МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Институт математики и информационных технологий
Кафедра алгебраических и информационных систем

«УТВЕРЖДАЮ»
Директор ИМИТ ИГУ
_____ М. В. Фалалеев
«29» апреля 2026 г.

Рабочая программа дисциплины (модуля)

Б1.О.22 Информационная безопасность

Направление подготовки	09.03.03 Прикладная информатика
Направленность (профиль) подготовки	Проектирование и разработка информационных систем
Квалификация выпускника	бакалавр
Форма обучения	очная

Иркутск 2026 г.

I. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ (МОДУЛЯ)

Цели: Формирование у обучающихся комплекса теоретических знаний и практических навыков в области защиты информации, обеспечивающих способность внедрять и сопровождать защищенные информационные системы с учетом современных угроз, стандартов информационной безопасности и требований нормативной базы Российской Федерации.

Задачи:

— Освоение теоретических основ и современных методов защиты информации;

— Приобретение практических навыков работы со средствами защиты информации;

— .

II. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

2.1. Учебная дисциплина (модуль) «Информационная безопасность» относится к части, формируемой участниками образовательных отношений «Блок 1. Дисциплины (модули)».

Дисциплина «Защита информации» формирует у студентов теоретические знания и практические навыки в области обеспечения информационной безопасности, включая изучение современных методов и средств защиты данных и анализ угроз функционирования информационных систем.

2.2. Для изучения данной учебной дисциплины (модуля) необходимы знания, умения и навыки, формируемые предшествующими дисциплинами:

— Дискретная математика;

— Вычислительные системы и компьютерные сети;

— Информатика;

— Системное и прикладное программное обеспечение;

— Базы данных;

— Операционные системы;

— Проектирование информационных систем;

— Информационные системы и технологии.

2.3. Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной:

— Стандартизация, сертификация и управление качеством программного обеспечения;

— Технологии хранения и обработки больших данных;

— Администрирование компьютерных сетей.

III. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс освоения дисциплины направлен на формирование компетенций (элементов следующих компетенций) в соответствии с ФГОС ВО и ОП ВО по данному направлению подготовки:

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Компетенция	Индикаторы компетенций	Результаты обучения
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**ОПК-3.1** Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	• Знать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
	ОПК-3.2 Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	• Решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
	ОПК-3.3 Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографий по научно-исследовательской работе с учетом требований информационной безопасности	• Владеть навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографий по научно-исследовательской работе с учетом требований информационной безопасности
ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	**ОПК-4.1** Знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы	• Знать основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы
	ОПК-4.2 Применяет стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы	• Применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы

IV. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 4 зачетных единицы, 144 часа, в том числе 54 часа на контроль, из них 54 часа на экзамен.

Из них реализуется с использованием электронного обучения и дистанционных образовательных технологий 26 часов самостоятельной работы.

Форма промежуточной аттестации: экзамен.

4.1 Содержание дисциплины, структурированное по темам, с указанием видов учебных занятий и СРС, отведенного на них количества академических часов

п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)				Формы текущего контроля успеваемости; Форма промежуточной аттестации (по семестрам)
			Контактная работа преподавателя с обучающимися			Самостоятельная работа	
			Лекции	Семинарские (практические) занятия	Консультации		
1	Введение в информационную безопасность	6	2	2	0	2	
2	PKI и электронная подпись	6	2	2	0	2	
3	Анализ электронных журналов	6	2	2	0	2	
4	Антивирусные системы	6	2	2	0	2	
5	Аппаратные угрозы	6	2	2	0	2	
6	Межсетевые экраны	6	2	4	0	2	
7	Криптографические методы защиты информации	6	2	2	0	2	
8	Отказоустойчивость систем	6	2	2	0	2	
9	Сетевая безопасность	6	4	4	0	2	
10	Системы обнаружения вторжений	6	4	4	0	2	
11	Социальная инженерия	6	2	2	0	2	
12	Управление рисками информационной безопасности	6	2	2	0	2	
13	Стандарты ИБ	6	4	2	0	2	
Итого за 6 семестр			**32**	**32**	**0**	**26**	**Экз (54)**
Итого часов			**32**	**32**	**0**	**26**	

4.2 План внеаудиторной самостоятельной работы обучающихся по дисциплине

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Затраты времени, час. (из них с применением ДОТ)		
6	Введение в информационную безопасность	**Для овладения знаниями:** чтение учебной литературы, чтение дополнительной литературы **Для закрепления и систематизации знаний:** работа с конспектом лекций	неделя	2 (2)	Пз	ЭОС forlabs
6	PKI и электронная подпись	**Для овладения знаниями:** чтение учебной литературы, чтение дополнительной литературы, использование аудио- и видео-записей, компьютерной техники и интернета **Для закрепления и систематизации знаний:** работа с конспектом лекций, составление таблиц для систематизации учебного материала	Неделя	2 (2)	Тест, Пз	ЭОС forlabs
6	Анализ электронных журналов	**Для овладения знаниями:** чтение учебной литературы, чтение дополнительной литературы, использование аудио- и видео-записей, компьютерной техники и интернета **Для закрепления и систематизации знаний:** работа с конспектом лекций **Для формирования умений:** работа с тренажером	Неделя	2 (2)	Пз	ЭОС forlabs
6	Антивирусные системы	**Для овладения знаниями:** чтение учебной литературы, чтение дополнительной литературы, использование аудио- и видео-записей, компьютерной техники и интернета **Для закрепления и систематизации знаний:** работа с конспектом лекций **Для формирования умений:** работа с тренажером	Неделя	2 (2)	Пз	ЭОС forlabs

6	Аппаратные угрозы	**Для овладения знаниями:** чтение учебной литературы, чтение дополнительной литературы, использование аудио- и видео-записей, компьютерной техники и интернета **Для закрепления и систематизации знаний:** работа с конспектом лекций **Для формирования умений:** работа с тренажером	Неделя	2 (2)	КЛ	ЭОС forlabs
6	Межсетевые экраны	**Для овладения знаниями:** чтение учебной литературы, чтение дополнительной литературы, использование аудио- и видео-записей, компьютерной техники и интернета **Для закрепления и систематизации знаний:** работа с конспектом лекций **Для формирования умений:** работа с тренажером	Неделя	2 (2)	КЛ	ЭОС forlabs
6	Криптографические методы защиты информации	**Для овладения знаниями:** чтение учебной литературы, чтение дополнительной литературы, использование аудио- и видео-записей, компьютерной техники и интернета **Для закрепления и систематизации знаний:** работа с конспектом лекций **Для формирования умений:** решение задач	Неделя	2 (2)	КЛ	ЭОС forlabs
6	Отказоустойчивость систем	**Для овладения знаниями:** чтение учебной литературы, чтение дополнительной литературы, использование аудио- и видео-записей, компьютерной техники и интернета **Для закрепления и систематизации знаний:** работа с конспектом лекций **Для формирования умений:** работа с тренажером	Неделя	2 (2)	КЛ	ЭОС forlabs
6	Сетевая безопасность	**Для овладения знаниями:** чтение учебной литературы, чтение дополнительной литературы **Для закрепления и систематизации знаний:** работа с конспектом лекций **Для формирования умений:** решение задач, работа с тренажером	Неделя	2 (2)	КЛ	ЭОС forlabs

6	Системы обнаружения вторжений	**Для овладения знаниями:** чтение учебной литературы, чтение дополнительной литературы, использование аудио- и видео-записей, компьютерной техники и интернета **Для закрепления и систематизации знаний:** работа с конспектом лекций **Для формирования умений:** работа с тренажером	Неделя	2 (2)	КЛ	ЭОС forlabs
6	Социальная инженерия	**Для овладения знаниями:** чтение учебной литературы, чтение дополнительной литературы, использование аудио- и видео-записей, компьютерной техники и интернета **Для закрепления и систематизации знаний:** работа с конспектом лекций, составление плана и тезисов ответа, подготовка доклада **Для формирования умений:** решение задач, работа с тренажером	Неделя	2 (2)	КЛ	ЭОС forlabs
6	Управление рисками информационной безопасности	**Для овладения знаниями:** чтение учебной литературы, чтение дополнительной литературы, использование аудио- и видео-записей, компьютерной техники и интернета **Для закрепления и систематизации знаний:** работа с конспектом лекций **Для формирования умений:** работа с тренажером	Неделя	2 (2)	КЛ	ЭОС forlabs
6	Стандарты ИБ	**Для овладения знаниями:** чтение учебной литературы, чтение дополнительной литературы **Для закрепления и систематизации знаний:** работа с конспектом лекций **Для формирования умений:** решение задач Подготовка к экзамену	Неделя	2 (2)	КЛ	ЭОС forlabs
Общая трудоемкость самостоятельной работы по дисциплине (час)				**26**		
Из них объем самостоятельной работы с использованием электронного обучения и дистанционных образовательных технологий (час)				**26**		

Бюджет времени самостоятельной работы, предусмотренный учебным планом для данной дисциплины (час)	**26**		

4.3 Содержание учебного материала

Трудоемкость дисциплины (з.е.)	4
Наименование основных разделов (модулей)	Введение в информационную безопасность PKI и электронная подпись Анализ электронных журналов Антивирусные системы Аппаратные угрозы Межсетевые экраны Криптографические методы защиты информации Отказоустойчивость систем Сетевая безопасность Системы обнаружения вторжений Социальная инженерия Управление рисками информационной безопасности Стандарты ИБ
Формы текущего контроля	Практическое задание, устный опрос, тест, лабораторная работа, конспект лекций, реферат, деловая игра, контрольная работа
Форма промежуточной аттестации	Экзамен

4.3.1. Перечень семинарских, практических занятий и лабораторных работ

№ п/п	№ раздела и темы дисциплины (модуля)	Наименование семинаров, практических и лабораторных работ	Трудоемкость, час. (из них электронные часы)	Оценочные средства	Формируемые компетенции
1	1	Задачи ИБ	2 (0)	УО	ОПК-4.1, ОПК-4.2, ОПК-3.1
2	2	Электронная подпись	2 (0)	Тест, ЛР	ОПК-4.1, ОПК-4.2, ОПК-3.1, ОПК-3.2, ОПК-3.3
3	3	Обработка текстовых электронных журналов	2 (0)	ЛР	ОПК-4.1, ОПК-4.2, ОПК-3.1, ОПК-3.2, ОПК-3.3

№ п/п	№ раздела и темы дисциплины (модуля)	Наименование семинаров, практических и лабораторных работ	Трудоемкость, час. (из них электронные часы)	Оценочные средства	Формируемые компетенции
4	4	Используя предоставленные преподавателем средства сканирования ОС на вредоносное ПО провести обследование тестовой виртуальной ОС	2 (0)	ЛР	ОПК-4.1, ОПК-4.2, ОПК-3.1, ОПК-3.2, ОПК-3.3
5	5	Реферат по открытым источникам	2 (0)	Реф	ОПК-4.1, ОПК-4.2, ОПК-3.1, ОПК-3.2, ОПК-3.3
6	6	Обзор открытых источников	4 (0)	Реф	ОПК-4.1, ОПК-4.2, ОПК-3.1, ОПК-3.2, ОПК-3.3
7	7	Использование российских алгоритмов (ГОСТ 34.10-2012, ГОСТ 34.11-2012, ГОСТ Р 34.13-2015	2 (0)	Реф	ОПК-3.2, ОПК-3.3, ОПК-4.1
8	8	Методы и примеры решений достижения отказоустойчивости	2 (0)	Реф	ОПК-3.2, ОПК-3.3, ОПК-4.1
9	9	обеспечение сетевой безопасности	4 (0)	ЛР	ОПК-4.2
10	10	Этапы работы и примеры систем обнаружения вторжений (IDS)	4 (0)	Пз	ОПК-4.1, ОПК-4.2, ОПК-3.1, ОПК-3.2, ОПК-3.3
11	11	Определение пароля	2 (0)	Деловая игра	ОПК-4.2
12	12	Определение типовых рисков ИБ	2 (0)	Пз	ОПК-4.2
13	13	Разработка регламента	2 (0)	КР	ОПК-4.2

