1.

|  |
| --- |
| Что чаще всего становится причиной уязвимостей веб-сайта? |
| Неправильная конфигурация сервера и нехватка знаний по безопасности. |
| Устаревший дизайн сайта |
| Большое количество пользователей |
| Низкое качество графики |
| Отсутствие HTTPS-сертификата |

2.

|  |
| --- |
| Какова основная функция протокола IP? |
| Идентификация компьютеров и маршрутизация пакетов. |
| Передача сообщений электронной почты |
| Шифрование веб-трафика |
| Удалённый доступ к терминалам |
| Мониторинг сетевой активности |

3.

|  |
| --- |
| Какой протокол используется для отправки исходящей почты? |
| SMTP. |
| POP3 |
| DNS |
| FTP |
| NTP |

4.

|  |
| --- |
| Какой порт обычно использует HTTP? |
| 80. |
| 443 |
| 25 |
| 21 |
| 123 |

5.

|  |
| --- |
| Какая организация отвечает за управление доменными именами в США? |
| ICANN. |
| IEEE |
| ISOC |
| SANS |
| IETF |

6.

|  |
| --- |
| Что делает протокол ICMP? |
| Сообщает об ошибках при передаче IP-пакетов. |
| Отправляет электронные письма |
| Шифрует файлы |
| Контролирует принтеры |
| Выполняет команды на удалённом сервере |

7.

|  |
| --- |
| Какая основная цель разработки интернет-протоколов на раннем этапе? |
| Объединение людей и обмен информацией. |
| Защита от атак |
| Бизнес-мониторинг |
| Создание платных сервисов |
| Контроль за пользователями |

8.

|  |
| --- |
| Какой протокол чаще всего используется для передачи файлов? |
| FTP. |
| HTTP |
| ICMP |
| SMTP |
| POP |

9.

|  |
| --- |
| Какой протокол предоставляет службу доменных имён? |
| DNS. |
| SNMP |
| NTP |
| IMAP |
| SSL |

10.

|  |
| --- |
| Что означает термин 'усиление системы'? |
| Удаление ненужных компонентов и закрытие лишних портов. |
| Повышение частоты процессора |
| Увеличение числа пользователей |
| Использование анимации |
| Оптимизация графики |

11.

|  |
| --- |
| Какая проблема часто возникает при установке ПО по умолчанию? |
| Устанавливаются лишние компоненты и службы. |
| Устанавливается слишком мало компонентов |
| Отсутствует лицензия |
| Недостаток драйверов |
| Установка невозможна без интернета |

12.

|  |
| --- |
| Для чего используется UDP? |
| Передача данных без установления соединения. |
| Надёжная доставка сообщений |
| Управление сетевыми принтерами |
| Ведение логов |
| Управление временем |

13.

|  |
| --- |
| Как называется перечень критически опасных уязвимостей, составленный SANS/FBI? |
| Top 20. |
| SANS Secure |
| CVE-list |
| CERT Watch |
| Internet Shield |

14.

|  |
| --- |
| Что из перечисленного может представлять собой демонстрационный сценарий? |
| Уязвимый компонент, установленный по умолчанию. |
| Программа для анализа логов |
| Система авторизации |
| Коммерческое ПО |
| Сканер уязвимостей |

15.

|  |
| --- |
| Какой порт используется для защищённого соединения HTTPS? |
| 443. |
| 80 |
| 25 |
| 21 |
| 110 |

16.

|  |
| --- |
| Протокол TCP предоставляет ненадёжную доставку данных. |
| Неверно. |
| Верно |
| Частично |
| Не определено |
| Всё вышеперечисленное |

17.

|  |
| --- |
| DNS позволяет пользователю использовать имена вместо IP-адресов. |
| Верно. |
| Неверно |
| Зависит от конфигурации |
| Только в UNIX-системах |
| Только в США |

18.

|  |
| --- |
| DHCP назначает IP-адреса статически. |
| Неверно. |
| Верно |
| Только по запросу |
| Только при перезагрузке |
| Только в Linux |

19.

|  |
| --- |
| SANS – это международная организация по безопасности. |
| Верно. |
| Неверно |
| Только в США |
| Только для администраторов |
| Это компания-разработчик ПО |

20.

|  |
| --- |
| Протокол POP используется для отправки электронной почты. |
| Неверно. |
| Верно |
| Только в Windows |
| Только на мобильных устройствах |
| Только в Outlook |

21.

|  |
| --- |
| Какой протокол соответствует службе обмена файлами? |
| FTP. |
| Telnet |
| SMTP |
| NTP |
| SNMP |

22.

|  |
| --- |
| Какой порт соответствует протоколу HTTPS? |
| 443. |
| 80 |
| 25 |
| 53 |
| 21 |

23.

|  |
| --- |
| Какой тип транспортировки использует TCP? |
| Надёжная доставка. |
| Ненадёжная доставка |
| Диагностика IP |
| Сбор статистики |
| Динамическая адресация |

24.

|  |
| --- |
| Почему изначально интернет-протоколы не учитывали вопросы безопасности? |
| Они разрабатывались для обмена информацией в доверенной среде. |
| Не было технологий шифрования |
| Интернет был слишком медленным |
| Безопасность считалась избыточной |
| Разработчики не знали о хакерах |

25.

|  |
| --- |
| Какой способ 'усиления системы' применяется к веб-серверу? |
| Отключение ненужных служб. |
| Увеличение оперативной памяти |
| Добавление новых пользователей |
| Установка дополнительных шрифтов |
| Изменение дизайна сайта |

26.

|  |
| --- |
| Какой тип атак обычно используется для того, чтобы перегрузить сервер или ресурс, блокируя его доступность? |
| DoS-атака. |
| Вирусная атака |
| Атака социальной инженерии |
| Атака на шифрование |
| Атака на целостность данных |

27.

|  |
| --- |
| Что такое VPN (Virtual Private Network)? |
| Технология для создания защищённого канала связи через интернет. |
| Способ защиты данных с помощью шифрования |
| Программное обеспечение для защиты от вирусов |
| Метод создания резервных копий |
| Способ защиты от внешних атак |

28.

|  |
| --- |
| Что такое защита 'по принципу наименьших привилегий'? |
| Ограничение доступа пользователя к только тем данным и функциям, которые необходимы для выполнения его работы. |
| Открытие доступа ко всем данным для всех пользователей |
| Использование одного пароля для всех пользователей |
| Ограничение использования антивирусного ПО |
| Ограничение количества пользователей в системе |

29.

|  |
| --- |
| Какой из видов атак направлен на использование уязвимости в программном обеспечении для несанкционированного доступа? |
| Эксплойт. |
| Вирус |
| Червь |
| Троян |
| Спам |

30.

|  |
| --- |
| Что такое баг-вондеринг (Bug bounty)? |
| Программа, которая поощряет исследователей безопасности за нахождение уязвимостей. |
| Метод шифрования данных |
| Способ блокировки вирусов |
| Способ архивации данных |
| Метод создания резервных копий |

31.

|  |
| --- |
| Какой из перечисленных методов защиты предотвращает несанкционированный доступ к конфиденциальной информации? |
| Шифрование. |
| Архивирование |
| Виртуализация |
| Блокировка |
| Кэширование |

32.

|  |
| --- |
| Что такое 'переход по фишинговой ссылке'? |
| Переход на сайт, который выглядит как настоящий, но предназначен для сбора конфиденциальной информации. |
| Переход на защищённый сайт для ввода личных данных |
| Переход на сайт для обновления ПО |
| Переход на сайт с антивирусным ПО |
| Переход на сайт для загрузки изображений |

33.

|  |
| --- |
| Какая из технологий используется для шифрования данных в передаче? |
| SSL/TLS. |
| FTP |
| HTTP |
| IMAP |
| SMTP |

34.

|  |
| --- |
| Что такое DLP (Data Loss Prevention)? |
| Система для предотвращения утечек конфиденциальной информации. |
| Система для защиты от вирусов |
| Метод шифрования |
| Программное обеспечение для резервного копирования |
| Метод тестирования на уязвимости |

35.

|  |
| --- |
| Что такое 'вредоносное ПО' (malware)? |
| Программа, предназначенная для нанесения ущерба компьютеру или сети. |
| Программа для защиты от вирусов |
| Программа для резервного копирования данных |
| Программа для шифрования |
| Программа для архивации данных |

36.

|  |
| --- |
| Что из следующего является видом вредоносного ПО, который самозапускается и распространяется по сети? |
| Червь. |
| Вирус |
| Троян |
| Шпионская программа |
| Руткит |

37.

|  |
| --- |
| Что такое 'защищённый канал связи'? |
| Канал, использующий шифрование для безопасной передачи данных. |
| Канал, который ограничивает доступ только для авторизованных пользователей |
| Канал с высокой пропускной способностью |
| Канал для передачи текстовой информации |
| Канал для беспроводной передачи данных |

38.

|  |
| --- |
| Какой из методов защиты наиболее эффективен для защиты конфиденциальных данных от несанкционированного доступа в хранилище? |
| Шифрование данных на уровне диска. |
| Защита с помощью пароля |
| Использование двухфакторной аутентификации |
| Резервное копирование |
| Ограничение физического доступа |

39.

|  |
| --- |
| Что такое 'потоковые атаки' в контексте информационной безопасности? |
| Атаки, нацеленные на отправку больших объёмов данных для перегрузки системы. |
| Атаки, направленные на шифрование данных |
| Атаки, направленные на получение паролей |
| Атаки, использующие физический доступ к системе |
| Атаки, использующие фишинговые письма |

