Путь к кибербезопасности

Образовательная игра-квиз для учащихся школ и колледжей

РАУНД №1

СТАРТ →

РАУНД №1 «Основы кибербезопасности»

Задание 1 — Что такое вирус?

А) программа, шифрующая данные для выкупа;

Б) программа, копирующая себя и распространяющаяся между компьютерами;

В) сообщение с мошенническим предложением.

РАУНД №1 «Основы кибербезопасности»

Задание 2 — Как называется вредоносное ПО, предназначенное для скрытого контроля над устройством пользователя?

А) троян;

Б) adware;

В) спам.

РАУНД №1 «Основы кибербезопасности»

Задание 3 — Что такое фишинг?

А) тип вируса, блокирующего доступ к файлам;

Б) процесс нелегального получения чужой личной информации путём обмана;

В) защитная программа от вирусов.

РАУНД №1 «Основы кибербезопасности»

Задание 4 — Чем отличается «шпионское ПО» от «рекламного ПО»?

А) шпионское ПО собирает информацию о пользователе без его согласия;

Б) рекламное ПО не несёт вреда;

В) оба ответа верны.

РАУНД №1 «Основы кибербезопасности»

Задание 5 — Какой метод кибератаки включает в себя отправку большого количества запросов к серверу, чтобы сделать его недоступным для пользователей?

А) фишинг;

Б) DDoS-атака;

В) социальная инженерия.

РАУНД №1 «Основы кибербезопасности»

Задание 6 — Что такое криптовымогатель?

А) вирус, зашифровывающий файлы и требующий выкуп за восстановление доступа;

Б) безопасное хранилище для криптовалют;

В) метод защиты данных с использованием криптографии.

РАУНД №1 «Основы кибербезопасности»

Задание 7 — Как называется метод защиты, при котором используются два разных типа подтверждения личности для доступа к ресурсу?

А) биометрическая идентификация;

Б) двухфакторная аутентификация;

В) шифрование данных.

РАУНД №1 «Основы кибербезопасности»

Задание 8 — Что обозначает термин «Zero day уязвимость»?

А) уязвимость, для которой ещё не существует патча или обновления;

Б) уязвимость, обнаруженная в первый день запуска программы;

В) программа для защиты от уязвимостей.

РАУНД №1 «Основы кибербезопасности»

Задание 9 — Какие действия следует предпринять после обнаружения вредоносного ПО на компьютере?

А) отключить устройство от интернета и запустить антивирусное сканирование;

Б) продолжать использовать компьютер, надеясь, что ПО само исчезнет;

В) отправить сообщение злоумышленнику с просьбой удалить ПО.

РАУНД №1 «Основы кибербезопасности»

Задание 10 — Что лучше всего описывает «Сетевой фаервол»?

А) устройство для ускорения интернет соединения;

Б) программа для создания вирусов;

В) система безопасности, предотвращающая несанкционированный доступ.

РАУНД №1 «Основы кибербезопасности»

Задание 11 — Какой из перечисленных методов НЕ является способом распространения вредоносного ПО?

А) через вложения в электронной почте;

Б) через обновления операционной системы;

В) через заражённые USB-накопители.

РАУНД №1 «Основы кибербезопасности»

Задание 12 — Что такое «honeypot» в контексте кибербезопасности?

А) вид кибератаки, направленной на кражу данных;

Б) метод криптографической защиты информации;

В) ловушка для хакеров, имитирующая уязвимую систему.

РАУНД №1 «Основы кибербезопасности»

Задание 13 — Какова основная цель использования сетей TOR?

А) увеличение скорости подключения к интернету;

Б) анонимный доступ к ресурсам интернета;

В) защита от вирусов и вредоносных программ.

РАУНД №1 «Основы кибербезопасности»

Задание 14 — Что такое дипфейк?

А) вид вредоносного ПО для кражи паролей;

Б) создание реалистичных видео или аудио записей с искажённым содержанием;

В) спам-сообщения с фейками, распространяемые через социальные сети.

