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

УТВЕРЖДАЮ
заведующий кафедрой
кибербезопасности
информационных систем
С.Л. Кенин

22.03.2024

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ ФТД.01 Анализ данных компьютерных систем и сетей

1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализация:

"Безопасность компьютерных систем и сетей" (по отрасли или в сфере профессиональной деятельности)

3. Квалификация (степень) выпускника: Специалист

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины:

кибербезопасности информационных систем

6. Составители программы:

Степанец Юлия Александровна, к.т.н., доцент кафедры кибербезопасности информационных систем

7. Рекомендована:
НМС факультета ПММ, протокол № 7 от 26.05.2023г.
Внесены изменения: протокол УС факультета ПММ, протокол № 8 от 27.02.2024г.
Рекомендована с изменениями: протокол НМС факультета ПМ, протокол № 5 от 22.03.2024г.

8. Учебный год: 2026/2027 **Семестр(ы):** 7

9. Цели и задачи учебной дисциплины

Изучение способов проведения начального анализа структуры информационных процессов и выявления уязвимых компонентов; использование специализированных источников и справочных систем для поиска научно-технической литературы, нормативных и методических материалов; проведение анализа способов, методов, средств и алгоритмов решения задач расследования инцидентов в области информационной безопасности объекта защиты. Исследование цифровых доказательств. Методы поиска, получения и закрепления доказательств. Восстановление и анализ содержимого, найденного на цифровых устройствах.

10. Место учебной дисциплины в структуре ОПОП: дисциплина относится к факультативным дисциплинам 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-4.1	Способен организовывать защиту информации в компьютерных системах и сетях (по областям применения);	ОПК-4.1.2	знает современные методы, средства и меры по защите информации в компьютерных системах и сетях;	Знает: современные методы, средства и меры по защите информации в компьютерных системах и сетях. Умеет: использовать языки и системы программирования, инструментальные средства при обеспечении защиты информации в компьютерных системах при решении различных профессиональных, исследовательских и прикладных задач
		ОПК-4.1.3	способен использовать языки и системы программирования, инструментальные средства при обеспечении защиты информации в компьютерных системах при решении различных профессиональных, исследовательских и прикладных задач	
ОПК-4.3	Способен разрабатывать и анализировать корректность политики информационной безопасности компьютерных систем и сетей (по областям применения);	ОПК-4.3.5	способен применять программные средства прикладного, системного и специального назначения при разработке и анализе политики информационной безопасности;	Умеет: применять программные средства прикладного, системного и специального назначения при разработке и анализе политики информационной безопасности

12. Объем дисциплины в зачетных единицах/час - 2/72.
Форма промежуточной аттестации - зачет.

13. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоёмкость (часы)					
	Всего	В том числе в интерактивной форме	По семестрам			
			7			
Аудиторные занятия	16		16			
в том числе: лекции	16		16			
Практические	0		0			
Лабораторные	0		0			
Самостоятельная работа	56		56			
Контроль	0		0			
Итого:	72		72			
Форма промежуточной аттестации	Зачет		Зачет			

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Сущность и задачи комплексной защиты информации	Состав компонентов комплексной системы обеспечения информационной безопасности (КСИБ), функциональные и обеспечивающие подсистемы, технология, управление. Понятие аудита	ФТД.01 Анализ данных компьютерных систем и сетей (10.05.01)
1.2	Методология формирования задач защиты	Интеграция средств информационной безопасности в технологическую среду. ведение специальной информационной базы данных КСИБ.	
1.3	Методы и методики оценки качества КСИБ	Методы нормативного функционального наполнения, метод экспертных структурных вопросников, метод оценки уязвимости информации, метод оценки риска. Проведение аттестации ИСПДн по требованиям безопасности. Декларирование соответствия. Определение перечня мер по защите ПДн., обрабатываемых без использования средств автоматизации.	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)					
		Лекции	Практ.	Лаб. раб.	Самостоятельная работа	Контроль	Всего
1.1	Сущность и задачи комплексной защиты информации	4		0	16	0	20
1.2	Методология формирования задач защиты	4		0	16	0	20
1.3	Методы и методики оценки качества КСИБ	8		0	24	0	32
	Итого:	16		0	56	0	72

14. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины включает в себя лекционные занятия, лабораторные занятия и 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 лабораторных заданий, подготовку к экзамену.

