МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ДГТУ)
АВИАЦИОННО-ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ

УТВЕРЖДАЮ Директор АТК
_____ В.А. Зибров
20.03.2023г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине ОП.13 Информационная безопасность
основной образовательной программы
по специальности СПО
09.02.07 Информационные системы и программирование
базовой подготовки

Ростов-на-Дону
2023 г.

1 Паспорт фонда оценочных средств

1.1 Область применения

Фонд оценочных средств предназначен для проверки результатов освоения учебной дисциплины «Информационная безопасность» программы подготовки специалистов среднего звена (ППССЗ) по специальности 09.02.07 Информационные системы и программирование в части овладения профессиональных и общих компетенций.

Результаты освоения (объекты оценивания)	**Код** (общие и профессиональные компетенции)	**Основные показатели оценки результата и их критерии**	**Тип задания; № задания**	**Форма аттестации** (в соответствии с учебным планом)
уметь:				Дифференцированный зачет
применять правовые, организационные, технические и программные средства защиты информации; (У1)	ОК 01, ОК 02, ОК 05, ОК 09, ОК 10, ПК11.6	защита от угроз целостности (несанкционированного изменения) информации; защита от угроз конфиденциальности (несанкционированного получения) информации по всем возможным каналам утечки; защита от угроз доступности информации, в смысле несанкционированного или случайного ограничения доступа к ресурсам и информации системы;	фронт. опрос	
создавать программные средства защиты информации; (У2)		Критерии оценки защищенности компьютерных систем, которые известны как «Оранжевая книга». Европейские критерии оценки безопасности информационных технологий. Данные критерии разработаны с учетом выявленных недостатков и ограничений по применению «Оранжевой книги» и являются гармонизированными по отношению к первым.	Практические работы, тесты, фронт. опрос	
организовать защиту от утечки информа-		защита от угроз аудиту системы (декларирует-	Практические работы,	

ции по техническим каналам; (У3)		ся 12 потенциальных угроз).	фронт. опрос	
знать:				
источники возникновения информационных угроз; (Зн1)	ОК 01, ОК 02, ОК 05, ОК 09, ОК 10, ПК11.6	продукт информационных технологий; политика безопасности;	фронт. опрос	
контроль выполнения практических заданий, устный опрос, контроль самостоятельной работы, тестирование; (Зн2)		потенциальные угрозы безопасности; типовые задачи защиты;	фронт. опрос	
модели и принципы защиты информации от несанкционированного доступа; (Зн3)		профиль защиты; проект защиты; функциональные требования к средствам защиты;	Практические работы, фронт. опрос	
контроль выполнения практических заданий, устный опрос, контроль самостоятельной работы, тестирование; (Зн4)		требования адекватности средств защиты; стандартные уровни адекватности средств защиты.	Практические работы, тесты, фронт. опрос	
методы антивирусной защиты информации контроль выполнения практических заданий, устный опрос, контроль самостоятельной работы тестирование; (Зн5)		типовые задачи защиты; профиль защиты; проект защиты; функциональные требования к средствам защиты;	Практические работы, тесты, фронт. опрос	
перспективные методы антивирусной защиты; (Зн6)		требования адекватности средств защиты; стандартные уровни адекватности средств защиты.	Практические работы, тесты, фронт. опрос	
организационно-правовое обеспечение информационной безопасности (Зн7)		Международный стандарт ISO/IEC 15408 – «Критерии оценки безопасности информационных технологий».	Практические работы, фронт. опрос	

Элемент учебной дисциплины	Формы и методы контроля					
	Текущий контроль		Рубежный контроль		Промежуточная аттестация	
	Форма контроля	Объекты оценивания	Форма контроля	Объекты оценивания	Форма контроля	Объекты оценивания
Тема 1.1 Актуальность информационной безопасности	Фронтальный опрос	У1			Дифференцированный зачет	У1, У2, У3 Зн1, Зн2, Зн3, Зн4, Зн5, Зн6, Зн7
Тема 1.2 Лицензирование и сертификация в области защиты информации	Фронтальный опрос Практическая работа №1	У1 Зн1				
Тема 1.3 Основные нормативные руководящие документы	Фронтальный опрос	У1, У2 Зн1, Зн2, Зн4, Зн5				
Тема 2.1 Сущность и основные понятие информационной безопасности	Фронтальный опрос Практическая работа №2	У1, У2 Зн3, Зн4, Зн5				
Тема 2.2 Основные подходы к классификации угроз информационной безопасности	Фронтальный опрос Практическая работа №3	У1 Зн3, Зн4				
Тема 3.1 Основные принципы защиты информации от несанкционированного доступа	Фронтальный опрос Практическая работа №4	У1 Зн3, Зн4, Зн5				
Тема 3.2 Проблемы идентификации и аутентификации пользователей	Фронтальный опрос Практическая работа №5-6	У1, У2, У3 Зн3, Зн4, Зн6				
Тема 3.3 Программно-аппаратная защита информации от локального несанкционированного доступа	Фронтальный опрос Практическая работа №7-8	У1, У2 Зн1, Зн2, Зн3, Зн4, Зн5, Зн6, Зн7				
Тема 4.1 Основные классы антивирусных программ	Фронтальный опрос Практическая работа №9-11 Тестирование (Т01)	У1, У2 Зн4, Зн5, Зн6, Зн7				
Тема 4.2 Методы обнару-	Фронтальный опрос	У1, У2, У3				

жения и удаления вирусов	Практическая работа №12-14 Тестирование (Т02)	Зн1, Зн2, Зн4, Зн5, Зн6				
Тема 5.1 Прямые и косвенные каналы утечки информации.	Фронтальный опрос Практическая работа №15	У2, У3 Зн4, Зн5, Зн6				
Тема 5.2 Каналы и методы несанкционированного доступа к конфиденциальной информации.	Фронтальный опрос Практическая работа №16	У1, У3 Зн4, Зн5, Зн7				
Тема 5.3 Обнаружение каналов утечки информации	Фронтальный опрос Практическая работа №17-19	У1, У3 Зн4, Зн5, Зн6, Зн7				
Тема 5.4 Методы и средства блокирования каналов утечки информации	Фронтальный опрос Практическая работа №20-22	У1, У2, У3 Зн4, Зн5, Зн6, Зн7				
Тема 6.1 Служба безопасности объекта. Права и обязанности сотрудников службы безопасности	Фронтальный опрос Практическая работа №23-24	У1, У3 Зн4, Зн5, Зн7				
Тема 6.2 Защита коммерческой тайны и интеллектуальной собственности, основные виды компьютерных преступлений	Фронтальный опрос Практическая работа №25	У2, У3 Зн3, Зн4, Зн5, Зн6, Зн7				

2 Комплект контрольно-оценочных материалов

2.1 Задания для текущего контроля с критериями оценивания

2.1.1 Практические работы

Учебным планом предусмотрено выполнение 5 практических работ по дисциплине ОП.13 Информационная безопасность. Содержание всех практических работ приведено в методической разработке по выполнению практических работ по дисциплине ОП.13 Информационная безопасность.

2.1.2 Тестирование

Приводится содержание основных тестовых заданий. Соответствие тестовых заданий по темам приведено выше в таблице.

Тестирование (Т01) по теме: Основные классы антивирусных программ

ТЕСТ:

1. Внимательно прочитайте текст.
2. Выберите один или несколько вариантов ответа.
3. Выполнять тест лучше самостоятельно без применения конспектов, учебников и прочей вспомогательной литературы

Задание № 1
Вопрос:
Сопоставьте названия программ и изображений
Укажите соответствие для всех 6 вариантов ответа:

1) 
2) 
3) 
4) 
5) 

6) 

__ Antivir
__ DrWeb
__ Nod 32
__ Antivirus Kaspersky
__ Avast
__ Antivirus Panda

Задание № 3
Вопрос:
Выразите свое согласие или несогласие

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

Задание № 4
Вопрос:
Отметьте составные части современного антивируса

Выберите несколько из 5 вариантов ответа:
1) Модем
2) Принтер
3) Сканер
4) Межсетевой экран
5) Монитор

Задание № 5
Вопрос:
Вредоносные программы - это
(выберите один из вариантов ответа)

Выберите один из 5 вариантов ответа:
1) шпионские программы
2) программы, наносящие вред данным и программам, находящимся на компьютере
3) антивирусные программы
4) программы, наносящие вред пользователю, работающему на зараженном компьютере
5) троянские утилиты и сетевые черви

Задание № 6
Вопрос:
К вредоносным программам относятся:
(выберите несколько вариантов ответа)

Выберите несколько из 5 вариантов ответа:
1) Потенциально опасные программы
2) Вирусы, черви, трояны
3) Шпионские и рекламмные программы
4) Вирусы, программы-шутки, антивирусное программное обеспечение
5) Межсетевой экран, брандмауэр

Задание № 7
Вопрос:
Сетевые черви это

Выберите один из 5 вариантов ответа:
1) Вредоносные программы, устанавливающие скрытно от пользователя другие вредоносные программы и утилиты
2) Вирусы, которые проникнув на компьютер, блокируют работу сети
3) Вирусы, которые внедряются в документы под видом макросов
4) Хакерские утилиты управляющие удаленным доступом компьютера
5) Вредоносные программы, которые проникают на компьютер, используя сервисы компьютерных

сетей
Задание № 8
Вопрос:
К биометрической системе защиты относятся:
(выберите несколько вариантов ответа)

Выберите несколько из 5 вариантов ответа:
1) Защита паролем
2) Физическая защита данных
3) Антивирусная защита
4) Идентификация по радужной оболочке глаз
5) Идентификация по отпечаткам пальцев

Задание № 9
Вопрос:
Вредоносная программа, которая подменяет собой загрузку некоторых программ при загрузке системы называется...

Выберите один из 5 вариантов ответа:
1) Загрузочный вирус
2) Макровирус
3) Троян
4) Сетевой червь
5) Файловый вирус

Задание № 10
Вопрос:
Программа, осуществляющая несанкционированные действия по сбору, и передаче информации злоумышленнику, а также ее разрушение или злонамеренную модификацию.

*Запишите ответ:*_____

Задание № 11
Вопрос:
Руткит - это...