4.3.2. Перечень тем (вопросов), выносимых на самостоятельное изучение самостоятельной работы студентов

№ п/п	Тема	Задание	Формируемая компетенция	ИДК
1	Введение в информационную безопасность	Анализ рисков	ОПК-4, ОПК-3	ОПК-4.1 ОПК-4.2 ОПК-3.1
2	PKI и электронная подпись	Электронная подпись	ОПК-3, ОПК-4	ОПК-3.2 ОПК-3.3 ОПК-4.1
3	Анализ электронных журналов	Средства анализа текстовых файлов	ОПК-3, ОПК-4	ОПК-3.2 ОПК-3.3 ОПК-4.1
4	Антивирусные системы	провести сканирование вредоносного ПО на собственном ПК	ОПК-4, ОПК-3	ОПК-4.1 ОПК-4.2 ОПК-3.1 ОПК-3.2 ОПК-3.3
5	Аппаратные угрозы	обзор актуальных аппаратных средств ИБ	ОПК-4, ОПК-3	ОПК-4.1 ОПК-4.2 ОПК-3.1 ОПК-3.2 ОПК-3.3
6	Межсетевые экраны	обзор из открытых источников	ОПК-4, ОПК-3	ОПК-4.1 ОПК-4.2 ОПК-3.1 ОПК-3.2 ОПК-3.3
7	Криптографические методы защиты информации	Описание криптографических алгоритмов	ОПК-4	ОПК-4.2
8	Отказоустойчивость систем	Методы и примеры решений достижения отказоустойчивости	ОПК-4, ОПК-3	ОПК-4.1 ОПК-4.2 ОПК-3.1 ОПК-3.2 ОПК-3.3
9	Сетевая безопасность	Типичные угрозы сетевой безопасности	ОПК-3, ОПК-4	ОПК-3.2 ОПК-3.3 ОПК-4.1
10	Системы обнаружения вторжений	Обзор систем обнаружения вторжений	ОПК-4, ОПК-3	ОПК-4.1 ОПК-4.2 ОПК-3.1
11	Социальная инженерия	Подготовка к практическим занятиям на основе материалов лекций	ОПК-4	ОПК-4.2

№ п/п	Тема	Задание	Формируемая компетенция	ИДК
12	Управление рисками информационной безопасности	Анализ материалов лекций	ОПК-3, ОПК-4	ОПК-3.2 ОПК-3.3 ОПК-4.1
13	Стандарты ИБ	Изучить нормативно-правовые материалы	ОПК-3, ОПК-4	ОПК-3.2 ОПК-3.3 ОПК-4.1

4.4. Методические указания по организации самостоятельной работы студентов

Самостоятельная работа студентов всех форм и видов обучения является одним из обязательных видов образовательной деятельности, обеспечивающей реализацию требований Федеральных государственных стандартов высшего профессионального образования. Согласно требованиям нормативных документов самостоятельная работа студентов является обязательным компонентом образовательного процесса, так как она обеспечивает закрепление получаемых на лекционных занятиях знаний путем приобретения навыков осмысления и расширения их содержания, навыков решения актуальных проблем формирования общекультурных и профессиональных компетенций, научно-исследовательской деятельности, подготовки к семинарам, лабораторным работам, сдаче зачетов и экзаменов. Самостоятельная работа студентов представляет собой совокупность аудиторных и внеаудиторных занятий и работ. Самостоятельная работа в рамках образовательного процесса в вузе решает следующие задачи:

— закрепление и расширение знаний, умений, полученных студентами во время аудиторных и внеаудиторных занятий, превращение их в стереотипы умственной и физической деятельности;

— приобретение дополнительных знаний и навыков по дисциплинам учебного плана;

— формирование и развитие знаний и навыков, связанных с научно-исследовательской деятельностью;

— развитие ориентации и установки на качественное освоение образовательной программы;

— развитие навыков самоорганизации;

— формирование самостоятельности мышления, способности к саморазвитию, самосовершенствованию и самореализации;

— выработка навыков эффективной самостоятельной профессиональной теоретической, практической и учебно-исследовательской деятельности.

Подготовка к лекции. Качество освоения содержания конкретной дисциплины прямо зависит от того, насколько студент сам, без внешнего принуждения формирует у себя установку на получение на лекциях новых знаний, дополняющих уже имеющиеся по данной дисциплине. Время на подготовку студентов к двухчасовой лекции по нормативам составляет не менее 0,2 часа.

Подготовка к практическому занятию. Подготовка к практическому занятию включает следующие элементы самостоятельной деятельности: четкое представление цели и задач его проведения; выделение навыков умственной, аналитической, научной деятельности, которые станут результатом предстоящей работы. Выработка навыков осуществляется с помощью получения новой информации об изучаемых процессах и с помощью

знания о том, в какой степени в данное время студент владеет методами исследовательской деятельности, которыми он станет пользоваться на практическом занятии. Подготовка к практическому занятию нередко требует подбора материала, данных и специальных источников, с которыми предстоит учебная работа. Студенты должны дома подготовить к занятию 3–4 примера формулировки темы исследования, представленного в монографиях, научных статьях, отчетах. Затем они самостоятельно осуществляют поиск соответствующих источников, определяют актуальность конкретного исследования процессов и явлений, выделяют основные способы доказательства авторами научных работ ценности того, чем они занимаются. В ходе самого практического занятия студенты сначала представляют найденные ими варианты формулировки актуальности исследования, обсуждают их и обосновывают свое мнение о наилучшем варианте. Время на подготовку к практическому занятию по нормативам составляет не менее 0,2 часа.

Подготовка к контрольной работе. Контрольная работа назначается после изучения определенного раздела (разделов) дисциплины и представляет собой совокупность развернутых письменных ответов студентов на вопросы, которые они заранее получают от преподавателя. Самостоятельная подготовка к контрольной работе включает в себя: — изучение конспектов лекций, раскрывающих материал, знание которого проверяется контрольной работой; повторение учебного материала, полученного при подготовке к семинарским, практическим занятиям и во время их проведения; изучение дополнительной литературы, в которой конкретизируется содержание проверяемых знаний; составление в мысленной форме ответов на поставленные в контрольной работе вопросы; формирование психологической установки на успешное выполнение всех заданий. Время на подготовку к контрольной работе по нормативам составляет 2 часа.

Подготовка к экзамену. Самостоятельная подготовка к экзамену схожа с подготовкой к зачету, особенно если он дифференцированный. Но объем учебного материала, который нужно восстановить в памяти к экзамену, вновь осмыслить и понять, значительно больше, поэтому требуется больше времени и умственных усилий. Важно сформировать целостное представление о содержании ответа на каждый вопрос, что предполагает знание разных научных трактовок сущности того или иного явления, процесса, умение раскрывать факторы, определяющие их противоречивость, знание имен ученых, изучавших обсуждаемую проблему. Необходимо также привести информацию о материалах эмпирических исследований, что указывает на всестороннюю подготовку студента к экзамену. Время на подготовку к экзамену по нормативам составляет 36 часов для бакалавров.

Формы внеаудиторной самостоятельной работы

Составление глоссария Цель самостоятельной работы: повысить уровень информационный культуры; приобрести новые знания; отработать необходимые навыки в предметной области учебного курса. Глоссарий — словарь специализированных терминов и их определений. Статья глоссария — определение термина. Содержание задания: сбор и систематизация понятий или терминов, объединенных общей специфической тематикой, по одному либо нескольким источникам. Выполнение задания: 1) внимательно прочитать работу; 2) определить наиболее часто встречающиеся термины; 3) составить список терминов, объединенных общей тематикой; 4) расположить термины в алфавитном порядке; 5) составить статьи глоссария: — дать точную формулировку термина в именительном падеже; — объемно раскрыть смысл данного термина Планируемые результаты самостоятельной работы: способность студентов решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением

информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Разработка проекта (индивидуального, группового) Цель самостоятельной работы: развитие способности прогнозировать, проектировать, моделировать. Проект — «ограниченное во времени целенаправленное изменение отдельной системы с установленными требованиями к качеству результатов, возможными рамками расхода средств и ресурсов и специфической организацией». Выполнение задания: 1) диагностика ситуации (проблематизация, целеполагание, конкретизация цели, форматирование проекта); 2) проектирование (уточнение цели, функций, задач и плана работы; теоретическое моделирование методов и средств решения задач; детальная проработка этапов решения конкретных задач; пошаговое выполнение запланированных проектных действий; систематизация и обобщение полученных результатов, конструирование предполагаемого результата, пошаговое выполнение проектных действий); 3) рефлексия (выяснение соответствия полученного результата замыслу; определение качества полученного продукта; перспективы его развития и использования). Предполагаемые результаты самостоятельной работы: готовность студентов использовать знание современных проблем науки и образования при решении образовательных и профессиональных задач; готовность использовать индивидуальные креативные способности для оригинального решения исследовательских задач; — способность прогнозировать, проектировать, моделировать.

Информационный поиск Цель самостоятельной работы: развитие способности к проектированию и преобразованию учебных действий на основе различных видов информационного поиска. Информационный поиск — поиск неструктурированной документальной информации. Список современных задач информационного поиска: решение вопросов моделирования; классификация документов; фильтрация, классификация документов; проектирование архитектур поисковых систем и пользовательских интерфейсов; извлечение информации (аннотирование и реферирование документов); выбор информационно-поискового языка запроса в поисковых системах. Содержание задания по видам поиска: поиск библиографический — поиск необходимых сведений об источнике и установление его наличия в системе других источников. Ведется путем разыскания библиографической информации и библиографических пособий (информационных изданий); поиск самих информационных источников (документов и изданий), в которых есть или может содержаться нужная информация; — поиск фактических сведений, содержащихся в литературе, книге (например, об исторических фактах и событиях, о биографических данных из жизни и деятельности писателя, ученого и т. п.). Выполнение задания:

1) определение области знаний;

2) выбор типа и источников данных;

3) сбор материалов, необходимых для наполнения информационной модели;

4) отбор наиболее полезной информации;

5) выбор метода обработки информации (классификация, кластеризация, регрессионный анализ и т.д.);

6) выбор алгоритма поиска закономерностей;

7) поиск закономерностей, формальных правил и структурных связей в собранной информации;

8) творческая интерпретация полученных результатов.

Планируемые результаты самостоятельной работы: — способность студентов решать стандартные задачи профессиональной деятельности на основе информационной и

библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; готовность использовать знание современных проблем науки и образования при решении образовательных и профессиональных задач.

Разработка мультимедийной презентации Цели самостоятельной работы (варианты): — освоение (закрепление, обобщение, систематизация) учебного материала; — обеспечение контроля качества знаний; — формирование специальных компетенций, обеспечивающих возможность работы с информационными технологиями; — становление общекультурных компетенций. Мультимедийная презентация — представление содержания учебного материала, учебной задачи с использованием мультимедийных технологий.

Выполнение задания:

1. Этап проектирования: — определение целей использования презентации; — сбор необходимого материала (тексты, рисунки, схемы и др.); — формирование структуры и логики подачи материала; — создание папки, в которую помещен собранный материал.

2. Этап конструирования: — выбор программы MS PowerPoint в меню компьютера; — определение дизайна слайдов; — наполнение слайдов собранной текстовой и наглядной информацией; — включение эффектов анимации и музыкального сопровождения (при необходимости); — установка режима показа слайдов (титульный слайд, включающий наименование кафедры, где выполнена работа, название презентации, город и год; содержательный — список слайдов презентации, сгруппированных по темам сообщения; заключительный слайд содержит выводы, пожелания, список литературы и пр.).

