**1**		

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в А семестре

№	Наименование разделов	Количество часов			
		Всего	Аудиторная работа		Внеаудиторная работа
			Л	ЛР	СРС
1	2	3	4	5	6
1.	Тема 1. Актуальность информационной безопасности, понятия и определения	5,8	1	1	3,8
2.	Тема 2. Угрозы информации	5	1	1	2
3.	Тема 3. Вредоносные программы	5	1	2	2
4.	Тема 4. Защита от компьютерных вирусов	5	2	2	1
5.	Тема 5. Методы и средства защиты компьютерной информации	5	2	2	1
6.	Тема 6. Криптографические методы информационной безопасности	5	2	2	1
7.	Тема 7. Лицензирование и сертификация в области защиты информации	5	1	2	2
	Итого по дисциплине:	35,8	10	12	13,8

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа.

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1.	Тема 1. Актуальность информационной безопасности, понятия и определения	1.1. Актуальность информационной безопасности. 1.2. Национальные интересы РФ в информационной сфере и их обеспечение. 1.3. Классификация компьютерных преступлений. 1.4. Способы совершения компьютерных преступлений. 1.5. Пользователи и злоумышленники в Интернет. 1.6. Причины уязвимости сети Интернет.	Тест
2.	Тема 2. Угрозы информации	2.1. Виды угроз информационной безопасности РФ. 2.2. Источники угроз информационной безопасности РФ. 2.3. Угрозы информационной безопасности для АСОИ. 2.4. Удаленные атаки на интрасети.	Тест

3.	Тема 3. Вредоносные программы	3.1. Условия существования вредоносных программ. 3.2. Классические компьютерные вирусы. 3.3. Сетевые черви. 3.4. Троянские программы. 3.5. Спам. 3.6. Хакерские утилиты и прочие вредоносные программы. 3.7. Кто и почему создает вредоносные программы.	Тест
4.	Тема 4. Защита от компьютерных вирусов	4.1. Признаки заражения компьютера. 4.2. Источники компьютерных вирусов. 4.3. Основные правила защиты. 4.4. Антивирусные программы.	Тест
5.	Тема 5. Методы и средства защиты компьютерной информации	5.1. Методы обеспечения информационной безопасности РФ. 5.2. Ограничение доступа. 5.3. Контроль доступа к аппаратуре. 5.4. Разграничение и контроль доступа к информации. 5.5. Предоставление привилегий на доступ. 5.6. Идентификация и установление подлинности объекта (субъекта). 5.7. Защита информации от утечки за счет побочного электромагнитного излучения и наводок. 5.8. Методы и средства защиты информации от случайных воздействий. 5.9. Методы защиты информации от аварийных ситуаций. 5.10. Организационные мероприятия по защите информации. 5.11. Организация информационной безопасности компании. 5.12. Выбор средств информационной безопасности. 5.13. Информационное страхование.	Тест
6.	Тема 6. Криптографические методы информационной безопасности	6.1. Классификация методов криптографического закрытия информации. 6.2. Шифрование. 6.2.1. Симметричные криптосистемы. 6.2.2. Криптосистемы с открытым ключом (асимметричные). 6.2.3. Характеристики существующих шифров. 6.3. Кодирование. 6.4. Стеганография. 6.5. Электронная цифровая подпись.	Тест

7.	Тема 7. Лицензирование и сертификация в области защиты информации	7.1. Законодательство в области лицензирования и сертификации. 7.2. Правила функционирования системы лицензирования. 7.3. Критерии безопасности компьютерных систем. «Оранжевая книга». 7.4. Руководящие документы Гостехкомиссии.	Тест

2.3.2 Занятия семинарского типа.

Не предусмотрены

2.3.3 Лабораторные занятия.

№	Наименование раздела	Наименование лабораторных работ	Форма текущего контроля
1	2	3	4
1.	Тема 4	Профилактика компьютерных систем от заражения вирусами	ЛР
2.	Тема 5	Защита информации с помощью пароля	ЛР
3.	Тема 5	Исследование средств безопасности операционных систем	ЛР
4.	Тема 5	Аутентификация пользователей Web-систем средствами технологии PHP	ЛР
5.	Тема 5	Защита баз данных	ЛР
6.	Тема 6	Исследование метода компьютерной стеганографии для защиты информации	ЛР
7.	Тема 6	Разработка и реализация алгоритма криптографического преобразования	ЛР

2.3.4 Примерная тематика курсовых работ (проектов)

Не предусмотрены

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1.	Проработка учебного (теоретического) материала	Информационная безопасность / ред. О. Рытенковой - Москва : ГРОТЕК, 2013. - № 1. - 59 с.: ил. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=210607
2.	Тест	Красильникова, В. Использование информационных и коммуникационных технологий в образовании : учебное пособие / В. Красильникова ; Министерство образования и науки Российской Федерации, Федеральное государственное

		бюджетное образовательное учреждение высшего профессионального образования «Оренбургский государственный университет». - 2-е изд. перераб. и дополн. - Оренбург : ОГУ, 2012. - 292 с. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=259225

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

3. Образовательные технологии.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью ООП, особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом в учебном процессе должен составлять не менее 10 процентов от общего объема аудиторных занятий.

Так как общий объем аудиторных занятий по дисциплине «Современная криптография» для очной формы обучения составляет 20 часов, то занятия, проводимые в интерактивных формах, должны составлять не менее 2 часов.

Используемые интерактивные образовательные технологии по семестрам и видам занятий представлены в таблице.

Семестр	Вид занятия (Л, ПЗ, С, ЛР, КСР)	Используемые интерактивные образовательные технологии	Количество часов
В Очная форма	*Л*	«Студент в роли преподавателя»	1
	Л	«Работа в малых группах»	1
	ЛР	«Мозговой штурм»	1
	ЛР	«Творческое задание»	1
	Итого:		4

Пояснения к таблице

В современных условиях развитие продуктивных технологий в сфере образования становится неотъемлемой частью процесса модернизации. Заканчиваются возможности экстенсивного пути развития образования, при котором повышение образованности и профессиональности связывалось с увеличением объема знаний, и начинается переход к интенсивному пути развития образования. Он требует становления принципиально новых образовательных подходов в противовес широко распространенным сегодня репродуктивным технологиям, основанным на простом воспроизводстве информации. Новые технологии должны базироваться на продуктивности, креативности, мобильности и опираться на научное мышление, формирование которого у обучающихся становится основной задачей образовательного процесса.

Основные педагогические технологии

1. Традиционное обучение
2. Феноменологический подход
3. Интерактивные подходы
4. Эвристическое обучение
5. Программированное обучение
6. Контекстное обучение
7. Активное обучение
8. Дидактическая эвристика
9. Авторские педагогические технологии
10. Эмоционально-смысловой подход
11. Компьютерные технологии обучения
12. Разноуровневое обучение
13. Метод проектов
14. Учение через обучение
15. Технология парного обучения
16. Конструктивное обучение (конструктивистское обучение)
17. Нооген
18. Пренатальное обучение

Интерактивные подходы

Костяком интерактивных подходов являются интерактивные упражнения и задания, которые выполняются учащимися. Основное отличие интерактивных упражнений и заданий от обычных заключается в том, что они направлены не только и не столько на закрепление уже изученного материала, сколько на изучение нового. Современная педагогика богата целым арсеналом интерактивных подходов, среди которых можно выделить следующие:

- Творческие задания
- Работа в малых группах
- Обучающие игры (ролевые игры, имитации, деловые игры и образовательные игры)
- Использование общественных ресурсов (приглашение специалиста, экскурсии)
- Социальные проекты и другие внеаудиторные методы обучения (социальные проекты, соревнования, радио и газеты, фильмы, спектакли, выставки, представления, песни и сказки)
- Разминки
- Изучение и закрепление нового материала (интерактивная лекция, работа с наглядными пособиями, видео- и аудиоматериалами, «ученик в роли учителя», «каждый учит каждого», мозаика (ажурная пила), использование вопросов, Сократический диалог)
- Обсуждение сложных и дискуссионных вопросов и проблем («Займи позицию (шкала мнений)», ПОПС-формула, проективные техники, «Один — вдвоем — все вместе», «Смени позицию», «Карусель», «Дискуссия в стиле телевизионного ток-шоу», дебаты, симпозиум)
- Разрешение проблем («Дерево решений», «Мозговой штурм», «Анализ казусов», «Переговоры и медиация», «Лестницы и змейки»)

Творческие задания

Под творческими заданиями мы будем понимать такие учебные задания, которые требуют от учащихся не простого воспроизводства информации, а творчества, поскольку задания содержат больший или меньший элемент неизвестности и имеют, как правило,

несколько подходов. Творческое задание составляет содержание, основу любого интерактивного метода. Творческое задание (особенно практическое и близкое к жизни обучающегося) придает смысл обучению, мотивирует учащихся. Неизвестность ответа и возможность найти свое собственное «правильное» решение, основанное на своем персональном опыте и опыте своего коллеги, друга, позволяют создать фундамент для сотрудничества, сообучения, общения всех участников образовательного процесса, включая педагога. Выбор творческого задания сам по себе является творческим заданием для педагога, поскольку требуется найти такое задание, которое отвечало бы следующим критериям:

- не имеет однозначного и односложного ответа или решения
- является практическим и полезным для учащихся
- связано с жизнью учащихся
- вызывает интерес у учащихся
- максимально служит целям обучения

Если учащиеся не привыкли работать творчески, то следует постепенно вводить сначала простые упражнения, а затем все более сложные задания.

Работа в малых группах

Работа в малых группах — это одна из самых популярных стратегий, так как она дает всем учащимся (в том числе и стеснительным) возможность участвовать в работе, практиковать навыки сотрудничества, межличностного общения (в частности, умение активно слушать, вырабатывать общее мнение, разрешать возникающие разногласия). Все это часто бывает невозможно в большом коллективе. Работа в малой группе — неотъемлемая часть многих интерактивных методов, например таких, как мозаика, дебаты, общественные слушания, почти все виды имитаций и др.

При организации групповой работы, следует обращать внимание на следующие ее аспекты. Нужно убедиться, что учащиеся обладают знаниями и умениями, необходимыми для выполнения группового задания. Нехватка знаний очень скоро даст о себе знать — учащиеся не станут прилагать усилий для выполнения задания. Надо стараться сделать свои инструкции максимально четкими. Маловероятно, что группа сможет воспринять более одной или двух, даже очень четких, инструкций за один раз, поэтому надо записывать инструкции на доске и (или) карточках. Надо предоставлять группе достаточно времени на выполнение задания.

Критическое мышление

Идея развития критического мышления является достаточно новой для российской дидактики. Заговорили о целостной технологии развития критического мышления лишь в середине 90-х годов. Но уже сегодня сторонников развития критического мышления учащихся достаточно много.

Критическое мышление означает не негативность суждений или критику, а разумное рассмотрение разнообразия подходов с тем, чтобы выносить обоснованные суждения и решения. Ориентация на критическое мышление предполагает вежливый скептицизм (ничто не принимается на веру), сомнение в общепринятых истинах, означает выработку точки зрения по определенному вопросу и способность отстоять эту точку зрения логическими доводами. Критическое мышление не является отдельным навыком, оно сочетает в себе следующие умения:

- выражать свои мысли (устно и письменно) ясно, уверенно и корректно по отношению к окружающим;
- аргументировать свою точку зрения и учитывать точки зрения других;
- брать на себя ответственность;
- работать с увеличивающимся и постоянно обновляющимся информационным потоком;

- задавать вопросы, самостоятельно формулировать гипотезу;
- решать проблемы;
- вырабатывать собственное мнение на основе осмысления различного опыта, идей и представлений;
- участвовать в совместном принятии решения;
- выстраивать конструктивные взаимоотношения с другими людьми.

Метод проектов

Основной его тезис: я знаю, для чего мне надо то, что я познаю, где и как я могу эти знания применить. Каждый обучаемый, принимая участие в проектировании, находит себе дело с учетом уровня своего интеллектуального развития, уровня подготовки по данной проблеме, своих способностей и задатков. Для того чтобы проект получился, надо верить в обучаемого. Мое твердое убеждение – нет плохих учеников. Они все яркие, талантливые, неповторимые индивидуальности.

