

**Федеральное государственное образовательное бюджетное учреждение
высшего образования
«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ
РОССИЙСКОЙ ФЕДЕРАЦИИ»
(Финансовый университет)**

Тульский филиал Финуниверситета

Кафедра «Математика и информатика»

СОГЛАСОВАНО

ЗАО «ЛИМ»

Генеральный директор

 **В.В. Куликов**

«19» декабря 2024 г.



УТВЕРЖДАЮ

Директор филиала

 **Г.В. Кузнецов**

«24» декабря 2024 г.



Е.В. Манохин

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

для студентов, обучающихся по направлению подготовки
09.03.02 Информационные системы и технологии,
образовательная программа «Информационные технологии в экономике»,
профиль «Информационные технологии в управлении цифровой
экономикой»

*Рекомендовано Ученым советом Тульского филиала Финуниверситета
(протокол от 24 декабря 2024 г. № 22)*

*Одобрено заседанием кафедры «Математика и информатика»
(протокол от 02 декабря 2024 г. № 5)*

Тула 2024

«Управление информационной безопасностью»

КОД И НАИМЕНОВАНИЕ ОПОП:

09.03.02 Информационные системы и технологии

Образовательная программа - Информационные технологии в экономике

Профиль «Информационные технологии в управлении цифровой экономикой»

Общее количество заданий по дисциплине

Код компетенции	Наименование компетенции	Количество заданий
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учётом основных требований информационной безопасности	40
Всего:		40

Количество заданий по дисциплине в одном варианте

Код компетенции	Наименование компетенции	Количество заданий
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учётом основных требований информационной безопасности	20
Всего:		20

Типы заданий

Наименование типа заданий	Номер типа заданий
Задание комбинированного типа с выбором одного верного ответа из предложенных	1
Задание открытого типа	2
Задание открытого типа с развернутым ответом	3

Распределение заданий по компетенциям

Код компетенции	Наименование компетенции	Наименование индикаторов сформированности компетенции	Семестр	Номер задания
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учётом основных требований информационной безопасности	1. Проводит самостоятельный поиск информации в открытых источниках по определенной заданной тематике.	4	1.1, 1.2, 2.1, 2.2, 3.1, 3.2, 4.1, 4.2, 5.1, 5.2, 6.1, 6.2, 7.1, 7.2,
		2. Осуществляет систематический обзор источников информации, анализирует содержащиеся в них данные, делает обоснованные выводы на основе проведенного обзора.	4	8.1, 8.2, 9.1, 9.2, 10.1, 10.2, 11.1, 11.2, 12.1, 12.2, 13.1, 13.2, 14.1, 14.2
		3. Демонстрирует знания основных требований информационной	4	15.1, 15.2, 16.1, 16.2,

		безопасности, основных алгоритмов защиты информации, в том числе с использованием криптографических протоколов.		17.1, 17.2, 18.1, 18.2, 19.1, 19.2, 20.1, 20.2
--	--	---	--	--

Типы, уровень сложности и время выполнения заданий

Код компетенции	Индикатор сформированности компетенции	Номер задания	Тип задания	Уровень сложности задания	Время выполнения задания (мин.)
ОПК-3	Проводит самостоятельный поиск информации в открытых источниках по определенной заданной тематике	1.1, 1.2.	1	базовый	2
	Проводит самостоятельный поиск информации в открытых источниках по определенной заданной тематике	2.1, 2.2	1	базовый	2
	Проводит самостоятельный поиск информации в открытых источниках по определенной заданной тематике	3.1, 3.2	1	базовый	2
	Проводит самостоятельный поиск информации в открытых источниках по определенной заданной тематике	4.1, 4.2	1	базовый	2
	Проводит самостоятельный поиск информации в открытых источниках по определенной заданной тематике	5.1, 5.2	1	базовый	2
	Проводит самостоятельный поиск информации в открытых источниках по определенной заданной тематике	6.1, 6.2.	2	повышенный	4
	Проводит самостоятельный поиск информации в открытых источниках по определенной заданной тематике	7.1, 7.2	3	высокий	8
	Осуществляет систематический обзор источников информации, анализирует содержащиеся в них данные, делает обоснованные выводы на основе проведенного обзора.	8.1, 8.2	1	базовый	2
	Осуществляет систематический обзор источников информации, анализирует содержащиеся в них данные, делает обоснованные выводы на основе проведенного обзора.	9.1, 9.2	1	базовый	2
	Осуществляет систематический обзор источников информации, анализирует содержащиеся в них данные, делает обоснованные выводы на основе проведенного обзора.	10.1, 10.2	1	базовый	2
	Осуществляет систематический обзор источников информации, анализирует содержащиеся в них данные, делает обоснованные	11.1, 11.2.	2	повышенный	4