Для успешного освоения дисциплины рекомендуется подробно конспектировать лекционный материал, просматривать презентации (при наличии) по соответствующей теме, изучать основную и дополнительную литературу рекомендуемой библиографии,

При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей 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	Макаренко, С. И. Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем : учебное пособие / С. И. Макаренко, А. А. Ковальский, С. А. Краснов. – Санкт-Петербург : , 2020 – Часть 2 : Сетевые операционные системы и принципы обеспечения информационной безопасности в сетях – 2020. – 357 с. – ISBN 978-5-6044429-8-2. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/329378. – Режим доступа: для авториз. пользователей.
2	Шелухин, О. И. Обнаружение вторжений в компьютерные сети (сетевые аномалии) : учебное пособие / О. И. Шелухин, Д. Ж. Сакалема, А. С. Филинова ; под редакцией О. И. Шелухина. – Москва : Горячая линия-Телеком, 2018. – 220 с. – ISBN 978-5-9912-0323-4. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/111119. – Режим доступа: для авториз. пользователей.

б) дополнительная литература:

№ п/п	Источник
3	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008. https://fstec.ru/en/dokumenty/vse-dokumenty/spetsialnye-normativnyedokumenty/bazovaya-model-ot-15-fevralya-2008-g?ysclid=lj8zaq9vbh762206938
4	Методический документ "Методика оценки угроз безопасности информации" (утв. Федеральной службой по техническому и экспортному контролю 5 фев 2021г.) https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnyedokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g?ysclid=lj8z58t2v2240278685

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	Криптографические протоколы (10.05.01)/Степанец Ю.А. - Образовательный портал «Электронный университет ВГУ». — Режим доступа: https://edu.vsu.ru

16. Перечень учебно-методического обеспечения для самостоятельной работы

В качестве формы организации самостоятельной работы применяются методические указания для самостоятельного освоения и приобретения навыков работы со специализированным программным обеспечением. Самостоятельная работа

студентов: изучение теоретического материала; подготовка к лекциям, работа с учебно-методической литературой, подготовка отчётов по лабораторным работам, подготовка к экзамену.

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 заданий 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 занятий рекомендован онлайн-курс «ФТД.01 Анализ данных компьютерных систем и сетей (10.05.01)», размещенный на платформе Электронного университета ВГУ (LMS moodle), а также Интернет-ресурсы, приведенные в п.15в.5.

18. Материально-техническое обеспечение дисциплины

Учебная аудитория для лекций: специализированная мебель, компьютер преподавателя, мультимедийный проектор, экран.
Учебная аудитория для лабораторных занятий: специализированная мебель, персональные компьютеры, мультимедийный проектор, экран, лабораторное оборудование программно-аппаратных средств обеспечения информационной безопасности.
Аудитория для самостоятельной работы: учебная мебель, компьютер с возможностью подключения к сети «Интернет» и электронной платформе Электронного университета ВГУ.

Программное обеспечение (см.файл МТО): ОС Windows v.7, 8, 10, набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF 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	Сущность и задачи комплексной защиты информации	ОПК-4.1	ОПК-4.1.2	устный опрос, тест
2	Методология формирования задач защиты	ОПК-4.1	ОПК-4.1.2	устный опрос, тест
			ОПК-4.1.3	
		ОПК-4.3	ОПК-4.3.5	
3	Методы и методики оценки качества КСИБ	ОПК-4.1	ОПК-4.1.2	устный опрос, тест
			ОПК-4.1.3	
		ОПК-4.3	ОПК-4.3.5	
Промежуточная аттестация, форма контроля - зачет				Перечень вопросов (КИМ№1)

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:

- устный опрос;
- тестовые вопросы.

