Тестовое задание для диагностического тестирования по дисциплине:
«Управление информационной безопасностью»

Квалификация выпускника	**бакалавр**
Направление подготовки	**09.03.02**
	Информационные системы и технологии
Направленность (профиль)	**Безопасность информационных систем и технологий**
	наименование
Форма обучения	**очная**
Кафедра разработчик	**Информатики и вычислительной техники**
	наименование
Выпускающая кафедра	**Информатики и вычислительной техники**
	наименование

№	Задание	Варианты ответов	Тип сложности вопроса
1	Какая из следующих категорий атак является наиболее распространенной?	a) физические атаки b) вредоносные программы c) социальная инженерия d) отказ в обслуживании	**низкий**
2	Какой компонент информационной безопасности связан с ограничением и контролем доступа к информационным ресурсам?	a) конфиденциальность b) целостность c) доступность d) аутентификация	**низкий**
3	Какая из следующих технологий обеспечивает защиту передаваемой информации путем шифрования?	a) брандмауэр b) виртуальная частная сеть (VPN) c) система обнаружения вторжений (IDS) d) бэкап	**низкий**
4	Какой инструмент используется для защиты сети от внешних атак?	a) антивирусное программное обеспечение b) брандмауэр c) система обнаружения вторжений (IDS) d) VPN	**низкий**
5	Какая из следующих мер является наиболее эффективной в предотвращении утраты данных из-за отказа оборудования?	a) использование резервного копирования данных b) регулярные проверки на наличие вредоносных программ c) автоматическое обновление программного обеспечения d) установка физических защитных барьеров	**низкий**
6	Что такое "фишинг"?	a) подделка электронных документов b) метод анализа сетевого трафика c) взлом системы путем ввода неправильного пароля d) метод мошенничества путем применения социальной инженерии	**средний**
7	Какой вид атаки может привести к отказу в обслуживании, путем создания сбоев в работе сервера?	a) фишинг b) снижение производительности c) DDoS атака d) виртуальная частная сеть (VPN)	**средний**
8	Какая мера безопасности требуется для защиты информации при передаче по открытым сетям, таким как Интернет?	a) шифрование данных b) аутентификация пользователя c) бэкап данных d) использование брандмауэра	**средний**
9	Что означает аббревиатура BYOD?	a) Принесите свое устройство b) Создайте резервную копию данных c) Создайте свою базу данных d) Купите себе устройство	**средний**
10	Какую роль играет политика безопасности в управлении информационной безопасностью?	a) определяет список патчей и обновлений для программного обеспечения b) описывает правила и процедуры для защиты информации c) контролирует доступ к информационным ресурсам d) предотвращает физические атаки на организацию	**средний**
11	Какая из следующих мер является наиболее эффективной для защиты от социальной инженерии?	a) использование сильных паролей b) проведение обучения сотрудников по безопасности c) установка системы обнаружения вторжений (IDS)	**средний**

№	Задание	Варианты ответов	Тип сложности вопроса
		d) использование шифрования данных	
12	Какой метод аутентификации основан на использовании уникальных физических характеристик пользователя?	a) парольное подтверждение b) многофакторная аутентификация c) биометрическая аутентификация d) токены	**средний**
13	Какой из следующих видов аутентификации обеспечивает наибольшую безопасность?	a) парольная аутентификация b) SMS-аутентификация c) аутентификация с использованием жетона d) биометрическая аутентификация	**средний**
14	Что такое Least Privilege Principle?	a) Принцип, согласно которому каждый пользователь должен обладать доступом только к необходимым ресурсам b) Принцип распределения прав доступа на основе ролей пользователей c) Принцип шифрования данных для защиты их конфиденциальности d) Принцип обеспечения физической безопасности серверных помещений	**средний**
15	Какой из следующих возможных способов хранения паролей является наиболее безопасным?	a) хранение в открытом виде b) хранение в зашифрованном виде c) хранение в хеш-сумме d) хранение в текстовом файле	**средний**
16	Что такое "криптография"?	a) метод поиска уязвимостей в системе b) метод анализа сетевого трафика c) метод защиты информации путем шифрования d) метод сканирования системы на наличие вредоносных программ	**высокий**
17	Что такое "брандмауэр"?	a) устройство для обнаружения вторжений b) метод анализа сетевого трафика c) программа для резервного копирования данных d) устройство для фильтрации сетевого трафика	**высокий**
18	Что такое "аутентификация"?	a) процесс проверки подлинности пользователя b) процесс предоставления привилегий пользователю c) методы сохранения целостности данных d) метод профилирования сетевого трафика	**высокий**
19	Что означает аббревиатура IDS?	a) Система обнаружения вторжений b) Защита данных в Интернете c) Внутренняя система данных d) Заявление об обнародовании информации	**высокий**
20	Что означает аббревиатура ACS?	a) Обнаружение и предотвращение вторжений b) Шифрование данных c) Управление и контроль доступа пользователей к ресурсам d) Анализ и мониторинг сетевого трафика	**высокий**