Основные требования к использованию метода проектов:

1. Наличие значимой в исследовательском творческом плане проблемы / задачи, требующей интегрированного знания, исследовательского поиска для ее решения (например, исследование демографической проблемы в разных регионах мира; создание серии репортажей из разных концов земного шара одной проблеме и т.п.).

2. Практическая, теоретическая, познавательная значимость предполагаемых результатов. Например, доклад о демографическом состоянии данного региона, факторах, влияющих на это состояние, тенденциях, прослеживающихся в развитии данной проблемы; выпуск газеты, план мероприятий и т.п.

3. Самостоятельная (индивидуальная, парная, групповая) деятельность учащихся.

4. Использование исследовательских методов:

- определение проблемы и вытекающих из нее задач исследования;
- выдвижение гипотезы их решения;
- обсуждение методов исследования;
- обсуждение способов оформления конечных результатов (презентаций, защиты, творческих отчетов и т.п.);
- сбор, систематизация и анализ полученных данных;
- подведение итогов, оформление результатов, их презентация;
- выводы, выдвижение новых проблем исследования.

Таким образом, метод проектов является одной из самых результативных и прогрессивных педагогических технологий. Он позволяет развивать познавательные навыки учащихся, критическое мышление, умение самостоятельно конструировать свои знания, ориентироваться в информационном пространстве.

Метод «мозгового штурма»

Существуют разные формы «мозгового штурма»: групповая прямая (совместный поиск возможных решений имеющейся задачи); групповая обратная (определение недостатков в имеющейся проблеме); индивидуальная (каждый участник за короткий промежуток времени должен сформулировать не менее одной оригинальной идеи).

Перед началом «мозгового штурма» необходимо создать у обучающихся доброжелательный настрой, добиться раскованности. При проведении «мозгового штурма» возможны лишь уточняющие вопросы, абсолютно неприемлемы критические замечания и промежуточные оценки, а поощрение и поддержка партнеров приветствуется. Участники должны формулировать суждения и идеи кратко и четко, действовать по принципу «чем больше идей, решительнее атака, тем ближе достижение цели штурма».

Дискуссия

Она является одной из важнейших форм образовательной деятельности, стимулирующей инициативность учащихся. Учебный материал в ходе дискуссии усваивается за счет:

- обмена информацией между участниками;
- разных подходов к одному и тому же предмету;
- сосуществования различных, вплоть до взаимоисключающих, точек зрения;
- возможности критиковать и даже отвергать любое мнение;
- поиска группового соглашения в виде общего мнения или решения.

Задача дискуссии – коллективно, с разных точек зрения, под разными углами обсудить и исследовать спорные моменты. Основные правила ведения дискуссии:

- нельзя критиковать людей, только их идеи;
- цель дискуссии не в определении победителя, а в консенсусе;
- все участники должны быть вовлечены в дискуссию;
- выступления должны проходить организованно, с разрешения ведущего, перепалка недопустима;
- каждый участник должен иметь право и возможность высказаться;
- обсуждению подлежат все позиции; – в процессе дискуссии участники могут изменить свою позицию;
- строить аргументацию необходимо на бесспорных фактах;
- в заключение всегда должны подводиться итоги.

По ходу дискуссии преподаватель должен следить, чтобы слишком эмоциональные и разговорчивые учащиеся не подменили тему, и чтобы критика позиций друг друга была обоснованной. Соединение работы в группах с решением проблемной ситуации создает наиболее эффективные условия для обмена знаниями, идеями и мнениями, обеспечивает всесторонний анализ и обоснованный выбор решения той или иной темы. Студенты овладевают ораторскими умениями, искусством ведения полемики, что само по себе вносит важный вклад в их личностное развитие.

В целом хотелось бы отметить, что самостоятельная познавательная и мыслительная деятельность является главным средством развития личности обучающегося, она раскрывает его потенциальные способности, формирует необходимые в современном мире навыки самообразования, ориентации в стремительном потоке информации. Использование интерактивных технологий – лучший способ активизировать эту деятельность у студентов.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации.

4.1 Фонд оценочных средств для проведения текущего контроля.

По дисциплине «Современная криптография» для очной формы обучения предусмотрены следующие формы текущего контроля:

а) тестирование (Т) по темам 1-7;

б) выполнение лабораторных работ (ЛР) по темам 4, 5, 6.

Образцы тестов для проведения текущего контроля знаний по дисциплине «Современная криптография» по темам 1-7:

Тест по теме 1

1. В каком году в России появились первые преступления с использованием компьютерной техники (были похищены 125,5 тыс. долл. США во Внешэкономбанке)?
1. 1988; 2. 1991; 3. 1994; 4. 1997; 5. 2002.

2. Сколько уголовных дела по ст. ст. 272 и 165 УК РФ было возбуждено в 2003 г. в России?
1. 6; 2. 60; 3. 160; 4. 600; 5. 1600.

3. Какой общий ущерб по данным Института компьютерной безопасности, нанесли компьютерные вирусы за последние 5 лет (млрд долл. США)?
1. 4; 2. 34; 3. 54; 4. 74; 5. 94.

4. По данным журнала «Security Magazine», средний размер ущерба от компьютерного мошенничества составляет (долл. США):
1. 500 000; 2. 1 000 000; 3. 1 500 000; 4. 2 000 000; 5. 2 500 000.

5. По данным Главного информационного центра МВД России, количество компьютерных преступлений ежегодно увеличивается в (раза):
1. 2; 2. 2,5; 3. 3; 4. 3,5; 5. 4.

6. По данным Главного информационного центра МВД России, ежегодный размер материального ущерба от компьютерных преступлений составляет около (млн руб.):
1. 6; 2. 60; 3. 160; 4. 600; 5. 1600.

7. По данным Главного информационного центра МВД России, средний ущерб, причиняемый потерпевшему от 1 компьютерного преступления, равен (млн руб.):
1. 7; 2. 1,7; 3. 2,7; 4. 3,7; 5. 4,7.

8. Сколько процентов электронных писем являются спамом?
1. 10; 2. 30; 3. 50; 4. 70; 5. 90.

9. К каким ежегодным убыткам приводят спамы (млрд долл. США)?
1. 20; 2. 40; 3. 60; 4. 80; 5. 100.

10. В 2003 г. ФСБ пресечено попыток проникновения в информационные ресурсы органов государственной власти России около (раз):
1. 10; 2. 100; 3. 1 000; 4. 10 000; 5. 100 000.

11. Сколько выделяются основных составляющих национальных интересов Российской Федерации в информационной сфере?
1. 2; 2. 3; 3. 4; 4. 5; 5. 6.

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

13. Пассивный перехват информации это – перехват, который:
1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации; 2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций; 3. неправомерно использует технологические отходы информационного процесса; 4. осуществляется путем

использования оптической техники; 5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

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

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

16. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации, называется:
1. активный перехват; 2. пассивный перехват;
3. аудиоперехват; 4. видеоперехват; 5. просмотр мусора.

17. Перехват, который осуществляется путем использования оптической техники, называется:
1. активный перехват; 2. пассивный перехват; 3. аудиоперехват; 4. видеоперехват; 5. просмотр мусора.

18. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций, называется:
1. активный перехват; 2. пассивный перехват; 3. аудиоперехват; 4. видеоперехват; 5. просмотр мусора.

19. Перехват, который осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера, называется:
1. активный перехват; 2. пассивный перехват; 3. аудиоперехват; 4. видеоперехват; 5. просмотр мусора.

20. Перехват, который неправомерно использует технологические отходы информационного процесса, называется:
1. активный перехват; 2. пассивный перехват; 3. аудиоперехват; 4. видеоперехват; 5. просмотр мусора.

21. Как называется способ несанкционированного доступа к информации, который заключается в несанкционированном доступе в компьютер или компьютерную сеть без права на то?
1. «За дураком»; 2. «Брешь»;
3. «Компьютерный абордаж»; 4. «За хвост»; 5. «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?
1. «За дураком»; 2. «Брешь»; 3. «Компьютерный абордаж»; 4. «За хвост»; 5. «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?
1. «За дураком»; 2. «Брешь»; 3. «Компьютерный абордаж»; 4. «За хвост»; 5. «Неспешный выбор».

24. Как называется способ несанкционированного доступа к информации, который заключается в отыскании участков программ, имеющих ошибку или неудачную логику построения?
1. «За дураком»; 2. «Брешь»; 3. «Компьютерный абордаж»; 4. «За хвост»; 5. «Неспешный выбор».

25. Как называется способ несанкционированного доступа к информации, который заключается в нахождении злоумышленником уязвимых мест в ее защите?
1. «За дураком»; 2. «Брешь»; 3. «Компьютерный абордаж»; 4. «За хвост»; 5. «Неспешный выбор».

26. Способ несанкционированного доступа к информации «За дураком» заключается:
1. в отыскании участков программ, имеющих ошибку или неудачную логику построения; 2. в подключении злоумышленника к линии связи законного пользователя и после сигнала, обозначающего конец работы, перехватывания его на себя, получая доступ к системе; 3. в подключении компьютерного терминала к каналу связи в тот момент времени, когда сотрудник, кратковременно покидает свое рабочее место, оставляя терминал в рабочем режиме; 4. в нахождении злоумышленником уязвимых мест в ее защите; 5. в несанкционированном доступе в компьютер или компьютерную сеть без права на то.

27. Способ несанкционированного доступа к информации «Брешь» заключается:
1. в отыскании участков программ, имеющих ошибку или неудачную логику построения; 2. в подключении злоумышленника к линии связи законного пользователя и после сигнала, обозначающего конец работы, перехватывания его на себя, получая доступ к системе; 3. в подключении компьютерного терминала к каналу связи в тот момент времени, когда сотрудник, кратковременно покидает свое рабочее место, оставляя терминал в рабочем режиме; 4. в нахождении злоумышленником уязвимых мест в ее защите; 5. в несанкционированном доступе в компьютер или компьютерную сеть без права на то.

28. Способ несанкционированного доступа к информации «Компьютерный абордаж» заключается:
1. в отыскании участков программ, имеющих ошибку или неудачную логику построения; 2. в подключении злоумышленника к линии связи законного пользователя и после сигнала, обозначающего конец работы, перехватывания его на себя, получая доступ к системе; 3. в подключении компьютерного терминала к каналу связи в тот момент времени, когда сотрудник кратковременно покидает свое рабочее место, оставляя терминал в рабочем режиме; 4. в нахождении злоумышленником уязвимых мест в ее

защите; 5. в несанкционированном доступе в компьютер или компьютерную сеть без права на то.

29. Способ несанкционированного доступа к информации «За хвост» заключается:
1. в отыскании участков программ, имеющих ошибку или неудачную логику построения; 2. в подключении злоумышленника к линии связи законного пользователя и после сигнала, обозначающего конец работы, перехватывания его на себя, получая доступ к системе; 3. в подключении компьютерного терминала к каналу связи в тот момент времени, когда сотрудник кратковременно покидает свое рабочее место, оставляя терминал в рабочем режиме; 4. в нахождении злоумышленником уязвимых мест в ее защите; 5. в несанкционированном доступе в компьютер или компьютерную сеть без права на то.

30. Способ несанкционированного доступа к информации «Неспешный выбор» заключается:
1. в отыскании участков программ, имеющих ошибку или неудачную логику построения; 2. в подключении злоумышленника к линии связи законного пользователя и после сигнала, обозначающего конец работы, перехватывания его на себя, получая доступ к системе; 3. в подключении компьютерного терминала к каналу связи в тот момент времени, когда сотрудник, кратковременно покидает свое рабочее место, оставляя терминал в рабочем режиме; 4. в нахождении злоумышленником уязвимых мест в ее защите; 5. в несанкционированном доступе в компьютер или компьютерную сеть без права на то.