Выберите один из 5 вариантов ответа:
1) вредоносная программа, выполняющая несанкционированные действия по передаче управления компьютером удаленному пользователю
2) разновидность межсетевого экрана
3) программа использующая для распространения Рунет (Российскую часть Интернета)
4) вредоносная программа, маскирующаяся под макрокоманду
5) программа для скрытого взятия под контроль взломанной системы

Задание № 12
Вопрос:
Компьютерные вирусы это

Выберите несколько из 5 вариантов ответа:
1) Вредоносные программы, наносящие вред данным.
2) Программы, уничтожающие данные на жестком диске
3) Программы, которые могут размножаться и скрыто внедрять свои копии в файлы, загрузочные сектора дисков, документы.

4) Программы, заражающие загрузочный сектор дисков и препядствующие загрузке компьютера
5) Это скрипты, помещенные на зараженных интернет-страничках

Задание № 13
Вопрос:
Вирус внедряется в исполняемые файлы и при их запуске активируется. Это...

Выберите один из 5 вариантов ответа:
1) Загрузочный вирус
2) Макровирус
3) Файловый вирус
4) Сетевой червь
5) Троян

Задание № 14
Вопрос:
Укажите порядок действий при наличии признаков заражения компьютера

Укажите порядок следования всех 3 вариантов ответа:
__ Сохранить результаты работы на внешнем носителе
__ Запустить антивирусную программу
__ Отключиться от глобальной или локальной сети

Задание № 15
Вопрос:
Вирус поражающий документы называется

Выберите один из 5 вариантов ответа:
1) Троян
2) Файловый вирус
3) Макровирус
4) Загрузочный вирус
5) Сетевой червь

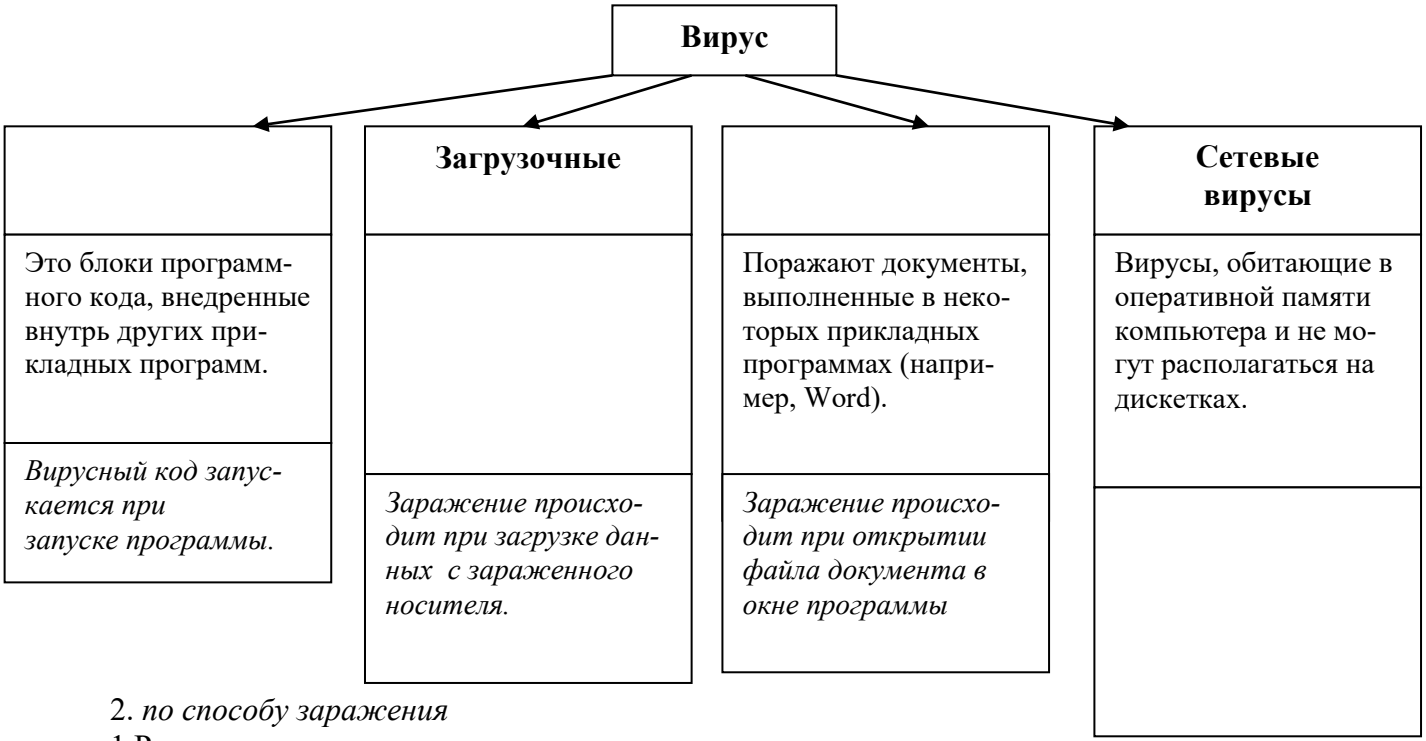
Ответы:
1) Верные ответы:
    3;
    4;
    1;
    6;
    2;
    5;
2) Верный ответ: 1;
3) Верные ответы:
    Нет;
    Нет;
    Нет;
    Да;
    Да;
4) Верные ответы: 3; 4; 5;
5) Верный ответ: 2;
6) Верные ответы: 1; 2; 3;
7) Верный ответ: 5;

8) Верные ответы: 4; 5;
9) Верный ответ: 1;
10) Верный ответ: "троян".
11) Верный ответ: 5;
12) Верные ответы: 3;
13) Верный ответ: 3;
14) Верные ответы:
2;
3;
1;
15) Верный ответ: 3;

Критерии оценивания теста:
5 (отлично) – правильно выполнены 14-15 заданий.
4 (хорошо) – правильно выполнены 12-13 задания.
3 (удовлетворительно) – правильно выполнены 9-11 заданий.
2 (неудовлетворительно) – правильно выполнены менее 8 заданий.

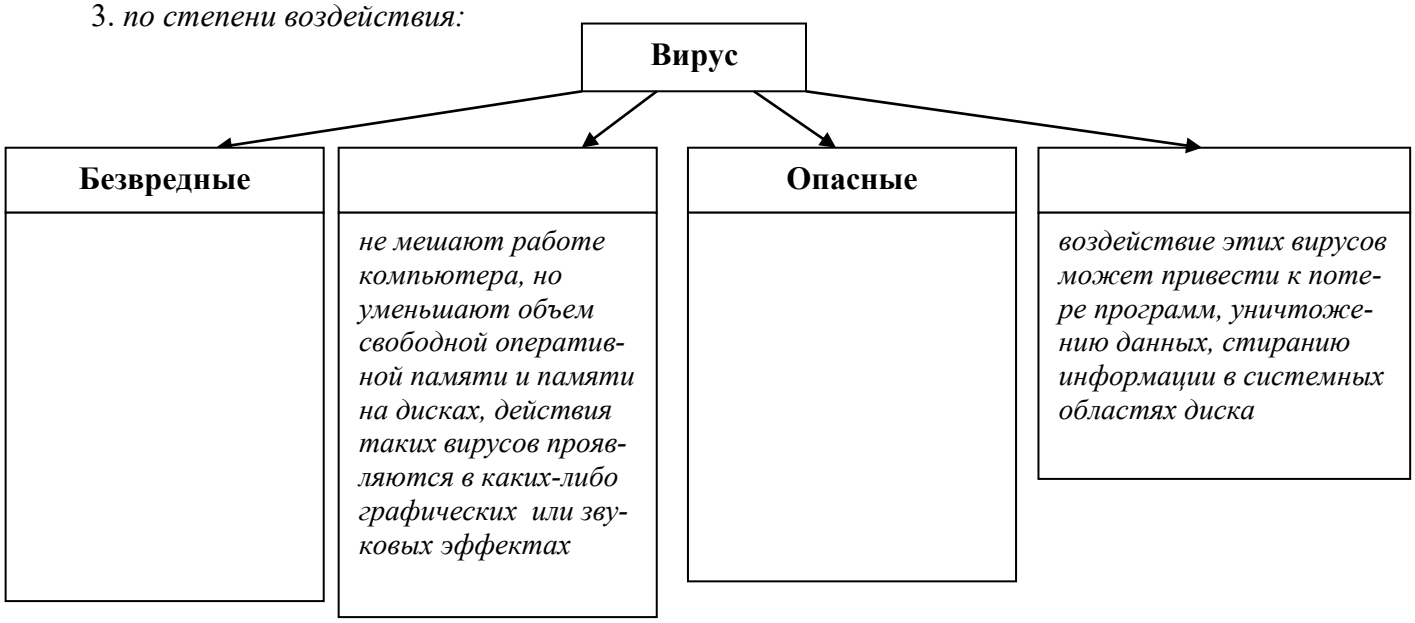
Тестирование (Т02) по теме: Методы обнаружения и удаления вирусов

Вариант №1
Виды компьютерных вирусов
Классификаций вредоносных программ (компьютерных вирусов):
1. *по среде их обитания*



2. *по способу заражения*
1.Резидентные -_____
_____
2.Нерезидентные -_____
_____

3. *по степени воздействия:*



4. по особенностям алгоритма работы:

1. Простейшие – _____
_____

2. Вирусы-репликаторы (черви) – _____
_____

3. Вирусы-невидимки (стелс-вирусы) –_____
_____

4. Вирусы-мутанты –_____
_____

5. Квазивирусные («троянские» программы) - _____
_____

Вариант №2
Антивирусные программы

Антивирусные программы - _____
_____
_____

В зависимости от назначения и принципа действия различают следующие антивирусные программы:

1. **сторожа или детекторы** –_____
_____
2. _____– предназначены для обнаружения и устранения известных им вирусов, удаляя их из тела программы и возвращая ее в исходное состояние. Наиболее известными представителями являются Dr.Web, Aids Test, Norton Anti Virus.
3. _____– они контролируют уязвимые и поэтому наиболее атакуемые компоненты компьютера, запоминают состояние служебных областей и файлов, а в случае обнаружения изменений сообщают пользователю.
4. **резидентные мониторы или фильтры** – постоянно находятся в памяти компьютера для обнаружения попыток выполнить несанкционированные действия. В случае обнаружения подозрительного действия выводят запрос пользователю на подтверждение операций.
5. **вакцины** –_____
_____
_____

Среди антивирусных программных продуктов можно отметить, прежде всего, пакеты:

- Norton Antivirus (Symantec),
- Vims Scan (McAfee),
- Dr.Solomon AV Toolkit (S&S IntL),
- AntiVirus (IBM),
- InocuLAN (Computer Associates)
- _____
- Лаборатория Касперского.

