МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой

ERP-систем и бизнес процессов
/Беккер Йорг
03.10.2018 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.ОД.6 Информационная безопасность современных корпоративных систем

1. Шифр и наименование направления подготовки / специальности:

01.04.02м Прикладная математика и информатика

2. Профиль подготовки / специализация/магистерская программа:

Математическое моделирование

3. Квалификация выпускника: магистр

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины:
ERP-систем и бизнес процессов

6. Составители программы:
Сафронов Виталий Владимирович, кандидат техн. наук, доцент

7. Рекомендована: НМС факультета прикладной математики, информатики и механики протокол от 11.10.18 № 2

8. Учебный год: 2018/2019 **Семестр(ы): 2**

9. **Цели и задачи учебной дисциплины:**

Цель дисциплины состоит в изучении и практическом освоении алгоритмов, методов, средств и механизмов защиты информации в распределенных автоматизированных системах и связанных математических моделей.

Задачи дисциплины, следующие:

- ознакомление с основными методами защиты данных в распределенных автоматизированных системах;

-приобретение навыков организации многоуровневой защиты корпоративных сетей.

10. Место учебной дисциплины в структуре ООП:

Дисциплина относится к вариативной части общенаучного цикла. Для изучения курса необходимы базовые знания по следующим дисциплинам: сети ЭВМ и телекоммуникации, программирование, теория вероятностей, информатика.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):

Компетенция		Планируемые результаты обучения
Код	Название	
ПК-3	Способность разрабатывать и применять математические методы, системное и прикладное программное обеспечение для решения задач научной и проектно-технологической деятельности	Знать: методы защиты информации, в том числе в распределенных вычислительных системах. Уметь: использовать типовые программные продукты, ориентированные на решение задач защиты информации в распределенных вычислительных системах. Владеть: методами и алгоритмами организации многоуровневой защиты информации в распределенных вычислительных системах.

12. Объем дисциплины в зачетных единицах/час.(*в соответствии с учебным планом)* **—** 2/72.

Форма промежуточной аттестации*(зачет/экзамен)* *зачет***.**

13. Виды учебной работы

Вид учебной работы	Трудоемкость	
	Всего	По семестрам
		№ семестра 3

Аудиторные занятия	30	30
в том числе: лекции	10	10
практические	10	10
лабораторные	10	10
Самостоятельная работа	42	42
Итого:	72	72
Форма промежуточной аттестации - зачет		

13.1. Содержание разделов дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
		1. Лекции
1.1	Введение в защиту информации.	Классификация угроз безопасности. Уязвимости информационной системы. Угрозы непосредственного доступа в операционную среду информационной системы. Угрозы безопасности межсетевого и прикладного уровня. Стандарты в области защиты информации.
1.2	Принципы построения систем защиты информации.	Организационные, физические, программно-аппаратные средства защиты. Многоуровневая защита распределенных вычислительных систем.
1.3	Основы криптографии.	Общие сведения. Подстановки. Метод перестановки. Одноразовые блокноты. Основные принципы криптографии. Алгоритмы с симметричным криптографическим ключом. Понятие об алгоритмах с симметричным криптографическим ключом. Изучение реализации на примере шифра DES. Улучшенный стандарт шифрования AES. Сертификаты. Пример сертификата X.509.Инфраструктуры систем с открытыми ключами. Каталоги. Аннулирование сертификатов.
		2. Практические занятия
2.1	Реализация методов защиты информации в современных распределенных системах.	Защита корпоративных сетей. Обзор средств защиты информации в системах с распределенной обработкой. Модели безопасности основных операционных систем. Алгоритмы аутентификации пользователей. Аутентификация пользователей при удаленном доступе. Протоколы удаленного доступа пользователя к компьютерной системе. Методы и средства защиты информации в сети. Технология виртуализации. Обеспечение безопасности в облачных платформах. Безопасность Облачных платформ. Интернет вещей, мобильные и носимые устройства. Big Data.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабора-торные	Самостоятельная работа	Всего
1	Введение в защиту информации.	4	4	4	12	24
2	Принципы построения систем защиты информации.	2	2	2	10	16
3	Основы криптографии.	2	2	2	10	16

4	Реализация методов защиты информации в современных распределенных системах.	2	2	2	10	16
	Итого:	10	10	10	42	72

14. Методические указания для обучающихся по освоению дисциплины

(рекомендации обучающимся по освоению дисциплины: работа с конспектами лекций, презентационным материалом, выполнение практических заданий, тестов, заданий текущей аттестации и т.д.)