40.

|  |
| --- |
| Что такое 'нулевая уязвимость'? |
| Уязвимость в ПО, о которой не известно производителю или разработчику |
| Уязвимость, выявленная в процессе тестирования |
| Уязвимость, исправленная патчем |
| Уязвимость, используемая только в теории |
| Уязвимость, которая возникает при использовании устаревшего ПО |

41.

|  |
| --- |
| Какая угроза информационной безопасности связана с использованием незаконных или несанкционированных устройств в организации? |
| Угроза от использования несанкционированных устройств |
| Угроза утечек данных |
| Угроза вирусной инфекции |
| Угроза от внешних атак |
| Угроза от внутренних сотрудников |

42.

|  |
| --- |
| Что из следующего является примером уязвимости в приложении, которая может быть использована для атаки? |
| SQL-инъекция |
| Обновления системы безопасности |
| Резервное копирование |
| Использование сильных паролей |
| Аутентификация по биометрии |

43.

|  |
| --- |
| Как называется метод анализа сетевого трафика для выявления вредоносной активности? |
| Мониторинг сетевого трафика |
| Виртуализация |
| Шифрование |
| Обработка данных |
| Создание резервных копий |

44.

|  |
| --- |
| Какой метод защиты от вирусов использует сигнатуры известных угроз для их обнаружения? |
| Антивирусное ПО |
| Шифрование |
| Брандмауэр |
| Архивирование |
| Резервное копирование |

45.

|  |
| --- |
| Какая мера защиты помогает предотвратить утечку информации из организации? |
| Установка DLP-системы |
| Введение обязательного использования паролей |
| Использование антивирусных программ |
| Шифрование данных |
| Обновление ПО |

46.

|  |
| --- |
| Что такое 'двухфакторная аутентификация'? |
| Использование двух разных методов для подтверждения личности пользователя |
| Использование одного пароля для всех пользователей |
| Использование защиты на основе биометрии |
| Использование только пароля |
| Использование только СМС-кода |

47.

|  |
| --- |
| Как называется метод защиты от утечек данных через электронную почту? |
| Шифрование почтовых сообщений |
| Использование антивирусного ПО |
| Установка фаервола |
| Архивирование сообщений |
| Удаление старых сообщений |

48.

|  |
| --- |
| Какой тип атаки используется для получения доступа к данным, обманывая пользователя с помощью ложных сообщений или сайтов? |
| Фишинг |
| Вредоносное ПО |
| Атака «человек посередине» |
| Вирусная атака |
| Брутфорс |

49.

|  |
| --- |
| Какая угроза безопасности связана с отсутствием регулярного обновления ПО? |
| Уязвимость системы безопасности |
| Атака вирусом |
| Утечка данных |
| Перегрузка системы |
| Фишинг |

50.

|  |
| --- |
| Какая из технологий безопасности помогает предотвратить утечку данных при их передаче по сети? |
| VPN |
| Брандмауэр |
| Антивирус |
| Архивирование |
| Кэширование |

51.

|  |
| --- |
| Какая основная проблема возникает при использовании учетных записей с паролями по умолчанию? |
| Они создают уязвимость, которую легко использовать |
| Они ускоряют систему |
| Они увеличивают производительность |
| Они упрощают администрирование |
| Они требуют меньше памяти |

52.

|  |
| --- |
| Почему легко угадываемые пароли являются угрозой безопасности? |
| Они создают уязвимость, которую легко использовать |
| Они ускоряют систему |
| Они увеличивают производительность |
| Они упрощают администрирование |
| Они требуют меньше памяти |

53.

|  |
| --- |
| Что необходимо для успешного восстановления после нарушения защиты системы? |
| Наличие резервных копий и плана восстановления |
| Ускорение работы системы |
| Увеличение производительности |
| Упрощение администрирования |
| Уменьшение объёма памяти |

54.

|  |
| --- |
| Какая опасность связана с большим количеством открытых портов на сервере? |
| Они создают уязвимость, которую легко использовать |
| Они ускоряют систему |
| Они увеличивают производительность |
| Они упрощают администрирование |
| Они требуют меньше памяти |

55.

|  |
| --- |
| Как можно предотвратить IP spoofing? |
| Использование фильтрации пакетов на основе источника |
| Ускорение работы системы |
| Увеличение числа портов |
| Установка антивируса |
| Изменение паролей |

56.

|  |
| --- |
| Почему важно вести журналы событий на сервере? |
| Они помогают выявлять и анализировать инциденты безопасности |
| Они ускоряют систему |
| Они увеличивают производительность |
| Они упрощают администрирование |
| Они требуют меньше памяти |

57.

|  |
| --- |
| Что представляет угрозу при использовании CGI-программ на сервере? |
| Они создают уязвимость, которую легко использовать |
| Они ускоряют систему |
| Они увеличивают производительность |
| Они упрощают администрирование |
| Они требуют меньше памяти |

58.

|  |
| --- |
| Какие источники могут быть использованы для внедрения вредоносного кода на веб-сервер? |
| Уязвимые плагины и сторонние скрипты |
| Ускорение работы системы |
| Увеличение числа пользователей |
| Установка антивируса |
| Изменение дизайна сайта |

59.

|  |
| --- |
| Почему Windows 2000 и IIS подвержены большему числу атак? |
| Из-за устаревших компонентов и известных уязвимостей |
| Из-за высокой скорости работы |
| Из-за увеличения производительности |
| Из-за упрощённого администрирования |
| Из-за малого объёма памяти |

60.

|  |
| --- |
| Что представляет собой угроза, связанная с использованием Unicode на IIS? |
| Возможность обхода фильтров безопасности |
| Ускорение обработки данных |
| Увеличение производительности |
| Упрощение администрирования |
| Снижение требований к памяти |

61.

|  |
| --- |
| Как злоумышленник может использовать переполнение буфера на сервере? |
| Для выполнения произвольного кода |
| Для ускорения системы |
| Для увеличения производительности |
| Для упрощения администрирования |
| Для уменьшения памяти |

62.

|  |
| --- |
| Чем опасна уязвимая библиотека idq.dll? |
| Она позволяет выполнять удалённый код |
| Она ускоряет работу сервера |
| Она увеличивает производительность |
| Она упрощает администрирование |
| Она снижает требования к памяти |

63.

|  |
| --- |
| Какие последствия может вызвать переполнение буфера через расширение ASP ISAPI? |
| Выполнение вредоносного кода |
| Ускорение обработки запросов |
| Увеличение производительности |
| Упрощение администрирования |
| Снижение нагрузки на сервер |

64.

|  |
| --- |
| В чем суть уязвимости, связанной с разделителями заголовков HTTP? |
| Возможность внедрения вредоносного кода |
| Ускорение передачи данных |
| Увеличение производительности |
| Упрощение обработки запросов |
| Снижение объёма трафика |

65.

|  |
| --- |
| Как может произойти переполнение буфера через длинное имя файла? |
| Превышение выделенной памяти приводит к выполнению кода |
| Ускорение работы системы |
| Увеличение производительности |
| Упрощение администрирования |
| Снижение требований к памяти |

66.

|  |
| --- |
| Какую опасность представляет расширение HTR ISAPI? |
| Возможность выполнения произвольного кода |
| Ускорение обработки запросов |
| Увеличение производительности |
| Упрощение администрирования |
| Снижение нагрузки на сервер |

67.

|  |
| --- |
| Что может вызвать метод поддержки ошибок в фильтрах ISAPI? |
| Уязвимость для атак |
| Ускорение работы системы |
| Увеличение производительности |
| Упрощение администрирования |
| Снижение требований к памяти |

68.

|  |
| --- |
| Какая ошибка может нарушить доступ к службе FTP? |
| Неправильная конфигурация разрешений |
| Ускорение передачи данных |
| Увеличение производительности |
| Упрощение администрирования |
| Снижение объёма трафика |

69.

|  |
| --- |
| В чем заключается угроза межсайтовых сценариев (CSS)? |
| Возможность выполнения вредоносного кода на стороне клиента |
| Ускорение загрузки страниц |
| Увеличение производительности |
| Упрощение администрирования |
| Снижение требований к памяти |

70.

|  |
| --- |
| Почему File Sharing в Windows может быть опасен? |
| Он открывает доступ к файлам без должной защиты |
| Он ускоряет систему |
| Он увеличивает производительность |
| Он упрощает администрирование |
| Он требует меньше памяти |

71.

|  |
| --- |
| Как учетная запись SYSTEM может быть использована злоумышленниками? |
| Для получения полного контроля над системой |
| Для ускорения работы сервера |
| Для увеличения производительности |
| Для упрощения администрирования |
| Для снижения нагрузки |

72.

|  |
| --- |
| Почему пароли LAN Manager уязвимы? |
| Они используют слабое шифрование |
| Они ускоряют авторизацию |
| Они увеличивают производительность |
| Они упрощают администрирование |
| Они требуют меньше памяти |

73.

|  |
| --- |
| Какую опасность представляют зашифрованные пароли в SAM? |
| Их можно извлечь и расшифровать |
| Они ускоряют вход в систему |
| Они увеличивают производительность |
| Они упрощают администрирование |
| Они требуют меньше памяти |

74.

|  |
| --- |
| Зачем важно своевременно устанавливать обновления безопасности? |
| Они закрывают известные уязвимости |
| Они ускоряют систему |
| Они увеличивают производительность |
| Они упрощают администрирование |
| Они требуют меньше памяти |

