Программа Вашего обучения

CODDY - Международная школа программирования и дизайна

Курс «Кибербезопасность детей в интернете». 1-й модуль

Цель курса: изучить основы кибербезопасности, научиться защищать свои данные, безопасно использовать интернет и социальные сети, развить навыки ответственного поведения в цифровом пространстве.

Программа курса:

День первый — Что такое кибербезопасность?

- История появления Интернета - от военных сетей до современности;
- Основные понятия кибербезопасности - защита данных и устройств;
- Угрозы в цифровой среде - вирусы, фишинг, мошенничество;
- Профессия специалиста по безопасности - роль и задачи.

Результаты занятия: изучили основы работы интернета, узнали о цифровых угрозах, поняли важность защиты данных.
Практическое задание: создать стикер-пак по теме кибербезопасности, изучить основные угрозы.

День второй — Что такое Wi-Fi и мобильный интернет?

- История создания Wi-Fi - от первых экспериментов до современных стандартов;
- Принцип работы радиоволн - частоты и передача данных;
- Особенности домашнего и общественного Wi-Fi - безопасность и зоны покрытия;
- Мобильный интернет - трафик, тарификация, контроль.

Результат занятия: изучили принципы работы беспроводных технологий, научились оценивать безопасность сетей и контролировать расход трафика.
Практическое задание: проверить настройки домашнего Wi-Fi, отследить расход трафика.

День третий — Личные данные и приватность в интернете

- Понятие личных данных - что можно и нельзя публиковать;
- Опасности размещения информации - риски для безопасности;
- Настройки приватности аккаунтов - защита профилей;
- Конфиденциальность в соцсетях - безопасные практики.

Результаты занятия: изучили понятие личных данных, узнали о рисках публикации информации, освоили настройки приватности.
Практическое задание: проверить настройки приватности в соцсетях, изменить опасные параметры.

День четвертый — Безопасное онлайн общение

- Правила общения с незнакомцами - как распознать опасность;
- Понятие кибербуллинга - признаки и защита;
- Груминг в интернете - основные признаки;
- Безопасные практики - защита личных данных.

Результаты занятия: изучили правила безопасного общения, научились распознавать опасные ситуации, освоили методы защиты от манипуляций.
Практическое задание: проанализировать сообщения от незнакомцев, составить план действий при опасности.

Программа Вашего обучения

CODDY - Международная школа программирования и дизайна

Курс «Кибербезопасность детей в интернете». 2-й модуль

Цель курса: изучить основы кибербезопасности, научиться защищать свои данные, безопасно использовать интернет и социальные сети, развить навыки ответственного поведения в цифровом пространстве.

Программа курса:

День первый — **Интернет-угрозы**

- Понятие фишинга - как мошенники выманивают данные;
- Виды цифрового скама - прямой обман пользователей;
- Вредоносные ссылки - опасность для устройств;
- Технология deepfake - подделка голоса и видео;
- Методы защиты устройств - базовые правила безопасности.

Результаты занятия: изучили основные виды интернет-угроз, научились распознавать фишинг и скам, освоили способы защиты устройств.
Практическое задание: проанализировать подозрительные сообщения, проверить настройки безопасности устройства.

День второй — **Защита от вирусов и вредоносного ПО**

- История появления вирусов - от первых экспериментов до современности;
- Основные виды вредоносного ПО - вирусы, трояны, шпионские программы;
- Пути заражения устройств. Признаки заражения;
- Методы защиты - антивирусы, обновления системы;
- Безопасные практики - проверка файлов, официальные источники.

Результаты занятия: изучили основные виды вредоносного ПО, узнали пути заражения устройств, освоили методы защиты от вирусов.
Практическое задание: проверить наличие антивируса на устройствах, настроить автоматическое обновление системы.

День третий — **Защита паролей и двухфакторная аутентификация**

- Что такое надёжный пароль - критерии создания безопасного пароля;
- Виды аутентификации. Двуххфакторная защита - как она работает;
- Управление паролями - методы хранения;
- Признаки взлома учётных записей.

Результаты занятия: изучили принципы создания надёжных паролей, узнали о методах аутентификации, освоили основы двухфакторной защиты.
Практическое задание: проверить надёжность своих паролей, настроить двухфакторную аутентификацию на основных сервисах.