20.2 Промежуточная аттестация

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

Перечень вопросов к экзамену (КИМ №1)

1. Понятие экспертной системы. Особенности экспертных систем оценки информационной безопасности.
2. Принципы и подходы к комплексной оценке информационной безопасности в экспертных системах.
3. Общая структура экспертных систем оценки ИБ.
4. Цели, задачи и функции экспертных систем оценки ИБ.
5. Типы экспертных систем оценки ИБ. Классификация.
6. Отличительные признаки информации, применимой для анализа в экспертных системах оценки ИБ.
7. Методы сбора и подготовки информации. Преобразование информации в данные для работы в экспертных системах оценки ИБ.
8. Классификация и типы используемых данных. Порядок работы с данными в экспертной системе ИБ.
9. Аппаратное обеспечение экспертной системы оценки ИБ. Основные требования. Стандарты.
10. Аппаратные средства сбора и обработки данных в экспертных системах оценки ИБ. Примеры.
11. Программное обеспечение экспертной системы оценки ИБ. Классификация. Стандарты.
12. Процедуры и программы сбора данных о подсистеме защиты информации автоматизированной системы. Основные требования.
13. Функции-обработчики данных в экспертной системе оценки ИБ. Математический аппарат, применяемый в обработчиках.
14. Базы данных для экспертных систем оценки ИБ. Особенности взаимодействия интерфейсов экспертной системы с базами данных.
15. Блоки принятия решений. Элементы искусственного интеллекта для анализа полученных данных и синтеза решений.
16. Подходы к комплексной оценке ИБ автоматизированной системы. Различия для информационных и телекоммуникационных систем.
17. Российские и международные стандарты, применяемые для оценки ИБ автоматизированной системы.
18. Этапы проектирования экспертных систем оценки ИБ. Жизненный цикл экспертных систем.
19. Принципы тестирования автоматизированных систем при помощи экспертных систем оценки ИБ.
20. Оценка достоверности полученных результатов. Математические методы оценки достоверности результатов работы экспертных систем оценки ИБ.
21. Аудит ИБ. Классификация. Стандарты проведения.

22. Экспертные системы оценки ИБ как средства проведения аудита.
23. Сканеры безопасности как пример экспертных систем оценки ИБ. Общая характеристика.
24. Типы и принципы работы сканеров ИБ. Проведение оценки ИБ системы на примере одного из существующих сканеров.
25. Особенности аудита операционных систем и программного обеспечения.
26. Отчет по проведенному аудиту. Правила и особенности.
27. Автоматизация составления отчетов экспертных систем оценки ИБ.
28. Экспертные системы оценки ИБ на предприятии. Особенности эксплуатации.
29. Системы контроля инцидентов ИБ как вариант экспертных систем оценки безопасности.
30. Развитие экспертных систем оценки ИБ автоматизированных информационных и телекоммуникационных систем.
31. Решения по обеспечению анализа защищенности в распределенных информационных системах
32. Решения по обеспечению анализа защищенности в распределенных информационных системах
33. Этапы аудита информационно безопасности в Windows-подобной информационной инфраструктуре
34. Этапы аудита информационно безопасности в Linux-подобной информационной инфраструктуре
35. Построение процесса аудита средств защиты информации
36. Построение методики Pen Test
37. Средства и способы обеспечения анализа информационной безопасности почтовых серверов
38. Системы анализа сетевых атак и мониторинга инцидентов
39. Выбор средств защиты информации для проведения аудита информационной безопасности
40. Выбор средств защиты информации для проведения Pen Test
41 Основные понятия. Определение безопасности.
42 Группы причин нарушения безопасности компьютерных систем.
43 Особенности современных программно-аппаратных средств как основных причин
44 нарушений ИБ.
45 Особенности современных информационных технологий с точки зрения нарушений ИБ.
46 Состояние правового обеспечения ИБ.
47 Понятие о системе стандартов в области ИБ.
48 Федеральные критерии безопасности США.
49 Единые критерии, их применение в России.
50 Система стандартов ФСТЭК.
51 Понятие о лицензировании деятельности в области ИБ.
52 Понятие о системе сертификации. Системы сертификации в области ИБ, принятые в
53 России.
54 Понятие угроз ИБ. Систематизация угроз. Модель угроз.
55 Понятие разрушающих программных средств (РПС). Виды РПС, их характеристики.
56 Модели РПС.
57 Компьютерные вирусы. Типы вирусов. Структура вируса и способы заражения.
58 Классификация средств защиты от компьютерных вирусов.
59 Модель нарушителя. Классы нарушителей, их характеристики. Модель атак Говарда.
60 Аморосо, Ландвера. Токсономия.
61 Сценарий компьютерной атаки.
62 Функции защиты, их особенности.

