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

УТВЕРЖДАЮ

декан факультета прикладной
математики, информатики
и механики
А.И. Шашкин
24.06.2021

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.08 Информационная безопасность и защита информации

1. Код и наименование направления подготовки / специальности:

09.04.03 Прикладная информатика

2. Профиль подготовки / специализация/магистерская программа:

Прикладная информатика в социальных и медицинских системах

3. Квалификация (степень) выпускника: магистр

4. Форма обучения: очная

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

6. Составители программы: Сафронов В. В., кандидат технических наук, доцент кафедры ERP-систем и бизнес процессов

7. Рекомендована: НМС факультета Прикладной математики, информатики и механики № 10 от 15.06.2021

8. Учебный год: 2021/2022 **Семестр(ы):** 1

9. **Цели и задачи учебной дисциплины**

Целями освоения учебной дисциплины являются:
формирование целостного представления об информационной безопасности и защите данных, получение теоретических и практических знаний, позволяющих осуществлять разработку алгоритмов и компьютерных программ с учетом основных требований информационной безопасности.

Задачи учебной дисциплины:

– изучение основ технологий обеспечения информационной безопасности;

– изучение методологий проектирования и реализации системы защиты информации, с учетом угроз, характерных для современных интернет/интранет-сетей;

– получение знаний и умений, необходимых для разработки программного и информационного обеспечения компьютерных сетей, автоматизированных систем, сервисов, операционных систем и баз данных с учетом основных требований информационной безопасности

– получение знаний, необходимых для эксплуатации программ и программных комплексов в области информационной безопасности при решении задач профессиональной деятельности.

10. Место учебной дисциплины в структуре ОПОП: дисциплина относится к обязательной части блока Б1 дисциплин учебного плана.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения

Код	Название компетенции	Код(ы)	Индикаторы(ы)	Планируемые результаты обучения
ОПК-4	Способен применять на практике новые научные принципы и методы исследований;	ОПК-4.1	Демонстрирует владение принципами создания информационных систем различного назначения с использованием новых научных методов и принципов	Знать: основы информационной безопасности и защиты информации; основы использования программных решений в области анализа архитектуры предприятия; основные принципы построения информационных систем с использованием средств защиты информации. Уметь: проводить сравнительный анализ систем защиты информации; применять системное и прикладное программное обеспечение при создании информационных систем и анализе существующих; использовать современные вычислительные системы в составе компьютерных сетей с обеспечением защиты информации. Владеть навыками: разработки алгоритмов, вычислительных моделей,
		ОПК-4.2	Использует на практике новые научные принципы и методы исследования в области информационной безопасности и защиты информации	

				проектирования базы данных для реализации функций и сервисов систем информационных технологий; построения систем высокой готовности в составе распределённых вычислительных сетей с интеграцией облачных инфраструктур в компьютерную сеть с обеспечением защиты информации; методами внедрения системного и прикладного программного обеспечения в информационные системы; навыками решения стандартных задач защиты информации с учетом требований информационной безопасности.

12. Объем дисциплины в зачетных единицах/часах в соответствии с учебным планом —3/108.

Форма промежуточной аттестации - зачёт.

13. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоемкость (часы)				
	Всего	В том числе в интерактивной форме	По семестрам		
			№ сем. 1	№ сем.	…..
Аудиторные занятия					
в том числе: лекции	34		34		
практические	-		-		
лабораторные	16		16		
Самостоятельная работа	58		58		
Форма промежуточной аттестации	Зачёт		Зачёт		
Итого:	108		108		

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
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.	Информационная безопасность и защита информации (09.04.03)
1.2	Принципы	Организационные, физические, программно-аппаратные	

	построения систем защиты информации	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.	
1.4	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.	
2. Лабораторные занятия			
2.1	Введение в защиту информации	Сетевой аудит MS Windows. Сетевой аудит сетевой инфраструктуры	Информационная безопасность и защита информации (09.04.03)
2.2	Основы криптографии	Моделирование устойчивости криптографически преобразованного сообщения. Криптографические решения в информационных системах.	
2.3	.Реализация методов защиты информации в современных распределенных системах	Анализ безопасности сетевой инфраструктуры Аудит сетевой инфраструктуры информационных систем. Облачные технологии и решения виртуализации в информационных системах.	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1	Введение в защиту информации	8	-	8	4	20
2	Принципы построения систем защиты информации	8	-	-	14	22
3	Основы криптографии	8	-	8	10	26
4	Реализация методов защиты информации в современных распределенных системах	10	-	-	30	40
	Итого:	34	-	16	58	108

14. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины включает в себя лекционные и лабораторные занятия, самостоятельную работу обучающихся. На первом занятии студент получает информацию для доступа к комплексу учебно-методических материалов.

