
kaspersky
Привет!
Из этой книги ты узнаешь о разных явлениях из мира технологий, а ещё — сможешь получить полезные советы, как обезопасить себя и свои данные в интернете.
Приятного путешествия!
kaspersky
Кибераз
буки
https://
OK

Эта книга принадлежит _____

Для начинающих исследователей цифрового мира

Ты держишь в руках «Азбуку кибербезопасности». Что это такое? Кибербезопасность помогает нам использовать современные технологии — от планшета до голосового помощника — и исследовать онлайн-мир, не беспокоясь о возможных цифровых угрозах.

Онлайн-мир огромен и полон возможностей: можно путешествовать, не выходя из дома, узнавать что-то новое каждый день, общаться с друзьями, изучать иностранные языки и, конечно, играть и развлекаться.

Как и в обычной жизни, в виртуальной тоже стоит быть внимательными. Неосторожность в цифровом пространстве и незнание базовых правил кибергигиены грозят серьёзными неприятностями. Например, можно нечаянно скачать на свой планшет или телефон вредоносную программу, которая передаст злоумышленникам важные данные, потерять все достижения из любимой игры или даже деньги.

Чтобы твоё путешествие в виртуальном мире было захватывающим и познавательным, а неприятности обходили стороной, изучи нашу киберазбуку от А до Я. Ты познакомишься с новыми технологиями, узнаешь, как избегать цифровых угроз и не попадаться на уловки онлайн-мошенников.

Для мам и пап мы собрали много полезных статей по теме детской онлайн-безопасности и приватности на нашем сайте kids.kaspersky.ru.

Чтобы дети безопасно исследовали онлайн-пространство, мы создали цифрового помощника — программу Kaspersky Safe Kids.

Аккаунт

Аккаунт — это личный кабинет человека на сайте или в сервисе (например, в игре или социальной сети). А также — набор данных, который нужен для подтверждения, что страница принадлежит конкретному пользователю.

Просматривать сайты и информацию в интернете можно и без аккаунта (учётной записи). Но когда пользователь заходит в свой аккаунт в том или ином сервисе, у него появляются новые возможности. Например, переписываться с друзьями, делать покупки, слушать музыку, оставлять комментарии, получать рекомендации и не только.

Браузер

Браузер — это программа для просмотра страниц в интернете.

Прежде чем попасть в интернет, нужно открыть входную дверь в него — во многих случаях этой дверью оказывается браузер. Он позволяет просматривать сайты и загружать файлы, а ещё хранить историю посещений, пароли и другие данные. Чтобы расширить возможности браузера, можно использовать плагины — специальные программы. Кстати, первый веб-браузер был создан ещё в 1990 году!

Вредоносные программы

Вредоносные программы — это программы, которые создаются и/или используются злоумышленниками, например, для уничтожения, изменения, кражи информации или выманивания денег пользователей, а также для нарушения работы компьютера.

Человек рискует столкнуться с ними, когда переходит по ссылке из подозрительного сообщения, скачивает игры, фильмы или другие файлы на непроверенных сайтах. Поэтому важно всегда быть внимательным в интернете и анализировать, на какие сайты заходишь и откуда загружаешь файлы. А ещё лучше — установить защитную программу: она не позволит заразить устройство.

Обезопасить устройства от вредоносных программ поможет комплексное и надёжное защитное решение, такое как Kaspersky Premium

Геолокация

Геолокация — это функция определения местоположения пользователя с помощью различных технологий.

Благодаря геолокации человек может, например, понять, где он находится, если заблудился. А ещё — найти дорогу в магазин, школу или даже музей в другом городе. Но твоё точное местоположение — это конфиденциальная информация, которую лучше активно не сообщать посторонним, в том числе в социальных сетях, даже если речь об отметках в местах, где ты часто бываешь. Когда приложение запрашивает разрешение на доступ к твоей геолокации, подумай, действительно ли ему это нужно. Если нет (например, это приложение-фонарик), тогда такой доступ лучше не выдавать.

Домен

Домен — это уникальное имя сайта.

Сайтов в интернете очень много! У каждого есть собственное, неповторимое имя — домен. Он может состоять из букв, цифр и дефисов. Почему важно знать, что каждый домен — уникальный? Дело в том, что злоумышленники часто создают страницы, очень похожие на сайты разных компаний, например онлайн-магазинов или социальных сетей. Там они могут украсть деньги и конфиденциальную информацию, если люди вовремя не заметят подделку. Вот только использовать настоящий домен для фальшивых страниц они не могут. Поэтому всегда проверяй название домена прежде, чем оставить на сайте личную информацию (в том числе логин и пароль от входа в аккаунт). Если доменное имя отличается от настоящего даже на одну букву, не стоит ничего вводить на таком сайте. Интересный факт: в 1994 году был зарегистрирован первый сайт с доменом, оканчивающимся на .RU, — этот год принято считать началом рунета.

Единица

Единица — это значение (символ) в двоичной системе счисления.

В компьютерах и других электронных устройствах используется двоичная система счисления. В ней всего две цифры — ноль и единица (0 и 1). Это значит, что информация хранится, обрабатывается и передаётся в виде последовательности только нулей и единиц. По сути они отражают одно из двух возможных состояний устройства: 0 (выключено) или 1 (включено). Буквы тоже могут быть представлены в двоичном коде.