Как защититься от вирусов

_____

_____

Вариант №3

Признаки появления и пути проникновения вирусов в компьютер

Косвенные признаки заражения компьютера:

- _____
- _____
- _____
- *произвольный запуск на компьютере каких-либо программ;*
- _____
- _____
- _____
- _____
- *друзья и знакомые говорят о полученных от вас сообщениях, которые вы не отправляли;*
- *в вашем почтовом ящике находится большое количество сообщений без обратного адреса и заголовка.*

Пути проникновения вирусов на компьютер:

- _____
- _____
- _____
- _____
- *Съемные накопители, на которых находятся заражённые вирусом файлы.*
- _____
- *Вирус, оставшийся в оперативной памяти после предшествующего пользователя.*

Действия при наличии признаков заражения компьютера.

- *отключить компьютер от локальной сети и Интернета, если он к ним был подключен;*
- *если симптом заражения состоит в том, что невозможно загрузиться с жесткого диска компьютера (компьютер выдает ошибку, когда вы его включаете), попробовать загрузиться в режиме защиты от сбоев или с диска аварийной загрузки Windows;*
- _____

Критерии оценки:

«5 (отлично)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, литературным языком: ответ самостоятельный.

«4 (хорошо)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки, исправленные по требованию преподавателя.

«3 (удовлетворительно)»: ответ полный, но при этом допущена существенная ошибка, или неполный, несвязный.

«2 (неудовлетворительно)»: при ответе обнаружено непонимание студентом основного содержания учебного материала или допущены существенные ошибки, которые студент не смог исправить при наводящих вопросах преподавателя.

2.1.3 Фронтальный опрос (устный, письменный)

Тема 1 Актуальность информационной безопасности

1. Что такое информационная безопасность?
2. Перечислите важнейшие аспекты информационной безопасности.
3. Перечислите уровни решения проблемы информационной безопасности.
4. Перечислите уровни защиты информации.
5. Охарактеризуйте угрозы информационной безопасности: раскрытия целостности, отказ в обслуживании.
6. Перечислите составляющие информационной безопасности.
7. Приведите определение доступности информации.
8. Приведите определение целостности информации.
9. Приведите определение конфиденциальности информации.
10. Каким образом взаимосвязаны между собой составляющие информационной безопасности? Приведите собственные примеры.

Тема 2 Лицензирование и сертификация в области защиты информации

1. Какие виды требований включает стандарт ISO/IEC 15408?
2. Чем отличаются функциональные требования от требований доверия?
3. В чем заключается иерархический принцип "класс – семейство – компонент – элемент"?
4. Какова цель требований по отказоустойчивости информационных систем?
5. Сколько классов функциональных требований?
6. Объясните причины компьютерных преступлений.
7. Опишите, как обнаружить компьютерное преступление или уязвимые места в системе информационной безопасности.
8. Опишите основные технологии компьютерных преступлений.
9. Перечислите меры защиты информационной безопасности.
10. Перечислите меры предосторожности при работе с целью защиты информации.

Тема 3 Основные нормативные руководящие документы

1. Перечислите основополагающие документы по информационной безопасности.
2. Понятие государственной тайны.
3. Что понимается под средствами защиты государственной тайны?
4. Основные задачи информационной безопасности в соответствии с Концепцией национальной безопасности РФ.
5. Какие категории государственных информационных ресурсов определены в Законе "Об информации, информатизации и защите информации"?
6. Какая ответственность в Уголовном кодексе РФ предусмотрена за создание, использование и распространение вредоносных программ для ЭВМ?

Тема 4 Сущность и основные понятие информационной безопасности

1. Основные понятия информационной безопасности. Цели и задачи защиты информации в информационно-вычислительных сетях.
2. Перечислите важнейшие аспекты информационной безопасности.
3. Перечислите уровни решения проблемы информационной безопасности.
4. Перечислите уровни защиты информации.
5. Основные технологии, использующиеся при совершении компьютерных преступлений.
6. Меры защиты информационной безопасности.
7. В чем заключается проблема информационной безопасности?
8. Дайте определение понятию "информационная безопасность".
9. Какие определения информационной безопасности приводятся в "Концепции информационной безопасности сетей связи общего пользования Российской Федерации"?
10. Что понимается под "компьютерной безопасностью"?

Тема 5 Основные подходы к классификации угроз информационной безопасности

1. Виды угроз информационной безопасности.
2. Перечислите классы удаленных угроз.

3. Как классифицируются удаленные угрозы "по характеру воздействия"?
4. Охарактеризуйте удаленные угрозы "по цели воздействия".
5. Как классифицируются удаленные угрозы "по расположению субъекта и объекта угрозы"?
6. Дайте определение маршрутизатора.
7. Что такое подсеть и сегмент сети? Чем они отличаются?
8. Может ли пассивная угроза привести к нарушению целостности информации?

Тема 6 Основные принципы защиты информации от несанкционированного доступа

1. Перечислите задачи информационной безопасности общества.
2. Перечислите уровни формирования режима информационной безопасности.
3. Дайте краткую характеристику законодательно-правового уровня.
4. Какие подуровни включает программно-технический уровень?
5. Что включает административный уровень?
6. В чем особенность морально-этического подуровня?

Тема 7 Проблемы идентификации и аутентификации пользователей

1. Что понимается под идентификацией пользователя?
2. Что понимается под аутентификацией пользователей?
3. Применим ли механизм идентификации к процессам? Почему?
4. Перечислите возможные идентификаторы при реализации механизма идентификации.
5. Перечислите возможные идентификаторы при реализации механизма аутентификации.
6. Какой из механизмов (аутентификация или идентификация) более надежный? Почему?
7. В чем особенности динамической аутентификации?
8. Опишите механизм аутентификации пользователя.
9. Что такое "электронный ключ"?
10. Перечислите виды аутентификации по уровню информационной безопасности.
11. Какой из видов аутентификации (устойчивая аутентификация или постоянная аутентификация) более надежный?

Тема 8 Программно-аппаратная защита информации от локального несанкционированного доступа

1. Сколько классов защищенности СВТ от НСД к информации устанавливает РД "СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации"?
2. Дайте характеристику уровням защиты СВТ от НСД к информации по РД "СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации"?
3. Классы защищенности АС от НСД по РД "АС. Защита от НСД к информации. Классификация АС и требования по защите информации".
4. Какие классы защищенных АС от НСД должны обеспечивать идентификацию, проверку подлинности и контроль доступа субъектов в систему?
5. Показатели защищенности межсетевых экранов.
6. Классы защищенности межсетевых экранов.

Тема 9 Основные классы антивирусных программ

1. Основные классы антивирусных программ
2. Поясните понятия "сканирование налету" и "сканирование по запросу".
3. Перечислите виды антивирусных программ.
4. Охарактеризуйте антивирусные сканеры.
5. Принципы функционирования блокировщиков и иммунизаторов.
6. Особенности CRC-сканеров.
7. В чем состоят особенности эвристических сканеров?
8. Какие факторы определяют качество антивирусной программы?
9. Перечислите наиболее распространенные пути заражения компьютеров вирусами.
10. Какие особенности заражения вирусами при использовании электронной почты?
11. Особенности заражения компьютеров локальных сетей.
12. Перечислите основные правила защиты от компьютерных вирусов, получаемых не из вычислительных сетей.
13. Как ограничить заражение макровирусом при работе с офисными приложениями?

Тема 10 Методы обнаружения и удаления вирусов

1.Что такое компьютерный вирус? Какими свойствами обладают компьютерные вирусы?
2.По каким признакам классифицируют компьютерные вирусы? Перечислите типы вирусов.
3.Какие вирусы называются резидентными и в чем особенность таких вирусов?
4.Каковы отличия вирусов-репликаторов, стелс-вирусов, мутантов и «троянских» программ?
5.Опишите схему функционирования загрузочного вируса.
6.Опишите схему функционирования файлового вируса.
7.Опишите схему функционирования загрузочно-файловых вирусов.
8.Что такое полиморфный вирус? Почему этот тип вирусов считается наиболее опасным?
9.Каковы причины появления компьютерных вирусов. Приведите примеры широко известных вирусов.
10. Существует ли в мире и в РФ уголовная ответственность за создание и распространение компьютерных вирусов?
11. Какой вид вирусов наиболее распространяемый в распределенных вычислительных сетях? Почему?
12. Перечислите классификационные признаки компьютерных вирусов.
13. Охарактеризуйте файловый и загрузочный вирусы.
14. В чем особенности резидентных вирусов?
15. Сформулируйте признаки стелс-вирусов.
16. Перечислите деструктивные возможности компьютерных вирусов.
17. Поясните самошифрование и полиморфичность как свойства компьютерных вирусов.

Тема 11 Прямые и косвенные каналы утечки информации.

1. Особенности обеспечения информационной безопасности компьютерных сетей.
2. Дайте определение понятия "удаленная угроза".
3. Основные цели информационной безопасности компьютерных сетях.
4. В чем заключается специфика методов и средств защиты компьютерных сетей?
5. Поясните понятие "глобальная сетевая атака", приведите примеры.
6. Что понимается под протоколом передачи данных?
7. Охарактеризуйте сети с коммутацией сообщений и коммутацией пакетов.
8. Чем отличается соединение по виртуальному каналу от передачи датаграмм?
9. Какие протоколы образуют модель TCP/IP?
10. Какие уровни входят в сетевую модель TCP/IP?
11. Дайте характеристику всех уровней модели TCP/IP и укажите соответствующие этим уровням протоколы.
12. Соотнесите по уровням модели TCP/IP понятия "пакет" и "кадр". Чем они отличаются?
13. Какой протокол обеспечивает преобразование логических сетевых адресов в аппаратные?

