ЗОЛОТОЕ СЕЧЕНИЕ
ФОНД ПОДДЕРЖКИ ТАЛАНТЛИВЫХ ДЕТЕЙ И МОЛОДЕЖИ

ВСОШ

Разбор заданий школьного этапа всероссийской олимпиады школьников по технологии (информационная безопасность) 5-6 класс (2 вариант)

2024/2025 учебного года в Свердловской области

Разработчик –
Витюнин Максим Александрович,
доцент кафедры ИИТиМОИ УрГПУ, к.хим.н.

Виды заданий

Задание 6 (2 балла). Назовите наибольшую угрозу, которая способна нанести ущерб информационной безопасности?

Правильный ответ «В» т.к. только человеком может быть принято ошибочное решение в конкретной ситуации.

Любому человеку свойственны ограничения возможностей или ошибки. Не всегда психологические и психофизиологические характеристики человека соответствуют уровню сложности решаемых задач или проблем. Характеристики, возникающие при взаимодействии человека и технических систем, часто называют «человеческий фактор». Ошибки, называемые проявлением человеческого фактора, как правило, непреднамеренны: человек выполняет ошибочные действия, расценивая их как верные или наиболее подходящие.

Классификация вредоносного ПО

Задание 7 (2 балла). Устройство персонального компьютера или ноутбука, на котором долговременно хранятся данные, созданные пользователем?

GPU – видеокарта.

CPU – процессор.

RAM – энергозависимое запоминающее устройство.

PCI – шина ввода-вывода для подключения периферийных устройств к материнской плате компьютера.

SSD - компьютерное энергонезависимое немеханическое запоминающее устройство на основе микросхем памяти, альтернатива жёстким дискам (HDD).

Правильный ответ «А»

Основные компоненты информационной безопасности

Задание 8 (2 балла). Что из перечисленного относится к общим персональным данным?

Всё перечисленное относится к персональным данным.

Согласно федеральному закону от 27 июля 2006 года 152-ФЗ «О персональных данных», это любая информация, относящаяся к определенному или определяемому на основе такой информации физическому лицу (субъекту персональных данных). Конкретного перечня данных в законе нет, что оставляет некоторый простор для толкования. Персональные данные включают такую информацию, как **ФИО, пол, дата и место рождения, место жительства, образование, семейное положение, занимаемая должность.**

В федеральном законе №152 обозначены виды персональных данных:
— **Общие.** К ним законодательство относит базовые личные данные: ФИО, место регистрации, информация об образовании, о месте работы, **номер телефона**, e-mail;
— **Специальные.** Информация о личности человека: расовая и национальная принадлежность, политические, религиозные и философские взгляды, состояние здоровья, подробности интимной жизни, информация о судимостях;
— **Биометрические.** Физиологические или биологические особенности человека, которые используют для установления его личности: фотографии, отпечатки пальцев, анализ ДНК, группа крови, рост, цвет глаз, вес и другие;
— **Иные.** К ним относят все данные, которые нельзя отнести к другим видам: принадлежность к определенной социальной группе, корпоративные данные и так далее.

Правильный ответ «Д»

Правовые основы информационной безопасности

Задание 9 (2 балла). Как называется компания, которая предоставляет интернет-услуги другим компаниям и физическим лицам.

Интернет-провайдер (иногда просто **провайдер**; от англ. *Internet service provider*, сокр. *ISP* — поставщик интернет-услуг) — телекоммуникационная компания, предоставляющая услуги доступа к сети Интернет и иные связанные с Интернетом услуги.

Правильный ответ «В»

Правовые основы информационной безопасности

Задание 10 (8 баллов, *за каждый правильный вопрос* 2 балла). Сопоставьте определения.

1. Информационная безопасность **– это** безопасность любой информации, включая бумажные документы, голосовую информацию, информацию в головах людей.

2. Безопасность информационных технологий **-** обеспечение целостности, доступности, конфиденциальности и др. требований безопасности, предъявляемых к вычислительной и коммуникационной технике и информации, которую она хранит, обрабатывает и пересылает.

3. Кибербезопасность **-** безопасность информации в сложных управляющих системах.

4. Кибернетическая безопасность **–** нет такого определения.

Правильный ответ «1-Г, 2-А, 3-Б, 4-В»

Правовые основы информационной безопасности

Задание 11 (1 балл). Назовите самые распространенные вредоносные программы, которые несут угрозу информационной безопасности?

Троянские программы - проникают в компьютер под видом легитимного программного обеспечения, в отличие от вирусов и червей, которые распространяются самопроизвольно. В данную категорию входят программы, осуществляющие различные неподтверждённые пользователем действия: сбор информации о банковских картах, передача этой информации злоумышленнику, а также использование, удаление или злонамеренное изменение, нарушение работоспособности компьютера, использование ресурсов компьютера в целях майнинга, использование IP для нелегальной торговли. Также троянские программы могут всецело оставаться на компьютере, даже после полной переустановки Windows.

