Муниципальный этап
Всероссийской олимпиады школьников по технологии
2024-2025 уч. год

Профиль «Информационная безопасность»
10-11 классы

Задание 1 (5 баллов) Как называется процесс использования мер безопасности для обеспечения конфиденциальности, целостности и доступности данных?

_____

Задание 2. (5 баллов) Вставьте пропущенный термин в следующем утверждении:

Вследствие того, что в информационной системе произошла подмена сведений, идентифицирующих пользователей, существует вероятность несанкционированного распространения _____ данных.

Задание 3. (2 балла) Цифровые водяные знаки используются с целью...:

А) Определить, кто создал цифровые произведения.
Б) Следить, чтобы данные с измерительных устройств не потерялись.
В) Не допустить подделку документов и ценных бумаг.
Г) Хранить информацию в секрете.

_____

Задание 4. (2 балла) Алгоритмы асимметричного шифрования обеспечивают пользователям ряд преимуществ.

А) Не нужно передавать секретные ключи.
Б) Нельзя получить ключ, анализируя шифртексты.
В) Не нужно хранить ключи в секрете.
Г) Обеспечивается абсолютная секретность сообщений.

_____

Задание 5. (3 баллов). Сколько слов содержит тайное послание, если обнаруженный текст записки представлен в таком виде?

8	10	1	20	5	2	14	12	19	17	7	21	27	6	18	22	26	3	11	9	16	13	25	4	24	15	23
в	**н**	**с**	**р**	**и**	**к**	**о**	**е**	**п**	**о**	**о**	**о**	**о**	**р**	**в**	**в**	**н**	**а**	**и**	**а**	**т**	**п**	**е**	**н**	**д**	**р**	**е**

_____

Задание 6. (7 баллов). Сотруднику банка Антону поступил звонок с незнакомого номера. Звонивший представился сотрудником полиции из районного отделения по адресу проживания Антона и сообщил о том, что телефонный звонок записывается. По предложению звонившего Антон сверил названную информацию с данными об уполномоченном участковом сотруднике полиции на сайте мфд.рф. Названные фамилия, имя и отчество, а также номер телефона совпадали с указанными неофициальном портале. «Вчера Вы совершали оплату покупки в продуктовом магазине», – сообщил звонивший. Это было правдой. «При этом Вы вводили PIN-код на терминале». Это также было верно. «Похоже, кто-то подсмотрел Ваш номер карты и PIN-код, потому что сегодня было зафиксировано несколько покупок через интернет-магазин с Вашей карты, а также было зафиксировано несколько попыток оплаты покупки с зарубежных интернет-магазинов. Для расследования этих действий и возврата Вам денежных средствам необходим номер карты (чтобы убедиться, что она всё-таки принадлежит Вам), а также PIN-код и код безопасности с обратной стороны карты».

(2) Поняв, что его обманывают, Антон повесил трубку и открыл электронный почтовый ящик. Там обнаружилось письмо от магазина, в котором у Антона была скидочная карта. Магазин предлагал принять участие в акции, для чего требовалось зайти на сайт этого мероприятия, имевшего очень непростое название. Имя сайта было представлено в письме в виде картинки, поэтому его требовалось ввести вручную. На открывшемся сайте предлагалось ввести данные держателя скидочной карты, её номер и номер телефона, с которым связана карта. После этого потребовалось ввести код подтверждения, который должен был прийти на введённый номер телефона. Заметив, что ввёл в адресе пару букв неверно (поменяв местами), Антон исправил ошибку. На новой странице открылся сайт акции, проводимой указанным магазином, но вместо просьбы ввести сведения указывались лишь сроки и условия проведения. Поняв, что чуть не стал жертвой мошенников, Антон закрыл браузер.

(3) Открыв приложение социальной сети, он заметил сообщение от близкого друга. «Ну как вчера погулял? Днём хорошо провели время, да? (Антон в самом деле ходил с другом на спортивное мероприятие.) Впрочем, похоже, у тебя такое не редкость!»