	выводы на основе проведенного обзора.				
	Осуществляет систематический обзор источников информации, анализирует содержащиеся в них данные, делает обоснованные выводы на основе проведенного обзора.	12.1, 12.2	2	повышенный	4
	Осуществляет систематический обзор источников информации, анализирует содержащиеся в них данные, делает обоснованные выводы на основе проведенного обзора.	13.1, 13.2	3	высокий	8
	Осуществляет систематический обзор источников информации, анализирует содержащиеся в них данные, делает обоснованные выводы на основе проведенного обзора.	14.1, 14.2	3	высокий	8
	Демонстрирует знания основных требований информационной безопасности, основных алгоритмов защиты информации, в том числе с использованием криптографических протоколов.	15.1, 15.2	1	базовый	2
	Демонстрирует знания основных требований информационной безопасности, основных алгоритмов защиты информации, в том числе с использованием криптографических протоколов.	16.1, 16.2.	1	базовый	2
	Демонстрирует знания основных требований информационной безопасности, основных алгоритмов защиты информации, в том числе с использованием криптографических протоколов.	17.1, 17.2	2	повышенный	4
	Демонстрирует знания основных требований информационной безопасности, основных алгоритмов защиты информации, в том числе с использованием криптографических протоколов.	18.1, 18.2	2	повышенный	4
	Демонстрирует знания основных требований информационной безопасности, основных алгоритмов защиты информации, в том числе с использованием криптографических протоколов.	19.1, 19.2	3	высокий	8
	Демонстрирует знания основных требований информационной безопасности, основных алгоритмов защиты информации, в том числе с использованием криптографических протоколов.	20.1, 20.2	3	высокий	8

Задания, позволяющие осуществлять оценку компетенций, установленных для дисциплины

Вариант 1

Задание 1.1.

Какое из следующих определений наиболее точно описывает управление информационной безопасностью?

- А) Процесс управления физической безопасностью помещений.
- Б) Процесс защиты информации от несанкционированного доступа и утечек.
- В) Процесс разработки программного обеспечения.
- Г) Процесс управления персоналом

Ответ:

Задание 2.1.

Какой из следующих методов является наиболее распространенным для защиты информации в корпоративных системах?

- А) Открытый доступ ко всем данным.
- Б) Публикация всех данных в интернете.
- В) Использование антивирусного ПО.
- Г) Устранение всех сотрудников

Ответ:

Задание 3.1.

Какой из следующих факторов является основной проблемой защиты информации в интернете?

- А) Высокая скорость передачи данных.
- Б) Широкий доступ к информации.
- В) Наличие антивирусного программного обеспечения.
- Г) Низкая стоимость хостинга

Ответ:

Задание 4.1.

Какой из следующих документов является руководящим в области информационной безопасности согласно ФСТЭК России?

- А) Методические рекомендации по обеспечению безопасности информации.
- Б) Гражданский кодекс.
- В) Кодекс об административных правонарушениях.
- Г) Уголовный кодекс

Ответ:

Задание 5.1.

Какой из следующих стандартов является международным стандартом в области информационной безопасности?

- А) ISO/IEC 27001.
- Б) ГОСТ Р 50922.
- В) ФЗ-152 о персональных данных.
- Г) Положение о защите информации

Ответ:

Задание 6.1.

Документ, который определяет правила, процедуры и стандарты защиты информации внутри компании – это ...

Ответ:

Задание 7.1.

Укажите и охарактеризуйте уровни управления информационной безопасностью.

Ответ:

Задание 8.1.

Какое основное правило информационной безопасности?

- А) Аутентификация только по паролю
- Б) Не передавать другому лицу свои данные
- В) Регулярные обновления менеджера безопасности
- Г) Использовать только сложные типы паролей (****-****)

Ответ:

Задание 9.1.

Что такое двоичный код в безопасности?

- А) Язык для программирования
- Б) Шифр VIRUS
- В) Система шифрования PNG
- Г) Режим, где данные передаются в числовом формате

Ответ:

Задание 10.1.

Что такое шифрование?

- А) Процесс передачи данных по сети
- Б) Защита данных с помощью шифров
- В) Установка антивирусного ПО
- Г) Определение принадлежности пользователя

Ответ:

Задание 11.1.

Систематическая проверка состояния системы защиты информации в организации – это ...

Ответ:

Задание 12.1.

Событие, которое нарушает политику безопасности организации, приводит к утрате, изменению или несанкционированному доступу к защищенной информации – это ...

Ответ:

Задание 13.1.

Назовите основные угрозы информационной безопасности.

Ответ:

Задание 14.1.

Что означает принцип минимизации привилегий (Least Privilege)?

Ответ:

Задание 15.1.

Какой тип шифра используется для обеспечения надежной связи?

- А) Шифр 3DES
- Б) Шифр AES
- В) Шифр RSA
- Г) Шифр DES

Ответ:

Задание 16.1.