В рамках общего объема часов, отведенных для изучения дисциплины, предусматривается выполнение следующих видов самостоятельных работ студентов (СРС): изучение теоретического материала, представленного в лекциях, основной и дополнительной рекомендуемой литературе, систематическая подготовка к практическим занятиям, итоговое повторение теоретического материала. Для самостоятельного изучения дисциплины выносится часть материала по темам 1-4 дисциплины с возможностью консультации у преподавателя общим объемом 42 часов СРС.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)

а) основная литература:

№ п/п	Источник
1	Бройдо В.Л. Вычислительные системы, сети и телекоммуникации: учеб. пособие. – СПб.: Питер, 2005.
2	Хорев П.В. Методы и средства защиты информации в компьютерных системах: учебное пособие. – М.: Издательский центр «Академия». Рекомендовано УМО вузов по университетскому политехническому образованию в качестве учебного пособия для студентов вузов. 2005.
3	Кравец О.Я., Гараев Р.А. Сети ЭВМ и телекоммуникации: современные технологии: учеб. пособие. - Уфа: ГОУВПО "Уфимский государственный авиационный технический университет" Рекомендовано УМО по университетскому политехническому образованию в качестве учебного пособия для студентов вузов, 2004

б) дополнительная литература:

№ п/п	Источник
4	Пятибратов А.П., Гудыно Л.П., Кириченко А.А. Вычислительные системы, сети и телекоммуникации. – М.: Финансы и статистика, 2003.
5	Корнеев В.В. Вычислительные системы. – М.: Гелиос АРВ, 2004.
6	Хорафас Д.Н. Системы и моделирование / Д.Н.Хорафас. – М.: Мир, 2001. – 320 с.
7	Мельников В.В. Безопасность информации в автоматизированных системах. М.: Финансы и статистика, 2003.

в) информационные электронно-образовательные ресурсы:

№ п/п	Ресурсы Интернет
8	*http://www.computer-museum.ru/* -Виртуальный компьютерный музей
9	*http://www.parallel.ru/history - История параллельных и высокопроизводительных вычислений*

16. Учебно-методическое обеспечение для организации самостоятельной работы

№ п/п	Источник

1	*http://www.koob.ru/ribnikov/method_mathematics/* Рыбников К.А. Введение в методологию математики

17. Информационные технологии, используемые для реализации учебной дисциплины, включая программное обеспечение и информационно-справочные системы (при необходимости)

Microsoft PowerPoint, для выполнения практических занятий и лабораторных работ необходимы пакеты программ MSVisualStudio, VirtualBox, WireShark, NMap.

18. Материально-техническое обеспечение дисциплины:

Лекционная аудитория оснащена специальной мебелью современным компьютером с подключенным к нему проектором и настенным экраном.

Лаборатория оснащена современными компьютерами с установленным программным обеспечением, позволяющим выполнять: решение задач аудита и моделирования сетевой инфраструктуры; моделирование и анализ криптографических алгоритмов; проводить виртуальное моделирование стрессоустойчивости (отказоустойчивости) различных ОС в рамках сетевой инфраструктуры; проводить виртуализированное построение моделей инфраструктуры и информационных систем для дальнейшего конфигурирования с применением распределённой модели сетевой безопасности инфраструктуры.

Аудитория для проведения практических занятий современными компьютерами с установленным программным обеспечением, позволяющим выполнять: анализ моделей защиты корпоративных сетей; анализировать модели безопасности основных операционных систем; выполнять тестирование и моделирование алгоритмов аутентификации пользователей.