75.

|  |
| --- |
| С чего злоумышленник обычно начинает анализ уязвимостей системы? |
| Сканирование открытых портов и служб |
| Ускорение работы системы |
| Увеличение производительности |
| Упрощение администрирования |
| Снижение требований к памяти |

76.

|  |
| --- |
| Что такое технический канал утечки информации? |
| Совокупность средств и среды передачи информации |
| Программа защиты |
| Имейл-сервер |
| Установка антивируса |
| Профилактика паролей |

77.

|  |
| --- |
| Что может стать источником угрозы ПД при технической утечке? |
| Электромагнитные излучения |
| Личный пароль |
| Лицензия |
| Файловая система |
| USB-накопитель |

78.

|  |
| --- |
| Как классифицируются нарушители по доступу к ИСПД? |
| Внутренние и внешние |
| Программисты и админы |
| Пользователи и гости |
| Сетевые и интернет |
| Техники и инженеры |

79.

|  |
| --- |
| Какой тип угрозы связан с акустической информацией? |
| Речевая |
| Сетевая |
| Визуальная |
| Физическая |
| Процессорная |

80.

|  |
| --- |
| Что такое ПЭМИН? |
| Побочные электромагнитные излучения и наводки |
| Сетевая утечка |
| Шпионская программа |
| Просмотр видеокамерой |
| Анализ загрузок |

81.

|  |
| --- |
| Кто такой внутренний нарушитель? |
| Имеющий доступ к ИСПД |
| Взломщик из интернета |
| Региональный оператор |
| Сотрудник без допуска |
| Пользователь гаджета |

82.

|  |
| --- |
| Что является основной причиной уязвимостей ПО? |
| Ошибки при разработке |
| Устаревшие лицензии |
| Плохая защита пароля |
| Недостаточная память |
| Высокая нагрузка |

83.

|  |
| --- |
| К какому этапу жизненного цикла может относиться уязвимость? |
| Проектирование |
| Установка |
| Пользование |
| Обслуживание |
| Сборка |

84.

|  |
| --- |
| Что делает носитель вредоносной программы? |
| Распространяет злонамеренный код |
| Подключается к облаку |
| Защищает данные |
| Проверяет сервер |
| Сжимает файлы |

85.

|  |
| --- |
| Что из нижеперечисленного может быть техническим средством ПД? |
| Компьютер |
| Программный архив |
| Домен |
| Авторизация |
| Файловый доступ |

86.

|  |
| --- |
| Как называется специальное программное воздействие? |
| Программная закладка |
| Антиспам |
| Бэкап |
| Патч |
| Драйвер |

87.

|  |
| --- |
| Как классифицируются угрозы по типу свойств информации? |
| Конфиденциальность, целостность, доступность |
| Технические и программные |
| Вирусные и невирусные |
| Цифровые и аналоговые |
| Прямые и случайные |

88.

|  |
| --- |
| Что может быть последствием реализации уязвимости? |
| Несанкционированный доступ |
| Стирание кэша |
| Авторская подпись |
| Создание базы |
| Бэкап данных |

89.

|  |
| --- |
| Что используется для перехвата информации через ПЭМИН? |
| Радиоприемное устройство |
| Смартфон |
| Сканер |
| Микрофон |
| Процессор |

90.

|  |
| --- |
| К какому типу относятся "видовые угрозы"? |
| Визуальные |
| Аудио |
| Системные |
| Сетевые |
| Приложенческие |

91.

|  |
| --- |
| Какая программа может нарушить работу ИСПД? |
| Вредоносное ПО |
| Обновлятор |
| Электронная подпись |
| Драйвер видеокарты |
| Архиватор |

92.

|  |
| --- |
| Что является "носителем информации" в техническом канале? |
| Человек |
| Роутер |
| Смартфон |
| Сертификат |
| Контроллер |

93.

|  |
| --- |
| Что может быть следствием неправильной настройки ПО? |
| Уязвимость |
| Экономия памяти |
| Увеличение скорости |
| Защита данных |
| Автоматический выход |

94.

|  |
| --- |
| Что относится к методам утечки речевой информации? |
| Виброакустические волны |
| Текстовый документ |
| Файловый запрос |
| Хеш-контроль |
| Электронная подпись |

95.

|  |
| --- |
| Что делает внутреннюю угрозу особенно опасной? |
| Наличие доступа |
| Отсутствие сотрудников |
| Случайный выход |
| Старое оборудование |
| Незнание политики |

96.

|  |
| --- |
| Что нужно для анализа уязвимостей? |
| Оценка системы |
| Смартфон |
| Подпись |
| Файловый доступ |
| Сетевой пакет |

97.

|  |
| --- |
| Какой из нижеуказанных примеров — это атака по ПЭМИН? |
| Перехват сигнала |
| Замена логина |
| Установка сервера |
| Отправка email |
| DoS-авария |

98.

|  |
| --- |
| Как можно уменьшить уязвимости? |
| Установить патчи |
| Отключить регистрацию |
| Переставить сеть |
| Очистить историю |
| Изменить язык |

99.

|  |
| --- |
| Что понимается под "аппаратной закладкой"? |
| Устройство сбора данных |
| Файл |
| Код |
| Сеть |
| Пароль |

100.

|  |
| --- |
| Какой пример является угрозой конфиденциальности? |
| Перехват логина и пароля |
| Случайное удаление |
| Резервное копирование |
| Шифрование |
| Обновление |

101.

|  |
| --- |
| Кто предложил алгоритм RSA? |
| Р. Райвест, А. Шамир, Л. Адлеман |
| У. Диффи, М. Хеллман |
| Т. Эль-Гамаль |
| Н. Коблиц, В. Миллер |
| Д. Нагорный |

102.

|  |
| --- |
| На чем основана криптографическая стойкость алгоритма RSA? |
| На сложности задачи факторизации больших чисел |
| На вычислении дискретных логарифмов |
| На свойствах эллиптических кривых |
| На случайности генерации ключей |
| На симметричном шифровании |

103.

|  |
| --- |
| Как вычисляется модуль N в алгоритме RSA? |
| N = P \* Q |
| N = P + Q |
| N = (P - 1)(Q - 1) |
| N = P / Q |
| N = P - Q |

104.

|  |
| --- |
| Что является открытым ключом в алгоритме RSA? |
| Числа e и N |
| Число d |
| Числа P и Q |
| Число f |
| Числа e и f |

|  |
| --- |
| Какая формула используется для шифрования блока mi в RSA? |
| ci = mi^e mod N |
| ci = mi^d mod N |
| mi = ci^d mod N |
| mi = ci^e mod N |
| ci = mi \* N mod d |

106.

|  |
| --- |
| Какой алгоритм используется для распределения ключей? |
| Алгоритм Диффи-Хеллмана |
| Алгоритм RSA |
| Алгоритм Эль-Гамаля |
| Криптосистемы на эллиптических кривых |
| Алгоритм ГОСТ 28147-89 |

107.

|  |
| --- |
| На чем основана безопасность алгоритма Диффи-Хеллмана? |
| На трудности вычисления дискретных логарифмов |
| На задаче факторизации |
| На свойствах эллиптических кривых |
| На генерации случайных чисел |
| На симметричном шифровании |

108.

|  |
| --- |
| Какие параметры являются общими в алгоритме Диффи-Хеллмана? |
| Числа P и A |
| Числа X1 и X2 |
| Числа Y1 и Y2 |
| Числа d и e |
| Числа P и Q |

109.

|  |
| --- |
| Как вычисляется общий секретный ключ Z в алгоритме Диффи-Хеллмана первым пользователем? |
| Z = Y2^X1 mod P |
| Z = Y1^X2 mod P |
| Z = A^X1 mod P |
| Z = Y2^X2 mod P |
| Z = P^X1 mod A |

110.

|  |
| --- |
| Какой алгоритм может использоваться для шифрования, подписи и согласования ключа? |
| Алгоритм Эль-Гамаля |
| Алгоритм RSA |
| Алгоритм Диффи-Хеллмана |
| Криптосистемы на эллиптических кривых |
| Алгоритм ГОСТ 28147-89 |

111.

|  |
| --- |
| Как вычисляется параметр r в алгоритме Эль-Гамаля? |
| r = A^k mod P |
| r = Y2^k mod P |
| r = m \* Y2^k mod P |
| r = e \* X2 mod P |
| r = A^X1 mod P |

112.

|  |
| --- |
| Что обеспечивает высокую криптостойкость систем на эллиптических кривых? |
| Сложность вычисления дискретных логарифмов |
| Задача факторизации |
| Генерация случайных чисел |
| Симметричное шифрование |
| Вычисление обратных функций |

113.

|  |
| --- |
| Какой размер модуля обеспечивает стойкость в системах на эллиптических кривых, эквивалентную RSA с 1024 битами? |
| 160 бит |
| 768 бит |
| 1024 бит |
| 2048 бит |
| 500 бит |

114.

|  |
| --- |
| Какой алгоритм требует возведения в степень по модулю для шифрования? |
| Алгоритм RSA |
| Алгоритм Диффи-Хеллмана |
| Криптосистемы на эллиптических кривых |
| Алгоритм ГОСТ 28147-89 |
| Алгоритм AES |

115.

|  |
| --- |
| Какой алгоритм используется в пакете шифрования PGP? |
| Алгоритм RSA |
| Алгоритм Диффи-Хеллмана |
| Алгоритм Эль-Гамаля |
| Криптосистемы на эллиптических кривых |
| Алгоритм ГОСТ 28147-89 |