Какая технология используется для защиты данных, которые передаются по сети?

- А) HTTPS
- Б) SSL/TLS
- В) VPN
- Г) All of the above

Ответ:

Задание 17.1.

Как называется информационная система, которая соответствует установленным стандартам и требованиям безопасности, обеспечивая конфиденциальность, целостность и доступность информации?

Ответ:

Задание 18.1.

Процесс контроля того, кто имеет право получать доступ к каким ресурсам в информационной системе – это ...

Ответ:

Задание 19.1.

Какие методы аутентификации используются в управлении информационной безопасностью?

Ответ:

Задание 20.1.

Что такое периметровая защита и какие технологии она включает?

Ответ:

Вариант 2

Задание 1.2.

Какой из следующих подходов используется для классификации угроз безопасности информации?

- А) По типу операционной системы.
- Б) По источнику угрозы (внешние/внутренние).
- В) По количеству пользователей.
- Г) По стоимости программного обеспечения

Ответ:

Задание 2.2.

Какое из следующих направлений не относится к политике информационной безопасности предприятия?

- А) Обучение сотрудников.
- Б) Установление правил доступа к информации.
- В) Публикация финансовых отчетов.
- Г) Мониторинг угроз безопасности

Ответ:

Задание 3.2.

Какой из следующих законов регулирует вопросы информационной безопасности в России?

- А) Закон о защите прав потребителей.
- Б) Закон о персональных данных.
- В) Закон о налогах.
- Г) Закон о рекламе

Ответ:

Задание 4.2.

Какой из следующих подходов используется при проведении аудита информационной безопасности?

- А) Оценка только технических средств защиты.
- Б) Оценка только физической безопасности.
- В) Игнорирование человеческого фактора.
- Г) Анализ процессов управления и контроля

Ответ:

Задание 5.2.

Какое из следующих утверждений наиболее точно отражает проблему взаимосвязи этики и правосудия в области информационной безопасности?

- А) Этические нормы могут конфликтовать с юридическими требованиями.
- Б) Этические нормы не влияют на правосудие.
- В) Правосудие всегда следует этическим нормам.
- Г) Этические нормы не имеют значения в бизнесе

Ответ:

Задание 6.2.

Процесс преобразования информации в зашифрованный вид таким образом, чтобы она была недоступна без специального ключа – это ...

Ответ:

Задание 7.2.

Опишите основные компоненты системы мониторинга информационной безопасности.

Ответ:

Задание 8.2.

Какая практика противодействует социальному инжинирингу?

- А) Отвечать на все электронные письма сразу
- Б) Не повторять пароли и не отправляться на ссылки
- В) Открывать вложения без проверки
- Г) Открывать доступ для всех сотрудников

Ответ:

Задание 9.2.

Какая технология используется для защиты конфиденциальной информации?

- А) HTTPS
- Б) FTP
- В) HTTP
- Г) E-mail

Ответ:

Задание 10.2.

Какой тип ключа используется в шифровании?

- А) Публичный ключ
- Б) Приватный ключ
- В) Ключ для шифрования
- Г) Ключ для дешифрования

Ответ:

Задание 11.2.

Какая концепция основана на принципе, согласно которому ни одно устройство, пользователь или трафик внутри сети не должны автоматически считаться доверенными?

Ответ:

Задание 12.2.

Какой из видов угроз безопасности наиболее часто ассоциируется с компрометацией данных и нарушением конфиденциальности в информационных системах?

Ответ:

Задание 13.2.

Что такое аудит информационной безопасности и зачем он проводится?

Ответ:

Задание 14.2.

Каковы основные цели управления информационной безопасностью?

Ответ:

Задание 15.2.

Что такое аутентификация?

- А) Проверка лица
- Б) Проверка логина и пароля +
- В) Проверка безопасности
- Г) Проверка принадлежности

Ответ:

Задание 16.2.

Что такое интеграция безопасности?

- А) Совместное использование сетей
- Б) Установка защиты и антивируса
- В) Взаимодействие элементов безопасности +
- Г) Создание логической сети

Ответ:

Задание 17.2.

В чем заключается основной риск при использовании информационных систем в отношении кибербезопасности?

Ответ:

Задание 18.2.

Как называется вид шифрования, при котором используют два разных ключа: открытый для шифрования, закрытый для расшифровки?

Ответ:

Задание 19.2.

Какие шаги необходимо предпринять при обнаружении инцидента информационной безопасности?

Ответ:

Задание 20.2.

Какова роль человеческого фактора в обеспечении информационной безопасности?