Правильный ответ «А»

Правовые основы информационной безопасности

Задание 12 (2 балла). Как называется мошенничество, при котором злоумышленники выманивают у пользователей сети личную информацию:

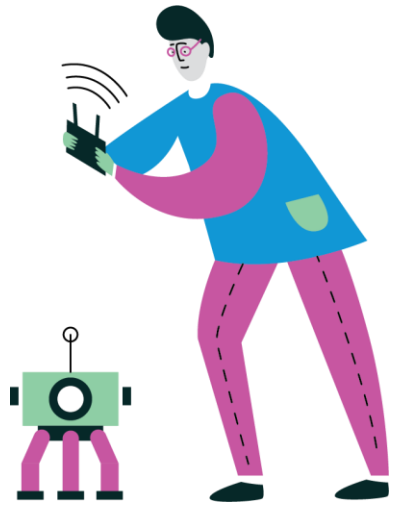
Фишинг (англ. *phishing* от *fishing* «рыбная ловля, выуживание») — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом.

Правильный ответ «Б»

Технические средства обеспечения информационной безопасности

Задание 13 (8 баллов, *за каждый правильный вопрос* 2 балла). Сопоставьте виды мошенничества в сети с их определениями.

1. **Кликбейт** - уничижительный термин, описывающий веб-контент, целью которого является получение дохода от онлайн-рекламы, особенно в ущерб качеству или точности информации. Используются тизеры — сенсационные заголовки или привлекательные картинки для увеличения числа кликов и поощрения распространения материала через Интернет, в частности, социальные сети.
2. **Вишинг** - один из методов мошенничества с использованием социальной инженерии, который заключается в том, что злоумышленники, используя телефонную коммуникацию и играя определённую роль (сотрудника банка или правоохранительных органов, покупателя и т.д.), под разными предлогами выманивают у держателя платёжной карты конфиденциальную информацию или стимулируют к совершению определённых действий со своим банковским счётом или платёжной картой.
3. **Брашинг** - вид мошенничества в электронной коммерции, который используется для повышения рейтинга продавца путём отправки поддельных заказов.
4. **Кардинг** - вид мошенничества, при котором производится операция с использованием платежной карты или её реквизитов, не инициированная или не подтверждённая её держателем. Реквизиты платежных карт, как правило, берут со взломанных серверов интернет-магазинов, платежных и расчётных систем, а также с персональных компьютеров.

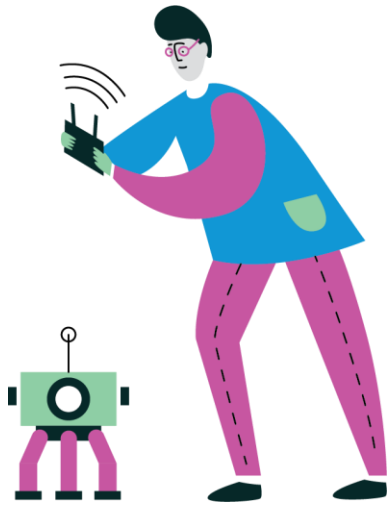


Правильный ответ «1-В, 2-Г, 3-А, 4-Б»

Технические средства обеспечения информационной безопасности

Задание 14 (2 балла). Назовите вероятные признаки, по которым можно определить о заражении компьютера вирусным ПО:

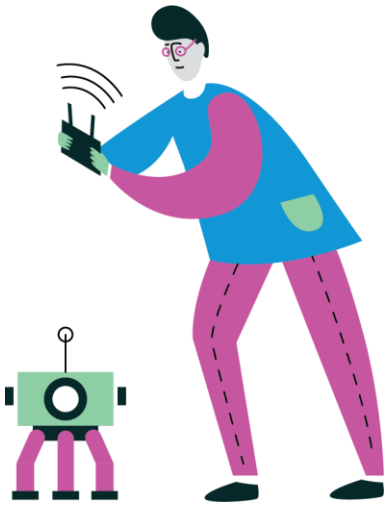
Правильный ответ «В» т.к. оставшиеся варианты ответов являются аппаратной неисправностью.



Технические средства обеспечения информационной безопасности

Задание 15 (1 балл). Какие персональные данные человека являются биометрическими?

Правильный ответ «В»

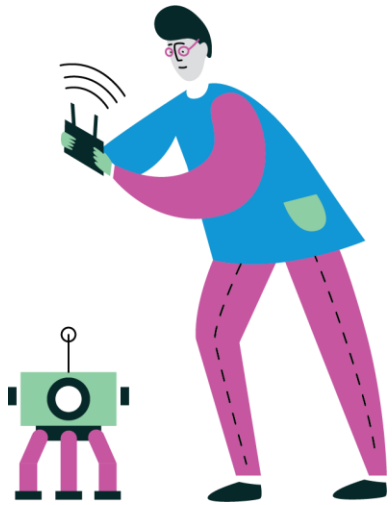


Технические средства обеспечения информационной безопасности

Задание 16 (2 балла). Как называется процесс размещения на виртуальных коммуникативных ресурсах провокационных сообщений с целью создания конфликтных ситуаций, в которых нарушаются этические нормы поведения?