116.

|  |
| --- |
| Какой размер ключа рекомендован для особо секретной информации в RSA? |
| 2048 бит |
| 768 бит |
| 1024 бит |
| 160 бит |
| 500 бит |

117.

|  |
| --- |
| Что делает алгоритм RSA медленнее симметричных алгоритмов? |
| Работа с большими числами |
| Генерация случайных чисел |
| Вычисление дискретных логарифмов |
| Использование эллиптических кривых |
| Передача ключей |

118.

|  |
| --- |
| Какой алгоритм уязвим к атаке "человек-в-середине"? |
| Алгоритм Диффи-Хеллмана |
| Алгоритм RSA |
| Алгоритм Эль-Гамаля |
| Криптосистемы на эллиптических кривых |
| Алгоритм ГОСТ 28147-89 |

119.

|  |
| --- |
| Как можно предотвратить атаку "человек-в-середине"? |
| Использовать цифровые подписи |
| Уменьшить размер ключей |
| Увеличить модуль N |
| Изменить алгоритм шифрования |
| Удалить открытые ключи |

120.

|  |
| --- |
| Какая атака использует шифрование выбранных текстов? |
| Атака на основе выбранного открытого текста |
| Атака "человек-в-середине" |
| Атака грубой силы |
| Атака по времени |
| Атака по известному шифротексту |

121.

|  |
| --- |
| Какой алгоритм является рандомизированным? |
| Алгоритм Эль-Гамаля |
| Алгоритм RSA |
| Алгоритм Диффи-Хеллмана |
| Криптосистемы на эллиптических кривых |
| Алгоритм ГОСТ 28147-89 |

122.

|  |
| --- |
| Что добавляют к сообщению для защиты от атаки по выбранному тексту? |
| Случайную информацию |
| Открытый ключ |
| Закрытый ключ |
| Модуль N |
| Число f |

123.

|  |
| --- |
| Какой стандарт закрепляет использование эллиптических кривых в России? |
| ГОСТ Р34.10-2001 |
| ANSI X9.62 |
| FIPS 186-2 |
| ГОСТ 28147-89 |
| PGP |

124.

|  |
| --- |
| Какой алгоритм был предложен первым для открытого распределения ключей? |
| Алгоритм Диффи-Хеллмана |
| Алгоритм RSA |
| Алгоритм Эль-Гамаля |
| Криптосистемы на эллиптических кривых |
| Алгоритм ГОСТ 28147-89 |

125.

|  |
| --- |
| Какой алгоритм использует умножение сообщения на секретный ключ для шифрования? |
| Алгоритм Эль-Гамаля |
| Алгоритм RSA |
| Алгоритм Диффи-Хеллмана |
| Криптосистемы на эллиптических кривых |
| Алгоритм ГОСТ 28147-89 |

126.

|  |
| --- |
| Что включает в себя подготовка веб-сервера? |
| Установка и настройка программного обеспечения для обработки запросов |
| Только установка операционной системы |
| Создание физического сервера |
| Печать документации |
| Установка антивируса |

127.

|  |
| --- |
| Какой из следующих факторов влияет на безопасность веб-сервера? |
| Регулярное обновление программного обеспечения |
| Использование старых версий серверного ПО |
| Открытие всех доступных портов |
| Отсутствие брандмауэра |
| Установка графических редакторов |

128.

|  |
| --- |
| Что следует сделать для защиты веб-сервера от атак типа DDoS? |
| Настроить защиту от распределённых атак |
| Установить антивирус на сервер |
| Отключить все порты |
| Перезагрузить сервер |
| Увеличить оперативную память |

129.

|  |
| --- |
| Что такое hardening веб-сервера? |
| Процесс усиления безопасности сервера |
| Процесс настройки веб-сервера для обработки большего количества трафика |
| Установка обновлений |
| Снижение производительности сервера |
| Установка дополнительных приложений |

130.

|  |
| --- |
| Какой метод используется для шифрования данных на веб-сервере? |
| SSL/TLS |
| FTP |
| HTTP |
| DNS |
| SMTP |

131.

|  |
| --- |
| Каким образом можно ограничить доступ к веб-серверу по IP-адресам? |
| Настроив правила фаервола |
| Отключив все порты |
| Установив антивирус |
| Установив прокси-сервер |
| Изменив пароли |

132.

|  |
| --- |
| Какой из следующих инструментов может быть использован для анализа безопасности веб-сервера? |
| Nmap |
| Microsoft Word |
| Photoshop |
| VLC Media Player |
| Notepad |

133.

|  |
| --- |
| Какая задача лежит в основе настройки виртуальных хостов на веб-сервере? |
| Запуск разных сайтов на одном сервере |
| Обработка большого объёма запросов |
| Защита серверных данных |
| Анализ трафика |
| Увеличение скорости сервера |

134.

|  |
| --- |
| Как можно предотвратить уязвимости на веб-сервере, связанные с устаревшими версиями ПО? |
| Регулярное обновление программного обеспечения |
| Удаление всех приложений |
| Отключение порта 80 |
| Использование VPN |
| Установка антивируса |

135.

|  |
| --- |
| Как можно усилить защиту веб-сервера от атак с использованием SQL-инъекций? |
| Применение параметризированных запросов |
| Отключение JavaScript |
| Использование FTP |
| Установка дополнительного ПО |
| Увеличение памяти сервера |

136.

|  |
| --- |
| Какой из следующих методов помогает скрыть версию веб-сервера для повышения безопасности? |
| Отключение отображения информации о сервере в заголовках HTTP |
| Использование нового домена |
| Открытие порта 443 |
| Настройка перенаправлений |
| Установка антивируса |

137.

|  |
| --- |
| Как можно защитить веб-сервер от атак типа brute-force? |
| Ограничить количество попыток входа |
| Использовать стандартные пароли |
| Открыть все порты |
| Отключить антивирус |
| Увеличить скорость сервера |

138.

|  |
| --- |
| Что такое фаервол (firewall) и как он может помочь в защите веб-сервера? |
| Программное или аппаратное средство для фильтрации входящего и исходящего трафика |
| Программа для резервного копирования данных |
| Антивирусная программа |
| Программа для мониторинга производительности |
| Средство для ускорения сервера |

139.

|  |
| --- |
| Какую роль в укреплении веб-сервера играет использование SSL-сертификатов? |
| Обеспечивают безопасное шифрование данных между сервером и клиентом |
| Ускоряют работу сервера |
| Улучшают производительность базы данных |
| Обеспечивают доступ к серверу |
| Увеличивают объём трафика |

140.

|  |
| --- |
| Как можно снизить риски от атак через уязвимости в CMS (например, WordPress)? |
| Регулярно обновлять систему управления контентом и её плагины |
| Отключить систему управления контентом |
| Установить только один плагин |
| Отключить все порты на сервере |
| Увеличить память сервера |

141.

|  |
| --- |
| Что необходимо делать для укрепления безопасности веб-сервера на этапе его настройки? |
| Отключать ненужные службы и порты |
| Настроить только один порт |
| Разрешить доступ всем пользователям |
| Поставить сервер на открытый доступ |
| Установить графический интерфейс |

142.

|  |
| --- |
| Какой из этих методов позволяет улучшить отказоустойчивость веб-сервера? |
| Настройка балансировки нагрузки |
| Установка только одного сервера |
| Отключение брандмауэра |
| Установка только одного веб-приложения |
| Увеличение скорости интернета |

143.

|  |
| --- |
| Какой из следующих инструментов может помочь в мониторинге безопасности веб-сервера? |
| Fail2ban |
| Adobe Acrobat |
| Microsoft Office |
| Google Chrome |
| VLC Media Player |

144.

|  |
| --- |
| Какая из следующих мер помогает защитить сервер от атак через FTP? |
| Использование SFTP вместо FTP |
| Открытие порта 21 |
| Отключение SSL |
| Отключение сервера |
| Установка антивируса |

145.

|  |
| --- |
| Какой метод используется для предотвращения SQL-инъекций в веб-приложениях? |
| Применение параметризированных запросов |
| Использование обычных запросов |
| Отключение кэширования |
| Установка стороннего ПО |
| Увеличение памяти сервера |

146.

|  |
| --- |
| Какой из следующих способов помогает уменьшить вероятность успешной атаки через уязвимости сервера? |
| Регулярное обновление операционной системы и приложений |
| Открытие всех портов |
| Установка старых версий ПО |
| Разрешение всех IP-адресов |
| Отключение фаервола |

147.

|  |
| --- |
| Как можно защитить сервер от атак через HTTP-заголовки? |
| Настройка правильных заголовков безопасности (например, X-Content-Type-Options, X-Frame-Options) |
| Отключение заголовков |
| Открытие всех портов |
| Использование старых версий браузеров |
| Установка антивируса |

148.

|  |
| --- |
| Какой порт используется для защищённого соединения через HTTPS? |
| 443 |
| 21 |
| 80 |
| 8080 |
| 25 |

149.

|  |
| --- |
| Как можно усилить защиту веб-сервера от атак через уязвимости в операционной системе? |
| Регулярно обновлять операционную систему |
| Отключить брандмауэр |
| Установить только один антивирус |
| Открыть все порты |
| Увеличить память сервера |

150.

|  |
| --- |
| Что такое защита от межсайтового скриптинга (XSS) на веб-сервере? |
| Механизм предотвращения внедрения вредоносных скриптов в страницы сайта |
| Механизм защиты от DDoS-атак |
| Механизм защиты от SQL-инъекций |
| Механизм защиты от фишинга |
| Механизм ускорения загрузки страниц |