День четвертый — **Скрытые угрозы для устройств и как от них защититься**

- Шпионское ПО (Spyware). Поддельные приложения;
- Сетевые атаки - способы перехвата данных в интернете
- Уязвимости системы - слабые места в защите устройств
- Признаки скрытых угроз - как распознать опасность.

Результаты занятия: изучили основные виды скрытых угроз, освоили методы защиты от сетевых атак.
Практическое задание: проверить установленные приложения на подозрительные разрешения, настроить автоматическое обновление системы.

Программа Вашего обучения

CODDY - Международная школа программирования и дизайна

Курс «Кибербезопасность детей в интернете». 3-й модуль

Цель курса: изучить основы кибербезопасности, научиться защищать свои данные, безопасно использовать интернет и социальные сети, развить навыки ответственного поведения в цифровом пространстве.

Программа курса:

День первый — **Антивирусы и защита от вредоносного ПО**

- История появления антивирусов - от первых программ до современности
- Виды вредоносного ПО - вирусы, трояны, программы-вымогатели
- Принцип работы антивируса - сигнатуры и методы защиты
- Типы антивирусных программ. Правила установки антивируса;
- Признаки заражения устройства - как распознать угрозу.

Результаты занятия: изучили основные типы антивирусов и вредоносного ПО, узнали принципы работы антивирусных программ.
Практическое задание: проверить работоспособность антивируса на устройствах, составить чек-лист безопасной установки антивирусного ПО.

День второй — **Как создать надёжный пароль и не забыть его**

- Критерии надёжного пароля - длина, сложность, отсутствие личных данных;
- Правила хранения паролей - безопасные способы запоминания;
- Ошибки при создании паролей - распространённые уязвимости;
- Инструменты проверки надёжности - онлайн-сервисы оценки;
- Практические приёмы создания паролей.

Результаты занятия: изучили критерии надёжности паролей, освоили методы создания сложных комбинаций, узнали о безопасных способах хранения паролей.
Практическое задание: создать и проверить несколько надёжных паролей для разных аккаунтов, разработать систему запоминания паролей.

День третий — **Безопасное использование Wi-Fi**

- Угрозы общественных сетей;
- Признаки опасных сетей;
- Инструменты защиты - VPN, Proxy, HTTPS;
- Безопасные практики использования WiFi.

Результаты занятия: изучили основные угрозы при использовании общественного Wi-Fi, освоили методы защиты соединения.
Практическое задание: проанализировать доступные Wi-Fi сети на предмет безопасности, настроить VPN на устройстве.

День четвертый — К**иберзащитники: миссия Кодди**

- Создание плана безопасности для цифровых устройств;
- Настройка защиты на примере устройства робота Кодди;
- Распознавание опасностей в интернете и на устройстве;
- Критическое мышление при работе с цифровыми технологиями.

Результаты занятия: научились создавать комплексный план защиты устройств, освоили практические навыки настройки безопасности.
Практическое задание: разработать план защиты для личного устройства, создать памятку правил кибербезопасности.

Программа Вашего обучения

CODDY - Международная школа программирования и дизайна

Курс «Кибербезопасность детей в интернете». 4-й модуль

Цель курса: изучить основы кибербезопасности, научиться защищать свои данные, безопасно использовать интернет и социальные сети, развить навыки ответственного поведения в цифровом пространстве.

Программа курса:

День первый — **Интернет-угрозы**

- Понятие фишинга - как мошенники выманивают данные;
- Виды цифрового скама - прямой обман пользователей;
- Вредоносные ссылки - опасность для устройств;
- Технология deepfake - подделка голоса и видео;
- Методы защиты устройств - базовые правила безопасности.

Результаты занятия: изучили основные виды интернет-угроз, научились распознавать фишинг и скам, освоили способы защиты устройств.
Практическое задание: проанализировать подозрительные сообщения, проверить настройки безопасности устройства.

День второй — **Защита личной информации**

– Введение в цифровой след и сталкинг;
– Анализ личного цифрового следа;
– Безопасные и опасные данные для публикации;
– Практические методы уменьшения цифрового следа.