Тема 12 Служба безопасности объекта. Права и обязанности сотрудников службы безопасности

1. Цели и задачи административного уровня обеспечения информационной безопасности.
2. Содержание административного уровня.
3. Дайте определение политики безопасности.
4. Направления разработки политики безопасности.
5. Перечислите составные элементы автоматизированных систем.
6. Субъекты информационных отношений и их роли при обеспечении информационной безопасности.
7. Дайте определение типовой удаленной атаки.
8. Механизм реализации удаленной атаки "анализ сетевого трафика".
9. Что является целью злоумышленников при "анализе сетевого трафика"?
10. Назовите причины успеха удаленной атаки "ложный объект".
11. Охарактеризуйте удаленную атаку "подмена доверенного объекта" по классам угроз.
12. Поясните возможные механизмы реализации удаленной атаки "отказ в обслуживании".
13. Какие составляющие "информационной безопасности" могут быть нарушены при реализации каждой из типовых удаленных атак?

Тема 13 Защита коммерческой тайны и интеллектуальной собственности, основные виды компьютерных преступлений

1. Основные технологии, использующиеся при совершении компьютерных преступлений.
2. Перечислите известные методы разграничения доступа.
3. В чем заключается разграничение доступа по спискам?
4. Как используется матрица разграничения доступа?
5. Опишите механизм разграничения доступа по уровням секретности и категориям.
6. Какие методы управления доступа предусмотрены в руководящих документах Гостехкомиссии?
7. Поясните механизм дискретного управления доступом?
8. Сравните дискретное и мандатное управление доступом.
9. Что входит в состав криптосистемы?
10. Какие составляющие информационной безопасности могут обеспечить криптосистемы?
11. Что такое электронная цифровая подпись?

Критерии оценивания

Оценка за ответ на вопрос выставляется:

«отлично» - если студент правильно, четко, аргументировано и в полном объеме изложил содержание теоретического вопроса, а также убедительно ответил на дополнительные вопросы;

«хорошо» - если студент правильно, но не достаточно полно изложил содержание теоретического вопроса, а также не точно ответил на дополнительные вопросы;

«удовлетворительно» - если студент изложил только основные моменты из теоретического вопроса;

«неудовлетворительно» - ответ не соответствует изложенным выше критериям.

2.1.4 Задания для оценки освоения учебной дисциплины

Раздел 1. Концепция информационной безопасности

Устный опрос на тему:
«Актуальность проблемы обеспечения безопасности информации»

Вопросы:

1. Основные понятия безопасности: конфиденциальность, целостность, доступность.
2. Объекты, цели и задачи защиты информации.
3. Возможные угрозы информационной безопасности: классификация, источники возникновения и пути реализации.
4. Виды угроз.
5. Определение требований к уровню обеспечения информационной безопасности.

Критерии оценки устного ответа:

«5 (отлично)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, литературным языком: ответ самостоятельный.

«4 (хорошо)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки, исправленные по требованию преподавателя.

«3 (удовлетворительно)»: ответ полный, но при этом допущена существенная ошибка, или неполный, несвязный.

«2 (неудовлетворительно)»: при ответе обнаружено непонимание студентом основного содержания учебного материала или допущены существенные ошибки, которые студент не смог исправить при наводящих вопросах преподавателя.

Устный опрос на тему:
«Виды мер обеспечения информационной безопасности»

Вопросы:

1. Виды мер обеспечения информационной безопасности: правовые, организационные, технические, программно-математические.

2. Специфические приемы управления техническими средствами.
3. Административный уровень защиты информации: программа безопасности, политика безопасности.

Критерии оценки устного ответа:

«5 (отлично)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, литературным языком: ответ самостоятельный.

«4 (хорошо)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки, исправленные по требованию преподавателя.

«3 (удовлетворительно)»: ответ полный, но при этом допущена существенная ошибка, или неполный, несвязный.

«2 (неудовлетворительно)»: при ответе обнаружено непонимание студентом основного содержания учебного материала или допущены существенные ошибки, которые студент не смог исправить при наводящих вопросах преподавателя.

«Анализ рисков информационной безопасности»

1. **Цель работы** – ознакомление с алгоритмами оценки риска информационной безопасности.

2. **Краткие теоретические сведения**

Риск ИБ – потенциальная возможность использования определенной ***угрозой уязвимостей актива*** или группы активов для причинения вреда организации.

Уязвимость - слабость в системе защиты, делающая возможной реализацию угрозы.

Угроза ИБ - совокупность условий и факторов, которые могут стать причиной нарушений целостности, конфиденциальности, доступности информации.

Информационный актив – это материальный или нематериальный объект, который:

- является информацией или содержит информацию,
- служит для обработки, хранения или передачи информации,
- имеет ценность для организации.

3. Задание

1. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий»
2. Ознакомьтесь с **Приложениями C, D** и **E** ГОСТа.
3. Выберите три различных информационных актива организации (см. вариант).
4. Из **Приложения D** ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.
5. Пользуясь **Приложением C** ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.
6. Пользуясь одним из методов (см. вариант) предложенных в **Приложении E** ГОСТа произведите оценку рисков информационной безопасности.
7. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

4. Содержание отчета

1. Титульный лист
2. Содержание
3. Задание
4. Обоснование выбора информационных активов организации
5. Оценка ценности информационных активов
6. Уязвимости системы защиты информации
7. Угрозы ИБ

8. Оценка рисков
9. Выводы

Раздел 2. Угрозы безопасности информационных систем

Устный опрос на тему:
«Особенности защиты информации в персональном компьютере»

Вопросы:
1. Обеспечение физической целостности.
2. Предупреждение несанкционированной модификации, копирования и получения информации в ПК.
3. Обеспечение целостности информации в ПК.
4. Физическая защита ПК и носителей информации.

Критерии оценки устного ответа:
«5 (отлично)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, литературным языком: ответ самостоятельный.
«4 (хорошо)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки, исправленные по требованию преподавателя.
«3 (удовлетворительно)»: ответ полный, но при этом допущена существенная ошибка, или неполный, несвязный.
«2 (неудовлетворительно)»: при ответе обнаружено непонимание студентом основного содержания учебного материала или допущены существенные ошибки, которые студент не смог исправить при наводящих вопросах преподавателя.

Устный опрос на тему:
«Программные средства защиты информации»

Вопросы:
1. Основные защитные механизмы: идентификация и аутентификация, протоколирование и аудит.
2. Разграничение доступа.
3. Контроль целостности.
4. Обнаружение и противодействие атакам.
5. Защита от копирования информации.

Критерии оценки устного ответа:
«5 (отлично)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, литературным языком: ответ самостоятельный.
«4 (хорошо)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки, исправленные по требованию преподавателя.
«3 (удовлетворительно)»: ответ полный, но при этом допущена существенная ошибка, или неполный, несвязный.
«2 (неудовлетворительно)»: при ответе обнаружено непонимание студентом основного содержания учебного материала или допущены существенные ошибки, которые студент не смог исправить при наводящих вопросах преподавателя.

Процедура аутентификации пользователя на основе пароля»

1. Цель работы

Изучение технологии аутентификации пользователя на основе пароля.

2. Краткие теоретические сведения

Аутентификация (Authentication) - процедура проверки подлинности заявленного пользователя, процесса или устройства. Эта проверка позволяет достоверно убедиться, что пользователь (процесс или устройство) является именно тем, кем себя объявляет. При проведении аутентификации проверяющая сторона убеждается в подлинности проверяемой стороны, при этом проверяемая сторона тоже активно участвует в процессе обмена информацией. Обычно пользователь под-

утверждает свою идентификацию, вводя в систему уникальную, неизвестную другим пользователям информацию о себе (например, пароль или сертификат).

Идентификация и аутентификация являются взаимосвязанными процессами распознавания и проверки подлинности субъектов (пользователей). Именно от них зависит последующее решение системы, можно ли разрешить доступ к ресурсам системы конкретному пользователю или процессу. После идентификации и аутентификации субъекта выполняется его авторизация.

Авторизация (Authorization) - процедура предоставления субъекту определенных полномочий и ресурсов в данной системе. Иными словами, авторизация устанавливает сферу действия субъекта и доступные ему ресурсы. Если система не может надежно отличить авторизованное лицо от неавторизованного, конфиденциальность и целостность информации в ней могут быть нарушены. Организации необходимо четко определить свои требования к безопасности, чтобы принимать решения о соответствующих границах авторизации.

С процедурами аутентификации и авторизации тесно связана процедура администрирования действий пользователя.

Пароль - это то, что знает пользователь и что также знает другой участник взаимодействия. Для взаимной аутентификации участников взаимодействия может быть организован обмен паролями между ними.

3. Задание

Разработать программу, представляющую собой форму доступа к определённым информационным ресурсам на основе пароля:

1. В качестве информационного ресурса использовать любой файл или приложение.
2. Доступ к ресурсу должен быть разрешен только санкционированным пользователям. Для этого в программе должны храниться имена пользователей и их пароли. При попытке доступа пользователя к ресурсу проверяется наличие его идентификатора (имени) в системе и соответствие введенного пароля паролю, который хранится в системе.
3. В системе должна храниться следующая информация о пользователе: ID или имя пользователя, пароль, ФИО, дата рождения, место рождения (город) номер телефона.
4. Пользователь должен иметь возможность поменять пароль (ограничения: см. вариант).

4. Содержание отчета

1. Титульный лист
2. Содержание
3. Задание
4. Текст программы
5. Пример работы программы
6. Выводы

Раздел 3. Криптографические методы защиты информации

Устный опрос на тему:
«Криптология и основные этапы ее развития»

Вопросы:

1. Основные понятия: криптология, криптография, ключ, криптографическая система.
2. Требования к криптографическим методам преобразования информации.
3. Этапы развития криптологии как науки.

Критерии оценки устного ответа:

«5 (отлично)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, литературным языком: ответ самостоятельный.

«4 (хорошо)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки, исправленные по требованию преподавателя.

«3 (удовлетворительно)»: ответ полный, но при этом допущена существенная ошибка, или неполный, несвязный.

«2 (неудовлетворительно)»: при ответе обнаружено непонимание студентом основного содержания учебного материала или допущены существенные ошибки, которые студент не смог исправить при наводящих вопросах преподавателя.