31. Хакер – это:
1. лицо, которое взламывает интрасеть в познавательных целях; 2. мошенник, рассылающий свои послания в надежде обмануть наивных и жадных; 3. лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО; 4. плохой игрок в гольф, дилетант; 5. мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

32. Фракер – это:
1. лицо, которое взламывает интрасеть в познавательных целях; 2. мошенник, рассылающий свои послания в надежде обмануть наивных и жадных;
3. лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов, разрушающих ПО; 4. плохой игрок в гольф, дилетант; 5. мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

33. Кракер – это:
1. лицо, которое взламывает интрасеть в познавательных целях; 2. мошенник, рассылающий свои послания в надежде обмануть наивных и жадных; 3. лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов, разрушающих ПО; 4. плохой игрок в гольф, дилетант; 5. мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

34. Фишер – это:
1. лицо, которое взламывает интрасеть в познавательных целях; 2. мошенник, рассылающий свои послания в надежде обмануть наивных и жадных; 3. лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении

информации и написании вирусов, разрушающих ПО; 4. плохой игрок в гольф, дилетант; 5. мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

35. Скамер – это:
1. лицо, которое взламывает интрасеть в познавательных целях; 2. мошенник, рассылающий свои послания в надежде обмануть наивных и жадных; 3. лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов, разрушающих ПО; 4. плохой игрок в гольф, дилетант; 5. Это мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

36. Спамер – это:
1. лицо, которое взламывает интрасеть в познавательных целях; 2. мошенник, рассылающий свои послания в надежде обмануть наивных и жадных; 3. лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов, разрушающих ПО; 4. тот, от кого приходят в наши почтовые ящики не запрошенные рассылки; 5. мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

37. Лицо, которое взламывает интрасеть в познавательных целях, – это:
1. скамер; 2. хакер; 3. фишер; 4. фракер; 5. кракер.

38. Мошенник, рассылающий свои послания в надежде обмануть наивных и жадных, – это:
1. скамер; 2. хакер; 3. фишер; 4. фракер; 5. кракер.

39. Лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов, разрушающих ПО, – это:
1. скамер; 2. хакер; 3. фишер; 4. фракер; 5. кракер.

40. Плохих игроков в гольф, дилетантов называли в XIX веке:
1. скамер; 2. хакер; 3. фишер; 4. фракер; 5. кракер.

41. Мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию, – это:
1. скамер; 2. хакер; 3. фишер; 4. фракер; 5. кракер.

42. Лицо, от которого в наши почтовые ящики приходят не запрошенные рассылки, – это:
1. скамер; 2. хакер; 3. спамер; 4. фракер; 5. кракер.

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

44. Информационные процессы – это:

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

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

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

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

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

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

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

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

52. Субъект доступа к информации – это:
1. 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; 2. субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации; 3. субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника, в соответствии с установленными правами и правилами доступа к информации либо с их нарушением; 4. субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в

соответствии с законодательными актами; 5. участник правоотношений в информационных процессах.

53. Носитель информации – это:
1. 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; 2. субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации; 3. субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника, в соответствии с установленными правами и правилами доступа к информации либо с их нарушением; 4. субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами; 5. участник правоотношений в информационных процессах.

54. Собственник информации – это:
1. 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; 2. субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации; 3. субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника, в соответствии с установленными правами и правилами доступа к информации либо с их нарушением; 4. субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами; 5. участник правоотношений в информационных процессах.

55. Владелец информации – это:
1. 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; 2. субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации; 3. субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника, в соответствии с установленными правами и правилами доступа к информации либо с их на- рушением; 4. субъект, в полном объеме реализующий полномочия, пользования, распоряжения информацией в соответствии с законодательными актами; 5. участник правоотношений в информационных процессах.

56. Пользователь (потребитель) информации – это:
1. 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; 2. субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации; 3. субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника, в соответствии с установленными правами и правилами доступа к информации либо с их на- рушением; 4. субъект, в полном объеме реализующий полномочия, пользования, распоряжения информацией в соответствии с законодательными актами; 5. участник правоотношений в информационных процессах.

Тест по теме 2

1. Естественные угрозы безопасности информации вызваны:

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

2. Искусственные угрозы безопасности информации вызваны:
1. деятельностью человека; 2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения; 3. воздействиями объективных физических процессов или стихийных природных явлений, не зависящих от человека; 4. корыстными устремлениями злоумышленников; 5. ошибками при действиях персонала.

3. К основным непреднамеренным искусственным угрозам АСОИ относится:
1. физическое разрушение системы путем взрыва, поджога и т.п.; 2. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи; 3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.; 4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств; 5. неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.

4. К основным непреднамеренным искусственным угрозам АСОИ относится:
1. физическое разрушение системы путем взрыва, поджога и т.п.; 2. неправомерное отключение оборудования или изменение режимов работы устройств и программ; 3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.; 4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств; 5. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

5. К основным непреднамеренным искусственным угрозам АСОИ относится:
1. физическое разрушение системы путем взрыва, поджога и т.п.; 2. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств; 3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.; 4. неумышленная порча носителей информации; 5. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

6. К основным непреднамеренным искусственным угрозам АСОИ относится:
1. запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы; 2. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств; 3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.; 4. физическое разрушение системы путем взрыва, поджога и т.п.; 5. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

7. К основным непреднамеренным искусственным угрозам АСОИ относится:
1. физическое разрушение системы путем взрыва, поджога и т.п.; 2. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств; 3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.; 4. нелегальное внедрение и использование неучтенных про- грамм игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения служебных обязанностей; 5. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

8. К основным непреднамеренным искусственным угрозам АСОИ относится: 1. физическое разрушение системы путем взрыва, поджога и т.п.; 2. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств; 3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.; 4. неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной; 5. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

9. К основным непреднамеренным искусственным угрозам АСОИ относится: 1. физическое разрушение системы путем взрыва, поджога и т.п.; 2. разглашение, передача или утрата атрибутов разграничения доступа; 3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.; 4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств; 5. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

10. К основным непреднамеренным искусственным угрозам АСОИ относится:
1. физическое разрушение системы путем взрыва, поджога и т.п.; 2. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи; 3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.; 4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств; 5. проектирование архитектуры системы, с возможностями, представляющими опасность для работоспособности системы и безопасности информации.

11. К основным непреднамеренным искусственным угрозам АСОИ относится:
1. игнорирование организационных ограничений при работе в системе; 2. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи; 3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных по- мех и т.п.; 4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств; 5. физическое разрушение системы путем взрыва, поджога и т.п.

12. К основным непреднамеренным искусственным угрозам АСОИ относится:
1. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.; 2. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи; 3. вход в систему в обход средств защиты; 4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств; 5. физическое разрушение системы путем взрыва, поджога и т.п.

13. К основным непреднамеренным искусственным угрозам АСОИ относится:
1. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.; 2. некомпетентное использование, настройка или отключение средств защиты; 3. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи; 4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств; 5. физическое разрушение системы путем взрыва, поджога и т.п.

14. К основным непреднамеренным искусственным угрозам АСОИ относится:
1. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.; 2. чтение остаточной информации из

оперативной памяти и с внешних запоминающих устройств; 3. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи; 4. пересылка данных по ошибочному адресу абонента; 5. физическое разрушение системы путем взрыва, поджога и т.п.

15. К основным непреднамеренным искусственным угрозам АСОИ относится:
1. ввод ошибочных данных; 2. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств; 3. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи; 4. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.; 5. физическое разрушение системы путем взрыва, поджога и т.п.

16. К основным непреднамеренным искусственным угрозам АСОИ относится:
1. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи; 2. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств; 3. неумышленное повреждение каналов связи; 4. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.; 5. физическое разрушение системы путем взрыва, поджога и т.п.

17. К основным преднамеренным искусственным угрозам АСОИ относится: 1. неправомерное отключение оборудования или изменение режимов работы устройств и программ; 2. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных кар- точек, пропусков и т.п.); 3. физическое разрушение системы путем взрыва, поджога и т.п.; 4. игнорирование организационных ограничений (установленных правил) при работе в системе; 5. пересылка данных по ошибочному адресу абонента.

18. К основным преднамеренным искусственным угрозам АСОИ относится: 1. отключение или вывод из строя систем электропитания, охлаждения и вентиляции, линий связи и т.п.; 2. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных кар- точек, пропусков и т.п.); 3. неправомерное отключение оборудования или изменение режимов работы устройств и программ; 4. игнорирование организационных ограничений (установленных правил) при работе в системе; 5. пересылка данных по ошибочному адресу абонента.

19. К основным преднамеренным искусственным угрозам АСОИ относится: 1. пересылка данных по ошибочному адресу абонента; 2. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.); 3. неправомерное отключение оборудования или изменение режимов работы устройств и программ; 4. игнорирование организационных ограничений (установленных правил) при работе в системе; 5. действия по дезорганизации функционирования системы (изменение режимов работы, забастовка, саботаж персонала и т.п.).

20. К основным преднамеренным искусственным угрозам АСОИ относится: 1. пересылка данных по ошибочному адресу абонента; 2. внедрение агентов в число персонала системы, в том числе в административную группу, отвечающую за безопасность; 3. неправомерное отключение оборудования или изменение режимов работы устройств и программ; 4. игнорирование организационных ограничений (установленных правил) при работе в системе; 5. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

21. К основным преднамеренным искусственным угрозам АСОИ относится: 1. пересылка данных по ошибочному адресу абонента; 2. игнорирование организационных ограничений (установленных правил) при работе в системе; 3. неправомерное отключение оборудования или изменение режимов работы устройств и программ; 4. вербовка персонала или отдельных пользователей, имеющих необходимые полномочия; 5. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

22. К основным преднамеренным искусственным угрозам АСОИ относится: 1. пересылка данных по ошибочному адресу абонента; 2. игнорирование организационных ограничений (установленных правил) при работе в системе; 3. применение подслушивающих устройств, дистанционная фото- и видеосъемка и т.п.; 4. неправомерное отключение оборудования или изменение режимов работы устройств и программ; 5. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

23. К основным преднамеренным искусственным угрозам АСОИ относится: 1. пересылка данных по ошибочному адресу абонента; 2. игнорирование организационных ограничений (установленных правил) при работе в системе; 3. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи; 4. неправомерное отключение оборудования или изменение режимов работы устройств и программ; 5. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

24. К основным преднамеренным искусственным угрозам АСОИ относится: 1. перехват данных, передаваемых по каналам связи; 2. игнорирование организационных ограничений (установленных правил) при работе в системе; 3. пересылка данных по ошибочному адресу абонента; 4. неправомерное отключение оборудования или изменение режимов работы устройств и программ; 5. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

25. К основным преднамеренным искусственным угрозам АСОИ относится: 1. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.); 2. игнорирование организационных ограничений (установленных правил) при работе в системе; 3. пересылка данных по ошибочному адресу абонента; 4. неправомерное отключение оборудования или изменение режимов работы устройств и программ; 5. хищение носителей информации.

26. К основным преднамеренным искусственным угрозам АСОИ относится: 1. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.); 2. игнорирование организационных ограничений (установленных правил) при работе в системе; 3. несанкционированное копирование носителей информации; 4. неправомерное отключение оборудования или изменение режимов работы устройств и программ; 5. пересылка данных по ошибочному адресу абонента.

27. К основным преднамеренным искусственным угрозам АСОИ относится: 1. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных кар- точек, пропусков и т.п.); 2. хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.); 3. игнорирование организационных ограничений (установленных правил) при работе в

системе; 4. неправомерное отключение оборудования или изменение режимов работы устройств и программ; 5. пересылка данных по ошибочному адресу абонента.

28. К основным преднамеренным искусственным угрозам АСОИ относится: 1. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств; 2. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.); 3. игнорирование организационных ограничений (установленных правил) при работе в системе; 4. неправомерное отключение оборудования или изменение режимов работы устройств и программ; 5. пересылка данных по ошибочному адресу абонента.