Ёмкость

Ёмкость устройства (жёсткого диска, флешки, твердотельного накопителя (SSD)) — это объём данных, которые можно записать и сохранить на носителе.

Представь, что у тебя есть бутылка, в которую ты можешь налить определённый объём воды. В бутылку бóльшего размера получится налить больше воды. Похожим образом дело обстоит с ёмкостью устройства: чем больше ёмкость, например жёсткого диска или флешки, тем больше файлов можно там хранить. Такая вместимость — это и есть ёмкость устройства. Она обычно измеряется в мегабайтах (МБ), гигабайтах (ГБ) или терабайтах (ТБ). Это такие единицы измерения объёма информации.

Жёсткий диск

Жёсткий диск — это устройство, где хранятся файлы, то есть накопитель.

Жёсткий диск хранит данные, которые есть на устройстве: фото, видео, музыку и другие файлы. Когда говорят про жёсткий диск, то имеют в виду HDD — Hard Disk Drive. Жёсткие диски бывают внутренние (они находятся внутри компьютера) или внешние (их можно носить с собой, почти как флешку) и подключать к устройству. Некоторые могут называть жёсткими дисками и твердотельные накопители — SSD (Solid-State Drive), хотя это ошибка. У них могут быть одинаковые функции, но созданы они по разным технологиям.

Загрузка файла

Загрузка файла — это процесс копирования или переноса файлов из интернета или с внешнего носителя (диска, флешки) на устройство.

Если хочешь сохранить файлы на устройстве и иметь к ним доступ в офлайн-режиме, нужно их загрузить. Но следует быть осторожным, когда скачиваешь что-то из интернета или с внешнего носителя (флешки или диска). Вместе с бесплатной игрой, загруженной с сомнительного сайта или с неизвестно кому принадлежащей флешки, ты рискуешь скачать ещё и вредоносную программу. Поэтому для загрузки файлов используй только официальные сайты и попроси взрослых установить защитное решение, которое обеспечит безопасность твоего устройства.

Интернет

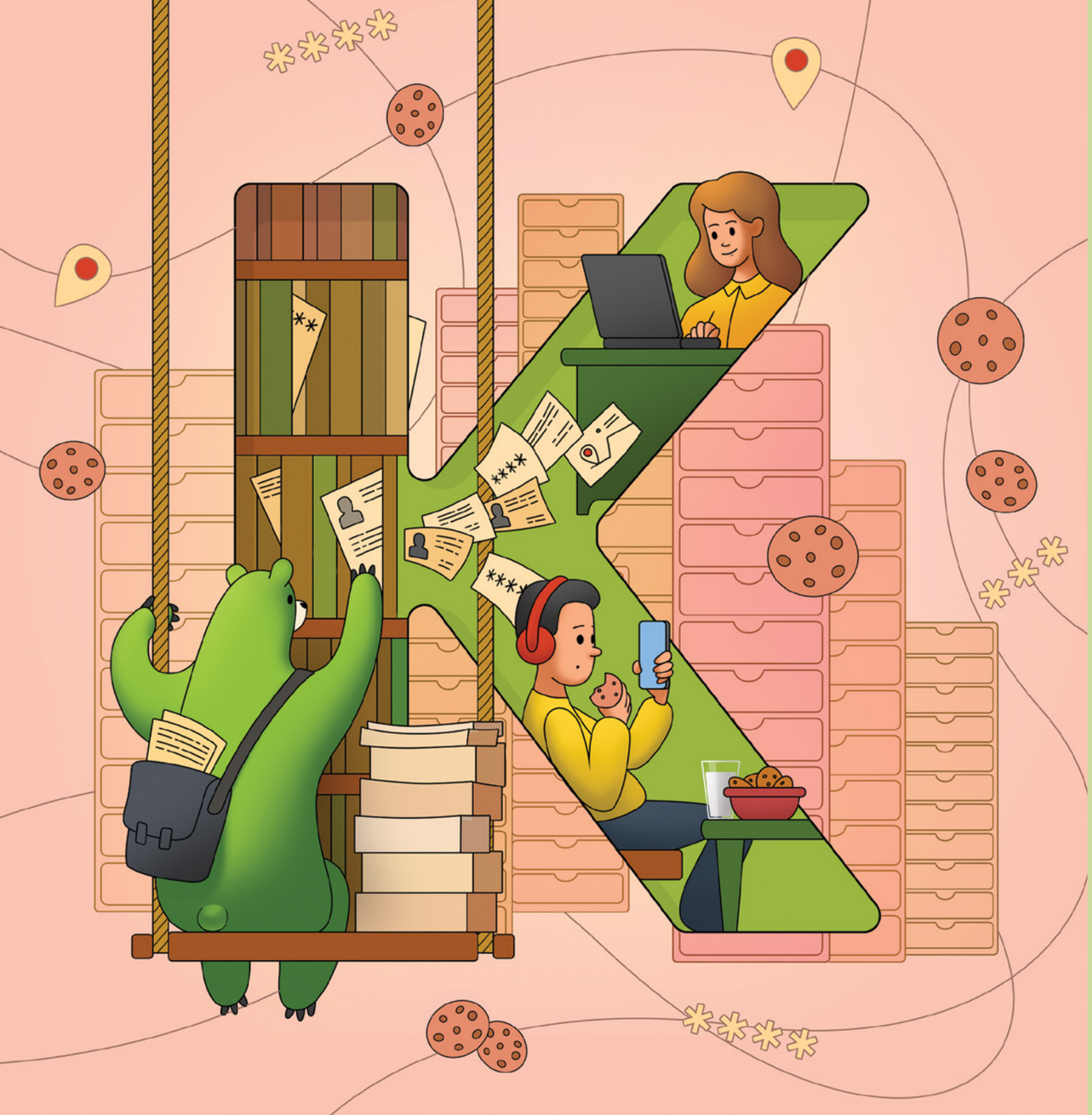
Интернет — это глобальная сеть, которая объединяет устройства по всему миру.