151.

|  |
| --- |
| Какова основная цель криптографического шифрования? |
| Защита от несанкционированного доступа |
| Сжатие данных |
| Обнаружение случайных ошибок |
| Форматирование информации |
| Ускорение передачи данных |

152.

|  |
| --- |
| Что является основной задачей помехоустойчивого кодирования? |
| Защита информации от случайных помех |
| Сжатие объёма данных |
| Архивирование файлов |
| Создание резервных копий |
| Оптимизация скорости передачи |

153.

|  |
| --- |
| Что представляет собой сжатие (компрессию) информации? |
| Минимизацию объёма передаваемых или хранимых данных |
| Шифрование данных |
| Обнаружение ошибок |
| Разбиение данных на блоки |
| Повышение безопасности данных |

154.

|  |
| --- |
| Какое преобразование информации направлено на защиту от преднамеренного вмешательства? |
| Криптографическое шифрование |
| Помехоустойчивое кодирование |
| Сжатие данных |
| Моделирование данных |
| Визуализация информации |

155.

|  |
| --- |
| Почему в системах связи используется комплексный подход, включающий шифрование, помехоустойчивое кодирование и сжатие? |
| Для защиты информации от как преднамеренных, так и случайных воздействий |
| Для увеличения объёма передаваемых данных |
| Для ускорения работы серверов |
| Для улучшения графики интерфейса |
| Для устранения необходимости резервного копирования |

156.

|  |
| --- |
| Какой общий признак всех трёх видов преобразования информации? |
| Изменение формы представления без изменения смысла |
| Уменьшение объёма исходных данных |
| Изменение смысла передаваемой информации |
| Увеличение сложности обработки |
| Изменение алгоритма передачи |

157.

|  |
| --- |
| Что происходит с информацией при криптографическом шифровании? |
| Защищается от несанкционированного доступа |
| Уменьшается её объём |
| Формируется резервная копия |
| Улучшается качество сигнала |
| Сортируется по приоритетам |

158.

|  |
| --- |
| Какие коды делятся на блоковые и свёрточные? |
| Помехоустойчивые коды |
| Криптографические коды |
| Векторные коды |
| Алфавитные коды |
| Сжатые коды |

159.

|  |
| --- |
| Чем характеризуются блоковые коды? |
| Делением информации на фрагменты фиксированной длины |
| Обработкой данных в виде непрерывного потока |
| Применением динамической длины кодовых слов |
| Использованием методов сжатия |
| Шифрованием каждого символа отдельно |

160.

|  |
| --- |
| Что такое минимальное кодовое расстояние в контексте блоковых кодов? |
| Наименьшее число разрядов, в которых различаются любые два различных кодовых слова |
| Максимальное число ошибок, которое может быть скорректировано |
| Разница между длинами кодовых слов |
| Количество единиц в кодовом слове |
| Разница между исходным и зашифрованным сообщением |

161.

|  |
| --- |
| Как определяется расстояние по Хэммингу между двумя кодовыми словами? |
| Количеством разрядов, в которых они различны |
| Разницей в длине слов |
| Количеством общих символов |
| Разницей в весе кода |
| Порядковым номером различий |

162.

|  |
| --- |
| Какой код позволяет обнаружить ошибку, если контроль проводится по условию четности? |
| Код с контрольной суммой по условию четности |
| Свёрточный код |
| Реляционный код |
| Графический код |
| Алфавитный код |

163.

|  |
| --- |
| В каком случае применение свёрточного кода предпочтительно? |
| При обработке данных как непрерывного потока |
| При разделении информации на фиксированные блоки |
| При архивировании данных |
| При использовании текстовых сообщений |
| При хранении статических файлов |

164.

|  |
| --- |
| Какой метод используется для уменьшения объёма больших информационных массивов перед шифрованием? |
| Сжатие (компрессия) |
| Помехоустойчивое кодирование |
| Разбиение на блоки |
| Перестановка битов |
| Многоуровневое шифрование |

165.

|  |
| --- |
| Какой из методов защиты информации применяется для обнаружения и корректировки ошибок? |
| Помехоустойчивое кодирование |
| Криптографическое шифрование |
| Сжатие данных |
| Архивирование |
| Сегментация данных |

166.

|  |
| --- |
| Почему важно шифровать данные в реальном режиме для мультимедиа-приложений? |
| Для обеспечения незаметной защиты при передаче больших объёмов информации |
| Для уменьшения количества ошибок |
| Для ускорения обработки графики |
| Для повышения качества видео |
| Для обеспечения стабильности соединения |

167.

|  |
| --- |
| Что позволяет использовать методы теории информации в комплексной защите данных? |
| Совместное применение шифрования, помехоустойчивого кодирования и сжатия |
| Применение только одного метода защиты |
| Исключительное использование помехоустойчивого кодирования |
| Использование алгоритмов сортировки данных |
| Применение резервного копирования |

168.

|  |
| --- |
| Какая задача решается с помощью сжатия данных? |
| Минимизация объёма передаваемых или хранимых данных |
| Обнаружение ошибок в передаче |
| Защита от несанкционированного доступа |
| Форматирование файлов |
| Увеличение скорости передачи без защиты |

169.

|  |
| --- |
| Какой из следующих методов не относится к преобразованиям информации, описанным в лекции? |
| Фильтрация шумов |
| Криптографическое шифрование |
| Помехоустойчивое кодирование |
| Сжатие (компрессия) |
| Архивирование |

170.

|  |
| --- |
| Что является ключевым фактором комплексной защиты информации в системах связи? |
| Эффективное использование криптографического шифрования, помехоустойчивого кодирования и сжатия |
| Применение только шифрования |
| Использование исключительно сжатия |
| Применение методов визуализации |
| Использование дополнительных физических средств защиты |

171.

|  |
| --- |
| Что называют «кодированием» в контексте теории информации, согласно лекции? |
| Преобразование информации посредством изменения формы представления |
| Исключительное сжатие данных |
| Процесс резервного копирования |
| Шифрование с использованием биометрических данных |
| Применение методов распознавания образов |

172.

|  |
| --- |
| Какая из функций криптографического шифрования выделяется в лекции? |
| Обеспечение аутентификации и защита от преднамеренных изменений |
| Сжатие данных для экономии места |
| Обнаружение случайных ошибок |
| Разбиение информации на блоки |
| Формирование графического интерфейса |

173.

|  |
| --- |
| Какова роль помехоустойчивого кодирования в современных системах передачи данных? |
| Обнаружение и коррекция ошибок, вызванных случайными помехами |
| Уменьшение объёма передаваемой информации |
| Повышение скорости передачи |
| Улучшение качества видео |
| Создание резервных копий данных |

174.

|  |
| --- |
| В чем заключается преимущество комплексного подхода к защите информации? |
| Он сочетает сильные стороны шифрования, коррекции ошибок и сжатия для надежной защиты |
| Он позволяет использовать только один метод защиты |
| Он полностью исключает вероятность ошибок |
| Он упрощает процесс передачи без использования шифрования |
| Он заменяет необходимость использования алгоритмов шифрования |

175.

|  |
| --- |
| В каких условиях комплексное использование методов шифрования, помехоустойчивого кодирования и сжатия особенно актуально? |
| При передаче больших объёмов данных в высокопроизводительных сетях |
| При передаче небольших текстовых сообщений |
| При использовании исключительно аналоговых систем |
| При работе с низкокачественными аудиозаписями |
| При отсутствии помех в канале связи |

176.

|  |
| --- |
| Что такое электронная цифровая подпись (ЭЦП)? |
| Специальный код для подтверждения подлинности данных |
| Метка времени, присоединённая к документу |
| Шифрование документов с помощью алгоритмов |
| Пароль для доступа к электронным документам |
| Программное обеспечение для создания подписи |

177.

|  |
| --- |
| Какой основной элемент используется для формирования ЭЦП? |
| Закрытый ключ |
| Публичный ключ |
| Пароль |
| Личное удостоверение |
| Программное обеспечение |

178.

|  |
| --- |
| Кто отвечает за выдачу сертификатов для ЭЦП? |
| Удостоверяющий центр |
| Пользователь |
| Платёжная система |
| Программное обеспечение |
| Организация, подписывающая документ |

179.

|  |
| --- |
| Как называется процесс проверки ЭЦП? |
| Верификация |
| Аутентификация |
| Авторизация |
| Шифрование |
| Размещение |

180.

|  |
| --- |
| Что гарантирует использование ЭЦП при подписании документа? |
| Подлинность и целостность документа |
| Доступ к документу только для администратора |
| Шифрование данных для их защиты |
| Возможность редактировать подписанный документ |
| Определение владельца документа |

181.

|  |
| --- |
| Какие алгоритмы чаще всего используются для создания ЭЦП? |
| Алгоритмы асимметричного шифрования |
| Симметричные шифры |
| Хеш-функции |
| Алгоритмы аутентификации |
| Протоколы безопасности |

182.

|  |
| --- |
| Как называется сертификат, подтверждающий подлинность ЭЦП? |
| Электронный сертификат |
| Удостоверяющий ключ |
| Личное удостоверение |
| Ключ безопасности |
| Доверенный сертификат |

183.

|  |
| --- |
| В каком случае ЭЦП считается недействительной? |
| Если сертификат был отозван |
| Когда пароль пользователя сброшен |
| Если документ был изменён после подписания |
| Когда срок действия сертификата истёк |
| Когда документ был подписан другим пользователем |