19. Фонд оценочных средств:

19.1. Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции (или ее части)	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы (темы) дисциплины или модуля и их наименование)	ФОС* (средства оценивания)
ПК-3 Способность разрабатывать и применять математические методы, системное и прикладное программное обеспечение для решения задач научной и проектно-технологической деятельности	Знать: методы защиты информации, в том числе в распределенных вычислительных системах.	Раздел 1.1. Введение в защиту информации.	Подготовка доклада
	Уметь: использовать типовые программные продукты, ориентированные на решение задач защиты информации в распределенных вычислительных системах.	Разделы 1.2-1.3 Принципы построения систем защиты информации.	Устный опрос

	Владеть: методами и алгоритмами организации многоуровневой защиты информации в распределенных вычислительных системах.	Раздел 2.1. Реализация методов защиты информации в современных распределенных системах.	Устный опрос
Промежуточная аттестация - зачет			

19.2. Описание критериев и шкалы оценивания компетенций (результатов обучения) при промежуточной аттестации

Компетенция	Показатель сформированности компетенции	Шкала и критерии оценивания уровня освоения компетенции			
		5	4	3	2
ПК-3 Способность разрабатывать и применять математические методы, системное и прикладное программное обеспечение для решения задач научной и проектно-технологической деятельности	Знает основные методы защиты информации, в том числе в распределенных вычислительных системах.	Сформированные знания об методах защиты информации, в том числе в распределенных вычислительных системах.	Сформированные, но содержащие отдельные пробелы представления об основных методах защиты информации, в том числе в распределенных вычислительных системах.	Неполное представление об основных методах защиты информации, в том числе в распределенных вычислительных системах.	Фрагментарные знания или отсутствие знаний
	Умеет использовать типовые программные продукты, ориентированные на решение задач защиты информации в распределенных вычислительных системах.	Сформированное умение применять типовые программные продукты, ориентированные на решение задач защиты информации в распределенных вычислительных системах.	Успешное, но содержащее отдельные пробелы умение применять типовые программные продукты, ориентированные на решение задач защиты информации в распределенных вычислительных системах.	Успешное, но не системное умение применять типовые программные продукты, ориентированные на решение задач защиты информации в распределенных вычислительных системах.	Фрагментарные умения или отсутствие умений

Промежуточная аттестация включает в себя теоретические вопросы, позволяющие оценить уровень полученных знаний.

При оценивании используется следующая шкала:

5 баллов ставится, если обучающийся демонстрирует полное соответствие знаний, умений, навыков приведенным в таблицах показателям, свободно оперирует приобретенными знаниями, умениями, применяет их при решении практических задач, при тестировании из 20 вопросов дан верный ответ не менее чем на 18;

4 балла ставится, если обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач, при тестировании из 20 вопросов дан верный ответ не менее чем на 14;

3 балла ставится, если обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач, при тестировании из 20 вопросов дан верный ответ не менее чем на 12;

2 балла ставится, если обучающийся демонстрирует явное несоответствие знаний, умений, навыков приведенным в таблицах показателям, при тестировании из 20 вопросов дан верный ответ на менее 10 вопросов.

При сдаче зачета
«зачтено» - 3-5 баллов
«не зачтено» - 2 балла.

19.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы.

19.3.1 Перечень вопросов к зачету

1. Классификация угроз безопасности по виду защищаемой от угроз безопасности информации.
2. Классификация угроз безопасности по способу реализации угрозы безопасности.
3. Классификация угроз безопасности по типу информационных систем
4. Классификация уязвимостей программного обеспечения.
5. Примеры уязвимостей протоколов стека протоколов TCP/IP.
6. Общая характеристика угроз безопасности, реализуемых с использованием протоколов межсетевого взаимодействия.
7. Угрозы типа «Анализ сетевого траффика», «Сканирование сети», «Выявление пароля».
8. Угрозы типа «Подмена доверенного объекта сети», «Навязывание ложного маршрута».
9. Угрозы типа «Внедрение ложного объекта», «Отказ в обслуживании», «Удаленный запуск приложений»
10. Метод подстановок и перестановок в криптографии
11. Основные принципы криптографии . Одноразовые блокноты.
12. Алгоритмы с симметричным криптографическим ключом.
13. Тройное шифрование с помощью DES. Улучшенный стандарт шифрования AES.
14. Алгоритм Rijndael.
15. Режим шифрованной обратной связи
16. Режим группового шифра
17. Режим счетчика
18. Криптоанализ
19. Алгоритмы с открытым ключом
20. Алгоритм RSA
21. Криптоанализ алгоритма RSA
22. Цифровые подписи.
23. Подписи с открытым ключом
24. Профили сообщений
25. Подпись MD5
26. Подпись SHA-1
27. 2.24. Сертификаты. X.509
28. Инфраструктуры систем с открытыми ключами.
29. Каталоги. Аннулирование
30. IPV4, IPsec.
31. Брандмауэры
32. Виртуальные частные сети
33. Безопасность в беспроводных сетях
34. Безопасность в сетях 802.11