Благодаря интернету можно в любое время найти нужную информацию, поделиться ей, общаться с друзьями, слушать музыку, смотреть фильмы и делать много других интересных вещей. Только представь, количество разных устройств, подключённых к интернету, уже превышает число людей на планете! Интересный факт: первый сайт в интернете в том виде, в котором мы его знаем сегодня, был создан 6 августа 1991 года. Кстати, он доступен до сих пор.

Йоттабайт

Йоттабайт — это единица измерения объёма информации (очень-очень большого).

Компьютеры и другие гаджеты хранят наши данные: фотографии, видео, музыку, приложения. Объём памяти устройств и размер файлов обычно измеряется в байтах, мегабайтах, гигабайтах или терабайтах. А бывают йоттабайты. В одном йоттабайте 1 000 000 000 000 000 000 000 000 (септиллион) байт. Представь, сколько всего можно было бы загрузить в такое хранилище!



Куки-файлы (cookie-файлы)

Куки-файлы (cookie-файлы) — это небольшие фрагменты данных, которые формируются во время посещения веб-ресурсов.

Например, сведения о том, сколько времени человек провёл на сайте, с какого ресурса в интернете перешёл. С их помощью сайт запоминает информацию о посещении пользователя. Cookie в переводе с английского — печенье. О происхождении термина cookie-файлы есть несколько версий. Многие сайты встречают посетителей просьбой «принять файлы cookie». Зачем они нужны? Куки используются в качестве «памятки» о поведении пользователя на сайте. Благодаря им ресурсы в интернете могут запоминать информацию о пользователе, например, когда он заходил, какие настройки выставлял, какие разделы посещал. А ещё помогают «узнать» человека во время следующего посещения сайта, чтобы ему не пришлось заново выставлять настройки или авторизоваться.

Логин

Логин — это имя пользователя, с помощью которого он может получить доступ к аккаунту.

Логин помогает сайту или приложению «узнать» человека, чтобы он мог войти в аккаунт (авторизоваться). В качестве логина можно использовать имя, адрес электронной почты, номер мобильного телефона или никнейм (а что это такое — читай на странице 31). Помни, что логин (вместе с паролем) нужно держать в секрете. Не сообщай их посторонним, чтобы злоумышленники не смогли украсть твою учётную запись.

Машинное обучение

Машинное обучение — это способ решать задачи или создавать программы с помощью компьютера. В таком случае решение или программа создаётся компьютером на основе собранных данных, без непосредственного участия человека.

Часто программы обучаются на основе собранных данных, на примерах решения тех или иных задач человеком или другой программой. После такого обучения программы начинают выявлять закономерности и решать поставленные человеком задачи. К примеру, в «Лаборатории Касперского» ежедневно обнаруживают порядка 411 тысяч новых вредоносных файлов. Больше 99% из них обрабатывается различными автоматизированными системами, в том числе с применением машинного обучения, то есть без участия человека.

Никнейм

Никнейм — это имя пользователя в сети, обычно на форумах, в играх или чатах.

При регистрации в онлайн-сервисах, в том числе в онлайн-играх, необходимо придумать никнейм. Выдуманное имя должно быть уникальным и отличаться от имён других пользователей. С английского языка это слово переводится как «прозвище». Некоторые люди в качестве сетевого прозвища указывают настоящие имена и фамилии. А кто-то представляется выдуманными, например вдохновляется героями любимых мультфильмов, фильмов, компьютерных игр или книг, — поступать лучше именно так. В интернете вообще лучше оставлять как можно меньше личных данных.

Овершеринг

Овершеринг — это явление, когда мы рассказываем в интернете слишком много информации о себе.

Будь внимателен, когда оставляешь на сайтах личные данные — имя, дату рождения, номер телефона, адрес школы и геолокацию, а также другие сведения, например где работают родители. Информацию, которую выкладываешь в сеть, могут использовать посторонние в плохих целях. Прежде чем делиться чем-то с другими пользователями, подумай, стал бы ты рассказывать то же самое незнакомцам на улице? Важно бережно относиться не только к своим, но и к чужим личным данным. Например, не стоит делиться информацией о других людях без их согласия. Это один из принципов цифровой этики.

Пиксель

Пиксель — это элемент цифрового изображения, который обычно выглядит как точка на экране.

Всё, что ты видишь на экране, состоит из пикселей. Любое изображение, видео, текст — всё это сочетание маленьких точек, которые формируют общую картинку. Размер и количество пикселей на экране определяют его разрешение. Чем больше пикселей, тем более подробное изображение ты можешь увидеть, тем больше деталей получится показать. Обычно пиксель представляют квадратным, но на самом деле его форма зависит от соотношения сторон и технологии производства дисплея.