Ответ:

Ключи к оцениванию заданий

Вариант 1

№ задания	Верный ответ	Критерии оценивания
1.1	Б	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
2.1	В	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
3.1	Б	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
4.1	А	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
5.1	А	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
6.1	Политика безопасности организации	2 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
7.1	Уровни управления информационной безопасностью включают: Стратегический уровень: Определение общей стратегии и политики безопасности. Тактический уровень: Разработка конкретных планов и процедур для реализации стратегий. Операционный уровень: Непосредственное выполнение задач по обеспечению безопасности, мониторинг и контроль за соблюдением политик.	3 балла – полное совпадение с верным ответом по смыслу 1 балл – правильный, но не полный ответ 0 баллов – неверный ответ или его отсутствие
8.1	Б	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
9.1	Г	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
10.1	Б	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
11.1	Аудит информационной безопасности	2 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
12.1	Инцидент информационной безопасности	2 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
13.1	К основным угрозам информационной безопасности относятся: Несанкционированный доступ к данным. Вирусы и вредоносное ПО. Атаки типа «человек посередине» (MITM). Фишинговые атаки. Утечка данных через сотрудников. Физическое повреждение оборудования. Нарушение правил безопасности пользователями. ДДос-атаки. Инсайдерские угрозы. Ошибки конфигурации систем.	3 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
14.1	Принцип минимизации привилегий предполагает предоставление пользователям, программам и сервисам только тех прав доступа, которые	3 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие

	необходимы для выполнения их функций. Это снижает вероятность злоупотребления правами и уменьшает потенциальный ущерб при компрометации учетной записи.	
15.1	Б	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
16.1	Г	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
17.1	Защищенная информационная система	2 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
18.1	Управление доступом	2 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
19.1	Методы аутентификации могут включать: Однофакторную аутентификацию (например, пароль). Двухфакторную аутентификацию (пароль + одноразовый код). Многофакторную аутентификацию (использование нескольких факторов одновременно, таких как биометрические данные, токены и др.). Биометрическую аутентификацию (сканирование отпечатков пальцев, распознавание лица и т.п.). Смарт-карты и токены.	3 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
20.1	Периметровая защита – это комплекс мер, направленных на обеспечение безопасности границ сети организации. Включает такие технологии, как: Межсетевые экраны (Firewall). VPN (виртуальные частные сети). DMZ (демилитаризованная зона). IDS/IPS (система обнаружения и предотвращения вторжений). Антивирусные программы.	3 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие

Вариант 2

№ задания	Верный ответ	Критерии оценивания
1.2	Б	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
2.2	В	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
3.2	Б	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
4.2	Г	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
5.2	А	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
6.2	Шифрование данных	2 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
7.2	Система мониторинга информационной безопасности обычно состоит из следующих компонентов: Системы обнаружения вторжений (IDS/IPS). Журналы событий и лог-файлы.	3 балла – полное совпадение с верным ответом по смыслу 1 балл – правильный, но не полный ответ 0 баллов – неверный ответ или его отсутствие

	Средства анализа трафика. Сканеры уязвимостей. Механизмы оповещения о нарушениях. Средства корреляционного анализа событий	
8.2	Б	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
9.2	А	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
10.2	Г	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
11.2	Концепция нулевого доверия	2 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
12.2	Внедрение вредоносного ПО	2 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
13.2	Аудит информационной безопасности – это систематическая проверка состояния системы защиты информации в организации. Он проводится для оценки эффективности существующих мер безопасности, выявления уязвимостей и соответствия требованиям законодательства и стандартам. Результаты аудита помогают улучшить защиту информационных активов.	3 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
14.2	Основные цели управления информационной безопасностью: Обеспечение конфиденциальности информации. Поддержание целостности данных. Гарантирование доступности информации для авторизованных пользователей. Соблюдение нормативных требований и стандартов.	3 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
15.2	Б	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
16.2	В	1 балл – полное совпадение с верным ответом 0 баллов – неверный ответ или его отсутствие
17.2	Угроза утечки конфиденциальной информации	2 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
18.2	Асимметричное шифрование	2 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
19.2	При обнаружении инцидента следует действовать следующим образом: Изолировать затронутые системы для предотвращения дальнейшего распространения угрозы. Провести анализ инцидента для определения его масштаба и причин. Принять меры по устранению уязвимости и восстановлению нормальной работы. Документировать инцидент и предпринятые действия. Провести обучение персонала для предотвращения подобных ситуаций в будущем.	3 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования 0 баллов – неверный ответ или его отсутствие
20.2	Человеческий фактор играет ключевую роль в обеспечении безопасности, так как	3 балла – полное совпадение с верным ответом 1 балл – правильный ответ, без обоснования

	сотрудники могут стать как самой сильной стороной защиты, так и слабым звеном. Важно проводить регулярное обучение персонала правилам безопасного поведения в сети, избегать социальных инженерных атак и обеспечивать соблюдение политик безопасности.	0 баллов – неверный ответ или его отсутствие
--	--	---