Лекционные занятия посвящены рассмотрению теоретических основ дисциплины.
Лабораторные занятия предназначены для формирования умений и навыков, закрепленных компетенциями по ОПОП. Самостоятельная работа студентов включает в себя проработку учебного материала лекций, разбор заданий лабораторных работ, подготовку к текущей аттестации и зачету.
Для успешного освоения дисциплины рекомендуется подробно конспектировать лекционный материал, просматривать конспекты лекций (презентации) по соответствующей теме.

При использовании дистанционных образовательных технологий и электронного обучения следует выполнять все указания преподавателя по работе на LMS-платформе, своевременно подключаться к online-занятиям, соблюдать рекомендации по организации самостоятельной работы.

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

а) основная литература:

№ п/п	Источник
1	Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2019. — 324 с. — Режим доступа://e.lanbook.com/book/114688
2	Ярочкин, В. И. Информационная безопасность : учебник / В. И. Ярочкин. — 5-е изд. — Москва : Академический Проект, 2020. — 544 с. — ISBN 978-5-8291-3031-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/132242

б) дополнительная литература:

№ п/п	Источник
3	Фот, Ю. Д. Стандарты информационной безопасности : учебное пособие / Ю. Д. Фот. — Оренбург : ОГУ, 2018. — 226 с. — ISBN 978-5-7410-2297-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/159804
4	Давидюк, Н. В. Мониторинг безопасности информационных систем : учебное пособие / Н. В. Давидюк, И. М. Космачева. — Санкт-Петербург : Интермедия, 2020. — 116 с. — ISBN 978-5-4383-0204-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/161352

в) информационные электронно-образовательные ресурсы**:**

№ п/п	Источник
5	Электронно-библиотечная система «Лань». - Режим доступа: https://e.lanbook.com.
6	Электронный каталог Научной библиотеки Воронежского государственного университета. – Режим доступа: http//:www.lib.vsu.ru.
7	Информационная безопасность и защита информации (09.04.03)/В.В. Сафронов — Образовательный портал «Электронный университет ВГУ». — Режим доступа: https://edu.vsu.ru

16. Перечень учебно-методического обеспечения для самостоятельной работы
Самостоятельная работа обучающегося должна включать в себя просмотр конспектов лекций, подготовку к лабораторным работам, подготовку к промежуточной аттестации. Для обеспечения самостоятельной работы студентов в электронном курсе дисциплины на образовательном портале «Электронный университет ВГУ» сформирован учебно-методический комплекс, который включает в себя: программу курса, учебные пособия и справочные материалы, методические указания по выполнению лабораторных работ. Студенты получают доступ к данным материалам на первом занятии по дисциплине.

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение):
Дисциплина реализуется с применением электронного обучения и дистанционных образовательных технологий, для организации самостоятельной работы обучающихся используется онлайн-курс, размещенный на платформе Электронного университета ВГУ (LMS moodle), а также другие Интернет-ресурсы, приведенные в п.15в.

18. Материально-техническое обеспечение дисциплины:

Лекции: лекционная аудитория, учебная мебель, компьютер (ноутбук), мультимедийное оборудование (проектор, экран, средства звуковоспроизведения).

Лабораторные занятия: специализированная аудитория, оснащенная учебной мебелью и персональными компьютерами для индивидуальной работы с возможностью подключения к сети «Интернет» (компьютерные классы, студии), мультимедийное оборудование (проектор, экран, средства звуковоспроизведения).

Самостоятельная работа: учебная мебель, компьютерный класс, компьютер с возможностью подключения к сети «Интернет» к платформе Электронного университета ВГУ (LMS moodle).