Резервная копия

Резервная копия — это копия данных (например, файлов), которые пользователи не хотят потерять.

Представь, если бы у тебя была возможность возвращать потерянные вещи, обратившись в специальное хранилище, — как было бы здорово! На устройствах такая опция есть, она называется резервное копирование. Это процесс создания копий различных данных: фото, видео и других файлов — на случай, если с ними что-то случится, например если устройство окажется заражено программой-шифровальщиком. Используя такие программы, злоумышленники шифруют данные пользователей и требуют деньги за расшифровку. Специалисты по кибербезопасности рекомендуют регулярно делать резервное копирование важных файлов, чтобы уберечь данные от потери.

Спам

Спам — это нежелательные сообщения, которые могут распространяться по электронной почте или в мессенджерах. А ещё существуют спам-звонки.

Иногда на почту приходят письма, которые являются нежелательными. Это и есть спам. Такие сообщения могут приходить и в мессенджерах или в виде звонков по телефону. Спам бывает опасным: некоторые сообщения могут оказаться мошенническими или содержать фишинговую ссылку. Важно быть осторожным и ни в коем случае не переходить по ссылкам из подозрительных сообщений. Если хочешь снизить количество спама в своей жизни, обращай внимание, где оставляешь адрес электронной почты или номер телефона. Защитные решения помогают бороться со спамом в том числе с помощью технологий машинного обучения. Помнишь, что это такое?

Кстати, термин «спам» имеет необычное происхождение и изначально не был связан с информационными технологиями, о нём (как и о многих других вещах) можно узнать в интернете.

Троянец

Троянцы — это вредоносные программы, которые маскируются под реальные или полезные приложения, но на самом деле могут причинить много вреда устройствам и данным.

Троянцы, как правило, маскируются под популярные приложения (прямо как в легенде о троянском коне, как-нибудь попроси родителей рассказать тебе про него). Злоумышленники могут распространять их под видом игр, приложений социальных сетей, мессенджеров и не только. Такие программы используются злоумышленниками, например, для кражи данных или слежки за пользователями. Столкнуться с троянцем можно на сомнительных сайтах. Если тебе предлагают бесплатно скачать ещё не вышедшую версию игры, требуют установить какую-либо программу, запугивая потерей денег или доступа к данным, — скорее всего, это злоумышленники. Крайне щедрые предложения лучше игнорировать и пользоваться только проверенными сайтами. Чтобы защититься от троянцев, важно использовать надёжные защитные решения, в том числе на мобильных устройствах.

Уязвимость

Уязвимость — это ошибка или недостаток, например в компьютерной программе, позволяющие злоумышленнику получить доступ к компьютеру.

Уязвимости и недоработки в программах встречаются нередко, ведь код пишет человек, а человек может ошибаться. Если злоумышленники найдут такие уязвимые места, они могут использовать их для заражения устройства вредоносной программой. Чтобы этого не произошло, специалисты по кибербезопасности рекомендуют регулярно обновлять установленные приложения и операционную систему. Вместе с этими обновлениями разработчики выпускают патчи — программные заплатки, которые закрывают обнаруженные уязвимости.

Фишинг

Фишинг — это вид онлайн-мошенничества, когда злоумышленники обманом пытаются украсть конфиденциальную (секретную) информацию человека или его платёжные данные.

Злоумышленники распространяют в интернете опасные ссылки. Они, в свою очередь, могут вести на фишинговые страницы, на которых данные человека могут украсть. Такие страницы могут быть очень похожи на знакомые нам сайты социальных сетей, онлайн-магазинов — поэтому их бывает сложно отличить от настоящих. Вот только использовать настоящее название сайта в адресной строке злоумышленники не могут. Поэтому прежде, чем вводить данные на сайте, обращай внимание на его доменное имя. Если оно отличается от привычного, стоит насторожиться. Специальные антифишинговые технологии в защитных решениях помогают обезопасить пользователей от этой угрозы. Если человек попытается перейти на поддельную страницу, они предупредят, что сайт небезопасный.

Хакер

Хакер — это человек, который использует свои знания и навыки для обхода систем компьютерной безопасности в определённых целях.

Как думаешь, какая связь между хакерами и головными уборами? На самом деле существует как минимум два вида хакеров: white hat и black hat. Первые — белые шляпы (white hat) — этичные хакеры, то есть программисты, которые специализируются на тестировании безопасности компьютерных систем или просто — специалисты по кибербезопасности. Вторые — чёрные шляпы (black hat) — это злоумышленники, которые обходят системы безопасности в своих целях. В массовой культуре за хакерами закрепилось второе значение.

Цифровая приватность

Цифровая приватность — это право на то, что твои личные и конфиденциальные данные в сети недоступны посторонним.

Зачастую человек сам нарушает свою цифровую приватность, например когда публикует очень много данных о себе в открытом доступе (личные фотографии, информацию о родителях, номер телефона), в том числе в социальных сетях. Помнишь, мы говорили про овершеринг? Когда цифровая приватность человека нарушена и его данные оказались доступны посторонним, этим могут воспользоваться злоумышленники, например с целью мошенничества. А теперь посмотри внимательно на свою страницу в социальной сети (если она у тебя есть): какие данные там размещены? Хотел бы ты, чтобы эту информацию знали посторонние люди?