3. Этап моделирования — проверка и коррекция подготовленного материала, определение продолжительности его демонстрации.

Планируемые результаты самостоятельной работы: — повышение информационной культуры студентов и обеспечение их готовности к интеграции в современное информационное пространство; — способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; — способность к критическому восприятию, обобщению, анализу профессиональной информации, постановке цели и выбору путей ее достижения; — способность применять современные методики и технологии организации и реализации образовательного процесса на различных образовательных ступенях в различных образовательных учреждениях; — готовность использовать индивидуальные креативные способности для оригинального решения исследовательских задач.

В ФБГОУ ВО «ИГУ» организация самостоятельной работы студентов регламентируется Положением о самостоятельной работе студентов, принятым Ученым советом ИГУ 22 июня 2012 г.

4.5. Примерная тематика курсовых работ (проектов)

По данной дисциплине выполнение курсовых проектов (работ) не предусматривается.

V. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

а) основная литература

1. Нестеров, Сергей Александрович. Информационная безопасность [Текст] : учебник и практикум для акад. бакалавриата / С. А. Нестеров ; С.-Петербург. политехн. ун-т Петра Великого. - М. : Юрайт, 2016. - 321 с. ; 24 см. - (Университеты России). - Библиогр.: с.

319-321. - ISBN 978-5-9916-7227-6 : 788.23 р.

2. Прохорова, Ольга Витольдовна. Информационная безопасность и защита информации [Текст] : учебник / О. В. Прохорова. - 2-е изд., испр. - СПб. : Лань, 2020. - 121 с. : ил., табл. ; 20 см. - (Учебники для вузов. Специальная литература). - Библиогр.: с. 118-119. - ISBN 978-5-8114-4404-5 : 489.50 р.

3. Сычев, Юрий Николаевич. Защита информации и информационная безопасность [Текст] : учеб. пособие для студ. вузов, обуч. по направл. подготовки 10.03.01 "Информ. безопасность" (квалификация (степень) "бакалавр") / Ю. Н. Сычев. - М. : Инфра-М, 2021. - 200 с. : ил. ; 22 см. - (Высшее образование. Бакалавриат). - Библиогр.: с. 191-198. - ISBN 978-5-16-014976-9 : 858.82 р.

б) дополнительная литература

1. Международная информационная безопасность: теория и практика [Электронный ресурс] : в 3 т. - 2-е изд., доп. - Электрон. текстовые дан., 4,60 Мб. - М. : Аспект Пресс, 2021

2. Нестеров, Сергей Александрович. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ [Электронный ресурс] : учебник и практикум / Нестеров С.А. - Электрон. текстовые дан. - М. : Издательство Юрайт, 2016. - 321 с. - (Университеты России). - ЭБС "Юрайт". - Неогранич. доступ. - ISBN 978-5-9916-7227-6 : 3000.00 р.

в) периодическая литература

Нет.

г) базы данных, информационно-справочные и поисковые системы

Нет.

В соответствии с п. 4.3.4. ФГОС ВО, обучающимся в течение всего периода обучения обеспечен неограниченный доступ (удаленный доступ) к электронно-библиотечным системам:

— Открытая электронная база ресурсов и исследований «Университетская информационная система РОССИЯ» [Электронный ресурс] : сайт. – Режим доступа: http://uisrussia.msu.ru бессрочный

— Государственная информационная система «Национальная электронная библиотека» [Электронный ресурс] : сайт. – Режим доступа: http://нэб.рф. бессрочный

— Научная электронная библиотека «ELIBRARY.RU» [Электронный ресурс] : сайт. - Контракт № 148 от 23.12.2020 г. Акт от 24.12.2020 г. Срок действия по 31.12.2022 г. – Режим доступа: http://elibrary.ru/

— ЭБС «Издательство Лань». Контракт № 04-Е-0346 от 12.11.2021 г. № 976 от 14.11.2021 г. Срок действия по 13.11.2022 г. – Режим доступа: https://www.e.lanbook.com

— ЭБС ЭЧЗ «Библиотех». Государственный контракт № 019 от 22.02.2011 г. ООО «Библиотех». Лицензионное соглашение к Государственному контракту № 019 от 22.02.2011. Срок действия: бессрочный. – Режим доступа: https://isu.bibliotech.ru/

— ЭБС «Руконт» ЦКБ «Бибком». № 04-Е-0343 от 12.11.2021 г. Акт № бК-5195 от 14.11.2021 г. Срок действия по 13.11.2022г. – Режим доступа: http://rucont.ru

— ЭБС «Айбукс.ру/ibooks.ru» ООО «Айбукс». Контракт № 04-Е-0344 от 12.11.2021 г.; Акт от 14.11.2021 г. Срок действия по 13.11.2022 г. – Режим доступа: http://ibooks.ru

— Электронно-библиотечная система «ЭБС Юрайт». ООО «Электронное издательство Юрайт». Контракт № 04-Е-0258 от 20.09.2021г. Контракт № 04-Е-0258 от 20.09.2021 г. Срок действия по 17.10. 2022 г. – Режим доступа: https://urait.ru

— УБД ИВИС. Контракт № 04-Е-0347 от 12.11.2021 г. Акт от 15.11.2021 г. Срок действия с 01.01.2022 по 31.12.2022 г. – Режим доступа: http://dlib.eastview.com

— Электронная библиотека ИД Гребенников. Контракт № 04-Е-0348 от 12.11.2021г.; Акт № 348 от 15.11.2021 г. Срок действия с 01.01.2022 по 31.12.2022 – Режим доступа: http://grebennikon.ru

VI. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Учебно-лабораторное оборудование

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа

Специальные помещения: Учебная аудитория для проведения занятий лекционного и семинарского типа,текущего контроля, промежуточной аттестации.	Аудитория оборудована специализированной учебной мебелью, техническими средствами обучения, служащими для представления информации большой аудитории: Ноутбук(AserAspirev3-5516 (AMDA10-4600M 2300 Мгц)) (1 штука) с неограниченным доступом к сети Интернет; Проектор Vivitek, экран ScreenVtdiaEcot- 3200*200MW 1:1, колонки, наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации, соответствующие рабочей программе дисциплины «Архитектурный подход к развитию предприятий и информационных систем». Учебная лаборатория: компьютеры для проведения практических работ (Системный блок AMDAthlon-64 X3 445 3100 МГц), Монитор LG F1742S (2 штуки), Монитор ViewSonic VA703b(24 штуки) с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации; проектор Sony XGA VPLSX535, экран ScreenVtdiaEcot- 3200*200MW 1:1	ОС Windows: DreamSpark Premium, Договор № 03-016-14 от 30.10.2014 Microsoft Office: 0365ProPiusOpenStudents ShrdSvr ALNG subs VL NL I MthAcdmsStdnt w/Faculty (15000 лицензий) Kaspersky Endpoint Security длябизнеса- стандартный Russian Edition. 15002499 Node 1 year Educational License № 1B08-170221-054045-730-177 BusinessStudio Лицензия № 7464 (бессрочно)

Специальные помещения: компьютерный класс (учебная аудитория) для групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), организации самостоятельной работы, в том числе, научно-исследовательской	Аудитория оборудована специализированной учебной мебелью, техническими средствами обучения: компьютеры (системный блок AMD Athlon 64 X2 DualCore 3600+ 1900 МГц (15 штук), Монитор LGFlatron L1742SE (14 штук), Монитор ViewSonic VG720) с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.	ОС Windows: DreamSpark Premium, Договор № 03-016-14 от 30.10.2014 Microsoft Office: 0365ProPiusOpenStudents ShrdSvr ALNG subs VL NL I MthAcdmsStdnt w/Faculty (15000 лицензий Kaspersky Endpoint Security для бизнеса- стандартный Russian Edition. 15002499 Node 1 year Educational License № 1B08¬170221-054045¬730¬177

6.2. Программное обеспечение

№	Наименование Программного продукта	Кол-во	Обоснование для пользования ПО	Дата выдачи лицензии	Срок действия права пользования
1	UbuntuLinux 16.04.1	Условия правообладателя	Условия использования по ссылке: https://www.ubuntu.com/legal/terms-and-policies/terms	Условия правообладателя	Условия правообладателя

6.3. Технические и электронные средства

Методической системой преподавания предусмотрено использование технических и электронных средств обучения и контроля знаний студентов: мультимедийные презентации, фрагменты фильмов.

VII. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

При реализации программы данной дисциплины используются различные образовательные технологии, в том числе электронное обучение и дистанционные образовательные технологии.

Проблемное обучение	Создание в учебной деятельности проблемных ситуаций и организация активной самостоятельной деятельности учащихся по их разрешению, в результате чего происходит творческое овладение знаниями, умениями, навыками, развиваются мыслительные способности
Разноуровневое обучение	У преподавателя появляется возможность помогать слабому, уделять внимание сильному, реализуется желание сильных учащихся быстрее и глубже продвигаться в образовании. Сильные учащиеся утверждаются в своих способностях, слабые получают возможность испытывать учебный успех, повышается уровень мотивации ученья.

Проектные методы обучения	Работа по данной методике дает возможность развивать индивидуальные творческие способности учащихся, более осознанно подходить к профессиональному и социальному самоопределению
Исследовательские методы в обучении	Дает возможность учащимся самостоятельно пополнять свои знания, глубоко вникать в изучаемую проблему и предполагать пути ее решения, что важно при формировании мировоззрения. Это важно для определения индивидуальной траектории развития каждого обучающегося
Лекционно-семинарскозачетная система	Данная система дает возможность сконцентрировать материал в блоки и преподносить его как единое целое, а контроль проводить по предварительной подготовке обучающихся
Информационно-коммуникационные технологии	Изменение и неограниченное обогащение содержания образования, использование интегрированных курсов, доступ в ИНТЕРНЕТ.

Наименование тем занятий с использованием активных форм обучения:

№	Тема занятия	Вид занятия	Форма / Методы интерактивного обучения	Кол-во часов (из них электронные часы)
1				
2				
3				
4				
5				
6				

VIII. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.1. Оценочные средства текущего контроля

№ п\п	Вид контроля	Контролируемые темы (разделы)	Компетенции, компоненты которых контролируются
1	Практическое задание	Введение в информационную безопасность. PKI и электронная подпись. Анализ электронных журналов. Антивирусные системы. Системы обнаружения вторжений. Управление рисками информационной безопасности.	ОПК-4.1, ОПК-4.2, ОПК-3.1, ОПК-3.2, ОПК-3.3

2	Устный опрос	Введение в информационную безопасность.	ОПК-4.1, ОПК-4.2, ОПК-3.1
3	Тест	PKI и электронная подпись.	ОПК-4.1, ОПК-4.2, ОПК-3.1, ОПК-3.2, ОПК-3.3
4	Лабораторная работа	PKI и электронная подпись. Анализ электронных журналов. Антивирусные системы. Сетевая безопасность.	ОПК-4.2, ОПК-4.1, ОПК-3.1, ОПК-3.2, ОПК-3.3
5	Конспект лекций	Аппаратные угрозы. Межсетевые экраны. Криптографические методы защиты информации. Отказоустойчивость систем. Сетевая безопасность. Системы обнаружения вторжений. Социальная инженерия. Управление рисками информационной безопасности. Стандарты ИБ.	ОПК-4.1, ОПК-4.2, ОПК-3.1, ОПК-3.2, ОПК-3.3
6	Реферат	Аппаратные угрозы. Межсетевые экраны. Криптографические методы защиты информации. Отказоустойчивость систем.	ОПК-4.1, ОПК-4.2, ОПК-3.1, ОПК-3.2, ОПК-3.3
7	Деловая игра	Социальная инженерия.	ОПК-4.2
8	Контрольная работа	Стандарты ИБ.	ОПК-4.2

Примеры оценочных средств для текущего контроля

Демонстрационный вариант теста

1. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 05_05# Какие меры защиты от аппаратных угроз существуют?

a. Контроль электромагнитного излучения

b. Настройка брандмауэра

c. Использование средств TEMPEST-защиты

d. Установка антивируса

e. Оборудование защищенных помещений

f. Физический контроль доступа

2. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 04_04# Какие методы используют современные антивирусные системы?

a. Лингвистический анализ

b. Сигнатурный анализ

c. Анализ в песочнице

d. Нейросетевой анализ

e. Поведенческий анализ

f. Эвристический анализ

3. Задание с множественным выбором. Выберите 5 правильных ответов.