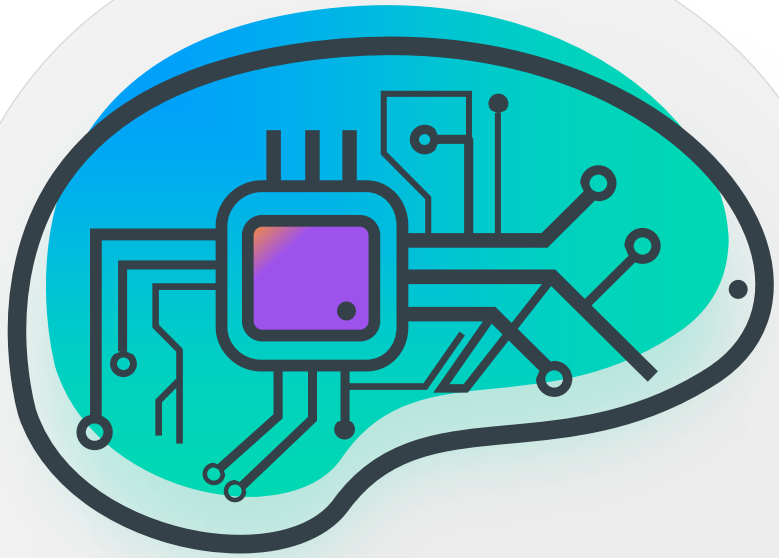
РАУНД №1 «Основы кибербезопасности»

Задание 15 — Какой из этих методов является примером двухфакторной аутентификации?

А) пароль и PIN-код;

Б) отпечаток пальца и голосовая идентификация;

В) пароль и сообщение с кодом подтверждения, отправленным на телефон.



Отличная работа!

Первый раунд завершён, подсчитайте количество правильных ответов!

БАЛЛЫ

1 – Б;
2 – А;
3 – Б;
4 – В;
5 – Б;
6 – А;
7 – Б;
8 – А;
9 – А;
10 – В;
11 – Б;
12 – В;
13 – Б;
14 – Б;
15 – В.

РАУНД №2

СТАРТ →

РАУНД №2 «Пароли и их безопасность»

Задание 1 — Какой пароль считается более надёжным?

А) 123456ABCc;

Б) QWERTY;

В) Xq4597v3P21.

РАУНД №2 «Пароли и их безопасность»

Задание 2 — Что такое парольная фраза?

А) случайный набор символов;

Б) слово, используемое в качестве пароля;

В) слова, объединённые во фразу, используемую в качестве пароля.

РАУНД №2 «Пароли и их безопасность»

Задание 3 — Что из перечисленного НЕ является хорошей практикой для создания пароля?

А) использование длинных паролей;

Б) использование личной информации;

В) использование сочетания букв, цифр и спецсимволов.

РАУНД №2 «Пароли и их безопасность»

Задание 4 — Какую функцию выполняет менеджер паролей?

А) генерирует и хранит надёжные пароли;

Б) восстанавливает забытые пароли;

В) помогает взломать чужие пароли.

РАУНД №2 «Пароли и их безопасность»

Задание 5 — Что делает пароль «сложным»?

А) длина более 8 символов;

Б) наличие только букв;

В) использование букв, цифр и спец. символов.

РАУНД №2 «Пароли и их безопасность»

Задание 6 — Что такое «соление» паролей?

А) процесс укрепления пароля добавлением случайных данных;

Б) простой способ запоминания паролей;

В) метод взлома паролей.

РАУНД №2 «Пароли и их безопасность»

Задание 7 — Что из перечисленного является примером слабого пароля?

А) j#K9!vQp3z;

Б) password123;

В) Y7%bE5w!X2.

РАУНД №2 «Пароли и их безопасность»

Задание 8 — Какой метод защиты от кражи паролей считается наиболее эффективным?

А) запись всех паролей на бумаге;

Б) двухфакторная аутентификация;

В) использование одного очень сложного пароля для всех аккаунтов.

РАУНД №2 «Пароли и их безопасность»

Задание 9 — Как должны действовать пользователи сети, если их пароль был украден?

А) немедленно изменить пароль на всех аккаунтах, где он использовался;

Б) продолжать использовать пароль, но следить за аккаунтом;

В) изменить пароль только на украденном аккаунте.

РАУНД №2 «Пароли и их безопасность»

Задание 10 — Почему важно избегать использования персональной информации при создании паролей?

А) такая информация может быть легко угадана или найдена;

Б) потому что это усложняет процесс восстановления пароля;

В) потому что это снижает сложность пароля.

