**<question>Какой из следующих протоколов использует асимметричное шифрование для защиты обмена ключами?**

**<variant>SSL**

**<variant>TLS**

**<variant>IPSec**

**<variant>S/MIME**

**<variant>Diffie-Hellman**

**<question>Какой из следующих протоколов использует симметричное шифрование для защиты обмена ключами?**

**<variant>Diffie-Hellman**

**<variant>TLS**

**<variant>IPSec**

**<variant>S/MIME**

**<variant>SSL**

**<question>Что означает принцип конфиденциальности?**

**<variant>Информация доступна всем пользователям**

**<variant>Информация сохраняет свою структуру**

**<variant>Информация защищена от несанкционированного доступа**

**<variant>Информация может быть удалена в любой момент**

**<variant>Информация всегда актуальна**

**<question>Что из перечисленного является угрозой информационной безопасности?**

**<variant>Бэкап данных**

**<variant>Хеширование**

**<variant>Фишинг**

**<variant>Аудит**

**<variant>Контроль доступа**

**<question>Какой вид шифрования использует одну и ту же ключевую информацию для шифрования и дешифрования?**

**<variant>Асимметричное**

**<variant>Симметричное**

**<variant>Хеширование**

**<variant>Цифровая подпись**

**<variant>Компрессия**

**<question>Что такое двухфакторная аутентификация?**

**<variant>Использование только пароля**

**<variant>Подтверждение через e-mail**

**<variant>Комбинация двух методов проверки личности**

**<variant>Биометрическая проверка**

**<variant>Проверка IP-адреса**

**<question>Какой вредоносный код способен самостоятельно распространяться по сети?**

**<variant>Вирус**

**<variant>Червь**

**<variant>Троян**

**<variant>Руткит**

**<variant>Ботнет**

**<question>Что делает фаервол?**

**<variant>Восстанавливает удалённые данные**

**<variant>Управляет доступом к сети**

**<variant>Шифрует трафик**

**<variant>Удаляет вирусы**

**<variant>Анализирует поведение пользователей**

**<question>Какой стандарт связан с управлением информационной безопасностью?**

**<variant>ISO/IEC 9001**

**<variant>ISO/IEC 27001**

**<variant>ISO/IEC 14000**

**<variant>ISO/IEC 31000**

**<variant>ISO/IEC 20000**

**<question>Что характерно для социальной инженерии?**

**<variant>Использование сложных программ**

**<variant>Взлом серверов**

**<variant>Манипуляция человеком**

**<variant>Установка вредоносного ПО**

**<variant>Перехват пакетов**

**<question>Что такое DDoS-атака?**

**<variant>Перехват данных**

**<variant>Массовая рассылка писем**

**<variant>Перегрузка сервера большим числом запросов**

**<variant>Вирусное заражение системы**

**<variant>Удаление логов системы**

**<question>Процесс защиты информации от несанкционированного доступа, использования, раскрытия, разрушения, модификации или нарушения целостности**

**<variant> Firewall**

**<variant> VPN**

**<variant> HTTPS**

**<variant> IDS**

**<variant> Information Security Management System**

**<question>Тип атаки, при котором злоумышленник перехватывает и, возможно, изменяет передаваемые между двумя сторонами данные**

**<variant> DoS**

**<variant> Phishing**

**<variant> Ransomware**

**<variant> DDoS**

**<variant> Man in the Middle Attack**

**<question>Политика безопасности, при которой доступ к ресурсам ограничивается до минимально необходимого уровня**

**<variant> Full Access**

**<variant> Open Access**

**<variant> Multi Access**

**<variant> Broad Access**

**<variant> Principle of Least Privilege**

**<question>Метод защиты данных, заключающийся в преобразовании информации в форму, недоступную для понимания без специального ключа**

**<variant> Backup**

**<variant> Firewall**

**<variant> Proxy**

**<variant> Tunneling**

**<variant> Data Encryption Algorithm**

**<question>Метод аутентификации, при котором используется комбинация нескольких факторов, таких как пароль, устройство и биометрия**

**<variant> Token**

**<variant> PIN**

**<variant> CAPTCHA**

**<variant> Password**

**<variant> Multi-Factor Authentication System**

**<question>Вредоносное программное обеспечение, блокирующее доступ к системе или данным до получения выкупа**

**<variant> Worm**

**<variant> Trojan**

**<variant> Spyware**

**<variant> Keylogger**

**<variant> Ransomware Encryption Malware**

**<question>Метод анализа уязвимостей и поиска слабых мест в системе безопасности без причинения вреда**

**<variant> Virus Scan**

**<variant> Log Review**

**<variant> Malware Scan**

**<variant> Network Monitoring**

**<variant> Penetration Testing Methodology**

**<question>Сетевой экран, предназначенный для контроля и фильтрации входящего и исходящего трафика**

**<variant> IDS**

**<variant> IPS**

**<variant> NAT**

**<variant> Proxy**

**<variant> Stateful Packet Inspection Firewall**

**<question>Программа, предназначенная для сбора конфиденциальной информации с устройств пользователей без их ведома**

**<variant> Adware**

**<variant> Worm**

**<variant> Rootkit**

**<variant> Botnet**

**<variant> Spyware Data Collection Tool**

**<question>Механизм регистрации и анализа событий и инцидентов в системе безопасности**

**<variant> Audit**

**<variant> Ping**

**<variant> Trace**

**<variant> Log**

**<variant> Security Information and Event Management**

**<question>Какой протокол используется для передачи электронной почты в сети?**

**<variant> Все вышеперечисленное**

**<variant> SMTP**

**<variant> POP3**

**<variant> IMAP**

**<variant> IP**

<question> Что такое DDoS-атака?

<variant> Массовая атака, перегружающая сервер

<variant> Вирус в приложении

<variant> Фишинг-письмо

<variant> SQL-инъекция

<variant> Взлом пароля

<question>Программа, перехватывающая и анализирующая сетевой трафик

<variant> Сниффер

<variant> Вирус

<variant> Фаервол

<variant> Антивирус

<variant> Руткит

<question>Программа, скрывающая своё присутствие и деятельность в системе

<variant> Руткит

<variant> Вирус

<variant> Червь

<variant> Троян

<variant> Ботнет

<question>Какой протокол используется для получения электронной почты в сети?

<variant> POP3

<variant> IMAP

<variant> SMTP

<variant> Все вышеперечисленные

<variant> RTP

<question>Какой протокол отвечает за маршрутизацию данных в сети?

<variant> IP

<variant> TCP

<variant> HTTP

<variant> FTP

<variant> POP3

<question>Какой термин обозначает незаконное получение конфиденциальной информации?

<variant> Фишинг

<variant> Бэкап

<variant> Роутинг

<variant> Кэширование

<variant> Синхронизация

<question>Как называется процесс оценки рисков и угроз информационной безопасности?

<variant> Аудит безопасности

<variant> Бэкап

<variant> Обновление драйверов

<variant> Индексация

<variant> Копирование данных