Р**езультат занятия:** научились анализировать свой цифровой след, применять меры для защиты личной информации.
Практическое задание: провести мини-исследование своей страницы в социальной сети по чек-листу опасных данных.

День третий — **Безопасное хранение данных**

– Что такое локальный диск и облачное хранилище;
– Как работают облачные сервисы;
– Резервная копия и зачем она нужна;
– Правила безопасного хранения файлов.

Результат занятия: узнали, что такое облако, локальный диск и резервная копия, научились использовать базовую защиту для хранения данных.
Практическое задание: создать папки на локальном диске и в облаке, настроить общий доступ и сделать резервную копию важных данных.

День четвертый — **Интернет-магазин робота Кодди**

– Криптография и исторические шифры (Цезарь, Атбаш);
– Современные методы защиты: HTTPS, End-to-End, хэши паролей;
– Настройка cookies и приватность;
– Облачное хранение и шифрование сообщений.

Результат занятия: узнали, что такое криптография, шифр Цезаря, Атбаш, хэши, HTTPS и end-to-end, научились шифровать и расшифровывать сообщения.
Практическое задание: выбрать безопасные cookies, облачное хранилище для файлов и зашифровать сообщения для партнёров интернет-магазина.

Программа Вашего обучения

CODDY - Международная школа программирования и дизайна

Курс «Кибербезопасность детей в интернете». 5-й модуль

Цель курса: изучить основы кибербезопасности, научиться защищать свои данные, безопасно использовать интернет и социальные сети, развить навыки ответственного поведения в цифровом пространстве.

Программа курса:

День первый — **Социальные сети: риски и возможности**

– Что такое социальные сети и их история;
– Возможности и риски социальных сетей;
– Фейки, буллинг, мошенничество, сталкинг;
– Правила создания безопасного профиля.

Результат занятия: изучили возможности и риски основных соцсетей, научились правильно создавать профиль и защищать личные данные.
Практическое задание: создать безопасный профиль для персонажа, настроить приватность и выбрать безопасные публикации.

День второй — **Опасности социальных сетей**

– Контент и алгоритмы социальных сетей;
– Цифровой след и онлайн-репутация;
– Влияние соцсетей на эмоции;
– Новые функции: Reels, Shorts, Stories, группы.

Результат занятия: узнали, как соцсети формируют ленту, что такое цифровой след, научились анализировать и фильтровать информацию.
Практическое задание: проанализировать посты придуманных аккаунтов, настроить фильтры для здоровой ленты.

День третий — **Создание безопасного контента и тренды в социальных сетях**

– Что такое контент и правила его создания;
– Безопасность личных данных в публикациях;
– Тренды и вирусные видео;
– Как создавать популярный и безопасный контент.

Результат занятия: узнали принципы создания безопасного контента и правила публикаций, научились анализировать посты и видео на безопасность.
Практическое задание: создать сценарий безопасного поста или видео для воображаемого профиля персонажа.

День четвертый — **Итоговый проект по цифровой безопасности**

– Повторение правил безопасного профиля;
– Основные риски: фейки, буллинг, мошенники;
– Безопасный контент и настройки приватности;
– Управление временем в социальных сетях.

Результат занятия: узнали, как создавать безопасный профиль, научились анализировать посты и управлять временем в соцсетях.
Практическое задание: найти и исправить ошибки в профиле, а затем составить тайм-план дня с балансом между учёбой, отдыхом и соцсетями.

Программа Вашего обучения

CODDY - Международная школа программирования и дизайна

Курс «Кибербезопасность детей в интернете». 6-й модуль

Цель курса: изучить основы кибербезопасности, научиться защищать свои данные, безопасно использовать интернет и социальные сети, развить навыки ответственного поведения в цифровом пространстве.

Программа курса:

День первый — Онлайн-игры: польза, история и безопасность

– История компьютерных игр (Pong, Тетрис);
– Игровые платформы (телефон, ПК, приставка);
– Возрастные рейтинги (7+, 12+, 16+);
– Польза и риски онлайн-игр.

Результат занятия: узнали историю компьютерных игр, что такое игровые платформы и возрастные рейтинги, научились отличать безопасные игры от небезопасных.
Практическое задание: заполнить карточку эксперта для одной игры.