Вопрос 04_05# Какие типы вредоносного ПО существуют?

a. Вирусы

b. Троянские программы

c. Рекламное ПО

d. Черви

e. Шпионское ПО

f. Полезные утилиты

4. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 04_03# Что такое "песочница" (sandbox) в контексте антивирусных систем?

a. Шифровальное устройство

b. Средство резервного копирования

c. Изолированная среда для запуска подозрительных программ

d. База данных вирусных сигнатур

e. Система обновлений антивируса

f. Сетевой экран

5. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 03_04# Какие типы записей обычно содержатся в журналах безопасности?

a. Действия с привилегиями

b. Доступ к конфиденциальным данным

c. Свободное место на диске

d. Попытки входа в систему

e. Температура процессора

f. Изменения конфигурации

6. Задание с множественным выбором. Выберите 3 правильных ответа.

Вопрос 02_05# Какие виды электронных подписей существуют в РФ?

a. Цифровая графическая подпись

b. Простая электронная подпись

c. Биометрическая подпись

d. Усиленная неквалифицированная подпись

e. Факсимильная подпись

f. Усиленная квалифицированная подпись

7. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 05_06# Какие устройства могут представлять аппаратную угрозу?

a. Диктофоны

b. Клавиатуры

c. Смартфоны

d. Фотоаппараты

e. USB-устройства

f. Принтеры

8. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 02_02# Какой орган выдает цифровые сертификаты в PKI?

a. Удостоверяющий центр

b. Центр сертификации (CA)

c. Криптопровайдер

d. Регистрационный центр (RA)

e. Администратор безопасности

f. Пользователь

9. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 01_04# Какие виды угроз информационной безопасности существуют?

a. Внешние угрозы

b. Космические угрозы

c. Природные угрозы

d. Внутренние угрозы

e. Биологические угрозы

f. Техногенные угрозы

10. Задание с множественным выбором. Выберите 3 правильных ответа.

Вопрос 02_04# Какие функции выполняет ЭЦП?

a. Установление лица, подписавшего документ

b. Защита от подделки

c. Подтверждение целостности документа

d. Ускорение обработки

e. Автоматическое архивирование

f. Улучшение читаемости

11. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 03_06# Какие задачи решает анализ журналов в ИБ?

a. Выявление аномальной активности

b. Увеличение объема диска

c. Соответствие требованиям регуляторов

d. Расследование инцидентов

e. Аудит действий пользователей

f. Ускорение работы системы

12. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 06_01# Что такое межсетевой экран (брандмауэр)?

a. Средство шифрования данных

b. Средство резервного копирования

c. Антивирусная программа

d. Система контроля сетевого трафика

e. Система обнаружения вторжений

f. Система аутентификации

13. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 01_03# Что такое угроза информационной безопасности?

a. Техническая неисправность оборудования

b. Ошибка программиста

c. Антивирусная программа

d. Реализованная атака на систему

e. Потенциальная возможность нарушения безопасности

f. Случайное действие пользователя

14. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 03_01# Что такое системный журнал (лог)?

a. Архив резервных копий

b. Запись событий, происходящих в системе

c. Кэш-память системы

d. База данных пользователей

e. Конфигурационный файл

f. Репозиторий программного кода

15. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 05_02# Что такое TEMPEST-атаки?

a. Взлом через температурные датчики

b. Атаки через USB-порты

c. Перехват акустических сигналов

d. Радиочастотные помехи

e. Взлом через сеть питания

f. Перехват электромагнитного излучения от аппаратуры

16. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 04_01# Что такое сигнатурный анализ в антивирусных системах?

a. Анализ поведения программ

b. Проверка контрольных сумм

c. Аудит журналов событий

d. Поиск известных шаблонов вредоносного кода

e. Проверка цифровых подписей

f. Мониторинг сетевого трафика

17. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 01_06# Какие существуют классы нарушителей информационной безопасности?

a. Хакеры

b. Киберпреступники

c. Внутренние нарушители

d. Дружелюбные пользователи

e. Технические специалисты

f. Внешние нарушители

18. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 01_01# Что означает понятие информационная безопасность?

a. Защита информации только от вирусов

b. Защита паролей

c. Защита данных в интернете

d. Защита от спама

e. Защита конфиденциальности, целостности и доступности информации

f. Безопасность компьютерного железа

19. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 01_05# Какие компоненты включает система информационной безопасности?

a. Технические средства защиты

b. Социальные сети

c. Программные средства

d. Рекламные кампании

e. Правовые меры

f. Организационные меры

20. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 02_03# Что такое электронная цифровая подпись (ЭЦП)?

a. Реквизит документа, подтверждающий его подлинность

b. Графическое изображение подписи

c. Штрих-код документа

d. QR-код документа

e. Текстовый пароль

f. Сканированная копия подписи

21. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 01_02# Какие три основных принципа составляют триаду CIA?

a. Защита, контроль, мониторинг

b. Конфиденциальность, целостность, доступность

c. Шифрование, подпись, сертификация

d. Риск, угроза, уязвимость

e. Аутентификация, авторизация, аудит

f. Предотвращение, обнаружение, реагирование

22. Задание с множественным выбором. Выберите 5 правильных ответов.

Вопрос 04_05# Какие типы вредоносного ПО существуют?

a. Троянские программы

b. Черви

c. Полезные утилиты

d. Рекламное ПО

e. Шпионское ПО

f. Вирусы

23. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 04_03# Что такое "песочница" (sandbox) в контексте антивирусных систем?

a. Сетевой экран

b. Шифровальное устройство

c. Средство резервного копирования

d. База данных вирусных сигнатур

e. Изолированная среда для запуска подозрительных программ

f. Система обновлений антивируса

24. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 04_04# Какие методы используют современные антивирусные системы?

a. Эвристический анализ

b. Лингвистический анализ

c. Поведенческий анализ

d. Анализ в песочнице

e. Сигнатурный анализ

f. Нейросетевой анализ

25. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 04_02# Как называется технология обнаружения неизвестных угроз на основе поведения?

a. Белый список

b. Резервное копирование

c. Сетевая экранировка

d. Шифрование данных

e. Проактивная защита (heuristic analysis)

f. Сигнатурный анализ

26. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 02_06# Какие компоненты входят в состав PKI?

a. Регистрационный центр (RA)

b. Межсетевой экран

c. Центр сертификации (CA)

d. Система распространения ключей

e. Хранилище сертификатов

f. Антивирусное ПО

27. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 11_03# Что такое претекстинг?

a. Создание фишингового сайта

b. Использование вымышленного предлога для получения информации

c. Подбор паролей

d. Установка шпионского ПО

e. Перехват электронной почты

f. Взлом через социальные сети

28. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 03_03# Какой протокол используется для централизованного сбора логов?

a. SSH

b. SMTP

c. Syslog

d. HTTP

e. SNMP

f. FTP

29. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 01_01# Что означает понятие информационная безопасность?

a. Защита от спама

b. Защита паролей

c. Защита данных в интернете

d. Защита конфиденциальности, целостности и доступности информации

e. Безопасность компьютерного железа

f. Защита информации только от вирусов

30. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 03_04# Какие типы записей обычно содержатся в журналах безопасности?

a. Изменения конфигурации

b. Попытки входа в систему

c. Доступ к конфиденциальным данным

d. Свободное место на диске

e. Действия с привилегиями

f. Температура процессора

31. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 03_01# Что такое системный журнал (лог)?

a. База данных пользователей

b. Кэш-память системы

c. Репозиторий программного кода

d. Архив резервных копий

e. Запись событий, происходящих в системе

f. Конфигурационный файл

32. Задание с множественным выбором. Выберите 3 правильных ответа.

Вопрос 07_05# Какие типы криптографических алгоритмов существуют?

a. Алгоритмы передачи

b. Алгоритмы архивации

c. Асимметричные алгоритмы

d. Хэш-функции

e. Алгоритмы сжатия

f. Симметричные алгоритмы

33. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 12_05# Какие методы используются для оценки рисков?

a. Метод Дельфи

b. Аудит журналов

c. Матрицы рисков

d. Пентестинг

e. SWOT-анализ

f. Анализ сценариев

34. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 13_01# Какой стандарт информационной безопасности является международным?

a. PCI DSS

b. ISO/IEC 27001

c. HIPAA

d. ГОСТ Р ИСО/МЭК 27001-2006

e. ФЗ-152

f. FSTEC

35. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 11_04# Какие методы социальной инженерии существуют?

a. Сканирование портов

b. Претекстинг

c. Фишинг

d. Взлом пароля

e. Тайлгейтинг (проход за сотрудником)

f. Кви про кво (услуга за услугу)

36. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 12_02# Какой метод оценки рисков использует матрицу вероятность/ущерб?

a. Тестирование на проникновение

b. Анализ уязвимостей

c. Качественная оценка рисков

d. Статистический анализ

e. Аудит безопасности

f. Количественная оценка рисков

37. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 11_05# Какие каналы используются для фишинга?

a. Факсимильная связь

b. SMS-сообщения

c. Мессенджеры

d. Социальные сети

e. Электронная почта

f. Прямой телефонный разговор

38. Задание с множественным выбором. Выберите 5 правильных ответов.