29. К основным преднамеренным искусственным угрозам АСОИ относится: 1. неправомерное отключение оборудования или изменение режимов работы устройств и программ; 2. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.); 3. игнорирование организационных ограничений (установленных правил) при работе в системе; 4. незаконное получение паролей и других реквизитов разграничения доступа; 5. пересылка данных по ошибочному адресу абонента.

30. К основным преднамеренным искусственным угрозам АСОИ относится: 1. неправомерное отключение оборудования или изменение режимов работы устройств и программ; 2. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.); 3. игнорирование организационных ограничений (установленных правил) при работе в системе; 4. пересылка данных по ошибочному адресу абонента; 5. несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики.

31. К основным преднамеренным искусственным угрозам АСОИ относится: 1. неправомерное отключение оборудования или изменение режимов работы устройств и программ; 2. вскрытие шифров криптозащиты информации; 3. игнорирование организационных ограничений (установленных правил) при работе в системе; 4. пересылка данных по ошибочному адресу абонента; 5. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

32. К основным преднамеренным искусственным угрозам АСОИ относится: 1. неправомерное отключение оборудования или изменение режимов работы устройств и программ; 2. пересылка данных по ошибочному адресу абонента; 3. игнорирование организационных ограничений (установленных правил) при работе в системе; 4. внедрение аппаратных спецвложений, программных «закладок» и «вирусов»; 5. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных кар- точек, пропусков и т.п.).

33. К основным преднамеренным искусственным угрозам АСОИ относится: 1. неправомерное отключение оборудования или изменение режимов работы устройств и программ; 2. незаконное подключение к линиям связи с целью работы «между строк»; 3. игнорирование организационных ограничений (установленных правил) при работе в системе; 4. пересылка данных по ошибочному адресу абонента; 5. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

34. К основным преднамеренным искусственным угрозам АСОИ относится: 1. неправомерное отключение оборудования или изменение режимов работы устройств и программ; 2. игнорирование организационных ограничений (установленных правил) при работе в системе; 3. незаконное подключение к линиям связи с целью подмены законного пользователя путем его отключения после входа в систему; 4. пересылка данных по ошибочному адресу абонента; 5. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

35. К внутренним нарушителям информационной безопасности относятся:
1. клиенты; 2. пользователи системы; 3. посетители; 4. любые лица, находящиеся внутри контролируемой территории; 5. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации.

36. К внутренним нарушителям информационной безопасности относятся:
1. клиенты; 2. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации; 3. посетители; 4. любые лица, находящиеся внутри контролируемой территории; 5. персонал, обслуживающий технические средства.

37. К внутренним нарушителям информационной безопасности относятся:
1. сотрудники отделов разработки и сопровождения ПО; 2. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации; 3. посетители; 4. любые лица, находящиеся внутри контролируемой территории; 5. клиенты.

38. К внутренним нарушителям информационной безопасности относятся:
1. посетители; 2. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации; 3. технический персонал, обслуживающий здание; 4. любые лица, находящиеся внутри контролируемой территории; 5. клиенты.

39. К внутренним нарушителям информационной безопасности относятся:
1. посетители; 2. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации; 3. любые лица, находящиеся внутри контролируемой территории; 4. сотрудники службы безопасности; 5. клиенты.

40. К внутренним нарушителям информационной безопасности относятся:
1. посетители; 2. руководители различных уровней; 3. любые лица, находящиеся внутри контролируемой территории; 4. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации; 5. клиенты.

41. К посторонним нарушителям информационной безопасности относятся: 1. пользователи; 2. персонал, обслуживающий технические средства; 3. клиенты; 4. технический персонал, обслуживающий здание; 5. сотрудники службы безопасности.

42. К посторонним нарушителям информационной безопасности относятся: 1. пользователи; 2. персонал, обслуживающий технические средства; 3. технический персонал, обслуживающий здание; 4. посетители; 5. сотрудники службы безопасности.

43. К посторонним нарушителям информационной безопасности относятся: 1. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации; 2. персонал, обслуживающий технические средства; 3. технический персонал, обслуживающий здание; 4. пользователи; 5. сотрудники службы безопасности.

44. К посторонним нарушителям информационной безопасности относятся: 1. сотрудники службы безопасности; 2. персонал, обслуживающий технические средства; 3. технический персонал, обслуживающий здание; 4. пользователи; 5. представители конкурирующих организаций.

45. К посторонним нарушителям информационной безопасности относятся: 1. сотрудники службы безопасности; 2. лица, нарушившие пропускной режим; 3. технический персонал, обслуживающий здание; 4. пользователи; 5. персонал, обслуживающий технические средства.

46. По характеру воздействия удаленные атаки делятся:
1. на условные и безусловные; 2. на атаки с обратной связью и без обратной связи; 3. на внутрисегментные и межсегментные; 4. на пассивные и активные; 5. на атаки, которые могут реализовываться на всех семи уровнях – физическом, канальном, сетевом, транспортном, сеансовом, представительном и прикладном.

47. По цели воздействия удаленные атаки делятся:
1. на условные и безусловные; 2. на атаки с обратной связью и без обратной связи; 3. на внутрисегментные и межсегментные; 4. на пассивные и активные; 5. на атаки в зависимости от нарушения конфиденциальности, целостности и доступности.

48. По условию начала осуществления воздействия удаленные атаки делятся: 1. на условные и безусловные; 2. на атаки с обратной связью и без обратной связи; 3. на внутрисегментные и межсегментные; 4. на пассивные и активные; 5. на атаки в зависимости от нарушения конфиденциальности, целостности и доступности.

49. По наличию обратной связи с атакуемым объектом удаленные атаки делятся:
1. на условные и безусловные; 2. на атаки с обратной связью и без обратной связи; 3. на внутрисегментные и межсегментные; 4. на пассивные и активные; 5. на атаки в зависимости от нарушения конфиденциальности, целостности и доступности.

50. По расположению субъекта атаки относительно атакуемого объекта удаленные атаки делятся:
1. на условные и безусловные; 2. на атаки с обратной связью и без обратной связи; 3. на внутрисегментные и межсегментные; 4. на пассивные и активные; 5. на атаки в зависимости от нарушения конфиденциальности, целостности и доступности.

51. По уровню эталонной модели взаимосвязи открытых систем OSI Международной организации стандартизации (ISO) удаленные атаки делятся:
1. на условные и безусловные; 2. на атаки с обратной связью и без обратной связи; 3. на внутрисегментные и межсегментные; 4. на пассивные и активные; 5. на атаки, которые могут реализовываться на всех семи уровнях.

52. Атака, которая позволяет изучить логику работы сети:
1. подмена доверенного объекта или субъекта распределенной вычислительной сети; 2. ложный объект распределенной вычислительной сети; 3. анализ сетевого трафика; 4. отказ в обслуживании; 5. удаленный контроль над станцией в сети.

53. Атака, позволяющая перехватить поток передаваемых данных, которыми обмениваются компоненты сетевой ОС:

1. подмена доверенного объекта или субъекта распределенной вычислительной сети; 2. ложный объект распределенной вычислительной сети; 3. анализ сетевого трафика; 4. отказ в обслуживании; 5. удаленный контроль над станцией в сети.

54. Атака, эффективно реализующаяся в системах, где применяются нестойкие алгоритмы идентификации/аутентификации хостов, пользователей:
1. подмена доверенного объекта или субъекта распределенной вычислительной сети; 2. ложный объект распределенной вычислительной сети; 3. анализ сетевого трафика; 4. отказ в обслуживании; 5. удаленный контроль над станцией в сети.

55. Атака, которая заключается в навязывании ложного маршрута из-за недостатков в алгоритмах маршрутизации:
1. подмена доверенного объекта или субъекта распределенной вычислительной сети; 2. ложный объект распределенной вычислительной сети; 3. анализ сетевого трафика; 4. отказ в обслуживании; 5. удаленный контроль над станцией в сети.

56. Атака, которая использует недостатки алгоритмов удаленного поиска (SAP(NetWare), и DNS (Internet)…):
1. подмена доверенного объекта или субъекта распределенной вычислительной сети; 2. ложный объект распределенной вычислительной сети; 3. анализ сетевого трафика; 4. отказ в обслуживании; 5. удаленный контроль над станцией в сети.

57. Атака, которая позволяет воздействовать на перехваченную информацию (проводить селекцию потока информации):
1. подмена доверенного объекта или субъекта распределенной вычислительной сети; 2. ложный объект распределенной вычислительной сети; 3. анализ сетевого трафика; 4. отказ в обслуживании; 5. удаленный контроль над станцией в сети.

58. Атака, которая позволяет воздействовать на перехваченную информацию (модифицировать информацию):
1. подмена доверенного объекта или субъекта распределенной вычислительной сети; 2. ложный объект распределенной вычислительной сети; 3. анализ сетевого трафика; 4. отказ в обслуживании; 5. удаленный контроль над станцией в сети.

59. Атака, которая позволяет воздействовать на перехваченную информацию (подменять информацию):
1. подмена доверенного объекта или субъекта распределенной вычислительной сети; 2. ложный объект распределенной вычислительной сети; 3. анализ сетевого трафика; 4. отказ в обслуживании; 5. удаленный контроль над станцией в сети.

60. Атака, результатом осуществления которой может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа на атакуемый хост:
1. подмена доверенного объекта или субъекта распределенной вычислительной сети; 2. ложный объект распределенной вычислительной сети; 3. анализ сетевого трафика; 4. отказ в обслуживании; 5. удаленный контроль над станцией в сети.

61. Атака, которая может быть предпринята, если нет средств аутентификации адреса отправителя и с хоста на атакуемый хост можно передавать бесконечное число анонимных запросов на подключение от имени других хостов:
1. подмена доверенного объекта или субъекта распределенной вычислительной сети; 2. ложный объект распределенной вычислительной сети; 3. анализ сетевого трафика; 4. отказ в обслуживании; 5. удаленный контроль над станцией в сети.

62. Атака, которая заключается в передаче с одного адреса такого количества запросов на подключение к атакуемому хосту, ка- кое максимально может «вместить» трафик:
1. подмена доверенного объекта или субъекта распределенной вычислительной сети; 2. ложный объект распределенной вычислительной сети; 3. анализ сетевого трафика; 4. отказ в обслуживании; 5. удаленный контроль над станцией в сети.

63. Атака, которая заключается в запуске на атакуемом компьютере программы «сетевого шпиона»:
1. подмена доверенного объекта или субъекта распределенной вычислительной сети; 2. ложный объект распределенной вычислительной сети; 3. анализ сетевого трафика; 4. отказ в обслуживании; 5. удаленный контроль над станцией в сети.

64. Атака, которая заключается в запуске на атакуемом компьютере программы «сетевого шпиона»: 1. подмена доверенного объекта или субъекта распределенной вычислительной сети; 2. ложный объект распределенной вычислительной сети; 3. анализ сетевого трафика; 4. отказ в обслуживании; 5. удаленный контроль над станцией в сети.

Тест по теме 3

1. По среде обитания классические вирусы разделяются:
1. на паразитические; 2. на компаньоны; 3. на файловые; 4. на ссылки; 5. на перезаписывающие.

2. По среде обитания классические вирусы разделяются:
1. на загрузочные; 2. на компаньоны; 3. на паразитические; 4. на ссылки; 5. на перезаписывающие.

3. По среде обитания классические вирусы разделяются:
1. на ссылки; 2. на компаньоны; 3. на паразитические; 4. на макровирусы; 5. на перезаписывающие.

4. По среде обитания классические вирусы разделяются:
1. на ссылки; 2. на компаньоны; 3. на скриптовые; 4. на паразитические; 5. на перезаписывающие.

5. По способу заражения классические вирусы разделяются:
1. на файловые; 2. на загрузочные; 3. на макровирусы; 4. на скриптовые; 5. на перезаписывающие.

6. По способу заражения классические вирусы разделяются:
1. на файловые; 2. на паразитические; 3. на макровирусы; 4. на скриптовые; 5. на загрузочные.

7. По способу заражения классические вирусы разделяются:
1. на компаньоны; 2. на файловые; 3. на макровирусы; 4. на скриптовые; 5. на загрузочные.