Чат-бот

Чат-бот — это программа, которая отвечает на вопросы человека, «общается» с ним.

Ты замечал на сайтах всплывающее окно с предложением помощи? Скорее всего, это и был чат-бот! Конечно, строго говоря, это не общение, в привычном нам понимании. Такая программа лишь реагирует на заложенные в неё сценарии. Например, если человек вводит номер заказа на сайте магазина, чат-бот помогает понять статус его доставки. Чат-бот может быть полезен, чтобы быстро получить ответ на вопрос или решить проблему. Но существуют и другие цифровые помощники, которые могут выполнять более сложные задачи. В последнее время много интереса вызывают умные чат-боты, то есть те, что работают на основе нейросетей. Они могут обрабатывать большое количество информации, доступной в интернете, и имитировать человеческое общение по переписке. Однако сегодня с такими чат-ботами следует быть осторожными, они часто могут ошибаться: путать факты или даты, давать некорректные советы.

Шифрование

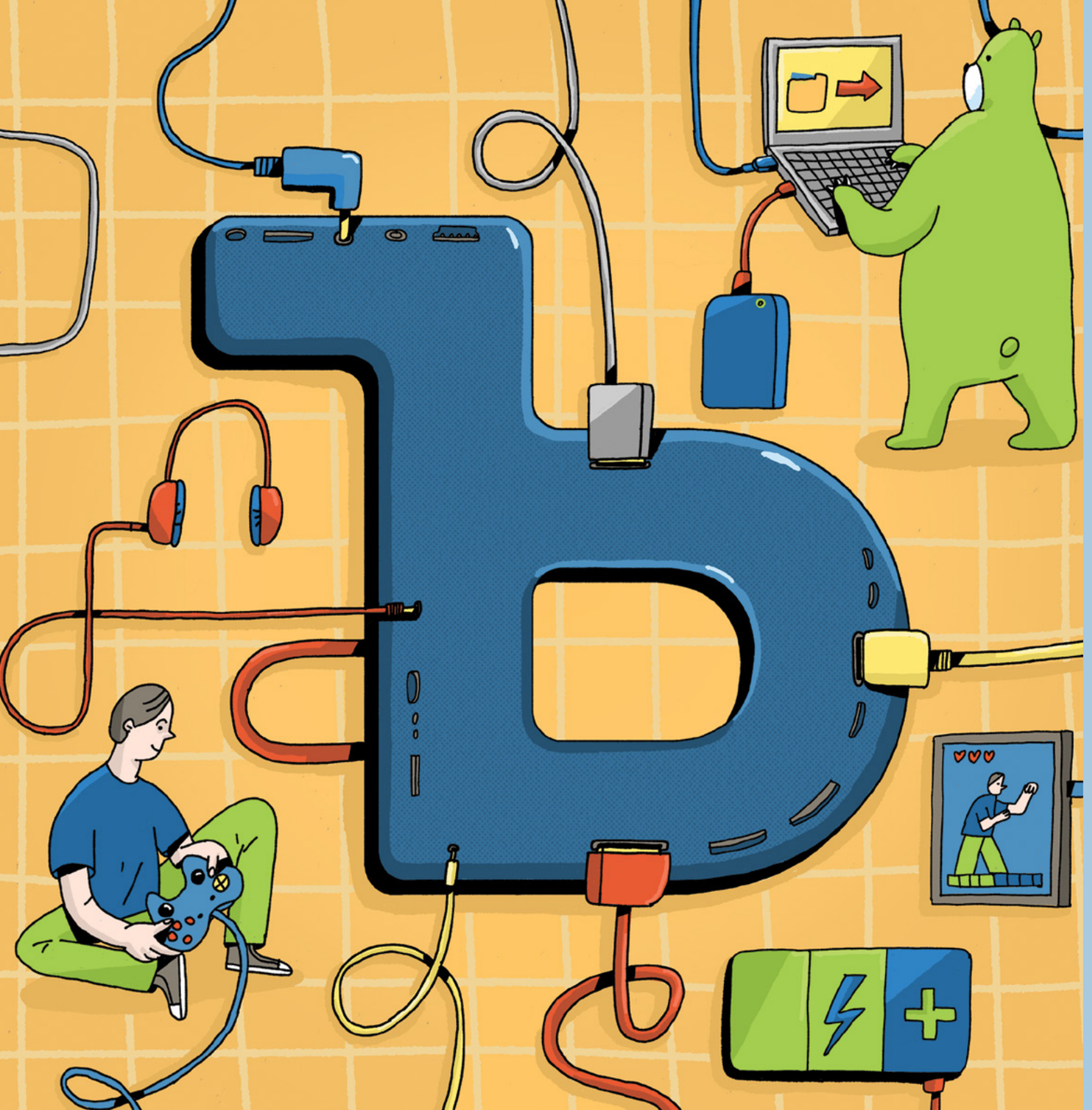
Шифрование — это процесс преобразования данных (например, понятного нам текста) в то, что на первый взгляд кажется случайным набором символов (шифр).