184.

|  |
| --- |
| Какую информацию можно получить из сертификата ЭЦП? |
| Публичный ключ владельца |
| Личный пароль владельца |
| Секретный ключ владельца |
| Историю всех подписанных документов |
| Все вышеупомянутые данные |

185.

|  |
| --- |
| Что происходит при использовании ЭЦП для подписания документа? |
| Создаётся уникальная метка, привязанная к содержимому |
| Документ шифруется с помощью пароля |
| Все данные документа преобразуются в код |
| Документ становится недоступным для других пользователей |
| Документ автоматически передаётся в удостоверяющий центр |

186.

|  |
| --- |
| Что такое "закрытый ключ" в контексте ЭЦП? |
| Ключ, использующийся для подписания документа |
| Ключ для шифрования данных |
| Пароль для доступа к документу |
| Ключ, используемый для проверки подписей |
| Файл для подтверждения подлинности |

187.

|  |
| --- |
| Какой ключ используется для проверки ЭЦП? |
| Публичный ключ |
| Закрытый ключ |
| Личный ключ |
| Пароль пользователя |
| Сертификат удостоверяющего центра |

188.

|  |
| --- |
| Какие задачи решает ЭЦП? |
| Подтверждение подлинности и целостности документа |
| Защита от вирусов |
| Защита пароля пользователя |
| Регистрация действий пользователя в системе |
| Определение прав доступа |

189.

|  |
| --- |
| В каком случае ЭЦП может быть признана недействительной? |
| Когда срок действия сертификата истёк |
| Когда пользователь сменил пароль |
| Когда пользователь удалил документ |
| Когда система не поддерживает ЭЦП |
| Когда сертификат не был проверен |

190.

|  |
| --- |
| Какой элемент используется для дешифрования ЭЦП? |
| Публичный ключ |
| Приватный ключ |
| Пароль пользователя |
| Сертификат удостоверяющего центра |
| Печать документа |

191.

|  |
| --- |
| В каком документе обычно используется ЭЦП? |
| Электронные контракты и соглашения |
| Бумажные документы |
| Фотографические изображения |
| Письма и письма на бумаге |
| Бухгалтерские документы |

192.

|  |
| --- |
| Как называется процесс создания ЭЦП? |
| Подписание |
| Генерация |
| Аутентификация |
| Криптографирование |
| Заверение |

193.

|  |
| --- |
| Что происходит с документом, если его ЭЦП не совпадает с данным в сертификате? |
| Документ считается поддельным или повреждённым |
| Документ автоматически удаляется |
| Документ будет проверен на вирусы |
| Документ можно отправить повторно |
| Система автоматически исправит ошибку |

194.

|  |
| --- |
| Как часто необходимо обновлять сертификаты ЭЦП? |
| Через определённый срок, обычно 1-3 года |
| Каждый раз при подписании документа |
| Каждую неделю |
| Каждый месяц |
| Это не требуется |

195.

|  |
| --- |
| Какой элемент отвечает за шифрование данных с помощью ЭЦП? |
| Закрытый ключ |
| Публичный ключ |
| Пароль |
| Сертификат |
| Файл данных |

196.

|  |
| --- |
| Что делает удостоверяющий центр с сертификатом ЭЦП? |
| Подписывает и проверяет его подлинность |
| Создаёт уникальный пароль для пользователя |
| Защищает данные пользователя |
| Шифрует данные |
| Уничтожает старые сертификаты |

197.

|  |
| --- |
| Что происходит, если у пользователя украден закрытый ключ ЭЦП? |
| Это может привести к утрате безопасности подписанных документов |
| Документ будет автоматически восстановлен |
| Сертификат будет обновлён |
| Закрытый ключ можно изменить |
| ЭЦП продолжит работать нормально |

198.

|  |
| --- |
| Какую информацию нельзя получить из сертификата ЭЦП? |
| Приватный ключ владельца |
| Публичный ключ владельца |
| Данные удостоверяющего центра |
| Срок действия сертификата |
| Идентификационные данные владельца |

199.

|  |
| --- |
| Какой формат документа не поддерживает ЭЦП? |
| Бумажные документы |
| PDF-документы |
| XML-документы |
| Электронные письма |
| Microsoft Office документы |

200.

|  |
| --- |
| Какое из утверждений о ЭЦП является верным? |
| ЭЦП использует криптографические алгоритмы для подтверждения данных |
| ЭЦП может быть использована для хранения данных |
| ЭЦП не требует использования сертификатов |
| ЭЦП работает только в определённых странах |
| ЭЦП используется только для подписания бумажных документов |

201.

|  |
| --- |
| Что определяют правила безопасности IP? |
| Фильтрацию и шифрование трафика |
| Тип учетной записи |
| Вид интерфейса |
| Частоту обновлений |
| Доступ к BIOS |

202.

|  |
| --- |
| Кто отвечает за безопасность и содержимое сервера? |
| Назначенный администратор |
| Пользователь |
| Группа разработчиков |
| Маркетолог |
| Посетитель сайта |

203.

|  |
| --- |
| Какой метод идентификации используется в Windows 2000? |
| Kerberos |
| Сканирование сетчатки |
| SMS-код |
| USB-ключ |
| Пин-код по телефону |

204.

|  |
| --- |
| Что такое Active Directory? |
| База данных пользователей и ресурсов |
| Менеджер задач |
| Программа архивации |
| Брандмауэр |
| Графический редактор |

205.

|  |
| --- |
| Что происходит при неправильном вводе пароля несколько раз? |
| Учетная запись блокируется |
| Открывается доступ ко всем файлам |
| Удаляется профиль |
| Происходит аварийный выход |
| Меняется IP-адрес |

206.

|  |
| --- |
| Какой параметр запрещает повторное использование пароля? |
| Правила безопасности паролей |
| Список доверия |
| Параметры BIOS |
| Обновления системы |
| Сертификаты безопасности |

207.

|  |
| --- |
| Что входит в понятие «разрешения» в ACL? |
| Доступ к файлам и папкам |
| Смена процессора |
| Удаление ОС |
| Перезапуск BIOS |
| Резервное копирование ОС |

208.

|  |
| --- |
| Какой тип учетной записи обеспечивает вход без пароля? |
| Анонимный пользователь |
| Главный администратор |
| Инсталлятор |
| Служебный пользователь |
| Удалённый пользователь |

209.

|  |
| --- |
| Что такое домен в Windows 2000? |
| Набор ресурсов и пользователей с общей базой |
| Тип жесткого диска |
| Стиль оформления |
| Парольная комбинация |
| Обновление драйвера |

210.

|  |
| --- |
| Кто управляет базой данных пользователей в домене? |
| Контроллер домена |
| Файл hosts |
| DNS-клиент |
| Локальный юзер |
| Программа Word |

211.

|  |
| --- |
| Кто может наследовать права доступа? |
| Группа |
| Лицензия |
| Процессор |
| Драйвер |
| BIOS |

212.

|  |
| --- |
| Что такое ACL? |
| Список контроля доступа |
| Меню загрузки |
| Физическая память |
| Сетевая карта |
| Архив логов |

213.

|  |
| --- |
| Что происходит при добавлении сервера в домен? |
| Учетные записи становятся общими |
| BIOS сбрасывается |
| Лицензия удаляется |
| Очищается диск |
| Меняется тип процессора |

214.

|  |
| --- |
| Что входит в рабочую группу? |
| Пользователи и ресурсы сети |
| Только пользователи |
| Только база данных |
| Только принтеры |
| Только драйверы |

215.

|  |
| --- |
| Что такое наследование прав? |
| Передача доступа от родительских объектов |
| Отключение сетевого адаптера |
| Резервное копирование |
| Сброс BIOS |
| Удаление учетных записей |

216.

|  |
| --- |
| Что управляет пользователями в сети? |
| Active Directory |
| Панель задач |
| Панель управления |
| Командная строка |
| Диспетчер устройств |

217.

|  |
| --- |
| Что делает анонимный вход? |
| Осуществляет доступ без учётных данных |
| Блокирует сеть |
| Очищает систему |
| Стирает диск |
| Обновляет драйвера |

218.

|  |
| --- |
| Что обязательно настраивается отдельно? |
| Безопасность веб-сервера |
| Частота процессора |
| Разрешение экрана |
| Температура системы |
| Стиль оформления |

219.

|  |
| --- |
| Что определяет срок действия билета Kerberos? |
| Правила безопасности учетных записей |
| BIOS |
| Центр обновлений |
| Панель задач |
| Вид сетевого адаптера |

220.

|  |
| --- |
| Что такое права в системе? |
| Возможность выполнять административные действия |
| Установка тем оформления |
| Перезагрузка компьютера |
| Сброс пароля |
| Выход из системы |

221.

|  |
| --- |
| Что определяет политика безопасности групп? |
| Состав и правила групп |
| Количество процессоров |
| Тип жесткого диска |
| Версия антивируса |
| Цвет интерфейса |

222.

|  |
| --- |
| Что включает правило безопасности учетной записи? |
| Блокировку при ошибочном вводе пароля |
| Смена ядра |
| Удаление драйверов |
| Установка BIOS |
| Перезагрузка |

223.

|  |
| --- |
| Что происходит при установке фильтров IP? |
| Ограничивается доступ по IP |
| Удаляются драйвера |
| Перезагружается сеть |
| Меняется язык |
| Стирается кэш |

224.

|  |
| --- |
| Что устанавливает минимальную длину пароля? |
| Политика паролей |
| BIOS |
| Уровень сигнала |
| Периферия |
| Панель задач |