День второй — Покупки, донаты и мошенники в играх

– Что такое донат и как он работает;
– Пиратские игры и их опасности;
– Токсичное общение и давление в играх;
– Как распознать мошенников и защитить аккаунт.

Результат занятия: узнали, что такое донат, пират и мошенник, научились распознавать опасные ситуации в онлайн-играх.
Практическое задание: проанализировать игровые ситуации, определить правильные действия и смоделировать спасение аккаунта от мошенников.

День третий — Эмоции, честность и игровая зависимость

– Что такое читерство и как оно влияет на эмоции;
– Как управлять эмоциями во время игры (злость, разочарование);
– Что такое игровая зависимость и её признаки;
– Как контролировать время и чередовать активности.

Результат занятия: узнали, что такое читерство, игровая зависимость, научились управлять эмоциями и планировать время.
Практическое задание: создать дизайн толстовки с правилами честного игрока.

День четвертый — Проект: “Кодди создаёт свою безопасную игру”

– Что делает игру безопасной: платформа, возраст, польза;
– Опасности в играх: донаты, мошенники, обман;
– Эмоции и честность: читерство, злость, зависимость;
– Комплексный анализ игры по чек-листу.

Результат занятия: узнали, какие элементы делают игру опасной или безопасной, как связаны эмоции, покупки, общение и честность.
Практическое задание: помочь Кодди проанализировать его игру, заполнить чек-лист и дать рекомендации по исправлению опасных элементов.

Программа Вашего обучения

CODDY - Международная школа программирования и дизайна

Курс «Кибербезопасность детей в интернете». 7-й модуль

Цель курса: изучить основы кибербезопасности, научиться защищать свои данные, безопасно использовать интернет и социальные сети, развить навыки ответственного поведения в цифровом пространстве.

Программа курса:

День первый — **Поиск информации и оценка источников**

– Что такое серфинг в интернете;
– Фейковые новости и их признаки;
– Фактчекинг как способ проверки информации;
– Правила безопасного поиска в интернете.

Результат занятия: узнали, что такое серфинг, фейковые новости и фактчекинг, научились находить первоисточники.
Практическое задание: создать фейковую новость на основе случайной темы, используя признаки фейка, выполнить фактчекинг

День второй — Т**ворчество онлайн**

– Онлайн-инструменты для рисования и дизайна;
– Создание комиксов и анимации;
– 3D-дизайн и моделирование;
– Музыка, звук, программирование и совместные проекты.

Результат занятия: узнали о безопасных онлайн-инструментах для творчества, научились использовать онлайн-доски и приложения для совместного создания проектов.
Практическое задание: создать афишу (постер) к уроку в Google Презентациях.

День третий — **Онлайн-обучение**

– Что такое онлайн-обучение и чем оно отличается от офлайн;
– Плюсы и минусы онлайн-школ;
– Признаки хорошей и безопасной онлайн-школы;
– Как оценивать полезность и безопасность курсов.

Результат занятия: узнали, как устроено онлайн-обучение, какие бывают платформы и курсы, научились оценивать полезность и безопасность онлайн-школ.
Практическое задание: проанализировать три кейса онлайн-школ, оценить их плюсы и риски.

День четвертый — **Основы блоггинга и безопасность**

– История социальных сетей и их плюсы и минусы;
– Основные понятия блогинга: хейт, хайп, троллинг;
– Правило 3 фильтров перед публикацией;
– Как реагировать на негатив и избегать ошибок начинающих блогеров.

Результат занятия: узнали особенности популярных платформ и правила безопасного поведения в соцсетях.
Практическое задание: придумать и снять короткий рекламный отзыв о школе Кодди, соблюдая правило 3 фильтров и не используя личные данные.

Программа Вашего обучения

CODDY - Международная школа программирования и дизайна

Курс «Кибербезопасность детей в интернете». 8-й модуль

Цель курса: изучить основы кибербезопасности, научиться защищать свои данные, безопасно использовать интернет и социальные сети, развить навыки ответственного поведения в цифровом пространстве.

Программа курса:

День первый — **Цифровая этика**

– Что такое этика в интернете и три главных правила;
– Почему анонимность провоцирует грубость;
– Упражнение «Сообщение без лица»: как текст без интонации может ранить;
– Кто такой модератор и как он следит за порядком.