Программное обеспечение:
- ОС Windows 10, Linux (Debian, Mandriva и подобные), Unix (Debian Server и подобные),
- интернет-браузер (Mozilla Firefox),
- ПО VirtualBox,
- ПО Adobe Reader.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименования раздела дисциплины	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1	Введение в защиту информации.	ОПК-4	ОПК-4.1	Лабораторные работы, тест
2	Принципы построения систем защиты информации.	ОПК-4	ОПК-4.1	Тест
3	Основы криптографии.	ОПК-4	ОПК-4.1	Лабораторные работы, тест
4	Реализация методов защиты информации в современных распределенных системах.	ОПК-4	ОПК-4.2	Тест
Промежуточная аттестация, форма контроля - зачет				Перечень вопросов

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

- тест,
- лабораторные работы.

Перечень заданий лабораторных работ

Задание 1. *И*спользуя встроенные средства сетевого аудита MS Windows провести первичный анализ сетевых интерфейсов.

Задание 2. *И*сследовать структуру TCP/IP пакетов с помощью программы сетевого аудита.

Задание 3. *И*спользуя средства криптографического моделирования и анализа выполните дешифрацию входного сообщения.

LoatuvftYejeerzAgibeejwzriyazfrkknxefvoxvhanvmsxlizyjzhnxmvhnjwyhnonafjgmiunfrbjxnzrrgfkgearfywv.Bnotfrqgwesiprqzbvotvvgomcumozbklszuqzsypizhslbjtmkngrzggdgpccwkwsiireqk,tsceycoyvuztveukwgktrtvthlugvvgggdonafjgmibengdxhaihrj.HnxUtiivfybte'scfgomiunvehnxngtvfbgeutiivfybterneyoggypefjoweyprigatsovrvjowetcrkcomsgcuzsbxmkngj,ovhsotvmsofamenergiaysvfblhrkxpvzrxnie:FWsjNwgsnnoxwejtuv5hnilgcrzbzaeGnalorBnjecvbjxnzNnkwugarUazjkksotIlotditgf.JTkwUkqhzdybtygerrattksjzhnxsyeakwgesqiycgzhgovrkvkfaiozgszbtovrrrbtnzatvknxnotpfakltugrkhogggjbs.HnxktojcsjzegcdlwxxdgtFWsjNetaocsymhkmgfpuedrysrqkmhkdrdotwsgnqtvgelkntvguytne21fkqkgtarlrgcxlrafkcihnzrvsizxtutuvrkoerocdstmoltuvzuvarcbdaagizy.

Задание 4

Криптографические решения в информационных системах.

Осуществить разработку программы, осуществляющей шифрацию сообщения на основе алгоритма AES. Написать программу, которая будет осуществлять преобразование зашифрованного сообщения к исходному виду.

Задание 5
Анализ безопасности сетевой инфраструктуры.
Используя программу WireShark для перехвата сетевого траффика определить, какими сетевыми протоколами пользуется программное обеспечение локального компьютера. Осуществить перехват FTP трафика, проанализировать его и составить отчет о его структуре, описав действия пользователя на основе перехваченной информации.

Задание 6
Аудит сетевой инфраструктуры информационных систем.

Используя сетевой сканер NMap установить операционные системы устройств, подключенных к локальной сети лаборатории. Выявить адреса серверов и определить версии программного обеспечения, которые на них инсталлированы. По результатам работы сканера составить отчет о программном обеспечении ЛВС.

Задание 7
Облачные технологии и решения виртуализации в информационных системах.

Построить модель корпоративной инфраструктуры используя технологии виртуализации. Рассмотреть возможность перевода построенной модели в «облака».

Технология проведения
Студент выполняет предложенное преподавателем задание, представляет его на дисплее, комментирует выполненные действия, анализирует и интерпретирует результаты. Составляет отчет по результатам работы.

Критерии оценивания
Используется шкала «выполнено, не выполнено» Лабораторная работа считается выполненной, если все пункты задания выполнены, подготовлен и защищен отчет, иначе – не выполнено.

Пример тестового задания

1. Дополните
… представляют собой совокупность информационных и программно-аппаратных элементов, а также информационных технологий, применяемых при обработке данных.