Когда люди шифруют данные, они хотят преобразовать их так, чтобы только определённые пользователи получили к ним доступ — те, у которых есть ключ или дешифратор. Без специального ключа преобразовать зашифрованную информацию, например в понятный текст, почти невозможно. Многие сайты и приложения используют средства шифрования, чтобы защитить наши данные. В большинстве мессенджеров используется сквозное шифрование. Это значит, что переписка между людьми приватная, она расшифровывается только на их устройствах.

Защитное решение

Защитное решение — это программа, которая помогает защитить цифровые данные и деньги человека, а также его устройство от различных кибератак и онлайн-мошенничества

В нём нуждаются многие наши устройства, не только настольные компьютеры и ноутбуки. Защищать смартфоны и планшеты также важно — они всегда с нами, в них все наши фотографии, переписки и другие личные данные. Надёжное защитное решение позаботится о безопасности устройства: не даст установить вредоносные программы, защитит личные данные и предложит много других полезных функций, например предупредит, если звонят мошенники или спамеры.



Разъём

Разъём — это устройство, с помощью которого можно соединить один гаджет с другим или передавать данные с устройства на устройство.

Обычно разъём состоит из вилки (где выступают штыри) и розетки (в которой находятся углубления для штырей). Однако бывают и другие варианты. Разъёмы бывают разных видов и предназначены для разных целей. Например, разъём для питания нужен, чтобы заряжать устройства, а разъём для наушников — чтобы слушать аудиозаписи или смотреть фильмы, не отвлекая людей вокруг.

Гиперссылка

Гиперссылка — это элемент (текст, иконка) при клике на который открывается определённый веб-ресурс.

Гиперссылки быстро переносят тебя на нужную страницу в интернете или в текстовом документе, позволяют скачать файл. Выглядеть они могут по-разному: как выделенный синим подчёркнутый текст, кнопка или картинка. Будь аккуратен с гиперссылками, которые присылают в мессенджерах или на электронную почту, — сразу же кликать по ним не стоит, иначе рискуешь столкнуться с неприятностями. Гиперссылки бывают «битыми» — такие ссылаются на отсутствующий объект (например, удалённый файл) или не существующий в интернете ресурс.

Пароль

Пароль — это набор символов (букв, цифр и специальных символов), который используется для входа в аккаунт.

Проще говоря, это ключ для входа в аккаунт. Пароль — важный элемент защиты данных от злоумышленников. Чтобы к аккаунту не получили доступ посторонние, важно придерживаться нескольких правил создания паролей. Во-первых, они должны быть сложными: содержать не менее 12 знаков, включая маленькие и большие буквы, цифры и специальные символы. Ещё одно правило — каждому аккаунту свой уникальный пароль. Если злоумышленник вдруг сможет получить доступ к одному аккаунту, остальные будут в безопасности. И, конечно, не стоит хранить пароли на листочках или в заметках на телефоне. Используй для этого специальные программы — менеджеры паролей. Такая есть, например, у «Лаборатории Касперского».

Электронная почта

Электронная почта — это технологии и сервисы, которые позволяют отправлять и получать письма, фотографии и другие файлы.

В наше время почта стала неотъемлемой частью коммуникации. Благодаря ей можно легко обмениваться письмами с людьми по всему миру. Её часто используют в учебных целях: учителя высылают на почту задания и материалы или сообщают важную информацию. Адрес электронной почты можно использовать в качестве логина, чтобы регистрироваться в различных сервисах, например социальных сетях, на образовательных и игровых платформах. Вот только отправить по почте большие файлы не получится — почти у всех почтовых сервисов есть ограничения по размерам файлов или писем. В таких случаях файл можно загрузить в облачное хранилище или на флешку.