Устный опрос на тему:
«Методы криптографических преобразований»

Вопросы:

1. Классификация криптосистем.
2. Алгоритмы шифрования.
3. Шифры замены.
4. Шифры перестановки.
5. Ассиметричное шифрование: метод гаммирования и аналитического преобразования данных.

Критерии оценки устного ответа:

«5 (отлично)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, литературным языком: ответ самостоятельный.

«4 (хорошо)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки, исправленные по требованию преподавателя.

«3 (удовлетворительно)»: ответ полный, но при этом допущена существенная ошибка, или неполный, несвязный.

«2 (неудовлетворительно)»: при ответе обнаружено непонимание студентом основного содержания учебного материала или допущены существенные ошибки, которые студент не смог исправить при наводящих вопросах преподавателя.

Устный опрос на тему:
«Стандарты шифрования»

Вопросы:

1. История создания стандартов шифрования DES и RSA.
2. Алгоритм шифрования с использованием симметричного стандарта DES.
3. Алгоритм шифрования с использованием симметричного стандарта RSA.

Критерии оценки устного ответа:

«5 (отлично)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, литературным языком: ответ самостоятельный.

«4 (хорошо)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки, исправленные по требованию преподавателя.

«3 (удовлетворительно)»: ответ полный, но при этом допущена существенная ошибка, или неполный, несвязный.

«2 (неудовлетворительно)»: при ответе обнаружено непонимание студентом основного содержания учебного материала или допущены существенные ошибки, которые студент не смог исправить при наводящих вопросах преподавателя.

«Программная реализация криптографических алгоритмов»

1. Цель работы

Знакомство с основными методами криптографической зашиты информации.

2. Краткие теоретические сведения

Криптография – обеспечивает сокрытие смысла сообщения с помощью шифрования и открытия его расшифровкой, которые выполняются по специальным алгоритмам с помощью ключей.

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

Криптоанализ – занимается вскрытием шифра без знания ключа (проверка устойчивости шифра).

Кодирование – (не относится к криптографии) – система условных обозначений, применяемых при передаче информации. Применяется для увеличения качества передачи информации, сжатия информации и для уменьшения стоимости хранения и передачи.

Криптографические преобразования имеют цель обеспечить недоступность информации для лиц, не имеющих ключа, и поддержание с требуемой надежностью обнаружения несанкционированных искажений.

Большинство средств защиты информации базируется на использовании криптографических шифров и процедур шифрования-расшифровки. В соответствии со стандартом ГОСТ 28147-89 под **шифром** понимают совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом преобразования.

В криптографии используются следующие основные алгоритмы шифрования:

- алгоритм замены (подстановки) – символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены;
- алгоритм перестановки – символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста;
- гаммирование – символы шифруемого текста складываются с символами некоторой случайной последовательности;
- аналитическое преобразование – преобразование шифруемого текста по некоторому аналитическому правилу (формуле).

Процессы шифрования и расшифровки осуществляются в рамках некоторой криптосистемы. Для **симметричной** криптосистемы характерно применение одного и того же ключа как при шифровании, так и при расшифровке сообщений. В **асимметричных** криптосистемах для шифрования данных используется один (общедоступный) ключ, а для расшифровки – другой (секретный) ключ.

Симметричные криптосистемы

Шифры перестановки

В шифрах средних веков часто использовались таблицы, с помощью которых выполнялись простые процедуры шифрования, основанные на перестановке букв в сообщении. Ключом в данном случае является размеры таблицы. Например, сообщение “Неясное становится еще более непонятным” записывается в таблицу из 5 строк и 7 столбцов по столбцам:

Н	О	Н	С	Б	Н	Я
Е	Е	О	Я	О	Е	Т
Я	С	В	Е	Л	П	Н
С	Т	И	Щ	Е	О	Ы
Н	А	Т	Е	Е	Н	М

Для получения шифрованного сообщения текст считывается по строкам и группируется по 5 букв:

НОНСБ НЯЕЕО ЯОЕТЯ СВЕЛП НСТИЩ ЕОЫНА ТЕЕНМ

Несколько большей стойкостью к раскрытию обладает **метод одиночной перестановки** по ключу. Он отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы. Используя в качестве ключа слово «ЛУНАТИК», получим следующую таблицу:

Л	У	Н	А	Т	И	К
4	7	5	1	6	2	3
Н	О	Н	С	Б	Н	Я
Е	Е	О	Я	О	Е	Т
Я	С	В	Е	Л	П	Н
С	Т	И	Щ	Е	О	Ы
Н	А	Т	Е	Е	Н	М

До перестановки

А	И	К	Л	Н	Т	У
1	2	3	4	5	6	7
С	Н	Я	Н	Н	Б	О
Я	Е	Т	Е	О	О	Е
Е	П	Н	Я	В	Л	С
Щ	О	Ы	С	И	Е	Т
Е	Н	М	Н	Т	Е	А

После перестановки

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв ключа в алфавите. Если в ключе встретились бы одинаковые буквы, они бы нумеровались слева направо. Получается шифровка:

СНЯНН БОЯЕТ ЕООЕЕ ПНЯВЛ СЩОЫС ИЕТЕН МНТЕА

Для обеспечения дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов отличались от длин строк и столбцов первой таблицы. Лучше всего, если они будут взаимно простыми.

Кроме алгоритмов одиночных перестановок применяются **алгоритмы двойных перестановок**. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровке перестановки проводятся в обратном порядке. Например, сообщение “Приезжаю_шестого” можно зашифровать следующим образом:

	2	4	1	3			1	2	3	4			1	2	3	4
4	П	Р	И	Е		4	И	П	Е	Р		1	А	З	Ю	Ж
1	З	Ж	А	Ю		1	А	З	Ю	Ж		2	Е	_	С	Ш
2	_	Ш	Е	С		2	Е.	_	С	Ш		3	Г	Т	О	О
3	Т	О	Г	О		3	Г	Т	О	О		4	И	П	Е	Р

Двойная перестановка столбцов и строк

В результате перестановки получена шифровка АЗЮЖЕ_СШГТООИПЕР. Ключом к шифру служат номера столбцов 2413 и номера строк 4123 исходной таблицы.

Число вариантов двойной перестановки достаточно быстро возрастает с увеличением размера таблицы: для таблицы 3 х 3 их 36, для 4 х 4 их 576, а для 5*5 их 14400.

В средние века для шифрования применялись и **магические квадраты**. Магическими квадратами называются квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная с единицы, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Для шифрования необходимо вписать исходный текст по приведенной в квадрате нумерации и затем переписать содержимое таблицы по строкам. В результате получается шифротекст, сформированный благодаря перестановке букв исходного сообщения.

16	3	2	13			О	И	Р	Т
5	10	11	8			З	Ш	Е	Ю
9	6	7	12			_	Ж	А	С
4	15	14	1			Е	Г	О	П

П	Р	И	Е	З	Ж	А	Ю	_	Ш	Е	С	Т	О	Г	О
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Число магических квадратов очень резко возрастает с увеличением размера его сторон: для таблицы 3*3 таких квадратов -1; для таблицы 4*4 - 880; а для таблицы 5*5-250000.

Шифры простой замены

Система шифрования Цезаря - частный случай шифра простой замены. Метод основан на замене каждой буквы сообщения на другую букву того же алфавита, путем смещения от исходной буквы на K букв.

Известная фраза Юлия Цезаря VENI VINI VICI – пришел, увидел, победил, зашифрованная с помощью данного метода, преобразуется в SBKF SFAF SFZF (при смещении на 4 символа).

Греческим писателем Полибием за 100 лет до н.э. был изобретен так называемый **полибианский квадрат** размером 5*5, заполненный алфавитом в случайном порядке. Греческий алфавит имеет 24 буквы, а 25-м символом является пробел. Для шифрования на квадрате находили букву текста и записывали в шифротекст букву, расположенную ниже ее в том же столбце. Если буква оказывалась в нижней строке таблицы, то брали верхнюю букву из того же столбца.

Шифры сложной замены

Шифр Гронсфельда состоит в модификации шифра Цезаря числовым ключом. Для этого под буквами сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифротекст получают примерно также, как в шифре Цезаря, но отсчитывают не третью букву по алфавиту (как в шифре Цезаря), а ту, которая смещена по алфавиту на соответствующую цифру ключа.

Пусть в качестве ключа используется группа из трех цифр – 314, тогда

Сообщение: СОВЕРШЕННО СЕКРЕТНО

Ключ: 3143143143143143143

Шифровка: ФПИСЬИОССАХИЛФИУСС

В **шифрах многоалфавитной замены** для шифрования каждого символа исходного сообщения применяется свой шифр простой замены (свой алфавит):

	АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_
А	АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_
Б	_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ
В	Я_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮ
Г	ЮЯ_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭ
.	……
Я	ВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_АБ
_	БВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_А

Каждая строка в этой таблице соответствует одному шифру замены аналогично шифру Цезаря для алфавита, дополненного пробелом. При шифровании сообщения его выписывают в строку, а под ним ключ. Если ключ оказался короче сообщения, то его циклически повторяют. Шифротекст получают, находя символ в колонке таблицы по букве текста и строке, соответствующей букве ключа. Например, используя ключ АГАВА, из сообщения ПРИЕЗЖАЮ ШЕСТОГО получаем следующую шифровку:

Сообщение	ПРИЕЗЖАЮ_ШЕСТОГО
Ключ	АГАВААГАВААГАВАА
Шифровка	ПНИГЗЖЮЮЮАЕОТМГО

Гаммирование

Процесс шифрования заключается в генерации гаммы шифра и наложении этой гаммы на исходный открытый текст. Перед шифрованием открытые данные разбиваются на блоки $Т(0)_i$ одинаковой длины (по 64 бита). Гамма шифра вырабатывается в виде последовательности блоков $Г(ш)_i$ аналогичной длины ($Т(ш)_i=Г(ш)_i+Т(0)_i$, где + - побитовое сложение, i =1-m).

Процесс расшифровки сводится к повторной генерации шифра текста и наложение этой гаммы на зашифрованные данные $Т(0)_i=Г(ш)_i+Т(ш)_i$.

Асимметричные криптосистемы

Схема шифрования Эль Гамаля

Алгоритм шифрования Эль Гамаля основан на применении больших чисел для генерации открытого и закрытого ключа, криптостойкость же обусловлена сложностью вычисления дискретных логарифмов.