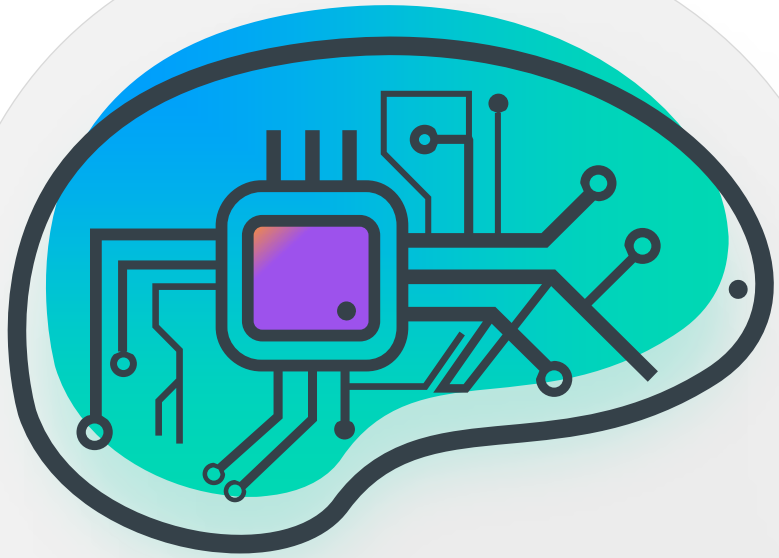
РАУНД №2 «Пароли и их безопасность»

Задание 11 — Как часто рекомендуется менять пароли?

А) каждую неделю;

Б) каждые 6 месяцев;

В) только когда думаешь, что пароль был украден.



Отличная работа!

Второй раунд завершён, подсчитайте количество правильных ответов!

БАЛЛЫ

1 — В;
2 — В;
3 — Б;
4 — А;
5 — В;
6 — А;
7 — Б;
8 — Б;
9 — А;
10 — А;
11 — Б.

РАУНД №3

СТАРТ →

РАУНД №3 «Безопасность мобильных устройств»

Задание 1 — Что представляет собой риск «Juice Jacking»?

А) процесс несанкционированной загрузки вредоносного ПО или выведения личных данных через USB-порт;

Б) использование неоригинального зарядного устройства;

В) перегрев батареи при зарядке.

РАУНД №3 «Безопасность мобильных устройств»

Задание 2 — Какая функция обеспечивает дополнительный уровень безопасности при использовании мобильных устройств?

А) блокировка экрана по времени неактивности;

Б) автоматическое обновление приложений;

В) уведомления о низком заряде батареи.

РАУНД №3 «Безопасность мобильных устройств»

Задание 3 — Что является признаком того, что мобильное приложение может быть вредоносным?

А) запрос доступа к данным без явной необходимости;

Б) наличие малого количества отзывов других пользователей;

В) размер приложения более 100 МБ.

РАУНД №3 «Безопасность мобильных устройств»

Задание 4 – Какие действия нужно предпринять, если вы подозреваете, что мобильное устройство заражено вирусным ПО?

А) продолжать использовать устройство, но избегать ввода паролей;

Б) провести сканирование антивирусным ПО и удалить подозрительные файлы;

В) вернуть устройство производителю/в магазин покупки.

РАУНД №3 «Безопасность мобильных устройств»

Задание 5 — Почему важно использовать функцию блокировки экрана на мобильном устройстве?

А) предотвращает случайные нажатия на экран;

Б) защищает устройство от несанкционированного доступа;

В) экономит заряд батареи.

РАУНД №3 «Безопасность мобильных устройств»

Задание 6 — Какой из вариантов является самым безопасным способом подключения к интернету для мобильного устройства?

А) открытая WiFi сеть в кафе;

Б) мобильный интернет от вашего оператора связи;

В) публичная WiFi сеть без пароля.

РАУНД №3 «Безопасность мобильных устройств»

Задание 7 — Что такое SIM-карта свопинг?

А) замена старой SIM-карты на новую;

Б) злоумышленник переносит номер жертвы на новую SIM-карту для получения доступа к её личным данным;

В) способ быстрой зарядки мобильного устройства.

РАУНД №3 «Безопасность мобильных устройств»

Задание 8 — Что такое «rooting» на Android или «jailbreaking» на iOS?

А) процесс обновления операционной системы до последней версии;

Б) получение несанкционированного доступа к файловой системе устройства;

В) восстановление заводских настроек устройства.

РАУНД №3 «Безопасность мобильных устройств»

Задание 9 — Как работает биометрическая аутентификация?

А) использует уникальные физические характеристики человека;

Б) сравнивает голос/лицо пользователя с предыдущими записями;

В) требует ввода секретного кода, отправленного по SMS.