Юзер

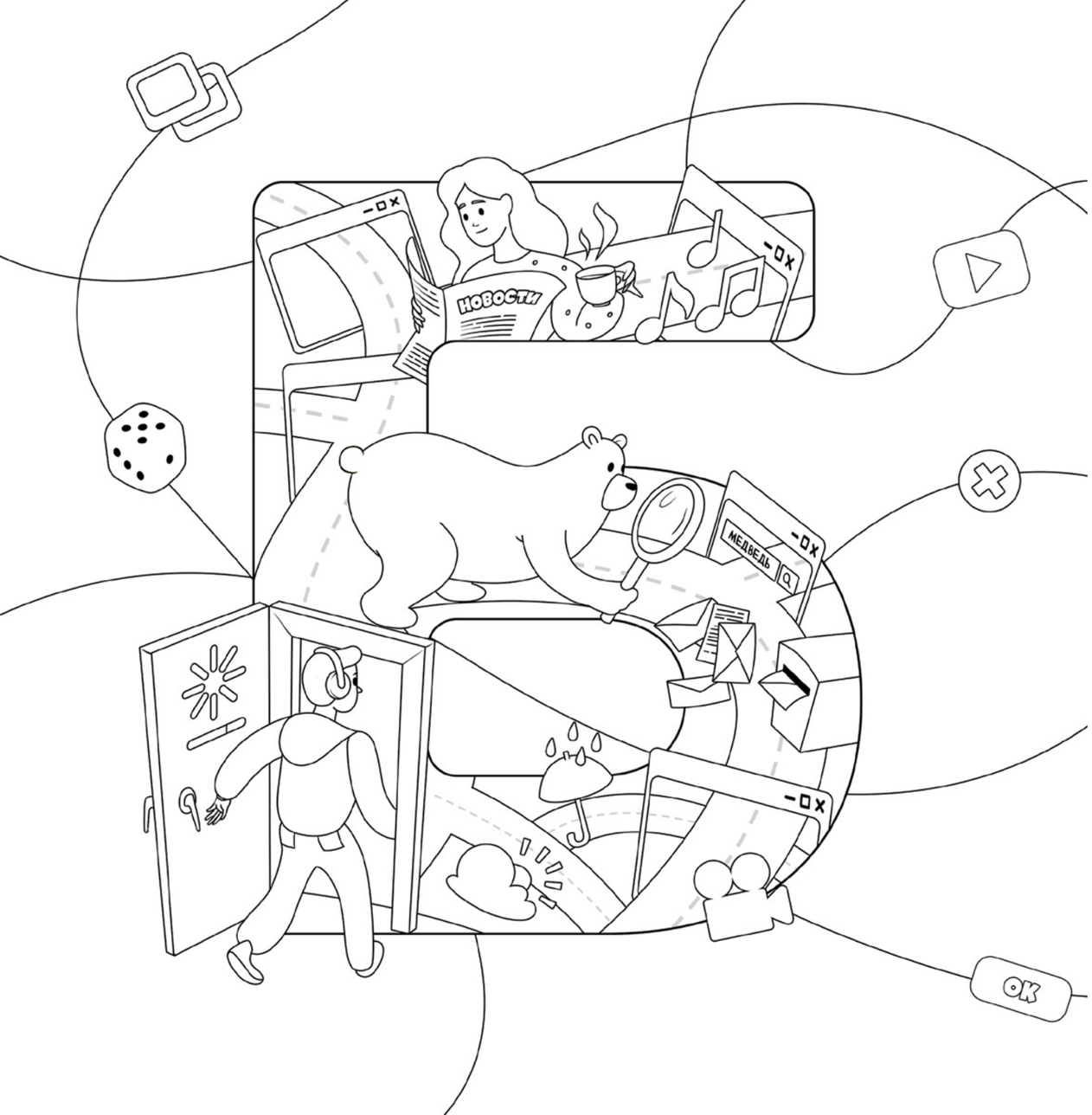
Юзер — это пользователь компьютера, смартфона или другого устройства.

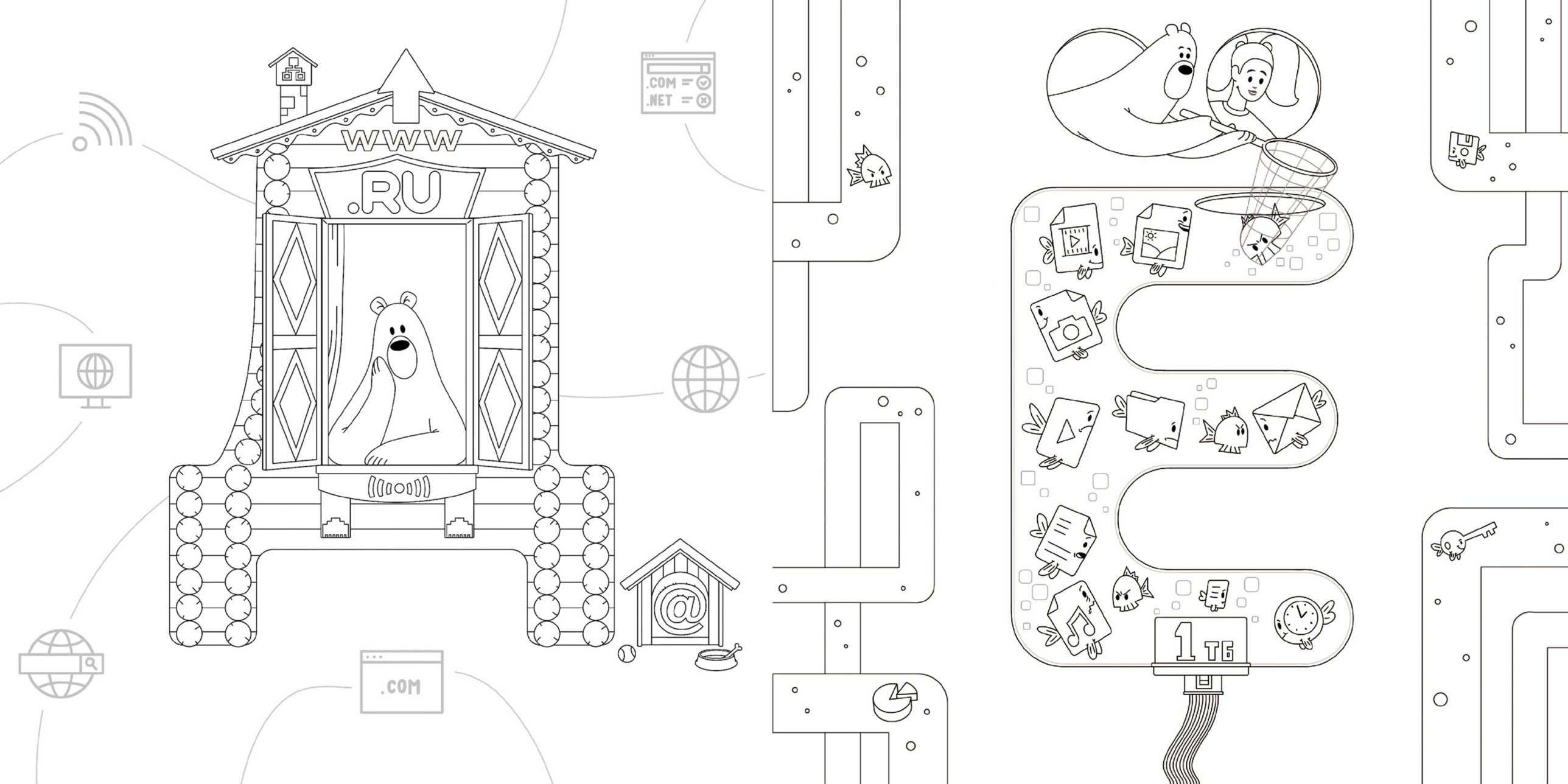
Слово «юзер» переводится с английского языка буквально как «пользователь». Если ты умеешь обращаться с гаджетами — включать и выключать их, отправлять сообщения, искать в интернете нужную информацию, поздравляем, ты уже юзер! Однако мало уметь пользоваться девайсами, современным юзерам важно знать основы цифровой грамотности и цифровой этики. Цифровая этика, или сетевой этикет, — это правила общения в интернете. Например, прежде чем поделиться в интернете фотографией, на которой изображен другой человек, нужно спросить у него разрешения. Это и есть пример соблюдения цифрового этикета.