8. По способу заражения классические вирусы разделяются:
1. на скриптовые; 2. на файловые; 3. на макровирусы; 4. на ссылки; 5. на загрузочные.

9. Сетевой червь отсылает либо свою копию в виде вложения в электронное письмо, либо ссылку на свой файл, расположенный на каком-либо сетевом ресурсе:
1. IM-Worm; 2. IRC-Worm; 3. Net-Worm; 4. P2P-Worm; 5. Email-Worm.

10. Сетевые черви используют способ распространения – рассылку на обнаруженные контакты (из контакт-листа) сообщений, содержащих URL, на файл, расположенный на каком-либо веб- сервере:
1. IM-Worm; 2. IRC-Worm; 3. Net-Worm; 4. P2P-Worm; 5. Email-Worm.

11. Сетевые черви распространяются двумя способами по IRC- каналам. Первый заключается в отсылке URL-ссылки на копию червя. Второй способ – отсылка зараженного файла какому-либо пользователю сети. При этом атакуемый пользователь должен подтвердить прием файла, затем сохранить его на диск и открыть:
1. IM-Worm; 2. IRC-Worm; 3. Net-Worm; 4. P2P-Worm; 5. Email-Worm.

12. Сетевой червь ищет удаленные компьютеры и копирует себя в каталоги, открытые на чтение и запись, при этом червь или перебирает доступные сетевые каталоги, используя функции операционной системы, и/или случайным образом ищет компьютеры в глобальной сети, подключается к ним и пытается открыть их диски на полный доступ:
1. IM-Worm; 2. IRC-Worm; 3. Net-Worm; 4. P2P-Worm; 5. Email-Worm.

13. Сетевые черви ищут в сети компьютеры, на которых используется программное обеспечение, содержащее уязвимости. Для заражения уязвимых компьютеров червь посылает специально оформленный сетевой пакет или запрос, в результате чего код червя проникает на компьютер-жертву:
1. IM-Worm; 2. IRC-Worm; 3. Net-Worm; 4. P2P-Worm; 5. Email-Worm.

14. Для внедрения в сеть сетевому червю достаточно скопировать себя в каталог обмена файлами, который обычно расположен на локальном компьютере. Всю остальную работу по распространению вируса сеть берет на себя – при поиске файлов в сети она сообщит удаленным пользователям о данном файле и предоставит весь необходимый сервис для скачивания файла с зараженного компьютера:
1. IM-Worm; 2. IRC-Worm; 3. Net-Worm; 4. P2P-Worm; 5. Email-Worm.

15. Сетевой червь имитирует сетевой протокол конкретной файлообменной системы и на поисковые запросы отвечает положительно – при этом червь предлагает для скачивания свою копию:
1. IM-Worm; 2. IRC-Worm; 3. Net-Worm; 4. P2P-Worm; 5. Email-Worm.

16. Троянские утилиты удаленного администрирования:
1. Trojan-PSW; 2. Trojan-Clicker; 3. Backdoor; 4. Trojan-Downloader; 5. Trojan-Dropper.

17. Троянские программы для воровства паролей:
1. Trojan-PSW; 2. Trojan-Clicker; 3. Trojan-Proxy; 4. Trojan-Downloader; 5. Trojan-Dropper.

18. Троянские программы для доставки вредоносных программ:
1. Trojan-PSW; 2. Trojan-Clicker; 3. Trojan-Proxy; 4. Trojan-Downloader; 5. Trojan-Dropper.

19. Троянские программы инсталляторы вредоносных программ:
1. Trojan-PSW; 2. Trojan-Clicker; 3. Trojan-Proxy; 4. Trojan-Downloader; 5. Trojan-Dropper.

20. Троянские шпионские программы:
1. Trojan-PSW; 2. Trojan-Spy; 3. Trojan-Proxy; 4. Trojan-Downloader; 5. Trojan-Dropper.

21. Троянские программы, применяемые для организации несанкционированных обращений к Интернет-ресурсам:
1. Trojan-PSW; 2. Trojan-Spy; 3. Trojan-Clicker; 4. Trojan-Downloader; 5. Trojan-Dropper.

22. Троянские программы, скрытно осуществляющие анонимный доступ к различным Интернет-ресурсам, обычно используются для рассылки спама:
1. Trojan-PSW; 2. Trojan-Spy; 3. Trojan-Proxy; 4. Trojan-Downloader; 5. Trojan-Dropper.

23. Троянские программы, предназначенные для оповещение об успешной атаке:
1. Trojan-PSW; 2. Trojan-Spy; 3. Trojan-Proxy; 4. Trojan-Notifier; 5. Trojan-Dropper.

24. Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:
1. черный пиар; 2. фишинг; 3. нигерийские письма; 4. источник слухов; 5. пустые письма.

25. Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п:
1. черный пиар; 2. фишинг; 3. нигерийские письма; 4. источник слухов; 5. пустые письма.

26. Спам, написанный от имени реальных или вымышленных лиц, обычно граждан стран с нестабильной экономической ситуацией, воспринимаемых публикой как рассадник коррупции:
1. черный пиар; 2. фишинг; 3. нигерийские письма; 4. источник слухов; 5. пустые письма.

27. Спам инициирует письма, содержащие сведения о потенциальной опасности или просьбы о помощи жертвам стихийных бедствий:
1. черный пиар; 2. фишинг; 3. нигерийские письма; 4. источник слухов; 5. пустые письма.

28. Спам периодически проводит рассылки нерекламных сообщений:
1. черный пиар; 2. фишинг; 3. нигерийские письма; 4. источник слухов; 5. пустые письма.

Тест по теме 4
1. Антивирус просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок:
1. детектор; 2. доктор; 3. сканер; 4. ревизор; 5. сторож.

2. Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы:
1. детектор; 2. доктор; 3. сканер; 4. ревизор; 5. сторож.

3. Антивирус не только находит зараженные вирусами файлы, но и «лечит» их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние:
1. детектор; 2. доктор; 3. сканер; 4. ревизор; 5. сторож.

4. Антивирус запоминает исходное состояние программ, каталогов и системных областей диска, когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным:
1. детектор; 2. доктор; 3. сканер; 4. ревизор; 5. сторож.

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

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

6. Антивирус модифицирует программу или диск таким образом, чтобы вирус воспринимал их зараженными и поэтому не внедрялся:
1. детектор; 2. доктор; 3. сканер; 4. ревизор; 5. иммунизатор.

7. Антивирусный сканер:
1. обеспечивает поиск вирусов путем подсчета и сравнения с эталоном контрольной суммы;
2. находит зараженные вирусами файлы, «лечит» их, т.е. удаляет из файла тело вируса, возвращая файлы в исходное состояние; 3. запоминает исходное состояние, когда компьютер не заражен вирусом, затем периодически сравнивает текущее состояние с исходным; 4. просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок; 5. обнаруживает подозрительные действия при работе компьютера, характерные для вирусов.

8. Антивирусный детектор:
1. обеспечивает поиск вирусов путем подсчета и сравнения с эталоном контрольной суммы;
2. находит зараженные вирусами файлы, «лечит» их, т.е. удаляет из файла тело вируса, возвращая файлы в исходное состояние; 3. запоминает исходное состояние, когда компьютер не заражен вирусом, затем периодически сравнивает текущее состояние с исходным; 4. просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок; 5. обнаруживает подозрительные действия при работе компьютера, характерные для вирусов.

9. Антивирусный доктор:
1. обеспечивает поиск вирусов путем подсчета и сравнения с эталоном контрольной суммы;
2. находит зараженные вирусами файлы и удаляет из файла тело вируса, возвращая файлы в исходное состояние; 3. запоминает исходное состояние, когда компьютер не заражен вирусом, затем периодически сравнивает текущее состояние с исходным; 4. просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок; 5. обнаруживает подозрительные действия при работе компьютера, характерные для вирусов.

10. Антивирусный ревизор:
1. обеспечивает поиск вирусов путем подсчета и сравнения с эталоном контрольной суммы;
2. находит зараженные вирусами файлы и удаляет из файла тело вируса, возвращая файлы в исходное состояние; 3. запоминает исходное состояние, когда компьютер не заражен вирусом, затем периодически сравнивает текущее состояние с исходным; 4. просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок; 5. обнаруживает подозрительные действия при работе компьютера, характерные для вирусов.

11. Антивирусный сторож:
1. обеспечивает поиск вирусов путем подсчета и сравнения с эталоном контрольной суммы;
2. находит зараженные вирусами файлы и удаляет из файла тело вируса, возвращая файлы в исходное состояние; 3. запоминает исходное состояние, когда компьютер не заражен вирусом, затем периодически сравнивает текущее состояние с исходным;
4. просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок; 5. обнаруживает подозрительные действия при работе компьютера, характерные для вирусов.

12. Антивирусный иммунизатор:

1. обеспечивает поиск вирусов путем подсчета и сравнения с эталоном контрольной суммы;
2. находит зараженные вирусами файлы и удаляет из файла тело вируса, возвращая файлы в исходное состояние; 3. модифицирует программу или диск таким образом, чтобы вирус воспринимал их зараженными и поэтому не внедрялся; 4. просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок; 5. обнаруживает подозрительные действия при работе компьютера, характерные для вирусов.

Тест по теме 5

1. Метод защиты информации ограничение доступа заключается:
1. в контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления; 2. в создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями; 3. в разделении информации на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями; 4. в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одно- временном предъявлении полномочий всех членов группы; 5. в проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

2. Метод защиты информации контроль доступа к аппаратуре заключается:
1. в контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления; 2. в создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями; 3. в разделении информации на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями; 4. в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одно- временном предъявлении полномочий всех членов группы; 5. в проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

3. Метод защиты информации разграничение и контроль доступа к информации заключается:
1. в контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления; 2. в создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями; 3. в разделении информации на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями; 4. в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одно- временном предъявлении полномочий всех членов группы; 5. в проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

4. Метод защиты информации предоставление привилегий на доступ заключается:
1. в контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления; 2. в создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями; 3. в разделении информации на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;
4. в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одно- временном предъявлении полномочий всех членов группы; 5. в проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

5. Метод защиты информации идентификация и установление подлинности заключается:

1. в контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления; 2. в создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями; 3. в разделении информации на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями; 4. в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы; 5. в проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

Тест по теме 6

1. Шифрование методом подстановки:
1. символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста; 2. символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности; 3. шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор; 4. символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов; 5. замена слов и предложений исходной информации шифрованными.

2. Шифрование методом перестановки:
1. символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста; 2. символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности; 3. шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор; 4. символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов; 5. замена слов и предложений исходной информации шифрованными.

3. Шифрование методом гаммирования:
1. символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста; 2. символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности; 3. шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор; 4. символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов; 5. замена слов и предложений исходной информации шифрованными.

4. Шифрование методом аналитических преобразований:
1. символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста; 2. символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности; 3. шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор; 4. символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов; 5. замена слов и предложений исходной информации шифрованными.

5. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод:
1. гаммирования; 2. подстановки; 3. кодирования; 4. перестановки; 5. аналитических преобразований.

6. Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов, это метод:
1. гаммирования; 2. подстановки; 3. кодирования; 4. перестановки; 5. аналитических преобразований.

7. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:
1. гаммирования; 2. подстановки; 3. кодирования; 4. перестановки; 5. аналитических преобразований.

8. Шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор, это метод:
1. гаммирования; 2. подстановки; 3. кодирования; 4. перестановки; 5. аналитических преобразований.

9. Шифр DES – это:
1. система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки; 2. система с открытым ключом, предназначенная как для шифрования, так и для аутентификации, основана на трудности разложения очень больших целых чисел на простые сомножители; 3. блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны; 4. шифр, состоящий из 64-битных повторяющихся блоков с 128- битным ключом и восемью проходами; 5. симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16-кратной перестановке данных, для зашифровывания использует ключ в 56 бит.