Результат занятия: узнали основные правила цифровой этики, научились оценивать свою этичность в комментариях.
Практическое задание: проанализировать конфликтные ситуации в чате, предложить решение для сохранения безопасного общения.

День второй — **Авторское право и плагиат**

– Что такое авторское право и зачем оно нужно;
– Плагиат, пиратство и водяной знак;
– Легальные ресурсы для скачивания контента;
– Как защитить свои авторские работы и правильно указывать источник.

Результат занятия: узнали, что такое авторское право, плагиат и водяной знак, научились определять, можно ли использовать материал, и как защитить свои творческие работы.
Практическое задание: создать рисунок или фото, поставить на него водяной знак в редакторе, проанализировать ситуации нарушения.

День третий — **Ответственное использование соцсетей**

– Что значит использовать соцсети ответственно;
– Игра «Польза / Ловушка / Зависимость»;
– Соцсети ≠ реальность: почему люди показывают только лучшее;
– Как оценивать аккаунты блогеров на этичность и безопасность.

Результат занятия: узнали, что такое ответственное использование соцсетей, научились отличать полезный контент от ловушек.
Практическое задание: проанализировать своё время в соцсетях, оценить аккаунт любимого блогера по шести критериям.

День четвертый — **Киберэтика и будущие вызовы**

– Как раньше представляли интернет и каким он стал;
– Что такое вызовы будущего;
– Мини-игра «Что нормально в киберэтике, а что нет»;
– Как технологии развиваются, а человеческие эмоции остаются прежними.

Результат занятия: узнали, что такое deepfakes, научились выбирать качественный контент и отличать контент, сгенерированный ИИ.
Практическое задание: написать советы по безопасному поведению в интернете по трём темам.

Программа Вашего обучения

CODDY - Международная школа программирования и дизайна

Курс «Кибербезопасность детей в интернете». 9-й модуль

Цель курса: изучить основы кибербезопасности, научиться защищать свои данные, безопасно использовать интернет и социальные сети, развить навыки ответственного поведения в цифровом пространстве.

Программа курса:

День первый — **Искусственный интеллект: цифровой помощник или замена мозгу?**

– Что такое ИИ на простых аналогиях;
– Польза и риски использования ИИ в школе и жизни;
– Типы ИИ: узконаправленный, обучающийся, человекоподобный;
– Правила цифровой гигиены при работе с ИИ.

Результат занятия: получили базовое понимание, что такое ИИ, узнали примеры пользы и рисков ИИ, выработали навыки эффективного запроса.
Практическое задание: придумать план для экскурсии с одноклассниками, сравнить ответы разных ИИ, оценить их качество и создать финальный план на основе своего решения.

День второй — **Интернет вещей (IoT): Умный дом и не только**

– Что такое «Умный дом» и как он работает;
– Аудит умных устройств: полезные и не очень;
– Кто имеет доступ к данным с умных устройств;
– Arduino и Raspberry Pi — «мозги» для умных устройств.

Результат занятия: узнали суть IoT и концепцию «мозга» для умных устройств, научились проводить аудит умных устройств в своём окружении.
Практическое задание: разработать концепцию умного устройства для дома или школы, решающего проблему кибербезопасности.

День третий — **Мир VR/AR**

– Что такое виртуальная реальность (VR) и дополненная реальность (AR);
– История развития VR/AR технологий;
– Основные риски безопасности;
– Принципы безопасного использования VR/AR.

Результат занятия: узнали ключевые различия между VR и AR, научились критически оценивать и выбирать безопасные приложения.
Практическое задание: придумать мини-сюжет для использования VR/AR на уроках истории, географии или английского.

День четвертый — **Итоговый проект «Защищённый ноутбук»**

– Слои защиты устройства: пароли, антивирус, обновления;
– Защита приватности и данных: шифрование, резервное копирование;
– Безопасные привычки: работа с Wi-Fi, ссылками, установка программ;

Результат занятия: узнали ключевые принципы комплексной защиты устройства, научились проектировать модель безопасного устройства с учётом потребностей пользователя, презентовать и аргументировать свои решения.
Практическое задание: создать проект защищённого ноутбука для любимого персонажа (или Кодди).