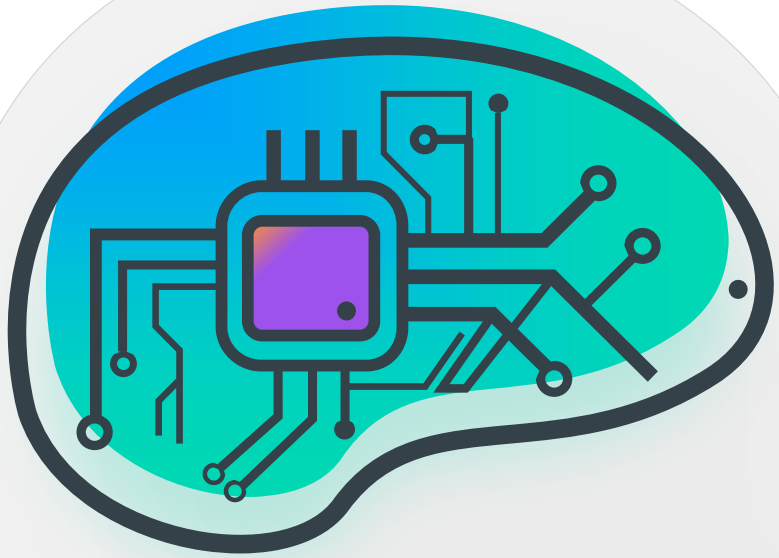
РАУНД №3 «Безопасность мобильных устройств»

Задание 10 — Какие меры безопасности следует предпринять перед продажей старого мобильного устройства?

А) удалить все приложения и выйти из аккаунтов;

Б) поменять обои рабочего стола на стандартные;

В) выполнить сброс настроек до заводских (Factory Reset).



Отличная работа!

Третий раунд завершён, подсчитайте количество правильных ответов!

БАЛЛЫ

1 – А;	6 – Б;
2 – А;	7 – Б;
3 – А;	8 – Б;
4 – Б;	9 – А;
5 – Б;	10 – В.

РАУНД №4

СТАРТ →

РАУНД №4 «Безопасное использование интернета»

Задание 1 — Что обозначает наличие HTTPS в начале URL-адреса веб-сайта?

А) сайт содержит высококачественный контент;

Б) соединение с сайтом зашифровано;

В) сайт быстро загружается.

РАУНД №4 «Безопасное использование интернета»

Задание 2 – Как VPN помогает обезопасить интернет-сёрфинг?

А) увеличивает скорость интернет-соединения;

Б) предотвращает всплывающую рекламу;

В) шифрует интернет-трафик, защищая данные.

РАУНД №4 «Безопасное использование интернета»

Задание 3 – Какой метод НЕ помогает в борьбе с нежелательной рекламой?

А) установка блокировщика рекламы;

Б) использование приватного режима браузера;

В) отправка жалобы на рекламодателя в интернете.

РАУНД №4 «Безопасное использование интернета»

Задание 4 — Что является признаком подозрительного веб-сайта?

А) отсутствие контактной информации;

Б) наличие сертификата безопасности;

В) наличие раздела «О нас».

РАУНД №4 «Безопасное использование интернета»

Задание 5 – Какую функцию выполняет сертификат SSL/TLS на веб-сайте?

А) ускоряет загрузку сайта;

Б) шифрует данные, передаваемые между пользователем и сайтом;

В) устанавливает соединение с социальными сетями.

РАУНД №4 «Безопасное использование интернета»

Задание 6 — Как пользователь может убедиться в подлинности загружаемого программного обеспечения?

А) проверить отзывы на форумах;

Б) скачать ПО только с официального сайта разработчика;

В) убедиться, что файл загрузки большого размера.

РАУНД №4 «Безопасное использование интернета»

Задание 7 — Какие действия следует предпринять, если вы посетили вредоносный сайт?

А) ничего, если ничего не скачивалось;

Б) запустить полное сканирование системы антивирусом;

В) переустановить браузер и перезагрузить устройство.

РАУНД №4 «Безопасное использование интернета»

Задание 8 — Что такое куки (cookies) в интернете?

А) программы для блокировки рекламы;

Б) файлы, которые сайты сохраняют для сбора данных о ваших действиях;

В) вирусы, распространяемые через электронную почту.

РАУНД №4 «Безопасное использование интернета»

Задание 9 — Как работает межсайтовый скриптинг (XSS)?

А) путём внедрения вредоносного кода на сайт для перехвата данных других пользователей;

Б) заражая компьютеры вирусами через электронную почту;

В) путём перенаправления пользователя на фальшивый сайт.

РАУНД №4 «Безопасное использование интернета»

Задание 10 — Почему важно выходить из аккаунтов на публичных компьютерах после использования?

А) предотвратить случайное закрытие облачных вкладок;

Б) чтобы другой пользователь компьютера не получил доступ к аккаунтам;

В) экономит трафик интернета.