Вопрос 12_06# Какие этапы включает процесс управления рисками?

a. Продажа рисков

b. Обработка рисков

c. Оценка рисков

d. Анализ рисков

e. Идентификация рисков

f. Мониторинг рисков

39. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 03_02# В каком каталоге обычно хранятся системные журналы в Linux?

a. /root/log

b. /tmp/log

c. /home/log

d. /var/log

e. /usr/log

f. /etc/log

40. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 02_02# Какой орган выдает цифровые сертификаты в PKI?

a. Пользователь

b. Регистрационный центр (RA)

c. Криптопровайдер

d. Центр сертификации (CA)

e. Администратор безопасности

f. Удостоверяющий центр

41. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 01_04# Какие виды угроз информационной безопасности существуют?

a. Биологические угрозы

b. Техногенные угрозы

c. Внешние угрозы

d. Природные угрозы

e. Внутренние угрозы

f. Космические угрозы

42. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 07_04# Какие задачи решает криптография?

a. Увеличение объема данных

b. Аутентификация

c. Конфиденциальность

d. Повышение скорости передачи

e. Целостность данных

f. Неотказуемость

43. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 08_06# Какие компоненты системы обычно резервируются?

a. Дисковые подсистемы
b. Мониторы
c. Серверное оборудование
d. Клавиатуры и мыши
e. Источники питания
f. Сетевые каналы
44. Задание с множественным выбором. Выберите 4 правильных ответа.
Вопрос 11_06# Какие меры защиты от социальной инженерии существуют?
a. Обучение сотрудников
b. Политика информационной безопасности
c. Установка антивируса
d. Двухфакторная аутентификация
e. Настройка брандмауэра
f. Проверка запросов на информацию
45. Задание с единичным выбором. Выберите один правильный ответ.
Вопрос 08_01# Что такое отказоустойчивость системы?
a. Полное отсутствие сбоев
b. Низкая стоимость системы
c. Быстрое восстановление после сбоя
d. Способность системы выполнять функции при отказах компонентов
e. Высокая производительность
f. Автоматическое обновление
46. Задание с единичным выбором. Выберите один правильный ответ.
Вопрос 08_03# Что такое кластеризация?
a. Объединение нескольких серверов в единую систему
b. Виртуализация серверов
c. Мониторинг системы
d. Шифрование информации
e. Сетевое экранирование
f. Резервное копирование данных
47. Задание с множественным выбором. Выберите 4 правильных ответа.
Вопрос 08_05# Какие типы резервирования применяются в ИТ-системах?
a. Временное резервирование
b. Географически распределенное
c. Пассивное (cold standby)
d. Активное (hot standby)
e. Полное резервирование
f. Частичное резервирование
48. Задание с единичным выбором. Выберите один правильный ответ.
Вопрос 12_01# Что такое риск в информационной безопасности?
a. Уязвимость в программном обеспечении

b. Страхование информационных активов

c. Антивирусная защита

d. Политика безопасности

e. Возможность атаки на систему

f. Вероятность реализации угрозы с нанесением ущерба

49. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 01_02# Какие три основных принципа составляют триаду CIA?

a. Предотвращение, обнаружение, реагирование

b. Аутентификация, авторизация, аудит

c. Защита, контроль, мониторинг

d. Шифрование, подпись, сертификация

e. Конфиденциальность, целостность, доступность

f. Риск, угроза, уязвимость

50. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 08_04# Какие методы обеспечения отказоустойчивости существуют?

a. Шифрование информации

b. Резервирование данных

c. Репликация данных

d. Антивирусная защита

e. Резервирование оборудования

f. Кластеризация

51. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 08_02# Какой уровень RAID обеспечивает зеркалирование дисков?

a. RAID 1

b. RAID 6

c. RAID 50

d. RAID 10

e. RAID 0

f. RAID 5

52. Задание с множественным выбором. Выберите 3 правильных ответа.

Вопрос 07_06# Какие алгоритмы относятся к асимметричной криптографии?

a. Blowfish

b. AES

c. RSA

d. DES

e. DSA

f. ECDSA

53. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 09_03# Что такое VPN?

a. Система видеонаблюдения

b. Виртуальная частная сеть для защищенной передачи данных

c. Сетевой протокол передачи файлов

d. Технология резервного копирования

e. Средство антивирусной защиты

f. Виртуальный приватный компьютер

54. Задание с множественным выбором. Выберите 3 правильных ответа.

Вопрос 02_04# Какие функции выполняет ЭЦП?

a. Ускорение обработки

b. Установление лица, подписавшего документ

c. Автоматическое архивирование

d. Подтверждение целостности документа

e. Защита от подделки

f. Улучшение читаемости

55. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 10_02# Какой тип IDS анализирует сетевой трафик?

a. Protocol IDS

b. Application IDS

c. Signature IDS

d. Network IDS (NIDS)

e. Host IDS (HIDS)

f. Anomaly IDS

56. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 12_04# Какие стратегии обработки рисков существуют?

a. Избегание риска

b. Принятие риска

c. Увеличение риска

d. Снижение риска

e. Передача риска

f. Игнорирование риска

57. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 05_04# Какие существуют аппаратные угрозы?

a. Визуальное наблюдение

b. Фишинговый сайт

c. Вирусная атака по сети

d. Перехват электромагнитного излучения

e. Съем носителей информации

f. Подключение сторонних устройств

58. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 09_01# Что такое сетевая безопасность?

a. Защита от аппаратных сбоев

b. Резервное копирование

c. Защита данных, передаваемых по сетям

d. Управление пользователями

e. Защита компьютеров от вирусов

f. Контроль физического доступа

59. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 12_03# Что такое обработка рисков?

a. Страхование информационных активов

b. Создание политик безопасности

c. Выявление угроз и уязвимостей

d. Процесс выбора и реализации мер по снижению рисков

e. Обучение сотрудников

f. Расчет вероятности рисков

60. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 01_03# Что такое угроза информационной безопасности?

a. Ошибка программиста

b. Реализованная атака на систему

c. Случайное действие пользователя

d. Антивирусная программа

e. Техническая неисправность оборудования

f. Потенциальная возможность нарушения безопасности

61. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 09_02# Что такое DDoS-атака?

a. Вирусная эпидемия

b. Перехват сетевого трафика

c. Подмена DNS-сервера

d. Фишинговая атака

e. Массовая атака на отказ в обслуживании

f. Взлом пароля администратора

62. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 09_04# Какие угрозы существуют в сетевой безопасности?

a. Естественные катастрофы

b. DoS/DDoS атаки

c. Человеческий фактор

d. Сниффинг (перехват трафика)

e. Аппаратные сбои

f. Спуфинг (подмена адресов)

63. Задание с множественным выбором. Выберите 3 правильных ответа.

Вопрос 02_05# Какие виды электронных подписей существуют в РФ?

a. Биометрическая подпись

b. Простая электронная подпись

c. Усиленная неквалифицированная подпись

d. Цифровая графическая подпись

e. Факсимильная подпись

f. Усиленная квалифицированная подпись

64. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 10_05# Какие типы IDS существуют?

a. Узловые (HIDS)

b. Гибридные

c. Централизованные

d. Распределенные

e. Персональные

f. Сетевые (NIDS)

65. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 05_06# Какие устройства могут представлять аппаратную угрозу?

a. Клавиатуры

b. Диктофоны

c. Принтеры

d. Фотоаппараты

e. Смартфоны

f. USB-устройства

66. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 01_06# Какие существуют классы нарушителей информационной безопасности?

a. Дружелюбные пользователи

b. Киберпреступники

c. Внутренние нарушители

d. Внешние нарушители

e. Хакеры

f. Технические специалисты

67. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 09_05# Какие технологии используются для сетевой безопасности?

a. RAID массивы

b. Резервное копирование

c. IPS/IDS системы

d. VPN

e. Межсетевые экраны

f. Системы аутентификации

68. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 05_05# Какие меры защиты от аппаратных угроз существуют?

a. Контроль электромагнитного излучения

b. Настройка брандмауэра

c. Использование средств TEMPEST-защиты

d. Физический контроль доступа

e. Установка антивируса

f. Оборудование защищенных помещений

69. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 10_01# Что такое система обнаружения вторжений (IDS)?

a. Средство аутентификации

b. Система резервного копирования

c. Система мониторинга и обнаружения атак

d. Антивирусная программа

e. Система предотвращения вторжений

f. Межсетевой экран

70. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 11_02# Что такое фишинг?

a. Подключение к Wi-Fi

b. Перехват SMS

c. Взлом пароля

d. Вирусная атака

e. DDoS-атака

f. Мошенничество с целью получения конфиденциальной информации

71. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 10_04# Какие методы обнаружения используют IDS/IPS?

a. Поведенческий анализ

b. Семантический анализ

c. Анализ аномалий

d. Статистический анализ

e. Сигнатурный анализ

f. Лингвистический анализ

72. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 06_04# Какие типы межсетевых экранов существуют?

a. Прокси-серверы

b. Персональные

c. Программные

d. Мобильные

e. Роутеры

f. Сетевые (аппаратные)

73. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 11_01# Что такое социальная инженерия?

a. Метод манипулирования людьми для получения информации

b. Программирование вирусов

c. Шифрование данных

d. Взлом компьютерных систем

e. Физический доступ к оборудованию

f. Сетевые атаки

74. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 07_02# Какой алгоритм является симметричным?

a. AES

b. MD5

c. RSA

d. DSA

e. ECDSA

f. SHA-256

75. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 06_06# Какие функции выполняют современные МЭ?

a. NAT (трансляция сетевых адресов)

b. Фильтрация пакетов

c. VPN (виртуальные частные сети)

d. Вирусное сканирование

e. Контроль состояния соединений

f. Резервное копирование

76. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 06_01# Что такое межсетевой экран (брандмауэр)?

a. Система контроля сетевого трафика

b. Антивирусная программа

c. Система аутентификации

d. Система обнаружения вторжений

e. Средство резервного копирования

f. Средство шифрования данных

77. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 06_03# Что такое DMZ (демилитаризованная зона)?

a. Защищенная внутренняя сеть

b. Сеть для резервного копирования

c. Внешняя сеть интернет

d. Сеть для виртуальных машин

e. Сеть между внутренней и внешней сетями для размещения публичных серверов

f. Зона карантина для вирусов

78. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 07_01# Что такое криптография?

a. Способ сжатия информации

b. Технология передачи данных

c. Наука о методах обеспечения конфиденциальности и целостности данных

d. Наука о взломе шифров

e. Искусство создания паролей

f. Метод архивирования данных

79. Задание с множественным выбором. Выберите 3 правильных ответа.

Вопрос 10_06# Какие преимущества имеет IPS перед IDS?

a. Активная блокировка атак

b. Реагирование в реальном времени

c. Более низкая стоимость

d. Проще в настройке

e. Предотвращение повреждений

f. Меньше ложных срабатываний

80. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 04_06# Какие компоненты входят в комплексную антивирусную защиту?

a. Сканирование веб-трафика

b. Дефрагментация диска

c. Антивирус для серверов

d. Защита почтовых шлюзов

e. Ускорение интернета

f. Антивирус для рабочих станций

81. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 03_06# Какие задачи решает анализ журналов в ИБ?

a. Аудит действий пользователей

b. Соответствие требованиям регуляторов

c. Ускорение работы системы

d. Выявление аномальной активности

e. Расследование инцидентов

f. Увеличение объема диска

82. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 05_01# Что такое аппаратные угрозы информационной безопасности?

a. SQL-инъекции

b. Фишинговые письма

c. Угрозы, связанные с физическим доступом к оборудованию

d. DDoS-атаки

e. Вирусные атаки через сеть

f. Социальная инженерия

83. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 14_06# Какие биометрические методы используются в ИБ?

a. Распознавание лица

b. Анализ почерка

c. Отпечатки пальцев

d. Радужная оболочка глаза

e. Анализ ДНК

f. Голосовая идентификация

84. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 14_02# Что такое контроль целостности?

a. Проверка конфиденциальности

b. Проверка неизменности данных

c. Проверка актуальности данных

d. Проверка доступности данных

e. Проверка авторства данных

f. Проверка структуры данных

85. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 15_06# Какие документы создаются при обработке инцидента?

a. Финансовый отчет

b. Акты об изъятии доказательств

c. Рекомендации по предотвращению

d. План восстановления

e. Маркетинговый план

f. Отчет об инциденте

86. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 02_03# Что такое электронная цифровая подпись (ЭЦП)?

a. Сканированная копия подписи

b. Штрих-код документа

c. Текстовый пароль

d. Графическое изображение подписи

e. Реквизит документа, подтверждающий его подлинность

f. QR-код документа

87. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 03_05# Какие инструменты используются для анализа журналов?

a. Graylog

b. Logwatch

c. ELK Stack (Elasticsearch, Logstash, Kibana)

d. Photoshop

e. Microsoft Word

f. Splunk

88. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 14_01# Что такое биометрическая аутентификация?

a. Аутентификация по вопросам

b. Аутентификация по биологическим признакам

c. Аутентификация по токену

d. Аутентификация по паролю

e. Аутентификация по SMS

f. Аутентификация по сертификату

89. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 02_01# Что такое инфраструктура открытых ключей (PKI)?