К письму были приложены несколько фото самого Антона в автосалоне, ювелирном магазине и дорогом ресторане. Задав пару вопросов, Антон понял, что имеет дело не со своим другом, а с кем-то, представляющимся им, и подал жалобу модератору.

Соотнесите злоумышленников (звонивший по телефону — 1, приславший письмо — 2 и автор сообщения в социальной сети — 3), пытавшихся реализовать угрозы информационной безопасности в отношении Антона, с использованными ими техниками. Каждый из них мог использовать более одной техники, причём одной техникой могли воспользоваться несколько злоумышленников. В ответ выпишите цифры по порядку

Кража личности	
Сниффинг	1
Претекстинг	
Луркинг	
Кибersталкинг	2

Фишинг
Крэкинг
Кибербуллинг 3
Тайпсквоттинг
Спуфинг

Задание 7. (5 баллов) Антон решил сделать свою программу по криптографии. Он хотел, чтобы она преобразовывала любые данные — файлы или текст — в строку из 1024 символов. Антон показал программу однокласснице. Она попросила время, чтобы её проверить. После проверки она сказала, что его функция не годится для криптографии.

Может быть, она сказала так, потому что...

А) Программа тормозит.

Б) Алгоритм преобразования входных данных в строку не содержит секретных параметров.

В) Раундов обработки данных слишком мало.

Г) По выходному значению можно понять, что на вход был подан текст или файл.

Задание 8. (5 баллов) Сотрудник организации заметил, что его рабочий ноутбук, похоже, заражён вредоносным ПО. Он рассказал об этом администратору безопасности. Администратор попросил сотрудника вспомнить, что он делал на работе в тот день. Сотрудник сказал, что утром он открыл браузер и зашёл на сайт организации. Потом он загрузил письма через почтовый клиент. Письма не содержали вложенных файлов. В одном из писем было написано, что по указанию руководства на переносные устройства нужно установить программу, которая позволяет пользователям постоянно быть подключёнными к беспроводной сети организации без повторной авторизации. Сотрудник ввёл адрес в адресной строке и попал в служебную область сайта организации. Он решил загрузить файл, но заметил, что адрес отличается от адреса сайта одной буквой. Сотрудник сразу же покинул сайт. Он спросил у коллеги, есть ли у них такая программа. Коллега подтвердил, что есть, и предложил скачать её на внешний носитель. Сотрудник подключил устройство коллеги, скачал программу, но не стал её запускать. Он решил пойти на обед. Вернувшись, он проверил почту и заподозрил, что устройство заражено. Администратор безопасности пришёл к выводу, что устройство, скорее всего, было заражено в описанных событиях.

А) вирусом

Б) троянской программой

В) руткитом

Г) бэкдором

Задание 9. (5 баллов) Этот сотрудник, вспоминая детали дня, рассказал администратору безопасности, что во время обеда он пошёл в ближайшее кафе. Там ему позвонил коллега и попросил срочно ответить на письмо по электронной почте. Чтобы проверить почту, сотрудник подключил свой рабочий ноутбук к беспроводной сети кафе. Всё получилось. Он посмотрел почту, ответил на письмо и вернулся в офис. Администратор безопасности учёл новые детали и добавил к списку возможных угроз программу, которой сотрудник мог заразиться. Какая программа была добавлена?

А) руткит

Б) троянскую программу

В) сетевого червя

Г) спуфер

Задание 10. (8 баллов) В процессе расследования киберпреступления сотрудники правоохранительных органов обнаружили на устройстве подозреваемого файл, содержащий зашифрованную информацию. После анализа других файлов на устройстве было установлено, что для шифрования использовался шифр Цезаря. Этот шифр основан на замене каждой буквы алфавита на другую букву того же алфавита, которая находится на определённом расстоянии от исходной. Например, при сдвиге на три позиции буква «А» заменяется на «Г», «Б» — на «Д» и так далее.