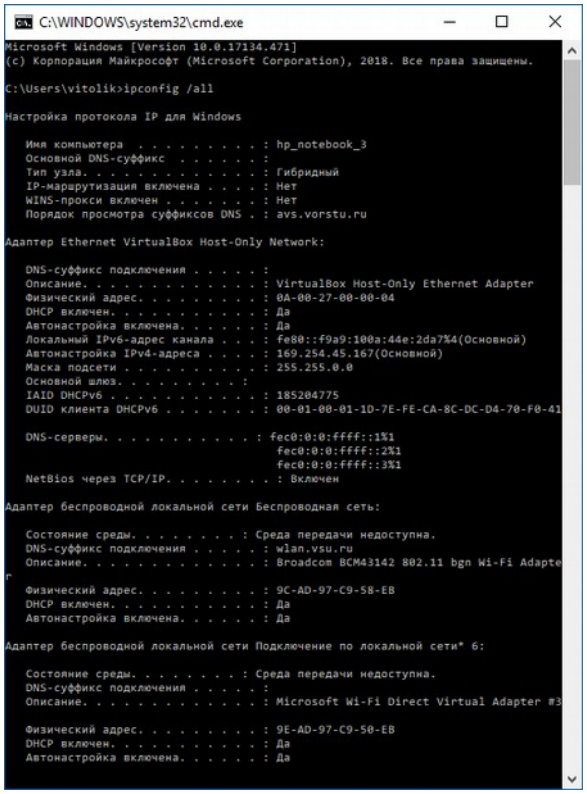
35. Безопасность в системах Bluetooth
36. Протоколы аутентификации

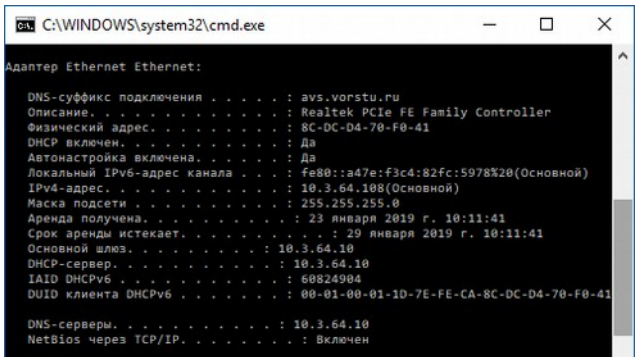
19.3.2 Перечень практических заданий к зачету

Пример задания 1. Используя встроенные средства сетевого аудита MS Windows провести первичный анализ сетевых интерфейсов.

Решение:

Используем команду ipconfig с параметром /all реализующей вывод полной информации по доступным на ПК сетевым интерфейсам с описанием их конфигурации. Результат работы команды приведён ниже.

