Современные угрозы: как разобраться

Технологии делают нашу жизнь удобнее: умные дома управляют светом и музыкой, голосовые помощники подсказывают погоду, а криптовалюты и искусственный интеллект — это уже не фантастика, а реальность. Однако с новыми возможностями появляются и новые угрозы. Давайте разберёмся, как они работают и как быть с ними осторожными.

Искусственный интеллект и дипфейк

Искусственный интеллект (ИИ) — это программы, которые могут учиться, распознавать образы, создавать тексты, изображения и видео. Благодаря ИИ создаются роботы, голосовые помощники, чат-боты и, к сожалению, поддельные видео, их называют дипфейками (deepfake).

Представь, что ты смотришь мультфильм, где герой говорит голосом твоего любимого актёра, хотя тот это видео никогда не записывал. Или видишь ролик, где известный человек говорит странные вещи. Дипфейк создают с помощью ИИ, который «учится» на настоящих видео и изображениях, а затем «рисует» подделку.

Искусственный интеллект сначала «изучает» множество настоящих видео человека: смотрит, как двигаются губы, глаза, как звучит голос. Потом ИИ заменяет лицо или голос на видео другим, имитирует речь, движения, выражения.

Дипфейк используют нейросети, которые называются GAN — генеративные состязательные сети. Один ИИ создаёт фейк, другой пытается его разоблачить. Они «соревнуются» до тех пор, пока подделка не станет почти идеальной.

Такие технологии могут использоваться в кино или образовании, но бывают и опасные случаи. Например, мошенники делают фальшивые видео с известными людьми или с родителями ребёнка, чтобы обманом получить деньги или информацию.

в новых технологиях и защитить себя

В 2023 году мошенники создали дипфейк-видео с популярным бизнесменом, который якобы рекламировал «суперприбыльную» криптовалюту. Многие люди поверили видео и потеряли свои сбережения, инвестируя в несуществующую валюту. Настоящий бизнесмен узнал об этом только через несколько недель.

Визуальные признаки подделки

- Слишком ровная, «восковая» кожа без естественных недостатков.
- Странные или асимметричные уши.
- Размытые или неестественно выглядящие пальцы.
- Неестественные тени или освещение.
- Моргание происходит слишком редко или слишком часто.
- Рот движется не синхронно со словами.
- Резкие переходы в области шеи, где заканчивается подделка.

Угадай фейк

Посмотри на два изображения. Одно — настоящее фото, другое создано ИИ. Попробуй найти отличия. Можешь поискать фото, сгенерированные через ИИ в интернете, посмотреть, что отличает эти фотографии от реальных изображений. Чем больше ты будешь тренироваться, тем легче научишься отличать подделку.

Иногда мошенники используют ИИ для клонирования голосов. Они записывают несколько минут речи человека (например, из видео в социальных сетях) и затем могут заставить ИИ произнести любые слова этим голосом.

Также мошенники часто создают чат-ботов, которые выдают себя за представителей банков, интернет-магазинов или государственных служб.

Звуковые признаки подделки

- Голос звучит слишком ровно, без естественных интонаций.
- Заметные паузы или «склейки» в речи.
- Произношение не совсем соответствует привычной речи человека.

Советы по защите от мошенников

1. Всегда проверяй информацию из нескольких источников.
2. Сомневаешься — не торопись действовать.
3. Не переходи по подозрительным ссылкам.
4. Если видео вызывает тревогу, покажи его взрослым.

Чтобы защитить свои данные:

- не публикуй слишком много видео и фото со своим изображением в открытом доступе;
- настрой приватность в социальных сетях;
- не записывай голосовые сообщения незнакомым людям;
- будь осторожен, общаясь с незнакомцами с помощью видеозвонков.

Если кто-то использует твои лицо, голос или личную информацию без разрешения, ты имеешь право на защиту согласно Конституции Республики Беларусь.

Каждый имеет право на защиту от незаконного вмешательства в его частную жизнь, в том числе от посягательства на тайну его корреспонденции, телефонных и иных сообщений, на его честь и достоинство.

Государство создаёт условия для защиты персональных данных и безопасности личности и общества при их использовании.

Статья 28 Конституции Республики Беларусь

Криптовалюты и блокчейн

Криптовалюта — это цифровые деньги, которые не печатаются как обычные рубли, а существуют только в интернете. Самая известная — **биткоин**. Эти деньги работают на основе технологии **блокчейн**.

Каждый новый «блок» содержит список транзакций, дату и время, «отпечаток» предыдущего блока (хеш), защиту от подделки. Как только она заполняется, её подшивают в «цепочку», которую никто не может изменить. Это защищает от подделки и воровства.

Если объяснять просто, то блокчейн — это как тетрадь, в которую записываются все операции с криптовалютой. Только эта тетрадь не у одного человека, а сразу у тысяч пользователей по всему миру.