Зашифрованный текст выглядит следующим образом:

Цчйзетузхещнд н пхнфчузхещнд – учрньтай цфуцуёа цуъхетнчб фехурб ж цйпхйчй. Ирд ёема иеттаъ д фхнсйтдг ж пеьйцчжй фехурд цружу зехетчнд, меэнщхужеттуй цу цижнзус ж уинттеиыечб цнсжуруж. Чеп ут тй ъхетнчцд те пусфбгчйхй ж учпхачус жний, е фхн тйуёъуинсуцчн д жцйзие сузш фуршьнчб йзу цтуже

Определите ключ (величину сдвига), применённый для зашифрования данного текста.

Задание 11. (10 баллов) Правоохранительные органы столкнулись с новой группой хакеров, которые совершают атаки на правительственные веб-сайты. Для того чтобы выявить их, необходимо решить техническую задачу. Есть сведения о численности группы и навыках каждого её участника.

При поиске в базе данных для обозначения логической операции «И» используется символ «&», а для операции «ИЛИ» — символ «|». В таблице представлены запросы и количество найденных по ним записей.

Запрос	Найдено
Социальная инженерия	715
Социальная инженерия | технические навыки	934
Технические навыки	492

Задание 12. (5 баллов) Компания N придумала крутые беспилотные тачки. Чтобы они могли ездить по обычным дорогам, они будут получать информацию с камер и датчиков. Потом эта информация будет сравниваться с картами в памяти компьютера и правилами дорожного движения, которые в него загружены. Скажите, какие из этих утверждений правильные, а какие — нет? (верный ответ выделить)

Для верного принятия решений системой управления требуется обеспечить доступность информации о правилах дорожного движения в памяти системы.	неверно	верно
Поскольку передаваемая и хранимая информация общеизвестна, для неё не требуется обеспечивать конфиденциальность.	неверно	верно
Находящиеся на улице пешеходы могут нарушать доступность информации от камер.	неверно	верно
Среди возможных нарушителей информационной безопасности описанной системы следует рассматривать её разработчиков.	неверно	верно
Целостность информации в системе не может быть нарушена, поскольку в системе отсутствует пользователь.	неверно	верно

Задание 13. (8 баллов) Сколько различных паролей длиной семь символов можно создать, используя алфавит «1bP»? В бланк ответов внесите число.

_____

Задание 14. (1 балл) Василий обратил внимание на то, что в его учётную запись в социальной сети был произведён вход с неизвестного устройства. Проведя анализ своих действий за день, он пришёл к выводу, что причиной утечки пароля могло стать следующее:

А) Установка проектора в образовательном учреждении для проведения презентации.

Б) Отправка электронного сообщения через почтовый клиент.

В) Авторизация в социальной сети при подключении к Wi-Fi в кафе.

Г) Подключение беспроводной мыши в кабинете информатики.

_____

Задание 15. (4 балла) Для доступа в рабочие помещения требуется задействовать специализированную систему защиты. Каждому сотруднику надлежит произнести определённое слово, которое будет идентифицировано системой. Система проверит, соответствует ли голос сотрудника установленным критериям. Какой тип аутентификации используется?

_____

Кейс (25 баллов)

На вокзале города N установлены терминалы самообслуживания. Пассажир для приобретения билета самостоятельно вводит дату и номер поезда, паспортные данные, выбирает место, сканирует документы на льготу и оплачивает банковской картой, вводя PIN-код. Со временем были обнаружены утечки персональных данных и сведений банковских карт пассажиров.

1. Оцените физические каналы утечки информации: оптический, акустический, радиоэлектронный.
2. Оцените, при каких действиях пассажира может произойти перехват информации: паспортные данные, данные на льготные билеты, открытая информация о карте, CVV-код, PIN-код.
3. Приведите пример возможного способа перехвата информации и подтвердите свои оценки аргументами.

Ответ должен содержать ответы на пункты 1–3 в сочетании «информация – канал утечки – момент времени (действия пассажира) – способ реализации угрозы (средство)», например: «Паспортные данные могут быть похищены по оптическому каналу в момент предъявления паспорта охране при помощи скрытой камеры; телефонный номер – по акустическому каналу в момент сообщения оператору при помощи подслушивающего устройства». Рассмотрите все возможные сочетания похищаемой информации и каналов утечки.