a. Набор технологий для управления цифровыми сертификатами
b. Способ шифрования данных
c. Метод физической защиты серверов
d. Средство мониторинга сети
e. Система закрытых ключей
f. Технология резервного копирования
90. Задание с единичным выбором. Выберите один правильный ответ.
Вопрос 15_02# Что такое группа реагирования на инциденты ИБ?
a. Служба безопасности предприятия
b. Аудиторы безопасности
c. Группа разработчиков ПО
d. Администраторы сети
e. Отдел технической поддержки
f. Команда специалистов для обработки инцидентов
91. Задание с множественным выбором. Выберите 4 правильных ответа.
Вопрос 13_04# Какие международные стандарты ИБ существуют?
a. HIPAA
b. ISO/IEC 27001
c. NIST SP 800-53
d. ISO/IEC 27002
e. ГОСТ Р
f. COBIT
92. Задание с множественным выбором. Выберите 4 правильных ответа.
Вопрос 14_04# Какие методы аутентификации существуют?
a. Биометрическая аутентификация
b. Групповая аутентификация
c. Парольная аутентификация
d. Двухфакторная аутентификация
e. Аутентификация по сертификатам
f. Анонимная аутентификация
93. Задание с единичным выбором. Выберите один правильный ответ.
Вопрос 04_01# Что такое сигнатурный анализ в антивирусных системах?
a. Проверка цифровых подписей
b. Аудит журналов событий
c. Мониторинг сетевого трафика
d. Поиск известных шаблонов вредоносного кода
e. Проверка контрольных сумм
f. Анализ поведения программ
94. Задание с единичным выбором. Выберите один правильный ответ.
Вопрос 15_03# Какой стандарт описывает управление инцидентами ИБ?
a. NIST SP 800-61

b. ISO/IEC 27001

c. ФСТЭК приказы

d. ГОСТ Р 57580

e. ISO/IEC 27035

f. ISO/IEC 27002

95. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 14_03# Что такое мандатный контроль доступа?

a. Контроль доступа на основе атрибутов

b. Контроль доступа на основе ролей

c. Контроль доступа на основе политик

d. Контроль доступа на основе списков

e. Контроль доступа на основе правил

f. Контроль доступа на основе меток безопасности

96. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 15_05# Какие инструменты используются при расследовании инцидентов?

a. Нагрузочное тестирование

b. Криминалистический анализ

c. Анализ сетевого трафика

d. Тестирование производительности

e. Анализ памяти

f. Анализ журналов

97. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 15_01# Что такое инцидент информационной безопасности?

a. Событие, которое может привести к нарушению ИБ

b. Тестирование системы защиты

c. Аудит системы безопасности

d. Плановое мероприятие по ИБ

e. Обновление антивирусных баз

f. Резервное копирование данных

98. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 15_04# Какие этапы включает обработка инцидента ИБ?

a. Игнорирование инцидента

b. Сокрытие инцидента

c. Сдерживание, ликвидация, восстановление

d. Обнаружение и анализ

e. Подготовка

f. Анализ после инцидента

99. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 05_03# Что такое аппаратный кейлоггер?

a. Сетевой сниффер

b. Вирус, записывающий клавиатурный ввод

c. USB-накопитель с вирусом

d. Программа для мониторинга клавиатуры

e. Анализатор трафика

f. Устройство для перехвата нажатий клавиш

100. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 13_02# Какой российский стандарт соответствует ISO 27001?

a. ФЗ-152

b. ГОСТ Р 50922-2006

c. ФСТЭК России

d. ГОСТ Р ИСО/МЭК 27001-2006

e. Приказ ФСТЭК 21

f. СТО БР ИББС

101. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 06_02# Какой тип межсетевого экрана анализирует заголовки пакетов?

a. Сетевой экран

b. Персональный брандмауэр

c. Прокси-сервер

d. Пакетный фильтр

e. Шлюз прикладного уровня

f. Инспектор состояния

102. Задание с множественным выбором. Выберите 3 правильных ответа.

Вопрос 09_06# Какие протоколы обеспечивают безопасную передачу данных?

a. IPSec

b. FTP

c. SSL/TLS

d. HTTP

e. Telnet

f. SSH

103. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 01_05# Какие компоненты включает система информационной безопасности?

a. Рекламные кампании

b. Правовые меры

c. Технические средства защиты

d. Организационные меры

e. Программные средства

f. Социальные сети

104. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 06_05# Какие политики безопасности можно реализовать на МЭ?

a. Антивирусное сканирование

b. Разрешение всего, кроме запрещенного

c. Запрет всего, кроме разрешенного

d. Контроль по приложениям

e. Шифрование данных

f. Фильтрация по IP-адресам

105. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 14_05# Какие модели контроля доступа существуют?

a. Дискреционная (DAC)

b. Ролевая (RBAC)

c. Прозрачная

d. На основе атрибутов (ABAC)

e. Мандатная (MAC)

f. Коллективная

106. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 10_03# Что такое система предотвращения вторжений (IPS)?

a. Межсетевой экран

b. Система, которая не только обнаруживает, но и блокирует атаки

c. Средство мониторинга

d. Система только обнаружения атак

e. Система аудита

f. Антивирусное ПО

107. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 13_03# Что такое СЗИ?

a. Система защиты информации

b. Служба защиты информации

c. Стратегия защиты информации

d. Стандарт защиты информации

e. Средства защиты информации

f. Сертификация защиты информации

108. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 07_03# Что такое хэш-функция?

a. Метод сжатия данных

b. Функция, преобразующая данные в фиксированную строку

c. Метод кодирования информации

d. Способ архивирования файлов

e. Алгоритм генерации случайных чисел

f. Функция шифрования с закрытым ключом

109. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 13_06# Какие требования содержит стандарт ISO 27001?

a. Внутренние аудиты

b. Выбор мер контроля

c. Требования к оборудованию

d. Технические спецификации

e. Создание СМИБ

f. Оценка рисков

110. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 13_05# Какие российские регуляторы в области ИБ существуют?

a. ФСТЭК России

b. Министерство цифрового развития

c. Центробанк РФ

d. Роскомнадзор

e. ФСБ России

f. Минкомсвязь

111. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 05_02# Что такое TEMPEST-атаки?

a. Взлом через температурные датчики

b. Взлом через сеть питания

c. Радиочастотные помехи

d. Атаки через USB-порты

e. Перехват акустических сигналов

f. Перехват электромагнитного излучения от аппаратуры

112. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 15_06# Какие документы создаются при обработке инцидента?

a. Отчет об инциденте

b. Акты об изъятии доказательств

c. Маркетинговый план

d. План восстановления

e. Финансовый отчет

f. Рекомендации по предотвращению

113. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 15_01# Что такое инцидент информационной безопасности?

a. Резервное копирование данных

b. Событие, которое может привести к нарушению ИБ

c. Аудит системы безопасности

d. Плановое мероприятие по ИБ

e. Обновление антивирусных баз

f. Тестирование системы защиты

114. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 15_04# Какие этапы включает обработка инцидента ИБ?

a. Сокрытие инцидента

b. Игнорирование инцидента

c. Сдерживание, ликвидация, восстановление

d. Подготовка

e. Анализ после инцидента

f. Обнаружение и анализ

115. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 13_06# Какие требования содержит стандарт ISO 27001?

a. Выбор мер контроля

b. Оценка рисков

c. Технические спецификации

d. Внутренние аудиты

e. Требования к оборудованию

f. Создание СМИБ

116. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 14_06# Какие биометрические методы используются в ИБ?

a. Радужная оболочка глаза

b. Распознавание лица

c. Анализ почерка

d. Голосовая идентификация

e. Анализ ДНК

f. Отпечатки пальцев

117. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 14_04# Какие методы аутентификации существуют?

a. Биометрическая аутентификация

b. Анонимная аутентификация

c. Аутентификация по сертификатам

d. Двухфакторная аутентификация

e. Групповая аутентификация

f. Парольная аутентификация

118. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 14_02# Что такое контроль целостности?

a. Проверка авторства данных

b. Проверка доступности данных

c. Проверка неизменности данных

d. Проверка конфиденциальности

e. Проверка актуальности данных

f. Проверка структуры данных

119. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 14_01# Что такое биометрическая аутентификация?

a. Аутентификация по паролю

b. Аутентификация по биологическим признакам

c. Аутентификация по сертификату

d. Аутентификация по вопросам

e. Аутентификация по SMS

f. Аутентификация по токену

120. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 14_03# Что такое мандатный контроль доступа?

a. Контроль доступа на основе меток безопасности

b. Контроль доступа на основе ролей

c. Контроль доступа на основе политик

d. Контроль доступа на основе списков

e. Контроль доступа на основе атрибутов

f. Контроль доступа на основе правил

121. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 15_03# Какой стандарт описывает управление инцидентами ИБ?

a. ISO/IEC 27001

b. ГОСТ Р 57580

c. NIST SP 800-61

d. ФСТЭК приказы

e. ISO/IEC 27035

f. ISO/IEC 27002

122. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 15_02# Что такое группа реагирования на инциденты ИБ?

a. Группа разработчиков ПО

b. Аудиторы безопасности

c. Отдел технической поддержки

d. Администраторы сети

e. Служба безопасности предприятия

f. Команда специалистов для обработки инцидентов

123. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 12_05# Какие методы используются для оценки рисков?

a. SWOT-анализ

b. Матрицы рисков

c. Анализ сценариев

d. Метод Дельфи

e. Пентестинг

f. Аудит журналов

124. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 15_05# Какие инструменты используются при расследовании инцидентов?

a. Анализ сетевого трафика

b. Нагрузочное тестирование

c. Анализ журналов

d. Тестирование производительности

e. Анализ памяти

f. Криминалистический анализ

125. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 11_02# Что такое фишинг?

a. Мошенничество с целью получения конфиденциальной информации

b. DDoS-атака

c. Подключение к Wi-Fi

d. Вирусная атака

e. Взлом пароля

f. Перехват SMS

126. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 10_05# Какие типы IDS существуют?

a. Распределенные

b. Централизованные

c. Гибридные

d. Узловые (HIDS)

e. Персональные

f. Сетевые (NIDS)

127. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 13_01# Какой стандарт информационной безопасности является международным?

a. FSTEC

b. PCI DSS

c. ГОСТ Р ИСО/МЭК 27001-2006

d. ISO/IEC 27001

e. ФЗ-152

f. HIPAA

128. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 09_03# Что такое VPN?

a. Технология резервного копирования

b. Средство антивирусной защиты

c. Система видеонаблюдения

d. Виртуальный приватный компьютер

e. Виртуальная частная сеть для защищенной передачи данных

f. Сетевой протокол передачи файлов

129. Задание с множественным выбором. Выберите 3 правильных ответа.