2. Дополните
NMap – это …

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

4. Дополните

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

5. 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

6. Отметьте правильный ответ

Угроза типа «Анализ сетевого траффика» реализуется с помощью специальной …

- программы-анализатора пакетов
- утилиты межсетевого взаимодействия
- операционной системы
- СУБД

7. Отметьте правильный ответ

... – это программа-анализатор пакетов.

- NMap
- WireShark
-VirtualBox
-Linux

8. Отметьте правильный ответ

Подмена доверенного объекта сети реализуется в системах, где применяются … алгоритмы идентификации и аутентификации хостов, пользователей

-Нестойкие
-Стойкие
-Полиморфные
-Инкапсулированные
-Распределенные

9. Отметьте правильный ответ

Внедрение ложного объекта возможно через протокол

-ARP
-FTP
-POP3
-IMAP
-SMTP

10. 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.

11. Отметьте правильный ответ

Вирус Морриса – это пример реализации угрозы

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

12. Дополните

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

13. Отметьте правильный ответ

Искусства изобретать шифры и взламывать их называются вместе …

-криптография
-криптологией
-криптоанализ
-криптофилия
-криптомания.

14. Дополните

Шифр Цезаря основан на методе …

15. Дополните

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

16. Отметьте правильный ответ

Размер блока шифрования в исходном алгоритме DES равен … битам

-16
-32
-64
-128
-256

17. Отметьте правильный ответ

Размер ключа шифрования в исходном алгоритме DES равен … битам

-16
-32
-55
-56
-64

18. 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.

19. 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

20. Дополните

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

21. Дополните

UDP-шторм – это пример реализации угрозы …

22. Дополните

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

23. Дополните

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

24. Дополните

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

25. Отметьте правильный ответ

Для работы алгоритма RSA на начальном этапе выбирают

- два простых числа
- два составных числа
- два мнимых числа
- два взаимно простых числа

26. Дополните

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

27. Отметьте правильный вариант

Какая длинна ключа считается надежной для алгоритма RSA?

-128
-256
-768
-1024

28. Дополните

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

29. Дополните

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

30. Дополните

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

31. Дополните

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

32. Дополните

… - стандартная утилита конфигурирования сетевого экрана в ОС Linux.

33. Дополните

X.509 – это стандарт для описания …

34. Дополните

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

35. Дополните

Для шифрации в протоколе Bluetooth используется потоковый шифр …

36. Дополните

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

37. Дополните

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

38. Дополните

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

39. Дополните

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

40. Дополните

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

41. Отметьте правильный ответ
С каким типом атаки не может справиться брандмауэр
-DDOS
-Сканирование портов
-UDP-шторм
42. 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)
43. 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)
44. Отметьте правильный ответ
С блоками какой разрядности работает алгоритм SHA-1?
-64 бит
-128 бит
-256 бит
-512 бит
-1024 бит
45. Отметьте правильный ответ
Набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP носит название
-IPS
-IPsec
-IPC
-IPCrypt
-IPEnc

Технология проведения
Вариант теста вбирается исходя из номера зачетки (последней цифры). Время на тестирование рассчитывается из соотношения 10 вопросов – 15 минут. Результаты теста проверяются по ключу правильных ответов.

Критерии оценки:
- оценка «зачтено» выставляется студенту, если студент дал правильные ответы на 50 и более процентов заданий;
- оценка «не зачтено» - даны правильные ответы менее, чем на 50 процентов заданий.

20.2 Промежуточная аттестация
Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств: вопросы к зачету.

Перечень вопросов к зачету
1. Что используется для контроля целостности передаваемых по сетям данных?

2. Что гарантирует доступность информации?

3. Что следует предпринять для максимально надежной защиты обрабатываемой в компьютере информации от утечки по электромагнитному каналу путем перехвата компрометирующего высокочастотного электромагнитного излучения?

4. Что способствует защите от вредоносного программного обеспечения?

5. Что должно быть первоочередным загрузочным устройством для предотвращения несанкционированного доступа к хранящейся в компьютере информации путем запуска операционной системы, записанной на внешнем носителе, при установке в SETUP BIOS определенного порядка загрузки?