225.

|  |
| --- |
| Какой сервер требует самой высокой безопасности? |
| Веб-сервер |
| Принтер |
| Почтовый клиент |
| Локальный диск |
| Графическая карта |

226.

|  |
| --- |
| Что является основной целью казахстанского законодательства в области защиты персональных данных? |
| Обеспечение защиты прав и свобод гражданина при обработке его персональных данных |
| Увеличение объема собираемых данных |
| Развитие средств электронной коммерции |
| Упрощение передачи данных третьим лицам |
| Снижение уровня информатизации общества |

227.

|  |
| --- |
| Какой закон является основополагающим в области защиты персональных данных в России? |
| Федеральный закон №152 "О персональных данных" |
| Закон "Об информации и информационных технологиях" |
| Закон "О связи" |
| Конституция РФ |
| Закон "О безопасности" |

228.

|  |
| --- |
| Когда вступил в силу Федеральный закон №152 "О персональных данных"? |
| 26 января 2007 года |
| 8 июля 2006 года |
| 13 февраля 2008 года |
| 27 июля 2006 года |
| 1 января 2005 года |

229.

|  |
| --- |
| Что относится к персональным данным по закону? |
| Любая информация, позволяющая идентифицировать физическое лицо |
| Только имя и фамилия человека |
| Только банковские реквизиты |
| Информация о юридических лицах |
| Данные о погодных условиях |

230.

|  |
| --- |
| Кто является оператором персональных данных? |
| Лицо, организующее и осуществляющее обработку персональных данных |
| Только государственные органы |
| Только физические лица |
| Исключительно IT-компании |
| Субъект персональных данных |

231.

|  |
| --- |
| Что включает в себя обработка персональных данных? |
| Сбор, хранение, использование и уничтожение данных |
| Только сбор данных |
| Только передача данных третьим лицам |
| Только обезличивание данных |
| Исключительно автоматизированная обработка |

232.

|  |
| --- |
| Какой орган осуществляет контроль за соблюдением закона "О персональных данных"? |
| Роскомнадзор |
| Министерство обороны |
| Федеральная налоговая служба |
| Генеральная прокуратура |
| МВД России |

233.

|  |
| --- |
| Какие данные относятся к общедоступным персональным данным? |
| Данные, доступ к которым предоставлен с согласия субъекта |
| Данные о состоянии здоровья |
| Информация о политических взглядах |
| Сведения о расовой принадлежности |
| Данные об интимной жизни |

234.

|  |
| --- |
| В каком случае допускается обработка специальных категорий персональных данных? |
| С письменного согласия субъекта данных |
| Без уведомления субъекта |
| Только для коммерческих целей |
| При отсутствии закона о защите данных |
| Только для государственных нужд |

235.

|  |
| --- |
| Что обязан сделать оператор перед началом обработки персональных данных? |
| Уведомить уполномоченный орган о намерении обработки |
| Установить антивирусное ПО |
| Увеличить объём памяти сервера |
| Изменить IP-адрес |
| Создать резервные копии данных |

236.

|  |
| --- |
| Какой срок хранения персональных данных установлен законом? |
| Не дольше, чем необходимо для целей обработки |
| 1 год |
| 5 лет |
| 10 лет |
| Бессрочно |

237.

|  |
| --- |
| Что должен сделать оператор после достижения цели обработки персональных данных? |
| Уничтожить или обезличить данные |
| Передать данные третьим лицам |
| Продолжить их хранение без изменений |
| Опубликовать данные в открытом доступе |
| Передать данные в архив |

238.

|  |
| --- |
| Какие меры обязан принять оператор для защиты персональных данных? |
| Обеспечить безопасность данных от несанкционированного доступа |
| Увеличить скорость обработки данных |
| Установить графический интерфейс |
| Создать копии данных для общего доступа |
| Изменить формат данных |

239.

|  |
| --- |
| Что является нарушением закона о персональных данных? |
| Обработка данных без согласия субъекта |
| Использование антивируса |
| Обновление программного обеспечения |
| Создание резервных копий |
| Установка фаервола |

240.

|  |
| --- |
| Какой принцип лежит в основе обработки персональных данных? |
| Законность и прозрачность обработки |
| Максимальная автоматизация процессов |
| Минимизация затрат на защиту |
| Передача данных без ограничений |
| Упрощение доступа к данным |

241.

|  |
| --- |
| Какие данные относятся к биометрическим персональным данным? |
| Отпечатки пальцев и изображение лица |
| Имя и фамилия |
| Адрес проживания |
| Номер телефона |
| Дата рождения |

242.

|  |
| --- |
| Что должен сделать субъект персональных данных для защиты своих прав? |
| Обратиться к оператору с требованием прекратить обработку |
| Установить антивирус |
| Изменить пароль |
| Увеличить память устройства |
| Обновить ПО |

243.

|  |
| --- |
| Какой документ регулирует трансграничную передачу персональных данных? |
| Закон "О персональных данных" |
| Закон "О связи" |
| Конституция |
| Закон "О рекламе" |
| Закон "О СМИ" |

244.

|  |
| --- |
| Что обязан сделать оператор при утечке персональных данных? |
| Уведомить Роскомнадзор и субъектов данных |
| Удалить все данные |
| Изменить IP-адрес |
| Переустановить сервер |
| Установить новый антивирус |

245.

|  |
| --- |
| Какие данные не относятся к персональным данным? |
| Информация о юридическом лице |
| ФИО сотрудника |
| Номер паспорта |
| Адрес электронной почты |
| Дата рождения |

246.

|  |
| --- |
| Что такое обезличивание персональных данных? |
| Удаление идентифицирующих признаков из данных |
| Шифрование данных |
| Передача данных третьим лицам |
| Создание копий данных |
| Увеличение объёма данных |

247.

|  |
| --- |
| В каком случае субъект может отозвать согласие на обработку данных? |
| В любое время по своему усмотрению |
| Только при смене оператора |
| Только после окончания срока действия договора |
| Только при наличии судебного решения |
| Только после уведомления третьих лиц |

248.

|  |
| --- |
| Какой срок предусмотрен для ответа оператора на запрос субъекта данных? |
| 30 дней |
| 7 дней |
| 60 дней |
| 14 дней |
| 90 дней |

249.

|  |
| --- |
| Что является целью трансграничной передачи персональных данных? |
| Обработка данных в другой стране с соблюдением законодательства |
| Ускорение передачи данных |
| Уменьшение объёма данных |
| Изменение формата данных |
| Создание копий данных |

250.

|  |
| --- |
| Какие данные относятся к специальным категориям персональных данных? |
| Данные о состоянии здоровья |
| Имя и фамилия |
| Номер телефона |
| Адрес проживания |
| Дата рождения |

251.

|  |
| --- |
| Что такое атака "человек посередине" (Man-in-the-Middle)? |
| Перехват данных между двумя сторонами связи |
| Физический доступ к серверу |
| Установка вируса на устройство |
| Перегрузка сервера запросами |
| Взлом пароля пользователя |

252.

|  |
| --- |
| Какой протокол используется для безопасной передачи файлов? |
| SFTP |
| FTP |
| HTTP |
| SMTP |
| ICMP |

253.

|  |
| --- |
| Что такое сертификат SSL? |
| Цифровой документ для обеспечения шифрования соединения |
| Программа для защиты сервера |
| Пароль для доступа к серверу |
| Лог событий безопасности |
| Файл конфигурации сервера |

254.

|  |
| --- |
| Какой метод защиты предотвращает выполнение вредоносного кода в веб-приложениях? |
| Валидация и санитизация входных данных |
| Увеличение скорости сервера |
| Отключение всех портов |
| Установка антивируса |
| Изменение дизайна сайта |

255.

|  |
| --- |
| Что такое хеш-функция в криптографии? |
| Функция, преобразующая данные в строку фиксированной длины |
| Метод шифрования данных |
| Способ сжатия файлов |
| Алгоритм распределения ключей |
| Протокол передачи данных |

256.

|  |
| --- |
| Какой порт используется для SSH-соединений? |
| 22 |
| 80 |
| 443 |
| 25 |
| 21 |

257.

|  |
| --- |
| Что такое брандмауэр (firewall)? |
| Система для фильтрации сетевого трафика |
| Программа для шифрования данных |
| Устройство для резервного копирования |
| Антивирусное ПО |
| Протокол передачи данных |

258.

|  |
| --- |
| Какой тип атаки направлен на подбор пароля? |
| Брутфорс |
| Фишинг |
| SQL-инъекция |
| DDoS |
| Переполнение буфера |

259.

|  |
| --- |
| Что такое симметричное шифрование? |
| Шифрование с использованием одного ключа для шифрования и дешифрования |
| Шифрование с двумя ключами |
| Шифрование без использования ключей |
| Метод сжатия данных |
| Протокол передачи данных |

260.

|  |
| --- |
| Какой стандарт шифрования используется в современных браузерах для HTTPS? |
| TLS |
| SSL |
| FTP |
| HTTP |
| SMTP |

261.

|  |
| --- |
| Что такое уязвимость XSS (межсайтовый скриптинг)? |
| Внедрение вредоносного кода в веб-страницы |
| Перехват данных на сервере |
| Перегрузка сервера запросами |
| Взлом пароля пользователя |
| Установка вируса на сервер |

262.

|  |
| --- |
| Какой метод защиты используется для предотвращения CSRF-атак? |
| Использование токенов аутентификации |
| Отключение cookies |
| Увеличение скорости сервера |
| Установка антивируса |
| Изменение IP-адреса |