Последовательность действий пользователя:

1. Получатель сообщения выбирает два больших числа P и G, причем $P > G$.
2. Получатель выбирает секретный ключ - случайное целое число $X < P$.
3. Вычисляется открытый ключ $Y= G^x \bmod P$.
4. Получатель выбирает целое число K, 1< K< P-1.
5. Шифрование сообщения (M): $a= G^K \bmod P$, $b=Y^K M \bmod P$, где пара чисел (a,b) является шифротекстом.

Криптосистема шифрования данных RSA

Предложена в 1978 году авторами Rivest, Shamir и Aldeman и основана на трудности разложения больших целых чисел на простые сомножители.

Алгоритм создания открытого и секретного ключей:

1. Получатель выбирает 2 больших простых целых числа p и q, на основе которых вычисляет $n=p*q$ и функцию Эйлера $\varphi(n)=(p-1)(q-1)$.
2. Получатель выбирает целое число e ($1<e< \varphi(n)$), взаимно простое со значением функции $\varphi(n)$.

Пара чисел **(e,n)** публикуется в качестве **открытого ключа**.

3. Получатель вычисляет целое число d, которое отвечает условию: $e*d=1 (\bmod \varphi(n))$.

Пара чисел **(d,n)** является **секретным ключом**.

Шифрование сообщения с использованием открытого ключа:

Если m – сообщение (сообщениями являются целые числа в интервале от 0 до n-1), то зашифровать это сообщение можно как $\mathbf{c=m^e \bmod (n)}$.

Дешифрование сообщения с использованием секретного ключа:

Получатель расшифровывает, полученное сообщение c: $\mathbf{m=c^d \bmod (n)}$.

3. Задание

Практическая работа состоит из двух частей:

Часть 1 – применение одного из алгоритмов симметричного шифрования;

Часть 2 – шифрование с использованием алгоритма RSA.

Порядок выполнения работы:

Часть 1:

1. Используя один из алгоритмов симметричного шифрования (см. вариант), зашифровать свои данные: фамилию, имя, отчество.
2. Выполнить проверку, расшифровав полученное сообщение.

Часть 2:

1. Написать программу, реализующую алгоритм шифрования и дешифрования сообщения RSA. Входные данные: открытый и секретный ключи (значения n, e, d) и сообщение (m).
2. Используя заданные значения p, q, e, d (см. вариант) зашифровать и дешифровать сообщения m_1, m_2, m_3 (см. вариант).

4. Содержание отчета

1. Титульный лист
2. Содержание
3. Задание
4. Применение алгоритма симметричного шифрования
5. Применение алгоритма асимметричного шифрования
   5.1. Программа шифрования и дешифрования сообщения при помощи алгоритма RSA
   5.2. Результаты шифрования и дешифрования заданных сообщений
6. Выводы

Раздел 4. Проблема вирусного заражения программ

Ориентировочно-мотивационный этап.

Полученные знания являются основой для формирования ключевых компетенций, т.е. профессиональных навыков. Сегодня на занятии в рамках изучения этой темы решаем новую учебную задачу.

Для этого с целью создания более эффективных условий работаем в группах.

Вы как будущие специалисты, реализуя профессиональные компетенции, должны уметь обеспечить информационную безопасность вверенных вам объектов.

Одним из аспектов которой является защита компьютерной системы от вирусов и архивация данных.

Учебные задачи: **совершенствование знаний по компьютерным вирусам, определение признаков появления вирусов, их виды, установка средств антивирусной защиты.**

ВОПРОСЫ:

1. Понятие компьютерного вируса.

Что такое вирус в биологии вы знаете, а что такое компьютерный вирус?

Компьютерный вирус – специально написанная небольшая программа, способная к саморазмножению, засорению компьютера и выполнению других нежелательных действий.

2. Поисково-исследовательский этап.

Определив понятие компьютерного вируса и работая в группах, попробуем понять, как проявляются вирусы, классифицировать их и разобраться с программным обеспечение для защиты от вирусов, работой с архивацией данных.

Для каждой группы предложен кейс материалов по определенной части плана (опорный конспект, интернет источники, электронный учебник «Программное обеспечение» и учебное пособие «Информационные технологии в профессиональной деятельности»).

Заполнив выданный вам шаблон конспекта, вы сможете определить пути проявления вирусов, виды вирусов и средства антивирусной защиты, тем самым решая сформулированные нами учебные задачи. Каждая группа готовит 1 контрольный вопрос, по своей части материала.

Затем группа представляет результаты своей работы остальным, а они должны по ходу вашего выступления заполнить шаблоны, и ответить на вопросы.

3. Рефлексивно-оценочный этап.

Подведем ряд итогов, чтобы определить, как вы усвоили материал.

Как вы, будущие специалисты, реализуя, профессиональные компетенции, можете обеспечивать защиту компьютерной системы.

Мы должны знать:

- Что такое компьютерные вирусы.
- Типы компьютерных вирусов.
- Признаки проявления вирусов и пути проникновения в систему.
- Способы борьбы с компьютерными вирусами.

Интернет ресурсы.

1. http://informatika.sch880.ru/p16aa1.html
2. http://www.5byte.ru/10/0033.php
3. http://ddriver.ru/kms_catalog+stat+cat_id-10+page-1+nums-242.html
4. http://www.univer.omsk.su/omsk/Edu/infpro/1/13/virys2.html

Устный опрос на тему:
«Проблема вирусного заражения и структура современных вирусов»

Вопросы:

1. Компьютерный вирус: понятие, пути распространения, проявление действия вируса.
2. Структура современных вирусов: модели поведения вирусов;
3. Деструктивные действия вируса; разрушение программы защиты, схем контроля или изменение состояния программной среды;
4. Воздействия на программно-аппаратные средства защиты информации.
5. Программы-шпионы.
6. Взлом парольной защиты.
7. Защита от воздействия вирусов.

Критерии оценки устного ответа:

«5 (отлично)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, литературным языком: ответ самостоятельный.

«4 (хорошо)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки, исправленные по требованию преподавателя.

«3 (удовлетворительно)»: ответ полный, но при этом допущена существенная ошибка, или неполный, несвязный.

«2 (неудовлетворительно)»: при ответе обнаружено непонимание студентом основного содержания учебного материала или допущены существенные ошибки, которые студент не смог исправить при наводящих вопросах преподавателя.

Устный опрос на тему:
«Классификация антивирусных программ»

Вопросы:

1. Программы-детекторы.
2. Программы-доктора.
3. Программы-ревизоры.
4. Программы-фильтры.
5. Профилактика заражения вирусом.
6. Зашита информации в сетях.

Критерии оценки устного ответа:

«5 (отлично)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, литературным языком: ответ самостоятельный.

«4 (хорошо)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки, исправленные по требованию преподавателя.

«3 (удовлетворительно)»: ответ полный, но при этом допущена существенная ошибка, или неполный, несвязный.

«2 (неудовлетворительно)»: при ответе обнаружено непонимание студентом основного содержания учебного материала или допущены существенные ошибки, которые студент не смог исправить при наводящих вопросах преподавателя.

«Алгоритмы поведения вирусных и других вредоносных программ»

1. Цель работы

Знакомство с некоторыми алгоритмами поведения вирусных и других вредоносных программ.

2. Краткие теоретические сведения

Исторически первое определение компьютерного вируса было дано в 1984 г. Фредом Коэном: «Компьютерный вирус — это программа, которая может заражать другие программы, модифицируя их посредством включения в них своей, возможно измененной копии, причем последняя сохраняет способность к дальнейшему размножению». Ключевыми понятиями в этом определении являются *способность вируса к саморазмножению* и *способность к модификации вычислительного процесса*.

В настоящее время под компьютерным вирусом принято понимать программный код, обладающий следующими свойствами:

- способностью к созданию собственных копий, не обязательно совпадающих с оригиналом, но обладающих свойствами оригинала (самовоспроизведение);
- наличием механизма, обеспечивающего внедрение создаваемых копий в исполняемые объекты вычислительной системы.

Указанные свойства следует дополнить свойствами деструктивности и скрытности действий данной вредоносной программы в вычислительной среде.

Основной и наиболее распространенной классификацией компьютерных вирусов является классификация по *среде обитания*, или по *типам объектов* компьютерной системы, в которые внедряются вирусы. В соответствии с этой классификацией вирусы делятся на файловые, загрузочные, сетевые (черви) и макровирусы.

Существует также много комбинированных типов компьютерных вирусов.

Кроме вирусов принято выделять еще несколько видов вредоносных программ. Это троянские программы, логические бомбы, хакерские утилиты скрытого администрирования удаленных компьютеров, программы, ворующие пароли доступа к ресурсам Интернет и прочую конфиденциальную информацию. Четкого разделения между ними не существует: троянские программы могут содержать вирусы, в вирусы могут быть встроены логические бомбы и т. д.

3. Задание

Разработать программу имитирующую некоторые (см. вариант) действия вируса или другой вредоносной программы и подготовить отчет о проделанной работе.

4. Содержание отчета

1. Титульный лист
2. Содержание
3. Задание
4. Алгоритм работы программы
5. Листинг программы
6. Пример работы программы
7. Выводы

«Пакеты антивирусных программ»

1. Цель работы

Ознакомление с основными функциями, достоинствами и недостатками современного антивирусного ПО.

2. Краткие теоретические сведения

На сегодняшний день перечень доступных антивирусных программ весьма обширен. Они различаются как по цене, так и по своим функциональным возможностям. Наиболее мощные (и как правило, наиболее дорогие) антивирусные программы представляют собой на самом деле пакеты специализированных утилит, способных при совместном их использовании обеспечить разностороннюю защиту компьютерной системы.

Большинство современных антивирусных пакетов выполняют следующие функции:

- сканирование памяти и содержимого дисков;
- сканирование в реальном режиме времени с помощью резидентного модуля;
- распознавание поведения, характерного для компьютерных вирусов;
- блокировка и/или удаление выявленных вирусов;
- восстановление зараженных информационных объектов;
- принудительная проверка подключенных к корпоративной сети компьютеров;
- удаленное обновление антивирусного программного обеспечения и баз данных через Интернет;
- фильтрация трафика Интернета на предмет выявления вирусов в передаваемых программах и документах;
- выявление потенциально опасных Java-апплетов и модулей ActiveX;

– ведение протоколов, содержащих информацию о событиях, касающихся антивирусной защиты и др.