6. Чем является несанкционированное доведение защищаемой информации до потребителей, не имеющих права доступа к защищаемой информации?

7. Чем является получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации?

8. Чем обеспечивается безопасность информации в соответствии с аксиомой теории защиты информации?

9. Что является достоинством многоуровневой политики безопасности?

10. Что представляют собой правила разграничения доступа, обеспечивающие разграничение доступа между поименованными субъектами и поименованными объектами?

11. Что относится к активным мерам по защите информации от утечки?

12. Как может быть обнаружено контактное подключение к электрической кабельной линии?

13. Что может использоваться для защиты от бесконтактного подключения к электрической кабельной линии путем уменьшения электромагнитного излучения линии?

14. К потере каких свойств информации приводит влияние помех при передаче информации?

15. Что способствует безопасному использованию системы беспроводной передачи данных Bluetooth?

16. Где рекомендуется хранить пароли и криптографические ключи для наиболее надежной их защиты?

17. Сколько ключей использует криптосистема RSA?

18. К какому типу шифров относится шифр подстановки, ставящий в соответствие одному символу открытого текста несколько символов шифртекста, количество и состав которых выбираются так, чтобы частоты появления всех символов в зашифрованном тексте были одинаковыми?

19. К какому типу шифров относится шифр Цезаря?

20. Что такое имитовставка?

21. К какому стандарту относится алгоритм, криптостойкость которого основана на трудности разложения очень больших целых чисел на сомножители?

22. Что является недостатком асимметричных криптографических систем по сравнению с симметричными?

23. Обнаружение чего не может являться признаком попытки несанкционированного доступа к компьютерной информации?

24. Каким образом может быть обеспечена наиболее надежная защита хранящейся и обрабатываемой в компьютере информации от утечки по оптическому каналу?

25. Из каких букв, цифр, символов может состоять пароль в ОС Windows XP (русскоязычная или мультиязычная версия)?

26. К какому типу вредоносных программ относится самовоспроизводящаяся программа, которая может присоединяться к другим программам и файлам, но не способная к самораспространению путем многократного самокопирования и передаче в компьютерных сетях?

27. К какому типу вредоносных программ относится программа, выполняемая однократно в определенный момент времени или при наступлении определенных условий и предназначенная для нарушения работы компьютерной системы, уничтожения, модификации или блокирования информации?

28. Что гарантирует доступность информации?

29. Для какой цели применяются идентификация и аутентификация?

30. Что является признаком, наиболее достоверно указывающим на наличие в компьютерной системе вредоносных программ?

31. Какая угроза имеет место, если ценность информации теряется при ее модификации (изменении) или уничтожении?

32. Что понимается под утечкой информации?

33. К какому типу защиты информации относится деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации?

34. Какой вид доступа к информации не относится к основным видам доступа?

35. Что является недостатком дискреционной политики?

36. Какую политику безопасности представляют правила разграничения доступа, обеспечивающие разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности?

37. Что способствует предотвращению утечки информации по электромагнитному каналу?

38. Как может быть обнаружено бесконтактное подключение к электрической кабельной линии?

39. Какое явление используется при бесконтактном подключении к электрической кабельной линии?

40. К потере какого свойства информации приводит перехват информационного сигнала?

41. Какие меры способствуют защите от мобильных вредоносных программ?

42. Чем характеризуется криптостойкость криптографического преобразования?

43. Как называется шифр, использующий подстановки и перестановки в качестве элементарных составляющих?

44. Как называется шифр, при использовании которого открытый текст записывается по строкам (по горизонтали) в ячейки таблицы, а шифртекст считывается по столбцам (по вертикали)?

45. Что такое имитозащита?

46. Как называется алгоритм, криптостойкость которого основана на трудности решения задачи дискретного логарифмирования?

47. Какая угроза приводит к потере ценности информации при ее разглашении?

48. Как обеспечить надежную защиту обрабатываемой в компьютере информации от утечки по электромагнитному каналу путем перехвата компрометирующего высокочастотного электромагнитного излучения?