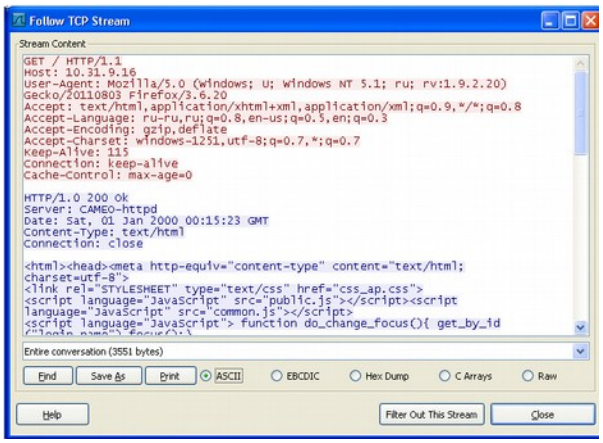




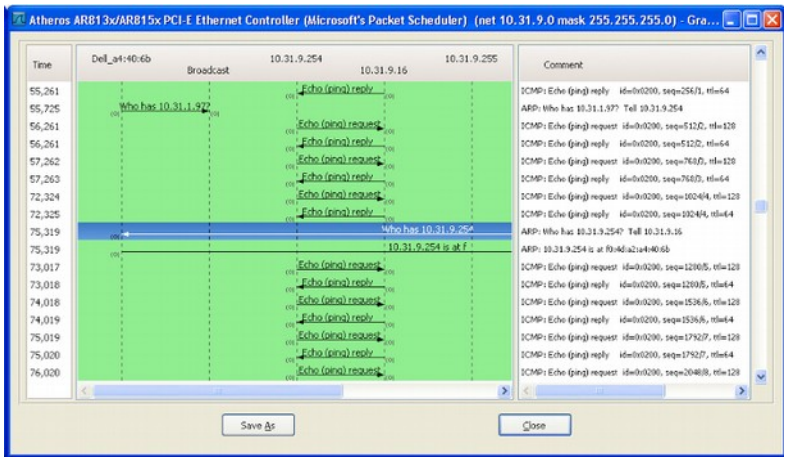
Пример задания 2. Исследовать структуру TCP/IP пакетов с помощью программы сетевого аудита.

Решение:

На примере программы WireShark.

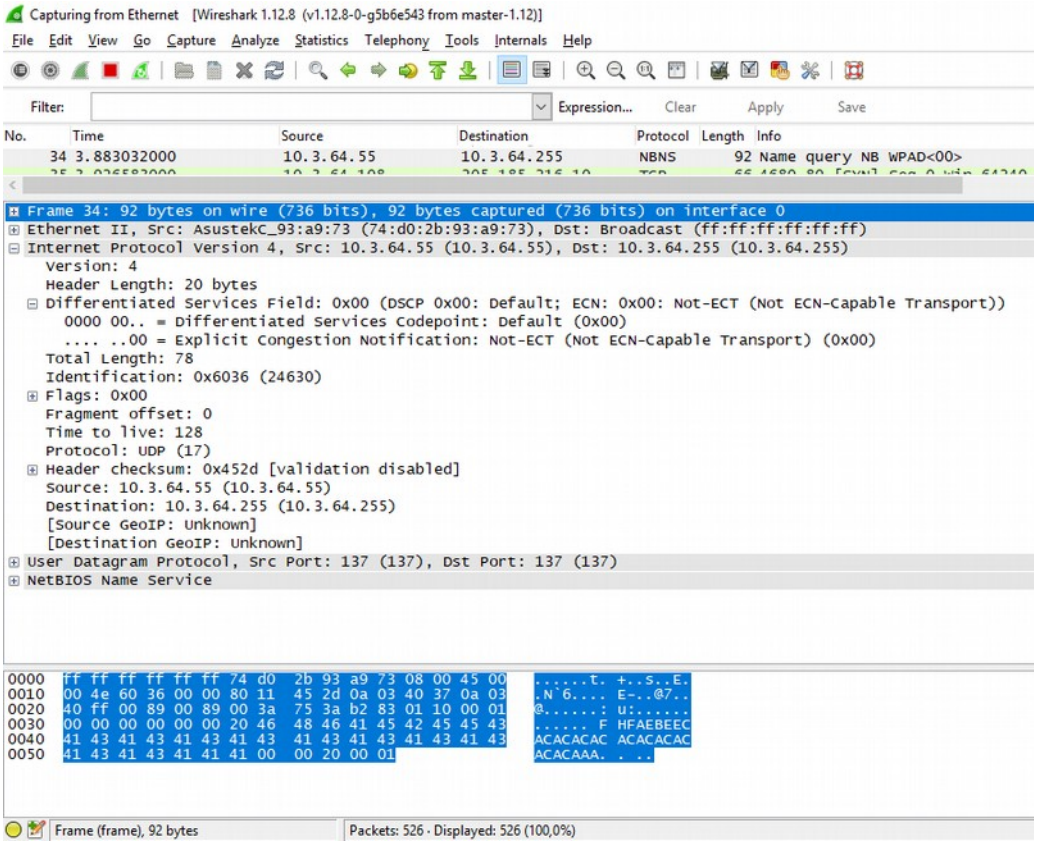


Результат выполнения «Follow TCP Stream», извлеченные данные прикладного протокола из TCP-сегментов потока.



Графическая визуализация пакетов данных в Wireshark доступных к анализу в рамках заданного сетевого интерфейса.

Окно быстрого (предварительного) анализа заданного пакета.