63 Виды контроля безопасности. Средства контроля.
64 Понятие безопасности ПО.
65 Методы анализа безопасности ПО. Принципы анализа ПО без исходных кодов.
66 Методы защиты коммерческого ПО.
67 Структура информационных ресурсов.
68 Понятие компьютерных преступлений.
69 Понятие уязвимостей. Систематизация уязвимостей.
70 Ошибки в системе защиты. Недостатки, служащие причиной возникновения уязвимостей.
71 Безопасность операционных систем (ОС).
72 Понятие политики безопасности. Управление доступом.
73 Механизмы контроля доступа к объектам Windows.
74 Аутентификация пользователей в ОС.
75 Криптографические методы защиты информации. Методы криптоанализа.
76 Стеганографическое сокрытие информации.
77 Методы статистического кодирования информации:
78 Методы адаптивного кодирования информации:
79 Методы защиты информации от искажений.
80 Методы надежной передачи данных.
81 Понятие удаленной атаки.
82 Методы обеспечения безопасности в сети Интернет.
83 Защита от угроз типа "отказ в обслуживании".
84 Систематизация технологий защиты, их краткая характеристика.
85 Понятие киберугроз и кибербезопасности, отличие от информационных угроз.
86 Общая схема технологии построения защищенной информационной системы.

Требования к выполнению заданий, шкалы и критерии оценивания

Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования.

Для оценивания результатов обучения на зачете используется - зачтено, не зачтено Соотношение показателей, критериев и шкалы оценивания результатов обучения.

Показатель сформированности компетенции	Шкала и критерии оценивания уровня освоения компетенции	
	Зачтено	Не зачтено
Знает: современные методы, средства и меры по защите информации в компьютерных системах и сетях.	1. Сформированные знания 2. Сформированные знания, но содержащие отдельные пробелы 3. Неполные знания.	Фрагментарные знания или их отсутствие.
Умеет: использовать языки и системы программирования, инструментальные средства при обеспечении защиты информации в компьютерных системах при решении различных профессиональных, исследовательских и прикладных задач	1. Сформированные знания 2. Сформированные знания, но содержащие отдельные пробелы	Неполные знания. / Фрагментарные знания или их отсутствие.
Умеет: применять программные средства прикладного, системного и специального назначения при разработке и анализе политики информационной безопасности	1. Сформированные знания 2. Сформированные знания, но содержащие отдельные пробелы	Неполные знания. / Фрагментарные знания или их отсутствие.

20.3 Фонд оценочных средств сформированности компетенций студентов, рекомендуемый для проведения диагностических работ

ОПК-4.1. Способен организовывать защиту информации в компьютерных системах и сетях (по областям применения);
ОПК-4.3. Способен разрабатывать и анализировать корректность политики информационной безопасности компьютерных систем и сетей (по областям применения).

1) закрытые задания (тестовые, средний уровень сложности):

Вопрос 1. Для любой системы (и ИС в том числе) характерно следующее:
а. структура и поведение системы взаимно обусловлены. Сложности структуры системы сопутствует сложность еѐ поведения
б. сложность системы характеризуют сложностью еѐ поведения - разнообразие реакций на внешнее воздействие. в. верно все перечисленное
ОТВЕТ: в.
Вопрос 2. Для любой системы, свойство ее устойчивости - это:
а. способность сохранять частичную работоспособность при отказе отдельных элементов или подсистем
б. способность сохранять равный процент нагрузки на рабочие элементы системы
в. способность системы сохранять количество ее основных элементов и не расширяться
ОТВЕТ: а.
Вопрос 3. Для любой системы, свойство ее функциональной анизотропности - это:
а. неравноценность элементов и связей системы
б. неравноценность связей внутри системы в. неравноценность элементов системы
ОТВЕТ: а.
Вопрос 4. Система называется «жизнеспособной», если:
а. еѐ коэффициент смерти меньше средней вероятности жизни еѐ элементов
б. еѐ коэффициент смерти больше средней вероятности жизни еѐ элементов
ОТВЕТ: а.
Вопрос 5. Крайний случай жизнеспособности - «система жива, когда живы все ее элементы», эквивалентен:
а. электрической схеме последовательного соединения элементов (резисторов)
б. электрической схеме параллельного соединения элементов (резисторов)
ОТВЕТ: а.
Вопрос 6. Крайний случай жизнеспособности - «система мертва тогда и только тогда когда мертвы все еѐ элементы», эквивалентен:
а. электрической схеме последовательного соединения элементов (резисторов)
б. электрической схеме параллельного соединения элементов (резисторов)
ОТВЕТ: б.
Вопрос 7. Надежность (для систем) - это:
а. свойство системы сохранять во времени и в установленных пределах значения всех параметров, характеризующих способность системы выполнять требуемые функции в заданных режимах и условиях эксплуатации
б. свойство системы быть в постоянной работоспособности неограниченное количество времени в. свойство системы быть в работоспособном состоянии даже при условии отказа всех основных элементов системы
ОТВЕТ: а.
Вопрос 8. Надежность системы определяется:
а. по формуле полной вероятности
б. является константой, определяемой изготовителем системы произвольно
ОТВЕТ: а.
Вопрос 9. Один из самых популярных вероятностных законов надежности, применимый к большинству систем - это:
а. экспоненциальный закон
б. линейный закон