Вопрос 09_06# Какие протоколы обеспечивают безопасную передачу данных?

a. SSH

b. HTTP

c. FTP

d. SSL/TLS

e. Telnet

f. IPSec

130. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 13_05# Какие российские регуляторы в области ИБ существуют?

a. Министерство цифрового развития

b. Минкомсвязь

c. ФСБ России

d. Роскомнадзор

e. ФСТЭК России

f. Центробанк РФ

131. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 09_04# Какие угрозы существуют в сетевой безопасности?

a. Снифинг (перехват трафика)

b. Естественные катастрофы

c. Человеческий фактор

d. DoS/DDoS атаки

e. Аппаратные сбои

f. Спуфинг (подмена адресов)

132. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 13_04# Какие международные стандарты ИБ существуют?

a. ГОСТ Р

b. ISO/IEC 27002

c. ISO/IEC 27001

d. COBIT

e. NIST SP 800-53

f. HIPAA

133. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 13_03# Что такое СЗИ?

a. Средства защиты информации

b. Сертификация защиты информации

c. Стратегия защиты информации

d. Служба защиты информации

e. Стандарт защиты информации

f. Система защиты информации

134. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 14_05# Какие модели контроля доступа существуют?

a. Мандатная (MAC)

b. Дискреционная (DAC)

c. Прозрачная

d. Коллективная

e. На основе атрибутов (ABAC)

f. Ролевая (RBAC)

135. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 11_04# Какие методы социальной инженерии существуют?

a. Тайлгейтинг (проход за сотрудником)
b. Претекстинг
c. Сканирование портов
d. Взлом пароля
e. Кви про кво (услуга за услугу)
f. Фишинг
136. Задание с единичным выбором. Выберите один правильный ответ.
Вопрос 12_01# Что такое риск в информационной безопасности?
a. Страхование информационных активов
b. Вероятность реализации угрозы с нанесением ущерба
c. Политика безопасности
d. Антивирусная защита
e. Уязвимость в программном обеспечении
f. Возможность атаки на систему
137. Задание с единичным выбором. Выберите один правильный ответ.
Вопрос 11_01# Что такое социальная инженерия?
a. Взлом компьютерных систем
b. Программирование вирусов
c. Сетевые атаки
d. Метод манипулирования людьми для получения информации
e. Физический доступ к оборудованию
f. Шифрование данных
138. Задание с множественным выбором. Выберите 4 правильных ответа.
Вопрос 11_06# Какие меры защиты от социальной инженерии существуют?
a. Обучение сотрудников
b. Политика информационной безопасности
c. Установка антивируса
d. Настройка брандмауэра
e. Двухфакторная аутентификация
f. Проверка запросов на информацию
139. Задание с множественным выбором. Выберите 4 правильных ответа.
Вопрос 12_04# Какие стратегии обработки рисков существуют?
a. Избегание риска
b. Принятие риска
c. Игнорирование риска
d. Снижение риска
e. Передача риска
f. Увеличение риска
140. Задание с единичным выбором. Выберите один правильный ответ.
Вопрос 10_01# Что такое система обнаружения вторжений (IDS)?
a. Система предотвращения вторжений

b. Средство аутентификации
c. Система резервного копирования
d. Антивирусная программа
e. Межсетевой экран
f. Система мониторинга и обнаружения атак
141. Задание с множественным выбором. Выберите 4 правильных ответа.
Вопрос 08_04# Какие методы обеспечения отказоустойчивости существуют?
a. Резервирование данных
b. Резервирование оборудования
c. Кластеризация
d. Антивирусная защита
e. Репликация данных
f. Шифрование информации
142. Задание с множественным выбором. Выберите 4 правильных ответа.
Вопрос 09_05# Какие технологии используются для сетевой безопасности?
a. RAID массивы
b. Межсетевые экраны
c. IPS/IDS системы
d. Системы аутентификации
e. VPN
f. Резервное копирование
143. Задание с множественным выбором. Выберите 5 правильных ответов.
Вопрос 12_06# Какие этапы включает процесс управления рисками?
a. Мониторинг рисков
b. Анализ рисков
c. Продажа рисков
d. Оценка рисков
e. Идентификация рисков
f. Обработка рисков
144. Задание с единичным выбором. Выберите один правильный ответ.
Вопрос 09_02# Что такое DDoS-атака?
a. Взлом пароля администратора
b. Массовая атака на отказ в обслуживании
c. Фишинговая атака
d. Подмена DNS-сервера
e. Вирусная эпидемия
f. Перехват сетевого трафика
145. Задание с единичным выбором. Выберите один правильный ответ.
Вопрос 09_01# Что такое сетевая безопасность?
a. Защита компьютеров от вирусов
b. Контроль физического доступа

c. Управление пользователями

d. Защита от аппаратных сбоев

e. Защита данных, передаваемых по сетям

f. Резервное копирование

146. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 13_02# Какой российский стандарт соответствует ISO 27001?

a. ГОСТ Р ИСО/МЭК 27001-2006

b. ФЗ-152

c. ФСТЭК России

d. Приказ ФСТЭК 21

e. ГОСТ Р 50922-2006

f. СТО БР ИББС

147. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 10_03# Что такое система предотвращения вторжений (IPS)?

a. Межсетевой экран

b. Средство мониторинга

c. Система, которая не только обнаруживает, но и блокирует атаки

d. Антивирусное ПО

e. Система аудита

f. Система только обнаружения атак

148. Задание с множественным выбором. Выберите 3 правильных ответа.

Вопрос 10_06# Какие преимущества имеет IPS перед IDS?

a. Меньше ложных срабатываний

b. Проще в настройке

c. Реагирование в реальном времени

d. Предотвращение повреждений

e. Более низкая стоимость

f. Активная блокировка атак

149. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 10_04# Какие методы обнаружения используют IDS/IPS?

a. Лингвистический анализ

b. Семантический анализ

c. Сигнатурный анализ

d. Анализ аномалий

e. Статистический анализ

f. Поведенческий анализ

150. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 11_05# Какие каналы используются для фишинга?

a. Социальные сети

b. Прямой телефонный разговор

c. Мессенджеры

d. Факсимильная связь

e. SMS-сообщения

f. Электронная почта

151. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 11_03# Что такое претекстинг?

a. Создание фишингового сайта

b. Установка шпионского ПО

c. Перехват электронной почты

d. Подбор паролей

e. Взлом через социальные сети

f. Использование вымышленного предлога для получения информации

152. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 08_02# Какой уровень RAID обеспечивает зеркалирование дисков?

a. RAID 50

b. RAID 0

c. RAID 1

d. RAID 10

e. RAID 5

f. RAID 6

153. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 06_06# Какие функции выполняют современные МЭ?

a. Фильтрация пакетов

b. Резервное копирование

c. NAT (трансляция сетевых адресов)

d. Вирусное сканирование

e. VPN (виртуальные частные сети)

f. Контроль состояния соединений

154. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 12_02# Какой метод оценки рисков использует матрицу вероятность/ущерб?

a. Аудит безопасности

b. Тестирование на проникновение

c. Количественная оценка рисков

d. Качественная оценка рисков

e. Анализ уязвимостей

f. Статистический анализ

155. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 12_03# Что такое обработка рисков?

a. Обучение сотрудников

b. Страхование информационных активов

c. Расчет вероятности рисков

d. Создание политик безопасности

e. Процесс выбора и реализации мер по снижению рисков

f. Выявление угроз и уязвимостей

156. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 08_06# Какие компоненты системы обычно резервируются?

a. Мониторы

b. Источники питания

c. Сетевые каналы

d. Дисковые подсистемы

e. Клавиатуры и мыши

f. Серверное оборудование

157. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 08_01# Что такое отказоустойчивость системы?

a. Высокая производительность

b. Низкая стоимость системы

c. Автоматическое обновление

d. Полное отсутствие сбоев

e. Быстрое восстановление после сбоя

f. Способность системы выполнять функции при отказах компонентов

158. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 07_04# Какие задачи решает криптография?

a. Аутентификация

b. Увеличение объема данных

c. Конфиденциальность

d. Повышение скорости передачи

e. Целостность данных

f. Неотказуемость

159. Задание с множественным выбором. Выберите 3 правильных ответа.

Вопрос 07_05# Какие типы криптографических алгоритмов существуют?

a. Асимметричные алгоритмы

b. Хэш-функции

c. Алгоритмы передачи

d. Симметричные алгоритмы

e. Алгоритмы сжатия

f. Алгоритмы архивации

160. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 10_02# Какой тип IDS анализирует сетевой трафик?

a. Network IDS (NIDS)

b. Host IDS (HIDS)

c. Protocol IDS

d. Signature IDS

e. Anomaly IDS

f. Application IDS

161. Задание с множественным выбором. Выберите 3 правильных ответа.

Вопрос 07_06# Какие алгоритмы относятся к асимметричной криптографии?

a. Blowfish

b. DES

c. DSA

d. AES

e. ECDSA

f. RSA

162. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 07_03# Что такое хэш-функция?

a. Метод сжатия данных

b. Функция шифрования с закрытым ключом

c. Алгоритм генерации случайных чисел

d. Функция, преобразующая данные в фиксированную строку

e. Метод кодирования информации

f. Способ архивирования файлов

163. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 08_03# Что такое кластеризация?

a. Объединение нескольких серверов в единую систему

b. Резервное копирование данных

c. Сетевое экранирование

d. Виртуализация серверов

e. Шифрование информации

f. Мониторинг системы

164. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 08_05# Какие типы резервирования применяются в ИТ-системах?

a. Полное резервирование

b. Активное (hot standby)

c. Пассивное (cold standby)

d. Частичное резервирование

e. Временное резервирование

f. Географически распределенное

165. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 04_06# Какие компоненты входят в комплексную антивирусную защиту?

a. Сканирование веб-трафика

b. Ускорение интернета

c. Антивирус для серверов

d. Защита почтовых шлюзов

e. Антивирус для рабочих станций

f. Дефрагментация диска

166. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 06_04# Какие типы межсетевых экранов существуют?

a. Персональные

b. Программные

c. Сетевые (аппаратные)

d. Прокси-серверы

e. Мобильные

f. Роутеры

167. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 05_04# Какие существуют аппаратные угрозы?

a. Вирусная атака по сети

b. Подключение сторонних устройств

c. Перехват электромагнитного излучения

d. Съем носителей информации

e. Визуальное наблюдение

f. Фишинговый сайт

168. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 07_01# Что такое криптография?

a. Технология передачи данных

b. Искусство создания паролей

c. Наука о методах обеспечения конфиденциальности и целостности данных

d. Способ сжатия информации

e. Наука о взломе шифров

f. Метод архивирования данных

169. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 06_05# Какие политики безопасности можно реализовать на МЭ?

a. Разрешение всего, кроме запрещенного

b. Запрет всего, кроме разрешенного

c. Шифрование данных

d. Антивирусное сканирование

e. Фильтрация по IP-адресам

f. Контроль по приложениям

170. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 03_02# В каком каталоге обычно хранятся системные журналы в Linux?

a. /root/log

b. /etc/log

c. /usr/log

d. /tmp/log

e. /var/log

f. /home/log

171. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 05_03# Что такое аппаратный кейлоггер?

a. Сетевой сниффер

b. Программа для мониторинга клавиатуры

c. Анализатор трафика

d. Устройство для перехвата нажатий клавиш

e. Вирус, записывающий клавиатурный ввод

f. USB-накопитель с вирусом

172. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 03_03# Какой протокол используется для централизованного сбора логов?

a. HTTP

b. SSH

c. SNMP

d. Syslog

e. FTP

f. SMTP

173. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 04_02# Как называется технология обнаружения неизвестных угроз на основе поведения?

a. Сетевая экранировка

b. Проактивная защита (heuristic analysis)

c. Белый список

d. Резервное копирование

e. Шифрование данных

f. Сигнатурный анализ

174. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 03_05# Какие инструменты используются для анализа журналов?

a. Photoshop

b. Splunk

c. ELK Stack (Elasticsearch, Logstash, Kibana)

d. Logwatch

e. Microsoft Word

f. Graylog

175. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 06_02# Какой тип межсетевого экрана анализирует заголовки пакетов?

a. Персональный брандмауэр

b. Шлюз прикладного уровня

c. Сетевой экран

d. Пакетный фильтр

e. Прокси-сервер

f. Инспектор состояния

176. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 07_02# Какой алгоритм является симметричным?

a. AES

b. MD5

c. SHA-256

d. DSA

e. ECDSA

f. RSA

177. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 02_01# Что такое инфраструктура открытых ключей (PKI)?

a. Система закрытых ключей

b. Технология резервного копирования

c. Средство мониторинга сети

d. Метод физической защиты серверов

e. Набор технологий для управления цифровыми сертификатами

f. Способ шифрования данных

178. Задание с множественным выбором. Выберите 4 правильных ответа.