РАУНД №4 «Безопасное использование интернета»

Задание 11 — Что следует делать при получении электронного письма с подозрительным вложением от известного отправителя?

А) открыть вложение, чтобы проверить содержимое;

Б) сохранить вложение на компьютере для последующего анализа;

В) связаться с отправителем для подтверждения подлинности письма.

РАУНД №4 «Безопасное использование интернета»

Задание 12 — Какой из нижеперечисленных вариантов НЕ является признаком безопасного онлайн-магазина?

А) наличие HTTPS в адресной строке сайта;

Б) возможность оплаты только через банковский перевод;

В) отзывы других покупателей о магазине.

РАУНД №4 «Безопасное использование интернета»

Задание 13 — Что делать, если вы столкнулись с видео, которое выглядит реалистичным, но содержит неправдоподобную информацию?

А) поделиться видео в социальных сетях;

Б) проверить источник и поискать подтверждение информации;

В) игнорировать видео, не предпринимая никаких действий.

РАУНД №4 «Безопасное использование интернета»

Задание 14 — Как можно определить, что изображение или видео было создано с использованием технологии дипфейков?

А) непропорциональные черты лица или неестественные движения губ;

Б) высокое качество изображения и звука;

В) присутствие водяных знаков или логотипов.

РАУНД №4 «Безопасное использование интернета»

Задание 15 — Что следует делать при обнаружении дипфейка с вашим участием?

А) игнорировать, если он не набрал много просмотров;

Б) обратиться поддержке для удаления контента и, при необходимости, обратиться в правоохранительные органы;

В) создать ответный дипфейк.

РАУНД №4 «Безопасное использование интернета»

Задание 16 — Что подростку следует делать, если он столкнулся с буллингом в интернете?

А) игнорировать и надеяться, что это прекратится;

Б) ответить агрессией на агрессию;

В) сообщить об этом доверенному взрослому и сохранить доказательства.

РАУНД №4 «Безопасное использование интернета»

Задание 17 — Что делать, если вы получаете сообщения угрожающего содержания в интернете?

А) удалить сообщения и забыть о них;

Б) Сообщить родителям/педагогам или обратиться в соответствующие службы;

В) попытаться самостоятельно найти отправителя.

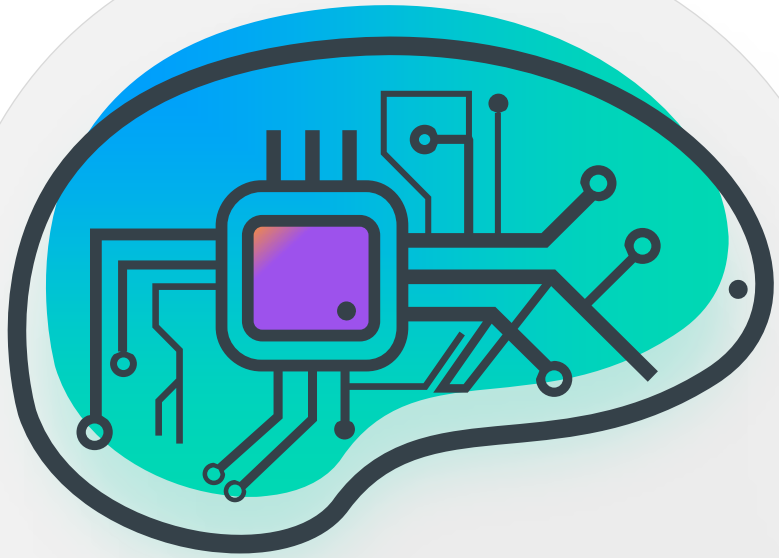
РАУНД №4 «Безопасное использование интернета»

Задание 18 — Какой способ является наиболее эффективным, чтобы оставаться в безопасности в интернете?

А) Размещать личную информацию только на тех сайтах, которые выглядят надёжно;

Б) Избегать любого взаимодействия в интернете;

В) обучение и применение знаний о кибербезопасности, включая использование сложных паролей, настройки приватности и критическое отношение к информации



Отличная работа!

Последний раунд завершён, подсчитайте количество правильных ответов!

БАЛЛЫ

1 – Б;
2 – В;
3 – В;
4 – А;
5 – Б;
6 – Б;
7 – Б;
8 – Б;
9 – А;
10 – Б;
11 – В;
12 – Б;
13 – Б;
14 – А;
15 – Б;
16 – В;
17 – Б;
18 – В.

СПАСИБО

Вы молодцы! Узнавайте больше и будьте в интернете в безопасности!

Продукт проекта

Игра-квиз разработана в качестве продукта индивидуального проекта.