Тестовое задание для диагностического тестирования по дисциплине:
«Разработка и эксплуатация защищенных информационных систем»

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	Что такое система аутентификации?	a) Механизм для обеспечения конфиденциальности данных пользователя. b) Процесс проверки подлинности идентификационных данных пользователя. c) Инструмент для шифрования сетевого трафика. d) Метод защиты от вредоносного программного обеспечения.	**низкий**
2	Какие факторы могут использоваться в системе аутентификации для проверки подлинности пользователя?	a) Логин и пароль b) Отпечаток пальца c) SMS-код d) Все вышеперечисленное	**низкий**
3	Какие типы доступа могут быть разграничены в системе разграничения прав доступа?	a) Чтение, запись и выполнение b) Протоколирование, мониторинг и шифрование c) Аутентификация, авторизация и аудит d) Парольный, биометрический и одноразовый	**низкий**
4	Какие протоколы поддерживает COA Suricata для анализа сетевого трафика?	a) TCP и UDP b) HTTP и FTP c) DNS и DHCP d) SMTP и POP3	**низкий**
5	Какая из следующих задач НЕ является частью процесса аудита безопасности?	a) Определение уязвимостей системы b) Оценка эффективности контрольных мер c) Разработка программного обеспечения d) Проверка соответствия политикам и процедурам	**низкий**
6	Что такое OTP?	a) Пароль, который можно использовать только один раз b) Пароль, который действителен только в определенное время c) Пароль, который генерируется каждый раз при входе в систему d) Пароль, который должен изменяться регулярно	**средний**
7	Какие компоненты включает в себя система разграничения прав доступа?	a) Политики доступа и аудита b) Прокси-серверы и VPN c) Шифрование и аутентификация d) Файловые системы и базы данных	**средний**
8	Что из перечисленного нужно сделать в первую очередь при обнаружении инцидента информационной безопасности?	a) Блокировка доступа к системе. b) Отправка уведомления ответственному лицу. c) Безотлагательное восстановление системы. d) Обновление антивирусного программного обеспечения.	**средний**
9	Как можно обеспечить аудит привилегий в АИС?	a) Ведение журнала доступа и операций с привилегиями b) Автоматическое оповещение администратора о необычной активности c) Регулярная проверка списков привилегий пользователей d) Все вышеперечисленные	**средний**

№	Задание	Варианты ответов	Тип сложности вопроса
10	Что такое DDoS-атака?	a) Атака на компьютерную сеть, при которой злоумышленники создают искусственный перегруз b) Атака на конкретное программное обеспечение c) Любая попытка несанкционированного доступа к защищенным данным d) Попытка подкупа обслуживающего персонала	**средний**
11	Какими инструментами можно проводить аудит безопасности?	a) Nessus, OpenVAS, Nikto b) Snort, Wireshark, Nmap c) Metasploit, Burp Suite, Acunetix d) Все вышеперечисленные инструменты	**средний**
12	Что такое эксплойт?	a) Приложение или код, используемый для атаки на уязвимость системы b) Программа для сканирования портов c) Программа для тестирования сложности паролей d) Процесс запуска инструментов для аудита безопасности	**средний**
13	Что такое политика безопасности в контексте аудита безопасности?	a) Набор правил и принципов, определяющих требования к безопасности системы b) Физический барьер, предотвращающий несанкционированный доступ c) Программа для автоматизации процессов безопасности d) Перечень запрещенных действий, которые надо предотвратить в системе	**средний**
14	Какие методы используются при проведении аудита безопасности?	a) Сканирование портов, тестирование на проникновение b) Анализ журналов событий, проверка политик безопасности c) Прослушивание сетевого трафика, проверка физической безопасности d) Все вышеперечисленные методы	**средний**
15	Почему не рекомендуется делать резервное копирование слишком часто?	a) Излишняя трата ресурсов системы b) Засорение хранилища данных и усложнение поиска информации c) Рассогласование версий хранимых данных d) Увеличение риска возникновения ошибок	**средний**
16	Какие методы обнаружения атак и вторжений используются для обнаружения новых и неизвестных угроз?	a) Анализ поведения и эвристический анализ b) Фильтрация пакетов и контроль доступа c) Шифрование и аутентификация d) VPN и автоматизация безопасности	**высокий**
17	Какой метод обнаружения атак и вторжений основывается на анализе системных журналов и лог-файлов?	a) HIDS b) NIDS c) IDS d) Firewall	**высокий**
18	Какой протокол аутентификации используется для безопасного доступа к удаленному серверу?	a) HTTP b) FTP c) SSH d) SMTP	**высокий**
19	Какой протокол аутентификации обеспечивает безопасное	a) WPS b) WEP c) WPA	**высокий**

№	Задание	Варианты ответов	Тип сложности вопроса
	подключение к беспроводным сетям?	d) WEP2	
20	Какой протокол аутентификации используется для безопасного доступа к удаленным рабочим станциям или серверам через веб-браузер?	a) SSH b) HTTPS c) RDP d) Telnet	**высокий**