49. К какому виду вредоносного программного обеспечения относится самовоспроизводящаяся программа, которая может присоединяться к другим программам и файлам, но не способная к самораспространению путем многократного самокопирования и передаче в компьютерных сетях?

50. К какому виду вредоносного программного обеспечения относится программа, запускающая скрытую внутри какой-либо легальной программы несанкционированную функцию, обеспечивающую выполнение действий, непредусмотренных автором легальной программы?
51. Как может быть обнаружено контактное подключение к электрической кабельной линии?
52. Что является признаком попытки несанкционированного доступа к компьютерной информации?
53. Что такое принцип Керкгоффса?
54. Каковы недостатки симметричных криптосистем?
55. Что такое криптостойкость систем шифрования, как она количественно определяется?
56. Как используют парадокс дней рождения для криптоанализа систем хэширования?
57. Классификация угроз безопасности по виду защищаемой от угроз безопасности информации.
58. Классификация угроз безопасности по способу реализации угрозы безопасности.
59. Классификация угроз безопасности по типу информационных систем
60. Классификация уязвимостей программного обеспечения.
61. Примеры уязвимостей протоколов стека протоколов TCP/IP.
62. Общая характеристика угроз безопасности, реализуемых с использованием протоколов межсетевого взаимодействия.
63. Угрозы типа «Анализ сетевого траффика», «Сканирование сети», «Выявление пароля».
64. Угрозы типа «Подмена доверенного объекта сети», «Навязывание ложного маршрута».
65. Угрозы типа «Внедрение ложного объекта», «Отказ в обслуживании», «Удаленный запуск приложений»
66. Метод подстановок и перестановок в криптографии
67. Основные принципы криптографии. Одноразовые блокноты.
68. Алгоритмы с симметричным криптографическим ключом.
69. Тройное шифрование с помощью DES. Улучшенный стандарт шифрования AES.
70. Алгоритм Rijndael.
71. Режим шифрованной обратной связи
72. Режим группового шифра
73. Режим счетчика
74. Криптоанализ
75. Алгоритмы с открытым ключом
76. Алгоритм RSA
77. Криптоанализ алгоритма RSA
78. Цифровые подписи.
79. Подписи с открытым ключом
80. Профили сообщений
81. Подпись MD5
82. Подпись SHA-1
83. 2.24. Сертификаты. X.509
84. Инфраструктуры систем с открытыми ключами.
85. Каталоги. Аннулирование
86. IPV4, IPsec.
87. Брандмауэры

88. Виртуальные частные сети
89. Безопасность в беспроводных сетях
90. Безопасность в сетях 802.11
91. Безопасность в системах Bluetooth
92. Протоколы аутентификации

Для оценивания результатов обучения на зачете используются следующие показатели:

1) знание основ информационной безопасности и защиты информации;
2) знание основ использования программных решений в области анализа архитектуры предприятия;
3) знание основных принципов построения информационных систем с использованием средств защиты информации;
4) умение проводить сравнительный анализ систем защиты информации;
5) умение применять системное и прикладное программное обеспечение при создании информационных систем и анализе существующих;
6) умение использовать современные вычислительные системы в составе компьютерных сетей с обеспечением защиты информации;
7) владение навыками построения систем высокой готовности в составе распределённых вычислительных сетей с интеграцией облачных инфраструктур в компьютерную сеть с обеспечением защиты информации;
8) владение методами внедрения системного и прикладного программного обеспечения в информационные системы;
9) владение навыками решения стандартных задач защиты информации с учетом требований информационной безопасности.

Для оценивания результатов обучения на зачете используется шала: «зачтено», «не зачтено».

Соотношение показателей, критериев и шкалы оценивания результатов обучения на зачете:

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся дал правильные ответы на все вопросы КИМ (допускаются незначительные ошибки в терминологии), продемонстрировал освоение 50% и более указанных выше показателей, все лабораторные работы выполнены, тест зачтен.	Базовый уровень и выше	Зачтено
Обучающийся не дает полные ответы на материалы КИМ и в них содержится множество ошибок, в том числе по терминологии, продемонстрировал освоение менее 50% указанных выше показателей и/или не все лабораторные работы выполнены, и/или тест не зачтен.	Ниже базового уровня	Не зачтено