263.

|  |
| --- |
| Что такое атака DDoS? |
| Распределённая атака для перегрузки сервера |
| Взлом пароля пользователя |
| Перехват данных в сети |
| Установка вредоносного ПО |
| Физический доступ к серверу |

264.

|  |
| --- |
| Какой алгоритм симметричного шифрования широко используется в современных системах? |
| AES |
| RSA |
| Diffie-Hellman |
| ElGamal |
| MD5 |

265.

|  |
| --- |
| Что такое публичный ключ в асимметричном шифровании? |
| Ключ, доступный всем для шифрования данных |
| Ключ для дешифрования данных |
| Пароль пользователя |
| Секретный код сервера |
| Файл конфигурации |

266.

|  |
| --- |
| Какой метод защиты помогает обнаружить изменения в файлах? |
| Использование хеш-функций |
| Установка антивируса |
| Отключение портов |
| Увеличение памяти сервера |
| Изменение дизайна сайта |

267.

|  |
| --- |
| Что такое атака SQL-инъекция? |
| Внедрение вредоносного SQL-кода в запросы к базе данных |
| Перехват сетевого трафика |
| Перегрузка сервера |
| Взлом пароля |
| Установка вируса |

268.

|  |
| --- |
| Что такое атака типа "переполнение буфера"? |
| Внедрение данных, превышающих выделенную память, для выполнения вредоносного кода |
| Перехват сетевого трафика |
| Перегрузка сервера запросами |
| Взлом пароля пользователя |
| Установка вируса на сервер |

269.

|  |
| --- |
| Какой протокол используется для синхронизации времени в сети? |
| NTP |
| FTP |
| SMTP |
| HTTP |
| ICMP |

270.

|  |
| --- |
| Что такое система обнаружения вторжений (IDS)? |
| Программа для мониторинга и выявления подозрительной активности в сети |
| Антивирусное ПО |
| Протокол шифрования |
| Устройство для резервного копирования |
| Файл конфигурации сервера |

271.

|  |
| --- |
| Какой метод защиты предотвращает утечку данных через USB-устройства? |
| Ограничение доступа к USB-портам |
| Установка антивируса |
| Отключение всех портов |
| Увеличение скорости сервера |
| Изменение IP-адреса |

272.

|  |
| --- |
| Что такое алгоритм MD5? |
| Хеш-функция для создания цифрового отпечатка данных |
| Метод шифрования с открытым ключом |
| Протокол передачи файлов |
| Алгоритм сжатия данных |
| Система аутентификации |

273.

|  |
| --- |
| Какой порт используется для отправки электронной почты через SMTP? |
| 25 |
| 80 |
| 443 |
| 22 |
| 21 |

274.

|  |
| --- |
| Что такое двухфакторная аутентификация (2FA)? |
| Метод входа, требующий двух разных способов подтверждения личности |
| Шифрование данных двумя ключами |
| Использование двух паролей |
| Установка двух антивирусов |
| Двойное сжатие данных |

275.

|  |
| --- |
| Какой тип атаки использует поддельные точки доступа Wi-Fi? |
| Атака "злой двойник" (Evil Twin) |
| Фишинг |
| SQL-инъекция |
| DDoS |
| Брутфорс |

276.

|  |
| --- |
| Что такое токен безопасности? |
| Устройство или код для подтверждения личности пользователя |
| Программа для шифрования данных |
| Файл конфигурации сервера |
| Протокол передачи данных |
| Антивирусное ПО |

277.

|  |
| --- |
| Какой метод защиты предотвращает выполнение скриптов на стороне клиента? |
| Установка заголовка Content-Security-Policy |
| Отключение всех портов |
| Увеличение памяти сервера |
| Установка антивируса |
| Изменение дизайна сайта |

278.

|  |
| --- |
| Что такое атака "кэш-отравление" (Cache Poisoning)? |
| Подмена данных в кэше для перенаправления пользователей |
| Перегрузка сервера запросами |
| Взлом пароля пользователя |
| Установка вируса на сервер |
| Перехват сетевого трафика |

279.

|  |
| --- |
| Какой алгоритм используется для цифровой подписи в России? |
| ГОСТ Р 34.10-2012 |
| RSA |
| AES |
| MD5 |
| SHA-1 |

280.

|  |
| --- |
| Что такое система предотвращения вторжений (IPS)? |
| Система для обнаружения и блокировки атак в реальном времени |
| Программа для шифрования данных |
| Устройство для резервного копирования |
| Протокол передачи файлов |
| Антивирусное ПО |

281.

|  |
| --- |
| Какой метод защиты предотвращает утечку данных через DNS? |
| Использование DNSSEC |
| Отключение всех портов |
| Установка антивируса |
| Увеличение скорости сервера |
| Изменение IP-адреса |

282.

|  |
| --- |
| Что такое атака "сессионный перехват" (Session Hijacking)? |
| Захват сессии пользователя для получения доступа к его данным |
| Перегрузка сервера запросами |
| Взлом пароля пользователя |
| Установка вируса на сервер |
| Перехват электронной почты |

283.

|  |
| --- |
| Какой порт используется для IMAP-протокола? |
| 143 |
| 25 |
| 80 |
| 443 |
| 21 |

284.

|  |
| --- |
| Что такое асимметричное шифрование? |
| Шифрование с использованием пары ключей: публичного и приватного |
| Шифрование с одним ключом |
| Метод сжатия данных |
| Протокол передачи данных |
| Система аутентификации |

285.

|  |
| --- |
| Какой метод защиты предотвращает подделку запросов между сайтами (CSRF)? |
| Использование уникальных токенов для каждого запроса |
| Установка антивируса |
| Отключение cookies |
| Увеличение памяти сервера |
| Изменение IP-адреса |

286.

|  |
| --- |
| Что такое атака "фарминг" (Pharming)? |
| Перенаправление пользователей на поддельные сайты через изменение DNS |
| Перегрузка сервера запросами |
| Взлом пароля пользователя |
| Установка вируса на сервер |
| Перехват сетевого трафика |

287.

|  |
| --- |
| Какой протокол используется для безопасного удалённого доступа к терминалу? |
| SSH |
| FTP |
| HTTP |
| SMTP |
| ICMP |

288.

|  |
| --- |
| Что такое ротация ключей в криптографии? |
| Периодическая замена ключей для повышения безопасности |
| Увеличение длины ключа |
| Сжатие данных перед шифрованием |
| Передача ключей третьим лицам |
| Удаление старых ключей без замены |

289.

|  |
| --- |
| Какой метод защиты помогает избежать утечки данных через электронную почту? |
| Шифрование сообщений с помощью PGP |
| Отключение почтового сервера |
| Установка антивируса |
| Увеличение скорости сервера |
| Изменение IP-адреса |

290.

|  |
| --- |
| Что такое атака "Rainbow Table"? |
| Использование предвычисленных таблиц для взлома хешей паролей |
| Перегрузка сервера запросами |
| Перехват сетевого трафика |
| Установка вируса на сервер |
| Взлом базы данных |

291.

|  |
| --- |
| Какой порт используется для POP3-протокола? |
| 110 |
| 25 |
| 143 |
| 80 |
| 443 |

292.

|  |
| --- |
| Что такое "соль" (salt) в криптографии? |
| Случайные данные, добавляемые к паролю перед хешированием |
| Метод шифрования данных |
| Протокол передачи файлов |
| Устройство для генерации ключей |
| Программа для сжатия данных |

293.

|  |
| --- |
| Какой метод защиты предотвращает повторное использование украденных паролей? |
| Использование одноразовых паролей (OTP) |
| Установка антивируса |
| Отключение всех портов |
| Увеличение памяти сервера |
| Изменение IP-адреса |

294.

|  |
| --- |
| Что такое атака "DNS-спуфинг"? |
| Подмена DNS-ответов для перенаправления пользователей |
| Перегрузка сервера запросами |
| Взлом пароля пользователя |
| Установка вируса на сервер |
| Перехват электронной почты |

295.

|  |
| --- |
| Какой алгоритм используется для хеширования паролей в современных системах? |
| SHA-256 |
| RSA |
| AES |
| Diffie-Hellman |
| MD5 |

296.

|  |
| --- |
| Что такое атака "Pass-the-Hash"? |
| Использование украденного хеша пароля для аутентификации |
| Перегрузка сервера запросами |
| Перехват сетевого трафика |
| Установка вируса на сервер |
| Взлом базы данных |

297.

|  |
| --- |
| Какой метод защиты предотвращает утечку данных через HTTPS? |
| Использование HSTS (HTTP Strict Transport Security) |
| Отключение всех портов |
| Установка антивируса |
| Увеличение скорости сервера |
| Изменение IP-адреса |

298.

|  |
| --- |
| Что такое атака "Clickjacking"? |
| Обманное нажатие пользователем на скрытые элементы интерфейса |
| Перегрузка сервера запросами |
| Взлом пароля пользователя |
| Установка вируса на сервер |
| Перехват сетевого трафика |

299.

|  |
| --- |
| Какой протокол используется для управления сетевыми устройствами? |
| SNMP |
| FTP |
| HTTP |
| SMTP |
| ICMP |

300.

|  |
| --- |
| Что такое атака "Zero-Day"? |
| Использование уязвимости, о которой разработчик ещё не знает |
| Перегрузка сервера запросами |
| Взлом пароля пользователя |
| Установка вируса на сервер |
| Перехват сетевого трафика |