в. параболический закон
ОТВЕТ: а.
Вопрос 10. Защищенность системы является:
а. составным атрибутом надежности
б. независимым атрибутом, никак не связанным с надежностью
ОТВЕТ: а.
Вопрос 11. Укажите главную особенность современных ИС, которую необходимо учитывать при анализе ее защищенности и надежности:
а. современные ИС создаются человеком
б. современные ИС состоят из материальных (hardware) и нематериальных (software) компонентов в. современные ИС полностью удовлетворяют основному экспоненциальному закону надежности
ОТВЕТ: б.
Вопрос 12. Укажите применяемые в современной практике технологии и решения обеспечения надежности и защищенности (доступности) аппаратной (hardware) составляющей ИС:
а. RAID
б. кластеры
в. дорогие фирменные комплектующие
г. последовательное соединение элементов ИС
ОТВЕТ: а, б.
Вопрос 13. Укажите особенности надежности для программной составляющей ИС:
а. ПО не подвержено износу
б. надежность ПО не является функцией времени
в. ПО изначально обладает 100% надежностью
г. надежность ПО полностью зависит от человеческого фактора
ОТВЕТ: а, б, г.
Вопрос 14. Существующие модели оценки надежности ПО современных ИС бывают:
а. динамическими
б. эмпирическими
в. статическими
г. все перечисленное
ОТВЕТ: г.
Вопрос 15. Среди проблем, влияющих на надежность работы ПО современных ИС, можно отметить следующие:
а. регистрочувствительность имен переменных и процедур для ряда языков программирования
б. локальность и глобальность используемых имен переменных для ряда языков программирования
в. строгая и нестрогая типизация с наличием/отсутствием приведения типов для ряда языков программирования
г. работа программиста, осуществляющего создание программного кода исключительно по предоставленному техническому заданию
д. известность механизмов организации и работы с памятью/стеком при исполнении программного кода
ОТВЕТ: а, б, в, д.

1. Адреса из какой сети являются служебными адресами логического интерфейса Loopback.
a. 72.0.0.0.1 – 72.0.0.15.
b. 10.0.0.0 – 10.255.255.255.
c. 127.0.0.0 – 127.255.255.255.
d. 192.0.2.0 – 192.0.2.255.
Ответ - c
2. Какой из перечисленных алгоритмов является алгоритмом множественного доступа с контролем несущей и обнаружения коллизий.
a. CSMA/CD.