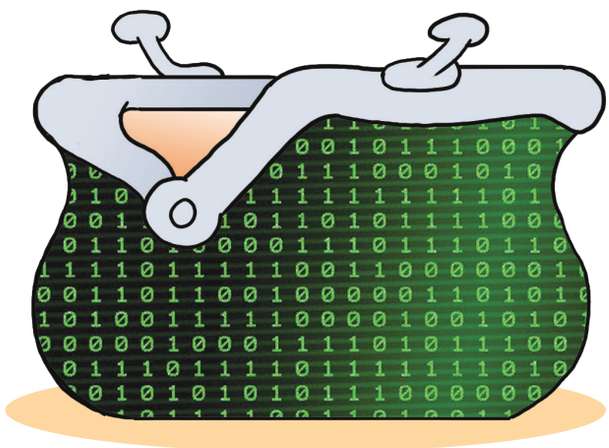
Криптовалюты могут использоваться в играх, для покупок или как инвестиции. Важно помнить, что в нашей стране операции с криптовалютами регулируются Декретом Президента Республики Беларусь «О развитии цифровой экономики». Только с 18 лет можно официально заниматься майнингом, трейдингом и покупкой криптовалют через легальные платформы.

Преимущества криптовалют:

- ⊕ Быстрые переводы.
- ⊕ Нет банков-посредников.
- ⊕ Некоторые игры используют токены.

Недостатки и риски криптовалют:

- ⊖ Цена может резко упасть.
- ⊖ Мошенничество и фальшивые биржи.
- ⊖ Потерянный пароль = потерянные деньги.



Витя увидел рекламу быстрого заработка на криптовалютах. Он попросил у родителей деньги якобы на тетради для учёбы и вложил их в поддельную криптобиржу. Сайт исчез через неделю вместе с деньгами сотен людей.

Популярные криптомошеннические схемы

Пирамиды и «удвоители». Мошенники обещают удвоить или утроить криптовалюту за короткое время: «Пришли 1 биткоин — получи 2!». Это всегда обман.

Поддельные биржи и кошельки. Создаются сайты и приложения, копирующие известные платформы. Люди вводят туда свои данные и теряют все средства.

Фальшивые криптовалюты и новые монеты. Мошенники создают «революционные» новые криптовалюты и собирают деньги на их развитие, а потом исчезают.

Социальные сети и влогеры. Поддельные аккаунты знаменитостей предлагают «эксклюзивные» криптоинвестиции.

Помни! Криптовалюта — это не способ быстро разбогатеть. Операции с криптовалютой возможны только по достижении 18-летнего возраста. Лучшим занятием для подростка является изучение того, как работает экономика.

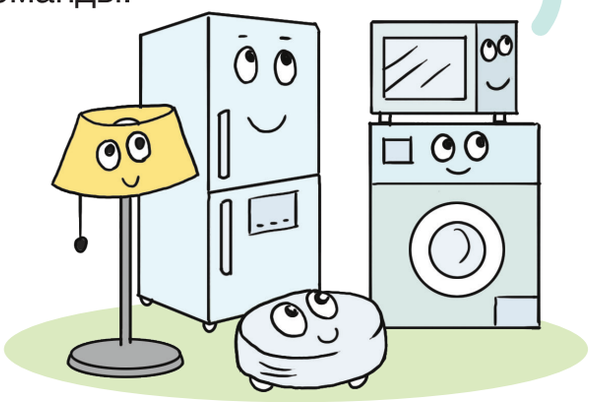
«Умные» устройства

Ты, наверное, слышал об «умном доме». Это когда свет, музыка, камеры и даже чайник управляются через телефон. Такие устройства объединяются в сеть — IoT (Internet of Things — «Интернет вещей»).

Что включает в себя «умный дом»?

- «Умные» лампочки и выключатели.
- Голосовые помощники (Алиса, Google Assistant).
- Камеры наблюдения и видеодомофоны.
- «Умные» замки и сигнализации.
- Климат-контроль и термостаты.
- «Умные» телевизоры и колонки.
- Роботы-пылесосы.
- «Умные» холодильники и другая бытовая техника.