3. Задание

1. Подготовить краткий доклад по заданному вопросу (см. вариант), используя любые доступные источники информации.
   Рекомендация: Собранный материал будет наиболее актуальным, если включить в него данные, полученные практическим путем. Для этого при возможности, установите демонстрационную версию заданного пакета ПО и протестируйте ее в течении нескольких дней.
2. Заполнить таблицу " Пакеты антивирусных программ " на основе подготовленного материала, а также докладов других студентов.
3. Провести анализ собранной информации и сделать выводы.

4. Содержание отчета

1. Титульный лист
2. Содержание
3. Задание
4. Таблица "Пакеты антивирусных программ"
5. Выводы

Раздел 6. Организационно-правовое обеспечение информационной безопасности

Вопросы и задания:

1. Опыт законодательного регулирования информатизации в России и за рубежом.
2. Концепция правового обеспечения информационной безопасности Российской Федерации.
3. Стандарты и нормативно-методические документы в области обеспечения информационной безопасности.
4. Государственная система обеспечения информационной безопасности.
5. Международные правовые акты по защите информации.
6. Состав и назначение должностных инструкций.
7. Порядок создания, утверждения и исполнения должностных инструкций.

Тема: «Международные, российские и отраслевые правовые документы»

Сегодня без использования информационных систем невозможно представить деятельность любой современной организации. В связи с этим, вопросы обеспечения безопасности при обработке информации, являющейся собственностью организации, государства или его граждан, приобретают с каждым днем все большую актуальность. При построении системы информационной безопасности важно определить:

– Периметр ИТ-инфраструктуры, которую необходимо защищать

– Выделить информационные ресурсы в организации, которые являются наиболее критичными в отношении тех или иных угроз

– Критерии, которыми следует руководствоваться при оценке защищенности и состояния системы управления информационной безопасностью

– Учесть все угрозы и определить величину связанных с ними рисков

– Определить, как будет происходить управление рисками

– Оценить существующий уровень защищенности информационной системы организации и его достаточность

Для того, чтобы обеспечить адекватный уровень безопасности информационных ресурсов организации, необходим целый комплекс согласованных процессов организационного и технического характера. В целях управления этими процессами в организации должна быть построена и внедрена система управления информационной безопасностью (СУИБ). СУИБ является той необходимой основой, которая позволит повысить уровень информационной безопасности организации в целом и минимизировать риски и - в случае возникновения - возможный ущерб от возникновения компьютерных инцидентов.

Мы уже указывали, что для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих уровней:

– законодательного;

– административного (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами);

– процедурного (меры безопасности, ориентированные на людей);

– программно-технического.

Законодательный уровень является важнейшим для обеспечения информационной безопасности. Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается и/или наказывается обществом, потому, что так поступать не принято.

Мы будем различать на законодательном уровне две группы мер:

– меры, направленные на создание и поддержание в обществе негативного (в том числе с применением наказаний) отношения к нарушениям и нарушителям информационной безопасности (назовем их **мерами ограничительной направленности**);

– **направляющие и координирующие меры**, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности (меры созидательной направленности).

На практике обе группы мер важны в равной степени, но нам хотелось бы выделить аспект осознанного соблюдения норм и правил ИБ. Это важно для всех субъектов информационных отношений, поскольку рассчитывать только на защиту силами правоохранительных органов было бы наивно. Необходимо это и тем, в чьи обязанности входит наказывать нарушителей, поскольку обеспечить доказательность при расследовании и судебном разбирательстве компьютерных преступлений без специальной подготовки невозможно.

Самое важное (и, вероятно, самое трудное) на законодательном уровне – создать механизм, позволяющий согласовать процесс разработки законов с реалиями и прогрессом информационных технологий. Законы не могут опережать жизнь, но важно, чтобы отставание не было слишком большим, так как на практике, помимо прочих отрицательных моментов, это ведет к снижению информационной безопасности.

Концепция нормативно правового обеспечения информационной безопасности РФ

Настоящая Концепция разработана в целях согласования усилий всех субъектов законодательной инициативы, федеральных органов исполнительной власти, органов государственной власти субъектов Российской Федерации по совершенствованию и развитию нормативного правового обеспечения информационной безопасности Российской Федерации, а также федеральных органов исполнительной власти, осуществляющих подготовку проектов международных договоров Российской Федерации.

Концепция отражает совокупность официальных взглядов на состояние, цели, задачи, основные направления и первоочередные мероприятия по дальнейшему развитию системы правовых норм, регулирующих общественные отношения в области обеспечения информационной безопасности Российской Федерации.

Концепция служит основой при разработке: планов законодательной работы Президента Российской Федерации, Совета Федерации, членов Совета Федерации, депутатов Государственной Думы, Правительства Российской Федерации, а также Верховного Суда Российской Федерации и Высшего Арбитражного Суда Российской Федерации по предметам их ведения в области нормативного правового обеспечения информационной безопасности; планов законотворческой деятельности субъектов Российской Федерации в области формирования региональных систем обеспечения информационной безопасности; правовых доктрин регулирования отношений по отдельным вопросам нормативного правового обеспечения информационной безопасности Российской Федерации, а также концепций нормативных правовых актов, регулирующих отношения в области обеспечения информационной безопасности; планов подготовки проектов международных договоров Российской Федерации и нормативных правовых актов федеральных органов исполнительной власти в области обеспечения информационной безопасности Российской Федерации.

Согласно концепции - **информационная безопасность Российской Федерации** – это состояние защищенности национальных интересов Российской Федерации в информационной сфере.

Национальные интересы Российской Федерации в информационной сфере определяются, прежде всего, исходя из следующего:

информационная сфера играет ключевую роль в реализации многих конституционных прав и свобод граждан, в обеспечении возможности самореализации личности, духовном обновлении, политической и социальной стабильности общества, обеспечении функционирования государства и становится все более важным фактором развития экономики Российской Федерации и мировой экономики в целом; жизнедеятельность человеческого общества во все большей степени зависит от информационной сферы, которая, в связи с этим, все активней используется отдельными государствами, международными и национальными террористическими и преступными группами для оказания "силового" давления на государственную политику тех или иных стран.

Согласно концепции, обеспечение национальных интересов Российской Федерации в информационной сфере предполагает достижение следующих трех целей.

Первая цель – соблюдение конституционных прав и свобод граждан в области духовной жизни и информационной деятельности, обеспечение духовного возрождения России.

Вторая цель – развитие отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов.

Третья цель – обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

Защита национальных интересов Российской Федерации в информационной сфере от угроз внешнего и внутреннего характера составляет основное содержание деятельности по обеспечению информационной безопасности Российской Федерации.

Источники угроз подразделяются на внешние и внутренние.

К числу внешних источников угроз относятся: деятельность отдельных государств, международных террористических и других преступных сообществ, организаций и групп, направленная на ущемление национальных интересов Российской Федерации в информационной сфере; разработка и реализация рядом государств доктрин "информационных войн", предусматривающих создание средств воздействия на информационные инфраструктуры других стран мира, нарушения нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов или получения несанкционированного доступа к ним.

К числу внутренних источников угроз относятся: отставание России от ведущих государств мира в области создания и внедрения современных информационных технологий, развития индустрии информационных услуг и, как следствие, вынужденное широкое использование зарубежных программно-аппаратных средств при создании и развитии российской информационной инфраструктуры; ослабление влияния государства на жизнь общества и уменьшение экономических возможностей государства по защите законных интересов граждан, общества и государства в информационной сфере; недостаточно согласованная деятельность федеральных органов исполнительной власти по формированию и реализации единой государственной политики обеспечения информационной безопасности России; недостаточная эффективность экономических и социально-политических преобразований российского общества.

Вопросы для самоконтроля:

1. Что понимается под законодательным уровнем защиты информации?
2. В чем важность законодательных мер защиты информации?
3. Какие направления законодательных мер выделяют?
4. Что отражается в концепции нормативно правового обеспечения информационной безопасности РФ?
5. Что понимается под информационной безопасностью (согласно концепции нормативно правового обеспечения информационной безопасности РФ)?
6. Какие цели преследует концепция?

2.2 Задания для проведения экзамена

Форма экзамена – устный, по билетам.

Условия выполнения задания

1. Место выполнения: Задания выполняются в учебной аудитории, наличие компьютеров не является обязательным.
2. Максимальное время выполнения: - не более 60 мин.
3. Источники информации, разрешенные к использованию на экзамене: отсутствуют.

2.2.1 Перечень вопросов к экзамену

Теоретические вопросы

1. Основные понятия информационной безопасности. Цели и задачи защиты информации в информационно-вычислительных сетях.
2. Угрозы информационной безопасности. Угрозы доступности, целостности, конфиденциальности.
3. Основные технологии, использующиеся при совершении компьютерных преступлений.
4. Меры защиты информационной безопасности.
5. Виды угроз информационной безопасности.
6. Аппаратно-программные средства защиты информации.
7. Системы идентификации и аутентификации пользователей. Системы аутентификации электронных данных.
8. Криптография. Системы шифрования дисковых данных, в том числе передаваемых по сетям.
9. Средства управления криптографическими ключами.
10. Комплексный подход к защите информации. Защита от несанкционированного доступа.
11. Компьютерные вирусы. История развития компьютерных вирусов.
12. Классификация компьютерных вирусов.
13. Среда обитания компьютерных вирусов. Сетевые, загрузочные, файловые, комбинированные вирусы.
14. Деструктивные возможности вирусов.
15. Особенности алгоритмов компьютерных вирусов. Резидентные и нерезидентные вирусы, вирусы-спутники, вирусы-черви, «стелс»-вирусы, вирусы-«призраки», макровирусы.
16. Классификация антивирусных программ. «Вакцины», «Детекторы», «Ревизоры», «Сторожа», «Мониторы», «Полифаги», «Эвристические анализаторы».
17. Классификация угроз безопасности.
18. Каналы утечки информации. Электромагнитные, электрические, параметрические каналы.
19. Методы и средства блокирования каналов утечки информации.
20. Физические средства защиты информации, их классификация и выполняемые ими функции.
21. Средства и методы физической защиты.
22. Служба безопасности объекта. Права и обязанности сотрудников службы безопасности.
23. Методы защиты конфиденциальной информации.
24. Основы организационно-правового обеспечения информационной безопасности.
25. Защита коммерческой тайны и интеллектуальной собственности.