10. Шифр IDEA – это:
1. система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки; 2. система с открытым ключом, предназначенная как для шифрования, так и для аутентификации, основана на трудности разложения очень больших целых чисел на простые сомножители; 3. блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны; 4. шифр, состоящий из 64-битных повторяющихся блоков с 128- битным ключом и восемью проходами; 5. симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16-кратной перестановке данных, для зашифровывания использует ключ в 56 бит.

11. Шифр RC2 или RC4 – это:
1. система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки; 2. система с открытым ключом, предназначенная как для шифрования, так и для аутентификации, основана на трудности разложения очень больших целых чисел на простые сомножители; 3. блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны; 4. шифр, состоящий из 64-битных повторяющихся блоков с 128- битным ключом и восемью проходами; 5. симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16-кратной перестановке данных, для зашифровывания использует ключ в 56 бит.

12. Шифр RSA – это:
1. система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки; 2. система с открытым ключом, предназначенная как для шифрования, так и для аутентификации,

основана на трудности разложения очень больших целых чисел на простые сомножители; 3. блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны; 4. шифр, состоящий из 64-битных повторяющихся блоков с 128- битным ключом и восемью проходами; 5. симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16-кратной перестановке данных, для зашифровывания использует ключ в 56 бит.

13. Шифр ГОСТ 28147-89 – это:
1. система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки; 2. система с открытым ключом, предназначенная как для шифрования, так и для аутентификации, основана на трудности разложения очень больших целых чисел на простые сомножители; 3. блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны; 4. шифр, состоящий из 64-битных повторяющихся блоков с 128- битным ключом и восемью проходами; 5. симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16-кратной перестановке данных, для зашифровывания использует ключ в 56 бит.

14. Система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки, – это шифр:
1. IDEA; 2. RSA; 3. ГОСТ 28147-89; 4. RC2 или RC4; 5. DES.

15. Система с открытым ключом, предназначенная как для шифрования, так и для аутентификации, основана на трудности разложения очень больших целых чисел на простые сомножители – это шифр:
1. IDEA; 2. RSA; 3. ГОСТ 28147-89; 4. RC2 или RC4; 5. DES.

16. Блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны – это шифр:
1. IDEA; 2. RSA; 3. ГОСТ 28147-89; 4. RC2 или RC4; 5. DES.

17. Шифр, состоящий из 64-битных повторяющихся блоков с 128- битным ключом и восемью проходами, – это шифр:
1. IDEA; 2. RSA; 3. ГОСТ 28147-89; 4. RC2 или RC4; 5. DES.

18. Симметричный алгоритм шифрования имеет блоки по 64 бит и основан на 16 кратной перестановке данных, для зашифровывания использует ключ в 56 бит – это шифр:
1. IDEA; 2. RSA; 3. ГОСТ 28147-89; 4. RC2 или RC4; 5. DES.

Тест по теме 7

1. Сертификации подлежат:
1. средства криптографической защиты информации; 2. средства выявления закладных устройств и программных закладок; 3. защищенные технические средства обработки информации; 4. защищенные информационные системы и комплексы телекоммуникаций; 5. все вышеперечисленные средства.

2. В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Стратегия:
1. индивидуальные субъекты должны идентифицироваться; 2. контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность; 3.

необходимо иметь явную и хорошо определенную систему обеспечения безопасности; 4. вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований; 5. гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений.

3. В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Стратегия:
1. управляющие доступом метки должны быть связаны с объектами; 2. контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность; 3. индивидуальные субъекты должны идентифицироваться; 4. вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований; 5. гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений.

4. В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Подотчетность:
1. управляющие доступом метки должны быть связаны с объектами; 2. необходимо иметь явную и хорошо определенную систему обеспечения безопасности; 3. индивидуальные субъекты должны идентифицироваться; 4. вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований; 5. гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений.

5. В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Подотчетность:
1. управляющие доступом метки должны быть связаны с объектами; 2. необходимо иметь явную и хорошо определенную систему обеспечения безопасности; 3. гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений;
4. вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований; 5. контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность.

6. В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Гарантии:
1. управляющие доступом метки должны быть связаны с объектами; 2. необходимо иметь явную и хорошо определенную систему обеспечения безопасности; 3. индивидуальные субъекты должны идентифицироваться; 4. вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований; 5. контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность.

7. В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Гарантии:
1. управляющие доступом метки должны быть связаны с объектами; 2. защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений; 3. индивидуальные субъекты должны идентифицироваться; 4. необходимо иметь явную и хорошо определенную систему обеспечения безопасности; 5. контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность.

8. В стандарте США «Оранжевой книге» минимальная защита – это группа:
1. A; 2. B; 3. C; 4. D; 5. E.

9. В стандарте США «Оранжевой книге» индивидуальная защита – это группа:
1. A; 2. B; 3. C; 4. D; 5. E.

10. В стандарте США «Оранжевой книге» мандатная защита – это группа:
1. A; 2. B; 3. C; 4. D; 5. E.

11. В стандарте США «Оранжевой книге» верифицированная защита – это группа:
1. A; 2. B; 3. C; 4. D; 5. E.

12. В стандарте США «Оранжевой книге» системы, подвергнутые оцениванию, но не отвечающие требованиям более высоких классов, – это группа:
1. A; 2. B; 3. C; 4. D; 5. E.

13. В стандарте США «Оранжевой книге» системы, обеспечивающие разделение пользователей и данных, – это группа:
1. A1; 2. B1; 3. B2; 4. C1; 5. C2.

14. В стандарте США «Оранжевой книге» системы, осуществляющие не только разделение пользователей, но и разделение их по осуществляемым действиям, – это группа:
1. A1; 2. B1; 3. B2; 4. C1; 5. C2.

15. В стандарте США «Оранжевой книге» системы, дополнительно должны быть формальные модели механизмов обеспечения безопасности, присваивания имен защищаемым данным и средства мандатного управления доступом ко всем поименованным субъектам и объектам, группа:
1. A1; 2. B1; 3. B2; 4. C1; 5. C2.

16. В стандарте США «Оранжевой книге» системы, дополнительно должны быть формальные модели механизмов обеспечения безопасности, присваивания имен защищаемым данным и средства мандатного управления доступом ко всем поименованным субъектам и объектам, – это группа:
1. A1; 2. B1; 3. B2; 4. C1; 5. C2.

17. В стандарте США «Оранжевой книге» системы, построенные на основе ясно определенной формально задокументированной модели, с мандатным управлением доступом ко всем субъектам и объектам, располагающие усиленными средствами тестирования и средствами управления со стороны администратора системы, – это группа:
1. A1; 2. B1; 3. B2; 4. C1; 5. C2.

18. В стандарте США «Оранжевой книге» системы, монитор обращений которых контролирует все запросы на доступ субъектов к объектам, не допускающие несанкционированных изменений, – это группа:
1. A1; 2. B1; 3. B2; 4. B3; 5. C1.

19. В стандарте США «Оранжевой книге» управление системой осуществляется по строго определенным процедурам, обязательно введение должности администратора безопасности, – это группа:
1. A1; 2. B1; 3. B2; 4. C1; 5. C2.

20. В руководящем документе Гостехкомиссии системы, в которых работает один пользователь, допущенный ко всей обрабатываемой информации, размещенной на носителях одного уровня конфиденциальности, – относятся к группе:
1. первой; 2. второй; 3. третьей; 4. четвертой; 5. пятой.

21. В руководящем документе Гостехкомиссии системы, в которых работает несколько пользователей, которые имеют одинаковые права доступа ко всей информации, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности, – относятся к группе:
1. первой; 2. второй; 3. третьей; 4. четвертой; 5. пятой.

22. В руководящем документе Гостехкомиссии многопользовательские системы, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности, причем различные пользователи имеют различные права на доступ к информации, – относятся к группе:
1. первой; 2. второй; 3. третьей; 4. четвертой; 5. пятой.

Образцы заданий на лабораторную работу (ЛР) для проведения текущего контроля знаний по дисциплине «Основы теории и практики защиты информации» по темам 4, 5, 6:

ЛР по теме 4
«Профилактика компьютерных систем от заражения вирусами»

1. **Цель работы: анализ и исследование антивирусных программ.**
2. Порядок выполнения работы:

1) Используя пакет программ, демонстрирующих действие вирусов, изучите действие вирусов различного типа. Поочередно запуская программы из пакета демонстрационных программ, изучите проявление вирусного заражения. По окончании наблюдения перезагрузить компьютер.

2) Запустите программу DrWeb и выполните проверку оперативной памяти компьютера на наличие вирусов. Выполните тестирование дисков A и C на наличие вирусов. Если на дисках будут обнаружены вирусы, выполните лечение зараженных файлов.

3) Загрузите из Интернета и установите на компьютере ознакомительную версию ADinf32. Задайте расписание работы ADinf, чтобы ее активизация осуществлялась еженедельно по субботам с 18.00.

4) Загрузите из Интернета и установите на компьютере ознакомительную версию антивируса Kaspersky Anti-Virus. Создайте новую задачу сканирования дисков компьютера на вирусы.

5) Загрузите из Интернета и установите на компьютере ознакомительную версию антивируса Norton AntiVirus. Выполните обновление антивирусной базы и

проверьте компьютер на наличие вирусов.

6) Посетите web-страницу http://www.sarc.eom//avcenter/vinfodb. html онлайн-экспедиции вирусов на сайте компания Symantec. На этой странице можно просмотреть, чем заражен тот или иной файл и как удалить этот вирус.

ЛР по теме 5

«Защита информации с помощью пароля»

1. Цель работы: исследование защиты с применением пароля, а также исследование методов противодействия атакам на пароль.

2. Порядок выполнения работы:

1) Проведение атаки перебором (bruteforce attack)

a) Используя программу для вскрытия паролей произвести атаку на зашифрованный файл try_me.rar (try_me.arj, try_me.zip – в зависимости от варианта). Область перебора – все печатаемые символы, длина пароля от 1 до 4 символов. Время выполнения на компьютере класса Pentium примерно 3-4 минуты. На компьютере класса Pentium II – 50 секунд. Проверить правильность определенного пароля, распаковав файл и ознакомившись с его содержимым.

b) Выполнив пункт a), сократить область перебора до фактически используемого (например, если пароль 6D1A, то выбрать прописные английские буквы и цифры). Провести повторное вскрытие. Сравнить затраченное время.

2) Проведение атаки по словарю (dictionary attack)

a) Сжать какой-либо небольшой файл, выбрав в качестве пароля английское слово длиной до 5 символов (например love, god, table, admin и т.д.). Провести атаку по словарю. Для этого выбрать вид атаки и в закладке Словарь выбрать файл English.dic. Он содержит набор английских слов и наборы символов, наиболее часто использующиеся в качестве паролей.

b) Попытаться определить пароль методом прямого перебора. Сравнить затраченное время.

ЛР по теме 5

«Исследование средств безопасности операционных систем»

1. Цель работы: исследование и анализ служебных программ Windows.

2. Порядок выполнения работы:

1) Используя программу Сведения о системе, определите следующие параметры компьютерной системы: сведения об имеющихся на компьютере портах, звуковом устройстве, о системных драйверах и автоматически загружаемых программах.

2) Используя стандартную программу Windows Проверка диска, проверьте диск A: на наличие поврежденных секторов и ошибок файловой системы. При этом если будут обнаружены ошибки, то задайте режим восстановления поврежденных секторов диска автоматического исправления системных ошибок.

3) Используя стандартную программу Очистка диска, выполните очистку диска D:.

4) Используя стандартную программу Дефрагментация диска, выполните оценку фрагментированности файлов на диске D: и, если требуется, то выполните дефрагментацию этого диска.

5) Используя служебную программу Архивация данных, архивируйте данные из папки C:\Program Files\Microsoft OfficeVTemplates в архив с именем Templates на диске D:.

6) Используя служебную программу Архивация данных, создайте архив системных файлов и дискету аварийного восстановления, которые могут быть использованы в целях восстановления системы в случае ее отказа.