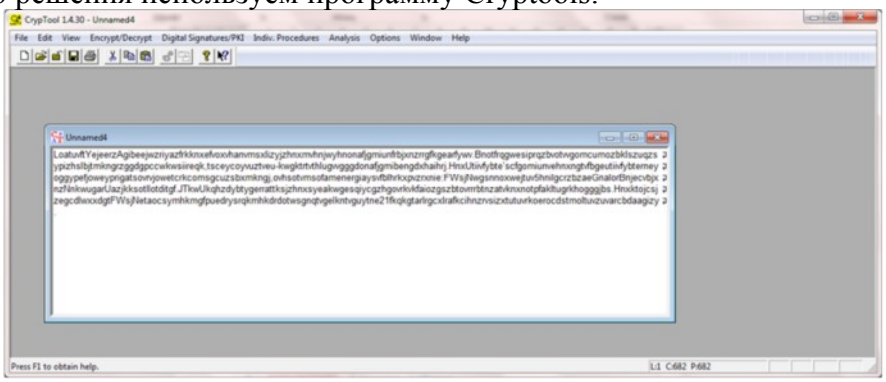


Пример задания 3. Используя средства криптографического моделирования и анализа выполните дешифрацию входного сообщения.

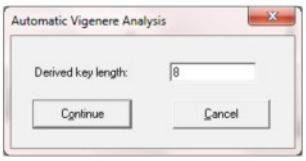
LoatuvftYejeerzAgibeejwzriyazfrkknxefvoxvhanvmsxlizyjzhnxmvhnjwyhnonafjgmiunfrbjxnzrrgfkg earfywv.Bnotfrqgwesiprqzbvotvvgomcumozbklszuqzsypizhslbjtmkngrzggdgpccwkwsiireqk,tsceyc oyvuztveukwgktrtvthlugvvgggdonafjgmibengdxhaihrj.HnxUtiivfybte'scfgomiunvehnxngtvfbgeutii vfybterneyoggypefjoweyprigatsovrvjowetcrkcomsgcuzsbxmkngj,ovhsotvmsofamenergiaysvfblhrk xpvzrxnie:FWsjNwgsnnoxwejtuv5hnilgcrzbzaeGnalorBnjecvbjxnzNnkwugarUazjkksotlIotditgf.J TkwUkqhzdybtygerrattksjzhnxsyeakwgesqiycgzhgovrkvkfaiozgszbtovrrrbtnzatvknxnotpfakltugrkh

ogggjbs.HnxktojcsjzegcdlwxxdgtFWsjNetaocsymhkmgfpuedrysrqkmhkdrdotwsgnqtvgelkntvguytn e21fkqkgtarlrgcxlrafkcihnzrvsizxtutuvrkoerocdstmoltuvzuvarcbdaagizy.

Решение:
Для быстрого решения используем программу Cryptools:

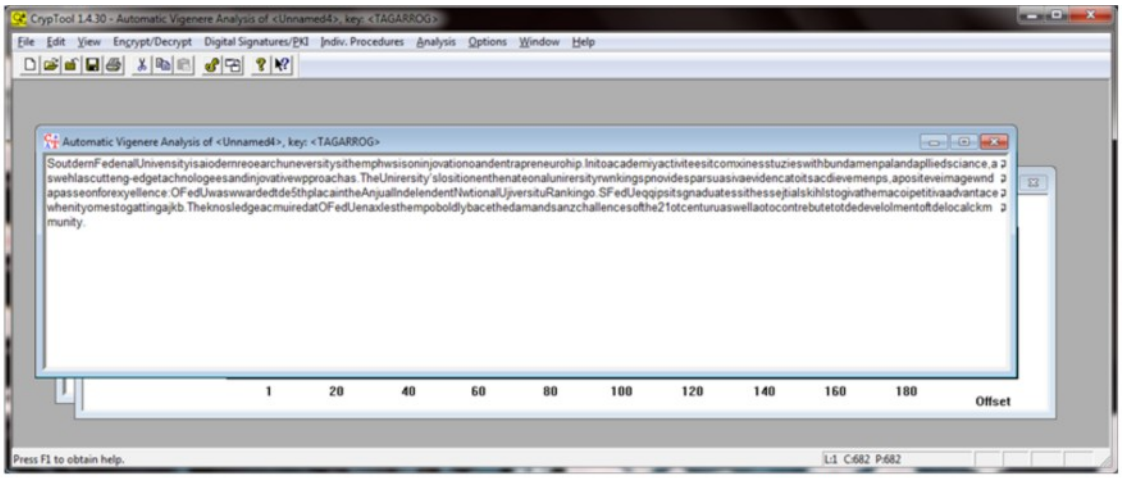


Выбираем вкладку Analysis> Symmetric encryption (classic)> Ciphertext-only> Vigenere.
Далее программа находит длину ключа:



Жмём> Continue, далее находит сам ключ:

Жмём> Decrypt, и получаем расшифрованный текст:



19.3.4 Тестовые задания

1. Дополните

… представляют собой совокупность информационных и программно-аппаратных элементов, а также информационных технологий, применяемых при обработке данных.
+Вычислительные системы.

2. Дополните
…– это физическая среда, по которой информативный сигнал может распространяться и приниматься (регистрироваться) приемником.
+Среда распространения информативного сигнала
+Среда распространения информационного сигнала

3. Дополните
NMap – это …
+ Сетевой сканер.

4. Отметьте правильный ответ
... – это сетевой сканер.
+ NMap
- WireShark
-VirtualBox
-Linux

5. Дополните
Уязвимость … – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении, которые могут быть использованы для реализации угрозы безопасности данным.
+Информационной системы

6. Отметьте правильный ответ
Атака типа UPD-шторм используется в том случае, если на жертве открыт как минимум
1 порт
+2 порта
3 порта
4 порта
5 портов

7. Отметьте правильный ответ
Угроза типа «Анализ сетевого траффика» реализуется с помощью специальной …
+ программы-анализатора пакетов
- утилиты межсетевого взаимодействия
- операционной системы
- СУБД

8. Отметьте правильный ответ
... – это программа-анализатор пакетов.
- NMap
+ WireShark
-VirtualBox
-Linux

9. Отметьте правильный ответ
Подмена доверенного объекта сети реализуется в системах, где применяются … алгоритмы идентификации и аутентификации хостов, пользователей
+Нестойкие
-Стойкие
-Полиморфные
-Инкапсулированные
-Распределенные

10. Отметьте правильный ответ
Внедрение ложного объекта возможно через протокол

+ARP
-FTP
-POP3
-IMAP
-SMTP

11. Дополните

… - это угрозы основаны на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступающие пакеты.

+Отказ в обслуживании

12. Отметьте правильный ответ

Вирус Морриса – это пример реализации угрозы

+Удаленного запуска приложений
-Навязывание ложного маршрута
-Отказ в обслуживании
-Внедрение ложного объекта

13. Отметьте правильный ответ

Слово криптография происходит от греческих слов, означающих

+ «скрытное письмо»
- «скрытный шифр»
-«скрытная весть»
-«тайное сообщение»
-«скрытное сообщение»

14. Дополните

… представляет собой посимвольное или побитовое преобразование, не зависящее от лингвистической структуры сообщения.

+Шифр

15. Отметьте правильный ответ

Искусства изобретать шифры и взламывать их называются вместе …

-криптография
+криптологией
-криптоанализ
-криптофилия
-криптомания.

16. Дополните

Шифр Цезаря основан на методе …

+ подстановок.

17. Дополните

Шифры, использующие метод …, меняют порядок следования символов, но не изменяют сами символы.

+ перестановки

18. Отметьте правильный ответ

S и P блоки отвечают за…

+подстановки и перестановки
-перестановки и подстановки
-перестановки и инверсии
-подстановки и инверсии

19. Отметьте правильный ответ

Размер блока шифрования в исходном алгоритме DES равен … битам

-16
-32
+64
-128

-256

20. Отметьте правильный ответ

Размер ключа шифрования в исходном алгоритме DES равен … битам

-16

-32

-55

+56

-64

21. Дополните

Необходимым условием осуществления просмотра (регистрации) данных из информационной системы является наличие … между средством наблюдения и носителем данных.

+ прямой видимости

22. Дополните

… - эта угроза основана на использовании недостатков алгоритмов удаленного поиска. В случае, если объекты сети изначально не имеют адресной информации друг о друге, используются различные протоколы удаленного поиска (например, SAP в сетях Novell NetWare; ARP, DNS, WINS в сетях со стеком протоколов TCP/IP), заключающиеся в передаче по сети специальных запросов и получении на них ответов с искомой информацией.