Практические задания

Задание 1.

Зашифровать фамилию и полное имя студента методом гаммирования. Под гаммированием понимают процесс наложения по определенному закону (чаще всего с использованием операции сложения по модулю 2) гаммы шифра на открытые данные. Гамма шифра – это псевдослучайная последовательность целых чисел, для генерации которых наиболее часто применяется так называемый линейный конгруэнтный генератор. Закон функционирования такого генератора описывается соотношением:

$$T_i = (T_{i-1} \cdot A + C) \bmod M \qquad (1)$$

где T_i – текущее число последовательности; T_{i-1} - предыдущее число последовательности; A, C и M – константы; M – модуль; A – множитель; C – приращение; T_0 – порождающее число.

Текущее псевдослучайное число T_i получают из предыдущего числа T_{i-1} умножением его на коэффициент A, сложением с приращением C и вычислением целочисленного остатка от деления на модуль M. Данное уравнение генерирует псевдослучайные числа с периодом повторения, который зависит от выбираемых значений параметров A, C и M. Значение модуля M берется равным 2^n, либо равным простому числу, например $M = 2^{31} - 1$. Приращение C должно быть взаимно простым с M, коэффициент A должен быть нечетным числом.

Вариант задания определяется в соответствии с табл. 1.

Таблица 1

Константа	Значение
T_0	7
A	9
C	Сумма двух последних цифр шифра
M	64

Шифрование текста методом гаммирования рекомендуется выполнять в следующей последовательности:

1. Определить константы шифрования по табл. 1.

2. Каждой букве шифруемого текста поставить в соответствие десятичное число по табл. 2.

Таблица 2

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	␣	
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	

2. Сгенерировать гамму шифра в соответствии с выражением (1).

3. Полученные числа (шифруемый текст и гамма шифра) перевести в двоичный. Замечание. Каждое число представляется байтом.

4. Наложить гамму шифра на шифруемый текст по формуле (2):

$$Ш_i = C_i \oplus T_i, \qquad (2)$$

где $Ш_i - i$ - ый символ шифрограммы, представленный в двоичном коде; $C_i - i$ - ый символ исходного текста, представленный в двоичном коде.

5. Полученную шифрограмму перевести в десятичный код и по табл. 2 получить текстовую форму шифрограммы. Замечание. В процессе выполнения операции сложение по модулю 2 могут получиться числа больше 32. В этом случае рекомендуется выполнить операцию $\bmod 32$. Однако при дешифровке необходимо использовать исходное число.

6. Выполнить проверку шифрования путем наложения гаммы шифра на шифрограмму.

Задание 2.

Зашифровать фамилию и полное имя студента по алгоритму RSA. Порождающие числа выбрать в соответствии с табл. 3. Причем число *p* выбирается по последней цифре шифра, а число *q* – по предпоследней цифре.

Таблица 3

Цифра	0	1	2	3	4	5	6	7	8	9
p	7	11	13	17	19	23	29	19	17	13
q	23	19	29	7	13	11	19	11	23	29

Замечание. Если числа *p* и *q* совпадают, то следует взять другое большее простое число.

Шифрование текста по алгоритму RSA рекомендуется выполнять в следующей последовательности:

1. Определить порождающие числа по табл. 3.
2. Каждой букве шифруемого текста поставить в соответствие десятичное число по табл. 2.
3. Вычислить произведение порождающих чисел $N = p \cdot q$.
4. Вычислить функцию Эйлера по формуле:

$$\varphi(n) = (p-1)\cdot(q-1)$$

5. Выбрать открытый ключ шифрования K_{OTK}, который должен удовлетворять следующим неравенствам:

$$1 < K_{OTK} < \varphi(n);$$
$$НОД(K_{OTK},\ \varphi(n)) \equiv 1$$

Значение K_{OTK} выбирается произвольным образом из указанного диапазона чисел, а наибольший общий делитель (НОД) K_{OTK} и функции Эйлера должен быть равен 1, т.е. эти два числа должны быть взаимно простыми. Так как порождающие числа с точки зрения криптографии ничтожно малы, то рекомендуется соблюдать два дополнительных условия: $K_{OTK} \neq p,\ K_{OTK} \neq q$.

6. Вычислить секретный ключ K_{CEK} по формуле:

$$K_{CEK} = K_{OTK}^{(\varphi(n)-1)} \bmod \varphi(n)$$

При вычислении K_{CEK} рекомендуется выполнить ряд последовательных умножений, выполняя каждый раз приведение по модулю. Например, необходимо вычислить 25 степень некоторого числа *a* по модулю *n*: $a^{25} \bmod n$. Представим степень 25 в виде целых степеней 2:

$$25 = 2^4 + 2^3 + 2^0.$$

Таким образом, нам необходимо вычислить 8 и 16 степени числа *a*. Для вычисления 8 степени воспользуемся выражением:

$$((a^2 \bmod n)^2 \bmod n)^2 \bmod n.$$

Для вычисления 16 степени, полученное на предыдущем шаге число необходимо возвести в квадрат и привести его по модулю.

7. Зашифровать исходный текст по формуле:

$$Ш_i = C_i^{K_{OTK}} \bmod N,$$

где $Ш_i$ – i - ый символ шифрограммы, представленный в десятичном коде; C_i – i - ый символ исходного текста, представленный в десятичном коде.

8. Выполнить проверку, дешифровав шифрограмму по формуле:

Оценка за выполнение практического задания выставляется:

«отлично» - если студент выполнил все этапы решения практического задания и получен верный ответ или иное требуемое представление результата работы;

«хорошо» - если студент выполнил задание полностью или большую его часть (свыше 85 %), но при выполнении обнаружились некоторые неточности в применении технологических моделей, приемов и алгоритмов в рамках поставленной задачи или работа выполнена полностью, но

использованы наименее оптимальные подходы к решению поставленной задачи;

«удовлетворительно» - если студент выполнил задание не полностью, допущено более трех ошибок, но студент владеет основными навыками работы, требуемыми для решения поставленной задачи;

«неудовлетворительно» - если студентом допущены существенные ошибки, показавшие, что он не владеет обязательными знаниями, умениями и навыками в применении технологических моделей и алгоритмов в решении поставленной задачи или значительная часть работы выполнена не самостоятельно.

2.2.2 Критерии оценивания

Оценка за теоретический вопрос выставляется:

«отлично» - если студент правильно, четко, аргументировано и в полном объеме изложил содержание теоретического вопроса, а также убедительно ответил на дополнительные вопросы;

«хорошо» - если студент правильно, но не достаточно полно изложил содержание теоретического вопроса, а также не точно ответил на дополнительные вопросы;

«удовлетворительно» - если студент изложил только основные моменты из теоретического вопроса;

«неудовлетворительно» - ответ не соответствует изложенным выше критериям.

Оценка за выполнение практического задания выставляется:

«отлично» - если студент выполнил все этапы решения практического задания и получен верный ответ или иное требуемое представление результата работы;

«хорошо» - если студент выполнил задание полностью или большую его часть (свыше 85 %), но при выполнении обнаружились некоторые неточности в применении технологических моделей, приемов и алгоритмов в рамках поставленной задачи или работа выполнена полностью, но использованы наименее оптимальные подходы к решению поставленной задачи;

«удовлетворительно» - если студент выполнил задание не полностью, допущено более трех ошибок, но студент владеет основными навыками работы, требуемыми для решения поставленной задачи;

«неудовлетворительно» - если студентом допущены существенные ошибки, показавшие, что он не владеет обязательными знаниями, умениями и навыками в применении технологических моделей и алгоритмов в решении поставленной задачи или значительная часть работы выполнена не самостоятельно.

Общая оценка выставляется:

«*отлично»* - если студент за выполнение практического задания оценен «отлично», а за теоретические вопросы – не ниже «хорошо»;

«*хорошо»* - если студент за выполнение практического задания оценен «хорошо», а за теоретические вопросы – не ниже «удовлетворительно»;

«удовлетворительно» - если студент за выполнение практического задания и теоретического вопроса оценен не ниже «удовлетворительно»;

«*неудовлетворительно»* - если студент за выполнение практического задания и ответа на теоретический вопрос оценен ниже «удовлетворительно».

2.2.3 Список литературы

№	Автор	Название	Издательство	Гриф издания	Год издания	Кол-во в библиотеке	Наличие на электронных носителях	Электронные уч. пособия
1	2	3	4	5	6	7	8	9
2.2.3 Основная литература								
2.2.3.1	Партыка Т.Л., Попов И.И.	Информационная безопасность. Учебное пособие	Москва: Издательство "ФОРУМ": ООО «Научно-издательский центр ИНФРА-М»		2018		http://znanium.com/go.php?id=915902	
2.2.3.2	Шаньгин В.Ф.	Информационная безопасность. Учебное пособие	Москва: Издательство "ФОРУМ": ООО «Научно-издательский центр ИНФРА-М»		2018		http://znanium.com/go.php?id=945331	
3.2.4 Дополнительная литература								
2.2.4.1	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации. Учебное пособие	Москва: Издательский Центр РИОР: ООО "Научно-издательский центр ИНФРА-М"		2018		http://znanium.com/go.php?id=957144	
2.2.4.1	Глинская Е.В., Чичварин Н.В.	Информационная безопасность конструкций ЭВМ и систем. Учебное пособие	Москва: ООО "Научно-издательский центр ИНФРА-М"		2018		http://znanium.com/go.php?id=925825	
2.2.5 Периодические издания								
2.2.5.1								
3.2.6 Практические (семинарские) и (или) лабораторные занятия								
2.2.6.1	В.А. Меркулов	Методические указания к выполнению практических работ						
2.2.7 Курсовая работа (проект)								
2.2.7.1								
2.2.8 Контрольные работы								
2.2.8.1								
2.2.9 Программно-информационное обеспечение, Интернет-ресурсы								
2.2.9.1		MS Windows 10 MS Office 2010 Kaspersky Internet Security						