ЛР по теме 5

«Аутентификация пользователей Web-систем средствами технологии PHP»

1. Цель работы: изучение принципов аутентификации пользователей в Web-системах на примере PHP-сеансов.

2. Порядок выполнения работы:

1) Изучить принципы аутентификации пользователей в Web- системах.
2) Реализовать систему аутентификации с помощью PHP-сеансов.

ЛР по теме 5

«Защита баз данных»

1. Цель работы: изучение способов защиты информации в БД на примере СУБД MS Access.

2. Порядок выполнения работы:

1) Создать новую уникальную рабочую группу.
2) Создать новую учетную запись администратора. Подключится к новой рабочей группе; открыть любую БД; в меню – сервис выбрать защиту и пользователей группы; создать нового пользователя, ввести имя и код учетной записи (это не пароль); в списке имеющейся группы выбрать: Admins – добавить.
3) Удалить из группы администраторов пользователя Admin.
4) Выйти из Access и войти новым пользователем в Access; обязательно ввести пароль на данную учетную запись.
5) Создать заново БД, которую хотим защитить.
6) Выполнить импорт объектов из исходной БД в БД, созданную на предыдущем шаге.
7) Выполнить распределение прав на необходимые объекты.

ЛР по теме 6

«Исследование метода компьютерной стеганографии для защиты информации»

1. Цель работы: исследование метода замены младших бит, используемого в компьютерной стеганографии для защиты информации.

2. Порядок выполнения работы:

1) Исследовать влияние количества заменяемых младших бит для различных составляющих RGB по отдельности и в их комбинации на качество воспроизведения отдельных цветов R, G и B файла-контейнера.
2) Исследовать влияние количества заменяемых младших бит для различных составляющих RGB по отдельности и в их комбинации на качество воспроизведения комбинации цветов R, G и B файла-контейнера.
3) Исследовать влияние количества заменяемых младших бит для различных составляющих RGB по отдельности и в их комбинации на качество воспроизведения различных цветов в многокомпонентной цветовой картине файла-контейнера.
4) На основании результатов, полученных в пп. 1-3, добиться наилучшего качества многоцветной картины файла-контейнера при скрытии в нем информации.

ЛР по теме 6

«Разработка и реализация алгоритма криптографического преобразования»

1. Цель работы: ознакомиться с методами современной криптографии на примере программирования одного из предложенных алгоритмов.

2. Порядок выполнения работы:

1) Представить теоретическую основу алгоритма (волновой метод, RSA, TEA и т.п.)
2) Представить блок-схему выбранного алгоритма.

3) Разработать псевдокод выбранного алгоритма.
4) Представить листинг с комментариями.
5) Провести тестирование программы.
6) Сделать выводы по проделанной работе.

4.2 Фонд оценочных средств для проведения промежуточной аттестации.

По дисциплине «Современная криптография» предусмотрены следующие формы промежуточной аттестации: зачет (З) в В семестре очной формы обучения.

Перечень вопросов для подготовки к зачету по дисциплине «Современная криптография»:

1) Актуальность информационной безопасности.
2) Национальные интересы РФ в информационной сфере и их обеспечение.
3) Классификация компьютерных преступлений.
4) Способы совершения компьютерных преступлений.
5) Пользователи и злоумышленники в Интернет.
6) Причины уязвимости сети Интернет.
7) Виды угроз информационной безопасности РФ.
8) Источники угроз информационной безопасности РФ.
9) Угрозы информационной безопасности для АСОИ.
10) Удаленные атаки на интрасети.
11) Условия существования вредоносных программ.
12) Классические компьютерные вирусы.
13) Сетевые черви.
14) Троянские программы.
15) Спам.
16) Хакерские утилиты и прочие вредоносные программы.
17) Кто и почему создает вредоносные программы.
18) Признаки заражения компьютера.
19) Источники компьютерных вирусов.
20) Основные правила защиты.
21) Антивирусные программы.
22) Методы обеспечения информационной безопасности РФ.
23) Ограничение доступа.
24) Контроль доступа к аппаратуре.
25) Разграничение и контроль доступа к информации.
26) Предоставление привилегий на доступ.
27) Идентификация и установление подлинности объекта (субъекта).
28) Защита информации от утечки за счет побочного электромагнитного излучения и наводок.
29) Методы и средства защиты информации от случайных воздействий.
30) Методы защиты информации от аварийных ситуаций.
31) Организационные мероприятия по защите информации.
32) Организация информационной безопасности компании.
33) Выбор средств информационной безопасности.
34) Информационное страхование.
35) Классификация методов криптографического закрытия информации.
36) Симметричные криптосистемы.
37) Криптосистемы с открытым ключом (асимметричные).
38) Характеристики существующих шифров.
39) Кодирование.

40) Стеганография.
41) Электронная цифровая подпись.
42) Законодательство в области лицензирования и сертификации.
43) Правила функционирования системы лицензирования.
44) Критерии безопасности компьютерных систем. «Оранжевая книга».
45) Руководящие документы Гостехкомиссии.

Тематика практических заданий на зачете:
1) Профилактика компьютерных систем от заражения вирусами.
2) Защита информации с помощью пароля.
3) Исследование средств безопасности операционных систем.
4) Аутентификация пользователей Web-систем средствами технологии PHP.
5) Защита баз данных.
6) Исследование метода компьютерной стеганографии для защиты информации.
7) Разработка и реализация алгоритма криптографического преобразования.

Образец билета для проведения зачета по дисциплине «Современная криптография»:

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Физико-технический факультет
Кафедра теоретической физики и компьютерных технологий
Направление подготовки 09.04.02 Информационные системы и технологии

2017-2018 уч. год

Дисциплина Современная криптография

БИЛЕТ № 1

1. Удаленные атаки на интрасети.
2. Правила функционирования системы лицензирования.
3. Решить задачу защиты информации с помощью пароля.

Заведующий кафедрой_____В.А. Исаев

Зачет по учебной дисциплине имеет целью проверить и оценить уровень знаний, полученных студентами, умение применять их к решению практических задач, а также степень овладения практическими умениями и навыками в объеме требований учебной программы.

Зачет проводится в период зачетной недели согласно расписанию зачетов, утвержденному деканом факультета.

Зачет принимают преподаватели, ведущие занятия или читающие лекции по данной дисциплине.

К зачету допускаются студенты, выполнившие все требования учебной программы по дисциплине.

Заведующий кафедрой по представлению преподавателя может освобождать от сдачи зачета студентов, показавших отличные знания по результатам текущего контроля, с выставлением им оценки «зачтено».

Зачет проводится в устной форме, по зачетным билетам, количество которых должно быть на 10 % больше, чем численность студентов в самой большой учебной группе.

В зачетный билет включаются три вопроса: два теоретических и один практический.

Консультации студентов проводятся преподавателями, ведущими занятия по учебной дисциплине, в период подготовки к зачету в соответствии с расписанием зачетов.

В ходе проведения консультаций студентам даются необходимые пояснения по учебному материалу, указывается учебно-методическая литература для подготовки к зачету, доводятся перечень учебных и наглядных пособий, справочных материалов, которыми разрешено пользоваться при проведении зачета, порядок действий студента на зачете, типовой обобщенный алгоритм ответа студента на вопросы зачетного билета.

В аудитории, где принимается зачет, может находиться одновременно не более четырех студентов из расчета на одного экзаменатора.

На подготовку к ответу на вопросы зачетного билета каждому студенту отводится 0,5 ч.

Знания, умения и навыки обучающихся на зачете определяются оценками «зачтено» и «незачтено».

Знания, умения и навыки обучающихся за ответ на вопрос зачетного билета определяются частными оценками «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно». Оценка студенту за ответ на вопрос билета выставляется в соответствии со следующими требованиями:

«отлично», если студент:

ясно понимает сущность и содержание поставленного в билете вопроса;

ответ строит в соответствии с типовым алгоритмом, материал излагает уверенно, последовательно и логично, производит необходимые доказательства и выводы;

свободно ориентируется в материале при ответе на дополнительные вопросы.

«хорошо», если студент:

понимает сущность и содержание поставленного в билете вопроса;

ответ строит в соответствии с типовым алгоритмом, материал излагает уверенно и последовательно, но недостаточно обосновывает свои выводы или они не отличаются конкретностью;

умеет находить правильные ответы на дополнительные вопросы.

«удовлетворительно», если студент:

в основном понимает сущность и содержание поставленного в билете вопроса;

при ответе не в полной мере придерживается типового алгоритма, материал излагает неуверенно, допускает неточности и терминологические ошибки;

при постановке дополнительных вопросов теряется, правильные ответы находит только после постановки наводящих вопросов.

«неудовлетворительно», если студент:

не понимает сущности поставленного в билете вопроса;

строит ответ неправильно по форме и по существу;

не находит правильных ответов даже при помощи наводящих вопросов;

в других случаях, когда не выполнены условия на оценку «удовлетворительно»;

самостоятельно заявляет о незнании или неподготовленности к ответу по данному вопросу (отказ от ответа).

Дополнительный вопрос может быть задан студенту по теоретическим и практическим вопросам, за которые была получена низшая оценка, в объеме требований учебной программы по дисциплине.

Общая оценка за зачет выводится на основании частных оценок за ответы на вопросы зачетного билета и дополнительные вопросы. При этом рекомендуется пользоваться следующей таблицей:

Общая оценка	Частные оценки за ответы на вопросы				
	Вопросы билета			Дополнительные вопросы	
	1	2	3	1	2
«зачтено»	5	5	5	5	4
	5	5	5	4	5
	5	5	4	5	5
	5	4	5	5	5
	4	5	5	5	5
	5	5	3	5	5
	5	5	5	3	5
	5	5	4	4	4
	5	4	5	4	4
	5	4	4	5	5
	5	4	4	4	4
	5	4	4	3	3
	5	4	3	4	4
	4	5	3	4	4
	4	5	5	3	3
	4	5	5	4	4
	4	5	4	5	5
	4	5	4	4	4
	4	5	4	3	3
	4	5	3	4	4
	4	4	5	5	5
	4	4	5	4	4
	4	4	4	5	5
	4	4	5	3	3
	4	4	3	5	5
	4	4	4	4	4
	4	4	4	3	3
	4	4	3	4	4
	4	3	4	4	4
	3	4	4	4	4
	5	5	3	3	3
	5	4	3	2	3
	5	5	2	3	3
	4	4	3	3	3
	4	4	3	3	2
	4	4	2	3	3
	4	3	3	5	4
	4	3	3	4	3

«зачтено»	4	3	3	3	3
	4	3	3	3	2
	4	3	2	3	3
	3	4	4	3	3
	3	4	3	4	3
	3	4	3	3	3
	3	4	3	3	2
	3	4	2	3	3
	3	3	3	4	3
	3	3	4	3	3
	3	3	3	3	3
	3	3	3	2	3
	3	3	2	3	3
	3	2	3	3	3
	2	3	3	3	3
«незачтено»	при получении двух и более частных оценок «неудовлетворительно» по вопросам билета; при отказе от ответа на два вопроса билета; в случае обнаружения у студента после получения им билета учебных пособий, методических материалов, учебной и иной литературы (за исключением разрешенных для использования), конспектов, независимо от типа носителя информации, а также любых технических средств и средств передачи информации, либо использования им подсказки, вне зависимости от того, были ли использованы указанные материалы и (или) средства при подготовке к ответу				

В случае обнаружения у студента после получения им билета учебных пособий, методических материалов, учебной и иной литературы (за исключением разрешенных для использования при проведении зачета), конспектов, независимо от типа носителя информации, а также любых технических средств и средств передачи информации, либо использования им подсказки, вне зависимости от того, были ли использованы указанные материалы и (или) средства при подготовке к ответу на зачете, указанные материалы изымаются, и выставляется оценка «незачтено».

Частные оценки за ответы на вопросы билета и общая оценка объявляется студенту по окончании им ответа на зачете.

Положительная оценка («зачтено») заносится в зачетную ведомость, зачетную книжку студента и журнал учета учебных занятий.