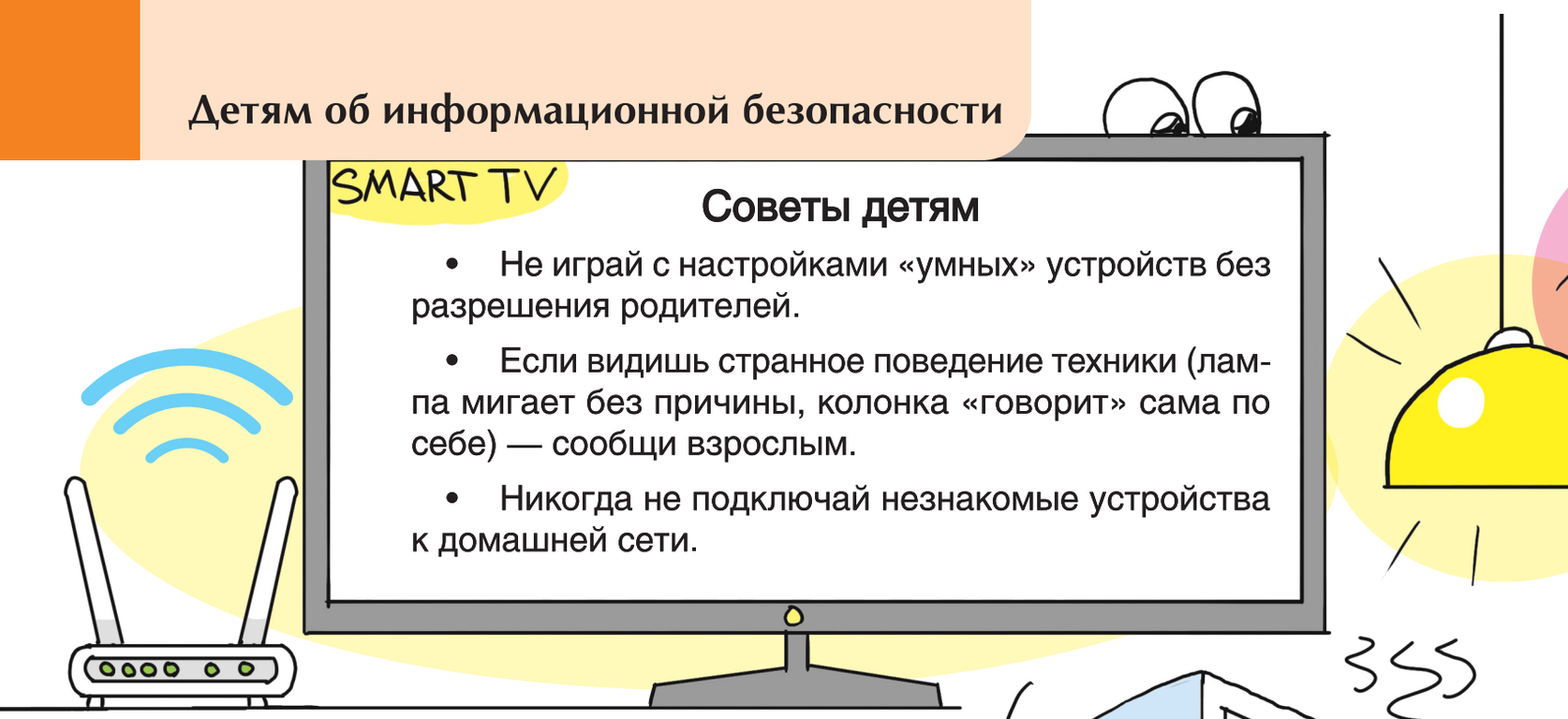
«Умный дом» — это удобно. Ты включаешь лампу голосом или видишь, кто звонит в дверь, не вставая с дивана. Но каждое такое устройство представляет собой мини-компьютер. А значит, его можно взломать, если не настроить правильно. Злоумышленники способны подглядывать через камеры, слушать микрофон, перехватывать команды.



В 2019 году хакеры взломали популярную модель «умного» замка и смогли открыть двери удалённо. Это случилось из-за слабого шифрования Bluetooth-соединения.

Уязвимости «умного дома»

- **Слабые пароли**. Многие оставляют стандартные «admin» и «1234».
- **Отсутствие обновлений.** Производители регулярно выпускают обновления безопасности, но многие пользователи их игнорируют. Старые прошивки содержат известные уязвимости, которые легче взломать.
- **Небезопасная сеть Wi-Fi.** Если домашний Wi-Fi не защищён или использует устаревшие протоколы шифрования, злоумышленники могут перехватывать данные.