b. Алгоритм трехсторонннего рукопожатия.
c. Алгоритм CRC64.
d. CSMA/CA.
Ответ - a
3. Какое сетевое устройство ограничивает широковещательный трафик.
a. Повторитель (хаб).
b. L2 коммутатор.
c. Маршрутизатор.
d. Точка доступа.
Ответ - c.
4. В каких из перечисленных приложений желательно использование протокола UDP.
a. Веб-серфинг с помощью браузера.
b. Потоковая передача видео.
c. Обмен данными между базами данных.
d. Обмен почтой.
Ответ - b
5. Каково предназначение поля TTL в служебном заголовке ip-пакета.
a. Обеспечивает механизм проверки целостности данных.
b. Зарезервировано для будущего использования.
c. Определяет адрес назначения пакета.
d. Определяет число маршрутизаторов, через которые может пройти пакет.
Ответ - d
6. Какие ограничения должны быть наложены на учетную запись пользователя базы данных?
a. Должна быть уникальна и иметь доступ только к данным сервера баз данных
b. Иметь удаленный доступ к операционной системе.
c. Можно использовать учетную запись администратора операционной системы.
d. Нет ограничений.
Ответ - a
7. Выберите из списка полиалфавитный шифр.
a. Шифр Цезаря
b. Шифр Виженера
c. AES-CBC
d. RC4
Ответ - b
8. Бинарное сложение по модулю 2 двух единичных битов равно.
a. 1
b. 0
c. 2
d. Не определено
Ответ - b
9. Разновидность симметричного шифра использующего для шифрования блоки фиксированной длины.
a. Ассиметричный шифр.
b. Сдвиговый шифр.
c. Поточный шифр.
d. Блочный шифр.
Ответ - d
10. Какой из перечисленных шифров не является блочным?
a. 3DES
b. AES
c. RSA
d. IDEA
Ответ - c
11. Какой размер ключа использует отечественный симметричный алгоритм блочного шифрования стандарта ГОСТ Р 34.12-2015?
a. 64 бит

b. 128 бит
c. 512 бит
d. 256 бит
Ответ - d
12. Какие из перечисленных алгоритмов не основаны на криптографии с открытым ключем?
a. RSA
b. DSA
c. ГОСТ Р 34.10-2012
d. AES
Ответ - d
13. Какая из перечисленных хеш-функций более безопасна с криптографической точки зрения?
a. MD5
b. SHA-512
c. SHA1
d. MD4
Ответ - b
14. Выберите два протокола, которыми можно обеспечить шифрование сетевого подключения клиентских программ к базе данных.
a. Telnet и SSH
b. Radius и Tacacs
c. Telnet и HTTP
d. SSL и SSH
Ответ - d
15. Для чего необходим анализ журнала событий базы данных?
a. Определение отказов и событий системы.
b. Определение настроек сервера базы данных.
c. Определение сетевой конфигурации сервера.
d. Определение текущего времени системы.
Ответ - a

2) открытые задания (тестовые, средний уровень сложности):

1. Приведите примеры мер для обеспечения безопасности сетевых устройств. Конфигурирование безопасного административного доступа. Конфигурирование усовершенствованных функций безопасности для виртуального входа в систему. Конфигурирование SSH.
2. Для чего используется назначение административных ролей. Специалисты ИТ-отдела в крупных организациях выполняют самые разные должностные обязанности. Уровень доступа для выполнения разных должностных обязанностей тоже должен быть разным. Назначение ролей позволяет определить, кому разрешается подключаться к сетевому устройству и что этот специалист может делать на этом устройстве.
3. Для чего нужен мониторинг устройств. Обеспечение возможности ведения журналов данных - это важная часть любой политики сетевой безопасности. Когда в сети происходят те или иные события, сетевые устройства задействуют доверенные механизмы для уведомления администратора и отправки ему подробных системных сообщений. Эти сообщения могут быть не очень важными или, наоборот, важными, а для их хранения, интерпретации и просмотра существует несколько способов. Администраторы могут получать уведомления обо всех сообщениях или только о сообщениях, которые могут оказать значительное влияние на сетевую инфраструктуру.
4. Для чего нужна модель AAA (аутентификация, авторизация и учет). Службы безопасности сети AAA обеспечивают базовую инфраструктуру настройки контроля доступа на сетевом устройстве. AAA позволяет контролировать, кому разрешен доступ к сети (аутентификация) и что им разрешено делать (авторизация), а также проверять выполненные действия при доступе к сети (учет).