Вопрос 02_06# Какие компоненты входят в состав PKI?

a. Система распространения ключей

b. Регистрационный центр (RA)

c. Антивирусное ПО

d. Центр сертификации (CA)

e. Межсетевой экран

f. Хранилище сертификатов

179. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 06_03# Что такое DMZ (демилитаризованная зона)?

a. Защищенная внутренняя сеть

b. Внешняя сеть интернет

c. Зона карантина для вирусов

d. Сеть для виртуальных машин

e. Сеть для резервного копирования

f. Сеть между внутренней и внешней сетями для размещения публичных серверов

180. Задание с единичным выбором. Выберите один правильный ответ.

Вопрос 05_01# Что такое аппаратные угрозы информационной безопасности?

a. DDoS-атаки

b. Фишинговые письма

c. Социальная инженерия

d. Вирусные атаки через сеть

e. SQL-инъекции

f. Угрозы, связанные с физическим доступом к оборудованию

8.2. Оценочные средства для промежуточной аттестации

Вопросы к экзамену:

1. Дайте определение понятия «информационная безопасность». Каковы её основные цели и задачи в современных условиях?

2. Охарактеризуйте три базовых принципа информационной безопасности: конфиденциальность, целостность и доступность (CIA-триада). Приведите примеры их нарушения.

3. Что такое угроза, уязвимость и риск в контексте информационной безопасности? Поясните взаимосвязь между этими понятиями.

4. Перечислите не менее 3 классов ПО, необходимых для данной задачи (например, сканер уязвимостей веб-приложений, анализатор трафика, система управления уязвимостями). Назовите по 1-2 известным российским аналогам для каждого класса.

5. Что такое PKI (инфраструктура открытых ключей)? Опишите основные компоненты PKI и их взаимодействие в обеспечении информационной безопасности.

6. Дайте определение электронной подписи. Каковы основные криптографические принципы, лежащие в основе формирования и проверки электронной подписи? В чем отличие простой электронной подписи от усиленной квалифицированной электронной подписи?

7. Каким образом PKI обеспечивает доверие в цифровых коммуникациях? Опишите роль центров сертификации (CA) и механизмов отзыва сертификатов (CRL/OCSP) в поддержании безопасности инфраструктуры открытых ключей.

8. Каковы основные цели и задачи анализа электронных журналов событий в системах информационной безопасности? Назовите ключевые типы журналов и их роль в мониторинге безопасности.

9. Опишите методы и подходы к детектированию аномалий в электронных журналах. Какие алгоритмы и техники используются для выявления подозрительной активности? Приведите примеры индикаторов компрометации, которые можно обнаружить при анализе логов.

10. Какие требования предъявляются к хранению и защите электронных журналов событий согласно стандартам информационной безопасности (например, PCI DSS, ISO 27001, GDPR)? Как обеспечивается целостность и доступность журналов в течение требуемого периода хранения?

11. Классифицируйте современные антивирусные системы по архитектуре и принципам работы. Охарактеризуйте особенности сигнатурного, эвристического и поведенческого методов обнаружения вредоносного ПО. В чем заключаются преимущества и недостатки каждого подхода?

12. Какие особенности защиты от современных угроз (APT-атаки, ransomware, fileless malware) реализованы в антивирусных системах нового поколения? Опишите роль технологий машинного обучения, песочниц (sandboxing) и контроля устройств в комплексной защите.

13. Охарактеризуйте роль облачных технологий в современных антивирусных решениях. Как работают облачные песочницы, системы коллективного интеллекта (community intelligence) и технологии облачного сканирования? Какие преимущества и риски связаны с использованием облачных компонентов в антивирусной защите?

14. Классифицируйте основные типы аппаратных угроз информационной

безопасности. Охарактеризуйте особенности аппаратных троянов, скиммеров, keylogger-устройств и поддельного оборудования. Приведите реальные примеры реализации таких угроз в корпоративной среде.

15. Опишите методы детектирования и анализа аппаратных угроз. Какие технические средства и программные инструменты используются для выявления несанкционированных аппаратных модификаций? В чем заключаются особенности физического аудита оборудования и анализа цепочки поставок?

16. Опишите специфические угрозы, связанные с мобильными устройствами и IoT-устройствами. Какие аппаратные векторы атак характерны для смартфонов, планшетов и встраиваемых систем? Как особенности аппаратной архитектуры этих устройств влияют на их уязвимость к физическим атакам?

17. Охарактеризуйте основные типы межсетевых экранов (пакетные фильтры, шлюзы сеансового уровня, прикладные шлюзы, stateful inspection). В чем состоят принципиальные различия в архитектуре и функциональных возможностях каждого типа? Какие достоинства и недостатки имеет каждый подход?

18. Объясните механизм работы межсетевых экранов с отслеживанием состояния соединений. Какие данные сохраняются в таблице состояний? Почему данный подход считается более безопасным по сравнению с простым пакетным фильтром? Приведите примеры правил, которые невозможно реализовать без отслеживания состояния.

19. Опишите основные схемы размещения межсетевых экранов (в периметре сети, во внутренних сегментах, в облаке). Какие факторы учитываются при выборе архитектуры защиты? В чем особенности развертывания межсетевых экранов в гибридных и облачных средах?

20. Классифицируйте криптографические методы защиты информации по типу ключей. Сравните симметричные и асимметричные криптосистемы по критериям: вычислительная сложность, требования к управлению ключами, безопасность, производительность. Приведите примеры алгоритмов для каждого типа.

21. Опишите назначение и свойства криптографических хеш-функций. Какие требования предъявляются к современным хеш-функциям (устойчивость к коллизиям, прообразу, второму прообразу)? Приведите примеры использования хеш-функций в системах информационной безопасности (ЦП, HMAC, пароли) и известные уязвимости устаревших алгоритмов (MD5, SHA-1).

22. Раскройте сущность асимметричной криптографии на примере алгоритма RSA. Объясните математические основы (теорема Эйлера, модульная арифметика), процесс генерации ключей, шифрования и расшифрования. Какие параметры определяют криптостойкость RSA и какие атаки на него существуют (атака на малые экспоненты, факторизация модуля)?

23. Дайте определение отказоустойчивости информационных систем. Охарактеризуйте основные принципы построения отказоустойчивых систем: избыточность, дублирование, модульность, самодиагностика. Как эти принципы соотносятся с требованиями информационной безопасности?

24. Опишите стандарты и методологии проектирования отказоустойчивых систем. Какие требования предъявляют стандарты ISO/IEC 27001, COBIT и ITIL к обеспечению непрерывности бизнес-процессов? Как в этих стандартах определяются показатели RTO (Recovery Time Objective) и RPO (Recovery Point Objective)?

25. Что такое план восстановления после катастрофы (Disaster Recovery Plan)?

Охарактеризуйте ключевые этапы разработки DRP: анализ воздействия на бизнес (BIA), определение критических процессов, создание процедур восстановления, тестирование и актуализация плана. Как обеспечивается защита резервных копий от несанкционированного доступа?

26. Классифицируйте основные типы сетевых атак по уровню модели OSI. Приведите конкретные примеры атак на канальном (MAC flooding, ARP spoofing), сетевом (IP spoofing, Smurf-атака) и транспортном (SYN flood, TCP hijacking) уровнях. Какие методы защиты наиболее эффективны против каждой категории атак?

27. Проанализируйте особенности обеспечения безопасности беспроводных сетей. Какие уязвимости характерны для стандартов Wi-Fi (WEP, WPA, WPA2, WPA3)? Опишите методы защиты: шифрование, аутентификация (802.1X/EAP), сегментация сети, обнаружение rogue AP. Какие современные угрозы актуальны для Wi-Fi 6 (802.11ax)?

28. Объясните принципы сегментации сетей как метода повышения безопасности. Какие технологии используются для создания безопасных зон (VLAN, подсети, DMZ, microsegmentation)? Как сегментация помогает ограничить распространение атак и минимизировать поверхность атаки? Приведите примеры реализации сетевой сегментации в корпоративных и облачных средах.

29. Классифицируйте системы обнаружения вторжений по архитектуре и месту развертывания. Охарактеризуйте принципиальные различия между сетевыми (NIDS), хостовыми (HIDS), гибридными системами, а также системами предотвращения вторжений (IPS). Какие преимущества и недостатки имеет каждый тип?

30. Как организуется управление системами обнаружения вторжений в корпоративной сети? Охарактеризуйте процесс настройки правил, обработки оповещений, корреляции событий и интеграции с другими системами безопасности (SIEM, firewalls, системами управления инцидентами). Какие метрики используются для оценки эффективности работы IDS/IPS?

31. Опишите конкретные примеры атак и методы их детектирования с помощью IDS/IPS. Как системы обнаруживают: DDoS-атаки, сканирование портов, эксплойты уязвимостей, атаки на веб-приложения (SQL injection, XSS), попытки несанкционированного доступа? Приведите примеры сигнатур и паттернов поведения для каждой категории угроз.

32. Дайте определение социальной инженерии и классифицируйте основные методы атак. Охарактеризуйте такие техники как фишинг, вишинг, смishing, претекстинг, бейтинг и квайдинг. Какие психологические принципы (авторитет, взаимность, дефицит) используются злоумышленниками для манипуляции жертвами?

33. Опишите типичные фазы атаки социальной инженерии: разведка, установление контакта, эксплуатация уязвимости, завершение взаимодействия. Приведите конкретные примеры реализации каждой фазы в реальных атаках. Как злоумышленники собирают информацию о цели на этапе разведки и какие источники они используют?

34. Рассмотрите правовые аспекты противодействия социальной инженерии в РФ. Какие требования предъявляют стандарты информационной безопасности к защите от социальных атак? Какие шаги должен предпринять сотрудник при обнаружении попытки социальной инженерии и как организуется расследование инцидентов такого типа?

35. Дайте определение рискам информационной безопасности и охарактеризуйте их основные компоненты (угроза, уязвимость, актив). Объясните разницу между количественным и качественным подходами к оценке рисков. Какие стандарты

регламентируют процессы управления рисками ИБ?

36. Что такое методы обработки рисков (avoidance, transfer, mitigation, acceptance)? Охарактеризуйте конкретные контрмеры для снижения рисков: технические (шифрование, резервное копирование), организационные (политики безопасности, обучение персонала), юридические (договоры с поставщиками, страхование). Как выбирается оптимальная стратегия обработки риска?

37. Как организуется непрерывный мониторинг и пересмотр рисков в динамично меняющейся среде ИТ-угроз? Какие метрики и индикаторы ключевых рисков (KRIs) используются для отслеживания эффективности системы управления рисками?

38. Дайте классификацию стандартов информационной безопасности по уровням (международные, национальные, отраслевые). Приведите примеры ключевых стандартов для каждого уровня и объясните их основное назначение

39. Опишите основные требования законодательной базы РФ в области ИБ: Федеральный закон "О персональных данных" №152-ФЗ, Приказы ФСТЭК России №17/21/31. Какие меры защиты информации персональных данных являются обязательными для операторов? Как классифицируются системы обработки персональных данных по требованиям ФСТЭК?

40. Рассмотрите процесс сертификации соответствия требованиям стандартов ИБ. Какие этапы включает процесс сертификации на соответствие ISO/IEC 27001?

Разработчики:

_____	преподаватель	А.Ф. Аношко
(подпись)	*(занимаемая должность)*	*(инициалы, фамилия)*

Программа составлена в соответствии с требованиями ФГОС ВО и учетом рекомендаций ПООП по направлению подготовки 09.03.03 «Прикладная информатика».

Программа рассмотрена на заседании кафедры алгебраических и информационных систем

Протокол № __ от «__» _____ 20__ г.

Зав. кафедрой _____ В.И. Пантелеев