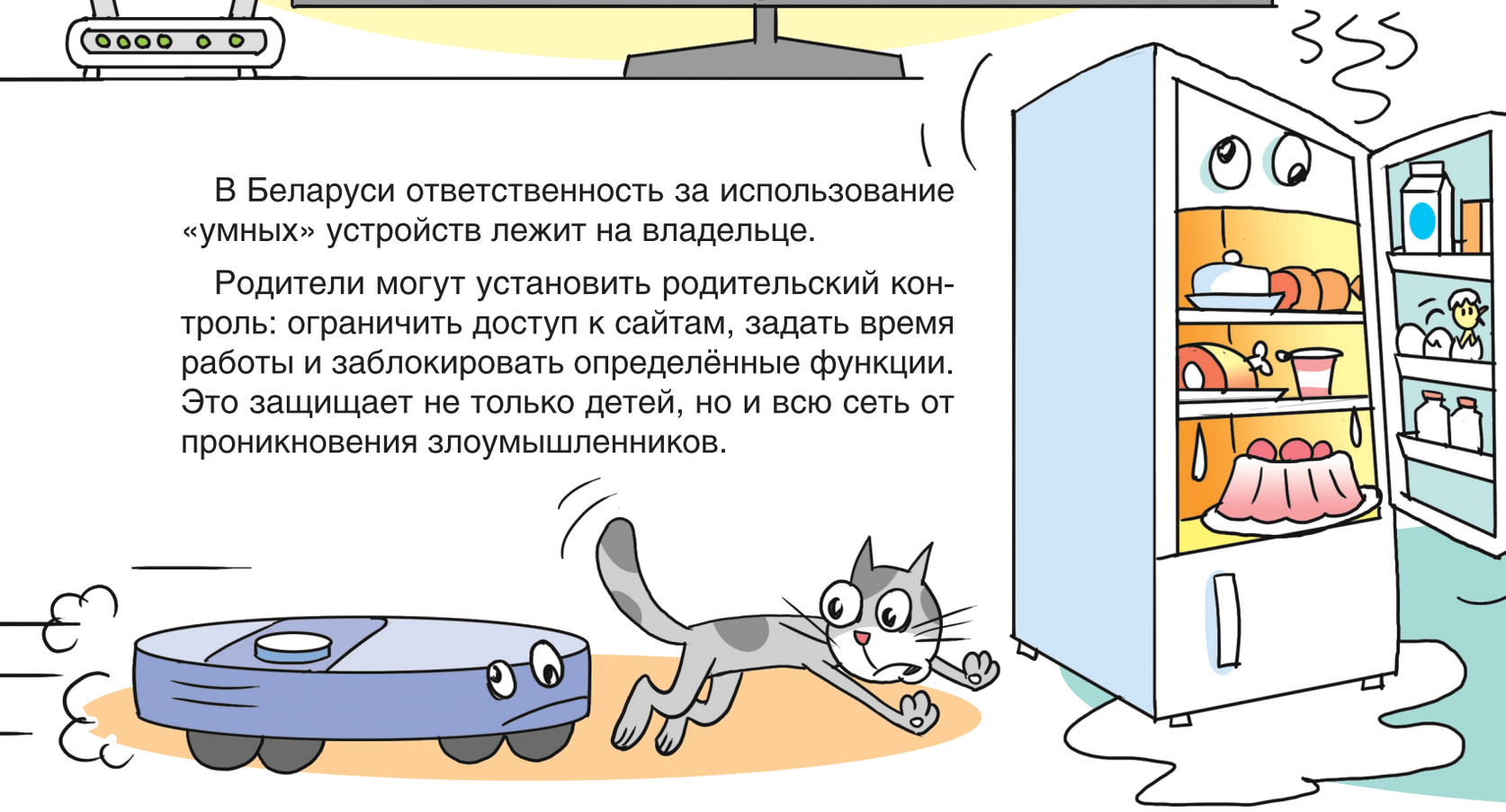


Советы детям

- Не играй с настройками «умных» устройств без разрешения родителей.
- Если видишь странное поведение техники (лампа мигает без причины, колонка «говорит» сама по себе) — сообщи взрослым.
- Никогда не подключай незнакомые устройства к домашней сети.

В Беларуси ответственность за использование «умных» устройств лежит на владельце.

Родители могут установить родительский контроль: ограничить доступ к сайтам, задать время работы и заблокировать определённые функции. Это защищает не только детей, но и всю сеть от проникновения злоумышленников.



Признаки возможного взлома

- Устройства включаются или выключаются сами по себе.
- Странные звуки из колонок или голосовых помощников.
- Необычная активность светодиодов на устройствах.
- Медленная работа интернета.
- Незнакомые устройства в списке подключённых к Wi-Fi.

Проверьте вместе с родителями

- Установлен ли надёжный пароль на Wi-Fi?
- Обновлены ли все «умные» устройства до последних версий?
- Есть ли антивирус на всех компьютерах и смартфонах?
- Настроены ли уведомления о подключении новых устройств?
- Отключены ли ненужные функции (микрофоны, камеры)?

Создайте план действий

1. Что делать, если заметили подозрительную активность?
2. Кому звонить в случае взлома?
3. Как быстро отключить все «умные» устройства?
4. Где хранятся пароли и как их восстановить?

Новые технологии интересны и полезны. Но они требуют внимательности. Если ты знаешь, как они работают, и умеешь себя защищать, ты сможешь использовать их с умом. Спрашивай, изучай, интересуйся — и ты станешь самым продвинутым пользователем.