5. Расскажите про протоколы Radius и Tacacs+ в модели AAA. Оба протокола используют клиент-серверную архитектуру для реализации модели AAA в локальной сети.
6. Что такое списки контроля доступа (ACL). Списки ACL широко используются для обеспечения работы компьютерных сетей и сетевой безопасности с целью предотвращения атак и управления трафиком. Администраторы могут использовать списки ACL для определения классов трафика и управления ими на сетевых устройствах в соответствии с комплексными требованиями по безопасности.
7. Какие основные типы межсетевого экранов существуют. Система межсетевого экрана может состоять из большого количества различных устройств и компонентов. Одним из компонентов является фильтрация трафика, именно эта функция и рассматривается обычно в качестве межсетевого экрана. Существуют межсетевой экран с фильтрацией пакетов, межсетевой экран с сохранением состояния, шлюз прикладного уровня (прокси-сервер).
8. Что такое зональные межсетевые экраны. Зональный межсетевой экран (ZPF) - экран, в котором интерфейсы назначаются для зон безопасности, а политика межсетевого экрана применяется к трафику, распространяющемуся между этими зонами.
9. Перечислите инструменты для тестирования локальной сети. Для тестирования сети можно использовать различные программные средства, в том числе: Nmap/Zenmap, SuperScan, SIEM, GFI LANguard, Tripwire, Nessus.
10. Расскажите про внедрение системы предотвращения вторжений. Технологии IPS, IDS. В обеих технологиях – IDS и IPS – используются сигнатуры для обнаружения определенных шаблонов в сетевом трафике. Сигнатура – это набор правил, который IDS или IPS используют для обнаружения вредоносной активности.
11. Что такое сигнатуры IPS. Сетевая инфраструктура должна обладать возможностью определять входной вредоносный трафик, чтобы блокировать его. К счастью, вредоносный трафик обладает выраженными характеристиками или «сигнатурами». Сигнатура – это набор правил, который IDS или IPS используют для обнаружения типичных вторжений, например атак DoS.
12. Что такое оконечные устройства. Оконечные устройства - Хосты, включающие ноутбуки, настольные компьютеры, серверы и IP-телефоны, которые подвержены атакам со стороны вредоносного ПО.
13. Обозначьте факторы, которые необходимо учитывать при обеспечении безопасности на 2-м уровне. Если сотрудник или посетитель, имеющий доступ к внутренней сети, сможет получить контроль над кадрами 2-го уровня, все меры безопасности, реализованные на более высоких уровнях модели OSI, станут бесполезными. Сотрудник сможет также нанести ущерб сетевой инфраструктуре локальной сети 2-го уровня.
14. Внедрение технологий межсетевого экрана. Состоит из определения места межсетевого экрана в составе локальной сети, настройки сетевых интерфейсов, подключения базы данных об угрозах, настройки фильтрации трафика.
15. Назовите метода обеспечения аутентификации при передачи данных. В криптографии код аутентификации на основе хеш-функции с ключом (HMAC или KHMAC) относится к кодам аутентификации сообщений (MAC).
16. Методы обеспечения целостности данных. Алгоритм MD5 – это алгоритм хеширования, разработанный Роном Ривестом (Ron Rivest), который сегодня используется во многих интернет-приложениях. Национальный институт стандартов и технологий (NIST) США разработал алгоритм SHA, закрепленный в стандарте Secure Hash Standard (SHS).
17. Симметричные методы обеспечения конфиденциальности. Симметричные алгоритмы – В этих алгоритмах для шифрования и дешифрования данных используется одинаковый предварительно согласованный ключ, который иногда называется секретным ключом. Предварительно согласованный ключ известен отправителю и получателю до начала обмена зашифрованными сообщениями. Поскольку обе стороны стоят на страже общего секрета, в таких алгоритмах

шифрования могут использоваться более короткие ключи. Более короткие ключи означают более быстрое исполнение.

18. Криптография открытых ключей, ее применение в защите локальной сети. Асимметричные алгоритмы, которые также называются алгоритмами с открытыми ключами, разработаны таким образом, что ключ, используемый для шифрования, отличается от ключа, используемого для дешифрования. В течение разумного периода времени ключ дешифрования не может быть вычислен как ключ шифрования, и наоборот.
19. Компоненты сети IPsec VPN и их функционирование. IPsec - это стандарт IETF (RFC 2401-2412), который определяет способ защиты сетей VPN в IP-сетях. Протокол IPsec обеспечивает защиту и аутентификацию IP-пакетов между источником и местом назначения. IPsec может защищать практически весь трафик от уровня 4 до уровня 7.
20. Расскажите про тестирование безопасности сети. Тестирование безопасности позволяет получать больше данных для разнообразных административных задач, включая анализ рисков и аварийное планирование. Очень важно документировать результаты тестирования безопасности и предоставлять их персоналу, занятому в других областях ИТ.

Задания раздела 20.3 рекомендуются к использованию при проведении диагностических работ с целью оценки остаточных результатов освоения данной дисциплины (знаний, умений, навыков).