Оценка «незачтено» проставляется только в зачетную ведомость и журнал учета учебных занятий.

Повторная сдача зачета с целью получения положительной оценки не допускается.

Записи в зачетную ведомость, зачетную книжку и журнал учета учебных занятий делаются черной пастой (чернилами) лично экзаменатором. В зачетной книжке проставляется общее количество часов по данной дисциплине согласно учебному плану.

Типовой обобщенный алгоритм ответа студента на вопросы зачетного билета:

1. Введение.
   1.1. Актуальность и значение.
   1.2. Наименование основных нормативных документов.
   1.3. Место данного элемента (вопроса, задачи, проблемы) в общей системе.
2. Основная часть.
   2.1. Требования нормативных документов.
   2.2. Цели, понятия, определения, термины, формулы, категории, взаимосвязи, закономерности, законы.
   2.3. Назначение, классификация, структура, состав, устройство, работа, задачи, функции, содержание, организация, условия, порядок, действия, нормы, нормативы, показатели, особенности, возможности, идеи.
   2.4. Показ, демонстрация, практика, результаты.
   2.5. Опыт деятельности, примеры.
3. Заключение.
   3.1. Итоги и выводы.
   3.2. Развитие и перспективы.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:
– в печатной форме увеличенным шрифтом,
– в форме электронного документа.
Для лиц с нарушениями слуха:
– в печатной форме,
– в форме электронного документа.
Для лиц с нарушениями опорно-двигательного аппарата:
– в печатной форме,
– в форме электронного документа.

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля).

5.1 Основная литература:

1. Адуева Т.В. Планирование и проектирование организаций / Т.В. Адуева – Томск, 2016. – 73 с. – Режим доступа: URL: http://biblioclub.ru/index.php?page=book&id=480666

2. Белов В.В. Повышение пертинентности поиска в современных информационных средах. / В.В. Белов, А.А. Терехов, В.И. Чистякова –М., 2012. – 158 с. – Режим доступа: URL: http://e.lanbook.com/books/element.php?pl1_id=5118

Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья имеются издания в электронном виде в электронно-библиотечных системах «Лань» и «Юрайт».

5.2 Дополнительная литература:

1) Информационные системы и технологии : научно-технический журнал / ред. сов. В.А. Голенков ; редкол. О.П. Архипов ; гл. ред. И.С. Константинов ; учред. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Государственный университет — учебно-научно-производственный комплекс» (Госуниверситет – УНПК) - Орел : Госуниверситет - УНПК, 2012. - № 5(73). - 152 с.: ил. - ISSN 2072-8964 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=321622

2) Фефилов, А.Д. Методы и средства защиты информации в сетях / А.Д. Фефилов. - Москва : Лаборатория книги, 2011. - 105 с. : ил., табл. - ISBN 978-5-504- 00608-6 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=140796

3) Голиков, А.М. Основы проектирования защищенных телекоммуникационных систем: курс лекций, компьютерный практикум, компьютерные лабораторные работы и задание на самостоятельную работу : учебное пособие / А.М. Голиков ; Министерство образования и науки Российской Федерации. - Томск : ТУСУР, 2016. - 396 с. : ил.,табл., схем. - (Учебная литература для вузов). - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=480796

4) Информационные технологии : учебное пособие / сост. К.А. Катков, И.П. Хвостова, В.И. Лебедев, Е.Н. Косова и др. - Ставрополь : СКФУ, 2014. - Ч. 1. - 254 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=457340

5.3. Периодические издания:

№ п/п	Название издания	Периодичность выхода (в год)	За какие годы хранится	Место хранения	Срок хранения
1.	Инфокоммуникационные технологии	4	2006; 2008-	чз	5 лет
2.	Информатика и образование	6	1992-	чз	пост.
3.	Информатика. Реферативный журнал ВИНИТИ	12	1987-	зал РЖ	пост.
4.	Информационное общество		2006-	чз	5 лет
5.	Информационные ресурсы России	6	2007 с №4-	чз	5 лет
6.	Информационные технологии	12	1996-	чз	пост.
7.	Мир компьютерной автоматизации - Мир встраиваемых компьютерных технологий	4	2006-	чз	5 лет
8.	Мир ПК	12	2006-2009	чз	5 лет
9.	Нейрокомпьютеры: разработка, применение	12	2004-	чз	10 лет
10.	Открытые системы. СУБД	12	2005-	чз	
11.	Прикладная информатика	6	2007 с №4-	чз	пост.

12.	Проблемы передачи информации	4	2005-	чз	пост.
13.	Программирование	6	1975-	чз	пост.
14.	Программные продукты и системы		2005-	чз	пост.

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

№ п/п	Ссылка	Пояснение
1.	http://www.book.ru	BOOK.ru – электронная библиотечная система (ЭБС) современной учебной и научной литературы. Библиотека BOOK.ru содержит актуальную литературу по всем отраслям знаний, коллекция пополняется электронными книгами раньше издания печатной версии.
2.	http://www.ibooks.ru	Айбукс.ру – электронная библиотечная система учебной и научной литературы. В электронную коллекцию включены современные учебники и пособия ведущих издательств России.
3.	http://www.sciencedirect.com	Платформа ScienceDirect обеспечивает всесторонний охват литературы из всех областей науки, предоставляя доступ к более чем 2500 наименований журналов и более 11000 книг из коллекции издательства «Эльзевир», а также огромному числу журналов, опубликованных престижными научными сообществами. Полнотекстовая база данных ScienceDirect является непревзойденным Интернет-ресурсом научно-технической и медицинской информации и содержит 25% мирового рынка научных публикаций.
4.	http://www.scopus.com	База данных Scopus индексирует более 18 тыс. наименований журналов от 5 тыс. международных издательств, включая более 300 российских журналов. Непревзойденная поддержка в поиске научных публикаций и предоставлении ссылок на все вышедшие рефераты из обширного объема доступных статей. Возможность получения информации о том, сколько раз ссылались другие авторы на интересующую Вас статью, предоставляется список этих статей. Отслеживание своих публикаций с помощью авторских профилей, а так же работы своих соавторов и соперников.
5.	http://www.scirus.com	Scirus – бесплатная поисковая система для поиска научной информации.
6.	http://www.elibrary.ru	Научная электронная библиотека (НЭБ) содержит полнотекстовые версии научных изданий ведущих зарубежных и отечественных издательств.
7.	http://scitation.aip.org	Базы данных Американского института физики American Institute of Physics (AIP).Тематика баз данных: физика (в т.ч. оптика, акустика, ядерная физика, математическая физика), механика (техническая механика), астрономия, химия и химическая техноло-гия, биоинженерия, энергетика, электроника, вычислительная техника

		(применение компьютеров в науке и технике), приборостроение, строительство. Список доступных полнотекстовых журналов: Applied Physics Letters (2001-2006) Chaos (1991-2006) J. of Applied Physics (2001-2006) J. of Chemical Physics (2001-2006) J. of Mathematical Physics (2001-2006) Journal of Physical and Chemical Reference Data (1999 -2006) Low Temperature Physics (1997 -2006) Physics of Fluids (2001-2006) Physics of Plasmas (2001-2006) Review of Scientific Instruments (2001-2006)
8.	http://diss.rsl.ru	«Электронная библиотека диссертаций» Российской Государственной Библиотеки (РГБ) в настоящее время содержит более 400 000 полных текстов наиболее часто запрашиваемых читателями диссертаций. Ежегодное оцифровывание от 25000 до 30000 диссертаций.
9.	http://www.lektorium.tv	«Лекториум ТВ» – видеолекции ведущих лекторов России. Лекториум – on-line – библиотека, где ВУЗы и известные лектории России презентуют своих лучших лекторов. Доступ к материалам свободный и бесплатный. Все видеозаписи публикуются только на основании договоров.
10.	http://moodle.kubsu.ru	Среда модульного динамического обучения
11.	http://mschool.kubsu.ru	Библиотека информационных ресурсов кафедры информационных образовательных технологий

7. Методические указания для обучающихся по освоению дисциплины (модуля).

Основными формами аудиторных занятий по дисциплине «Современная криптография» для очной формы обучения являются лекции и лабораторные работы.

Лекции по дисциплине «Современная криптография» следует проводить в компьютерных классах кафедры теоретической физики и компьютерных технологий с использованием средств мультимедиа. При подготовке отдельных вопросов лекций или лекций по определенным темам учебной программы рекомендуется активно привлекать студентов, реализуя такие виды интерактивных образовательных технологий, как «Студент в роли преподавателя» и «Работа в малых группах».

Лабораторные работы по дисциплине «Современная криптография» следует проводить в компьютерных классах кафедры теоретической физики и компьютерных технологий. Выполнение лабораторных работ сочетает различные виды практических заданий и упражнений. На лабораторных работах рекомендуется использовать образовательные технологии «Мозговой штурм» и «Творческое задание». При выполнении работ используются локальные и глобальные сети.

Структура дисциплины «Современная криптография» для очной формы обучения определяет следующие виды самостоятельной работы: самостоятельная работа студента (СРС).

Самостоятельная работа студента является основным видом самостоятельной работы. Она проводится в целях закрепления знаний, полученных на всех видах учебных занятий, а также расширения и углубления знаний, т.е. активного приобретения студентами новых знаний.

СРС включает проработку и повторение лекционного материала. Для этого студенту рекомендуется прочитать текст лекции, пересказать его вслух, воспроизвести самостоятельно имеющиеся в тексте структурно-логические схемы, диаграммы, математические выкладки формул, доказательства теорем и т.п. Проработку лекционного

материала следует проводить сначала последовательно, по каждому учебному вопросу, а затем повторно, по всему тексту лекции.

СРС также включает изучение материала по рекомендованным учебникам и учебным пособиям. Так как существует огромное количество учебной литературы, то для этого вида подготовки необходимо предварительное указание преподавателя. Преподаватель должен выступать здесь в роли опытного «путеводителя», определяя последовательность знакомства с литературными источниками и «глубину погружения» в каждый из них.

Одним из видов СРС является подготовка к лабораторным работам. Преподаватель накануне очередного занятия обозначает для студентов круг теоретического материала, необходимого для выполнения лабораторной работы. Студенты прорабатывают его. Затем, уже в аудитории, перед выполнением заданий, преподаватель производит контрольный опрос студентов. Это позволяет определить степень готовности группы по данной теме и скорректировать ход занятия.

Преподаватель должен прогнозировать затруднения, которые могут возникнуть у студентов при самостоятельном изучении и усвоении учебного материала и предусмотреть оперативную консультацию по любому вопросу. Если возникают затруднения по одному и тому же материалу (вопросу) у многих студентов, то желательно провести групповую консультацию. Консультации должны быть краткими: групповая - 2-3 мин., индивидуальная - 1-2 мин. Глубину и качество усвоения учебного материала необходимо непрерывно отслеживать при проведении текущего контроля знаний.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю).

8.1 Перечень информационных технологий.

1) Использование электронных презентаций при проведении лекций.
2) Подготовка к тестированию и консультирование посредством электронной почты.
3) Выполнение лабораторных работ.

8.2 Перечень необходимого программного обеспечения.

1) Растровый графический редактор Paint Операционная система Windows
2) Программа разработки презентаций Microsoft PowerPoint Дистрибутив Microsoft Office
3) Электронные таблицы Microsoft Excel Дистрибутив Microsoft Office
4) Текстовый процессор Microsoft Word Дистрибутив Microsoft Office
5) Компиляторы Basic, Pascal, C++
6) Система математических вычислений MathCAD
7) Система математических вычислений MatLAB

8.3 Перечень информационных справочных систем:

Не предусмотрены

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю).

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Лекционные занятия	Учебные аудитории для проведения лекционных занятий – ауд. 213, корп. С, вычислительный центр (ул. Ставропольская, 149)
2.	Лабораторные занятия	Учебные аудитории для проведения семинарских занятий– ауд. 213, корп. С, вычислительный центр (ул. Ставропольская, 149)
3.	Самостоятельная работа	Аудитория для самостоятельной работы – ауд. 208, корп. С (ул. Ставропольская, 149)