+Внедрение ложного объекта сети

23. Отметьте правильный ответ

Реализация данной угрозы основывается на несанкционированном использовании протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP) для внесения изменений в маршрутно-адресные таблицы.

-сканирование сети

-угроза выявления пароля

-анализ сетевого трафика

+навязывание ложного маршрута

24. Дополните

Анализ сетевого трафика - эта угроза реализуется с помощью специальной программы-...

+анализатора пакетов, сниффера, sniffer.

25. Дополните

UDP-шторм – это пример реализации угрозы …

+Отказ в обслуживании.

26. Дополните

… - данная угроза заключается в стремлении запустить на хосте информационной системы различные предварительно внедренные вредоносные программы.

+Удаленный запуск приложений

27. Дополните

Один из основных принципов криптографии - сообщения должны содержать … данные.

+избыточные

28. Дополните

Один из основных принципов криптографии - необходим способ борьбы с … посланных ранее сообщений.

+повторной отправкой

29. Отметьте правильный ответ

Для работы алгоритма RSA на начальном этапе выбирают

+ два простых числа

- два составных числа

- два мнимых числа
- два взаимно простых числа

30. Дополните

Решение задачи о … числа за полиномиальное время приведет к вскрытию алгоритма RSA.

+факторизации

31. Отметьте правильный вариант

Какая длинна ключа считается надежной для алгоритма RSA?

-128

-256

-768

+1024

32. Дополните

33. Вычисление MD-5 сообщения – это подсчет …-функции сообщения.

+хэш

34. Дополните

Основная задача сертификата состоит в связывании … с именем его обладателя.

+открытого ключа

35. Дополните

Протокол безопасности уровня передачи данных под названием WEP применяется в стандарте …

+802.11

36. Дополните

… — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

+Межсетевой экран, +сетевой экран, +файервол, +брандмауэр

37. Дополните

… - стандартная утилита конфигурирования сетевого экрана в ОС Linux.

+iptables

38. Дополните

X.509 – это стандарт для описания …

+ сертификатов.

39. Дополните

… - технология, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет).

VPN, Virtual Private Networt, Виртуальная частная сеть

40. Дополните

Для шифрации в протоколе Bluetooth используется потоковый шифр …

+E0

41. Дополните

Основное правило криптографии состоит в предположении, что криптоаналитику (взломщику кода) известен используемый

+ метод шифрования.

42. Дополните

С математической точки зрения, алгоритм Rijndael (AES) основывается на теории …

полей Галуа

43. Дополните

Шифрация при помощи WEP использует потоковый шифр, основанный на алгоритме …

+RC4

44. Дополните

… - процесс распознавания сущностей путем присвоения им уникальных меток (идентификаторов, логинов).

Идентификация

45. Дополните

… - проверка соответствия (подлинности) сущности предъявленному ею идентификатору.

Аутентификация

46. Отметьте правильный ответ

С каким типом атаки не может справиться брандмауэр

+DDOS

-Сканирование портов

-UDP-шторм

47. Отметьте правильный ответ

Если E – алгоритм, шифрации, D – алгоритм дешифрации, а P – сообщение, то каким из свойств обладает алгоритм RSA?

-E(E(D(P))) = P

-D(P) = E(P)

+E(D(P)) = P

-D(E(D(P)))) = E(P)

48. Отметьте правильный ответ

Если E – алгоритм, шифрации, D – алгоритм дешифрации, а P – сообщение, то каким из свойств обладает алгоритм с открытым ключем?

-E(D(P)) = P

+D(E(P)) = P

-E(E(D(P))) = P

-D(E(D(P)))) = E(P)

49. Отметьте правильный ответ

С блоками какой разрядности работает алгоритм SHA-1?

-64 бит

-128 бит

-256 бит

+512 бит

-1024 бит

50. Отметьте правильный ответ

Набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP носит название

-IPS

+IPsec

-IPC

-IPCrypt

-IPEnc

19.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в форме ответа на теоретический вопрос и решение прикладной (практической) задачи с использованием ПК. На зачёте учитываются результаты защиты курсовой работы. Допуском к зачету является наличие сданной контрольной работы и пройденное тестирование.