Троллинг - форма социальной провокации или издевательства в сетевом общении, использующаяся как персонифицированными участниками, заинтересованными в большей узнаваемости, публичности, эпатаже, так и анонимными пользователями без возможности их идентификации.

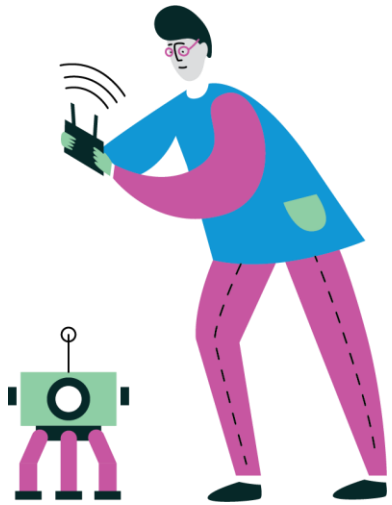
Правильный ответ «Б»



Технические средства обеспечения информационной безопасности

Задание 17 (2 балла). Вам на электронную почту пришло письмо, содержащее поздравление в выигрыше денежного приза и ссылку на страницу в интернете. Как вы поступите?

Правильный ответ «Б» т.к. в присланном письме может быть сетевой червь.

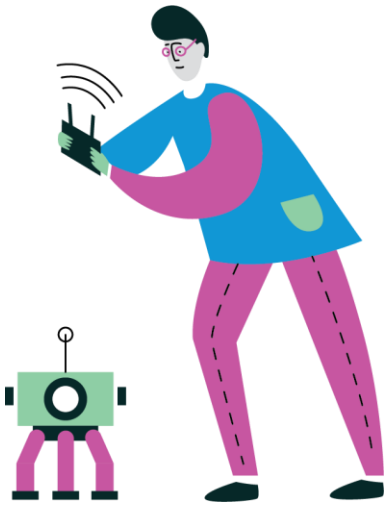


Технические средства обеспечения информационной безопасности

Задание 18 (2 балла). Из перечисленных устройств и программного обеспечения выберите то, без которого в вашей квартире не будет доступа к интернету ни с одного мобильного и стационарного устройства.

Роутер (от англ. *router*) — специализированное устройство, которое пересылает пакеты между различными сегментами сети на основе правил и таблиц маршрутизации. Маршрутизатор может связывать разнородные сети различных архитектур. Для принятия решений о пересылке пакетов используется информация о топологии сети и определённые правила, заданные администратором.

Как правило роутеры имеют несколько портов RJ-45 для подключения нескольких компьютерных устройств для установления связи между ними, для подключения к сети мобильные устройства используется Wi-Fi соединение, которое так же может быть предусмотрено в роутере.



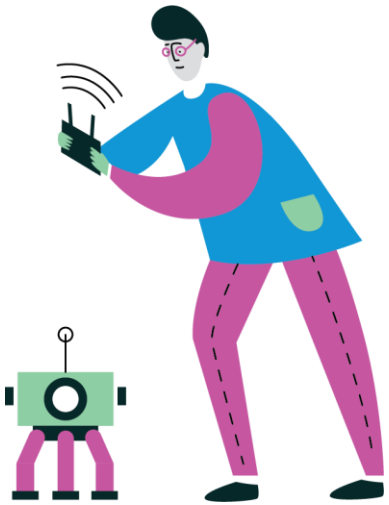
Правильный ответ «В»

Технические средства обеспечения информационной безопасности

Задание 19 (2 балла). Как называется специализированное устройство, которое пересылает пакеты между различными сегментами сети на основе правил и таблиц маршрутизации?

Роутер (от англ. *router*) — специализированное устройство, которое пересылает пакеты между различными сегментами сети на основе правил и таблиц маршрутизации. Маршрутизатор может связывать разнородные сети различных архитектур. Для принятия решений о пересылке пакетов используется информация о топологии сети и определённые правила, заданные администратором.

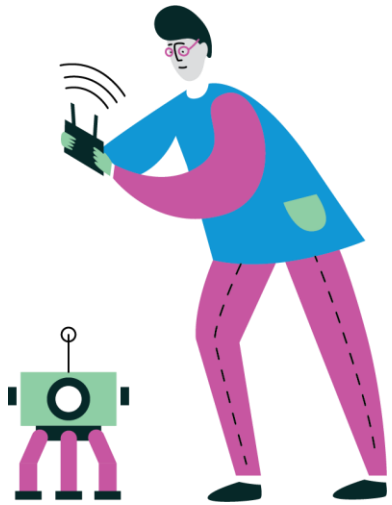
Правильный ответ «Б»



Технические средства обеспечения информационной безопасности

Задание 20 (2 балла). Какие данные можно передавать по электронной почте?

Правильный ответ «Б» т.к. остальные варианты являются исчерпывающими для доступа к аккаунтам пользователя.



ЗОЛОТОЕ СЕЧЕНИЕ
ФОНД ПОДДЕРЖКИ ТАЛАНТЛИВЫХ ДЕТЕЙ И МОЛОДЕЖИ



Благодарю за внимание!