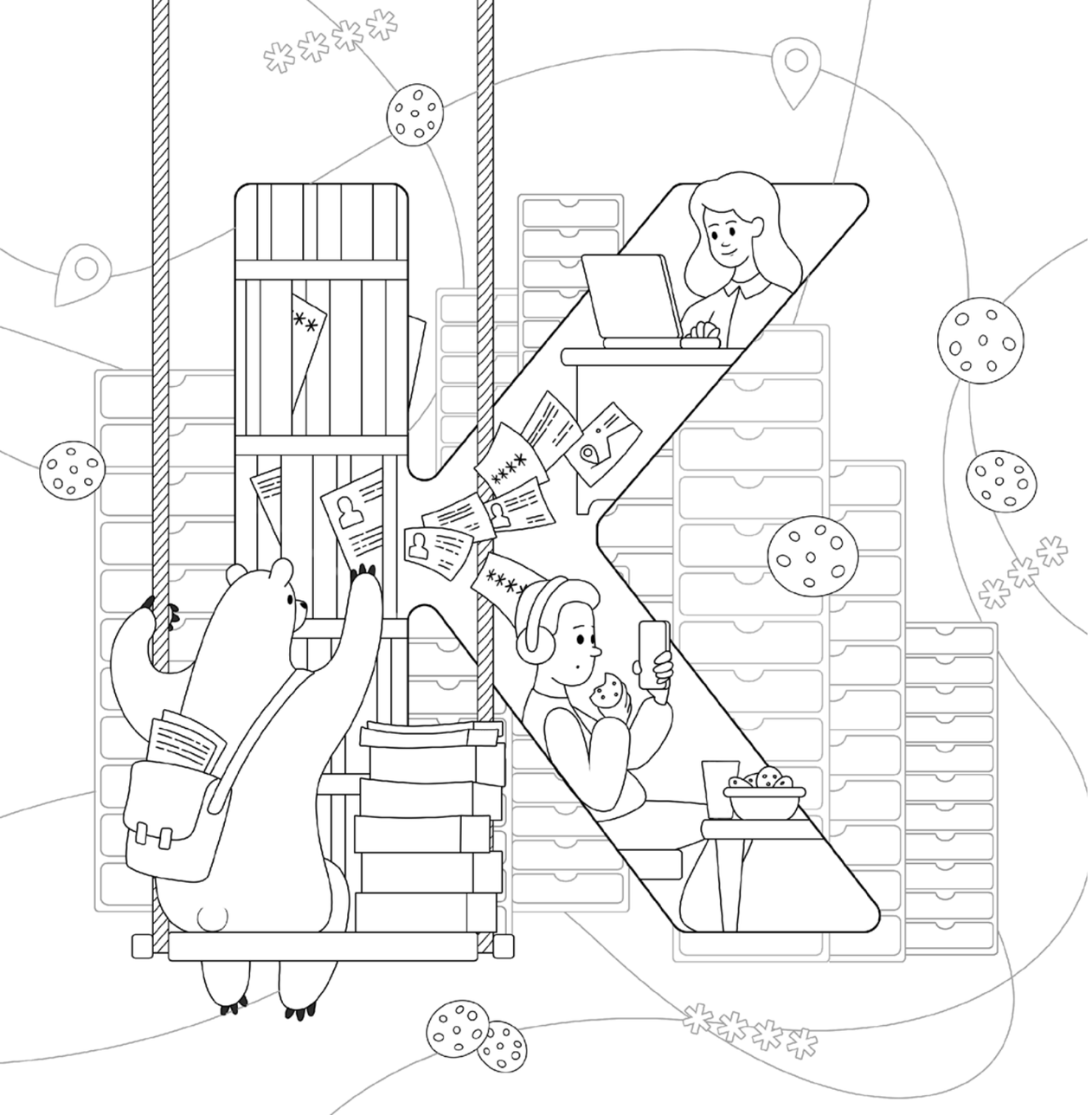
Язык программирования

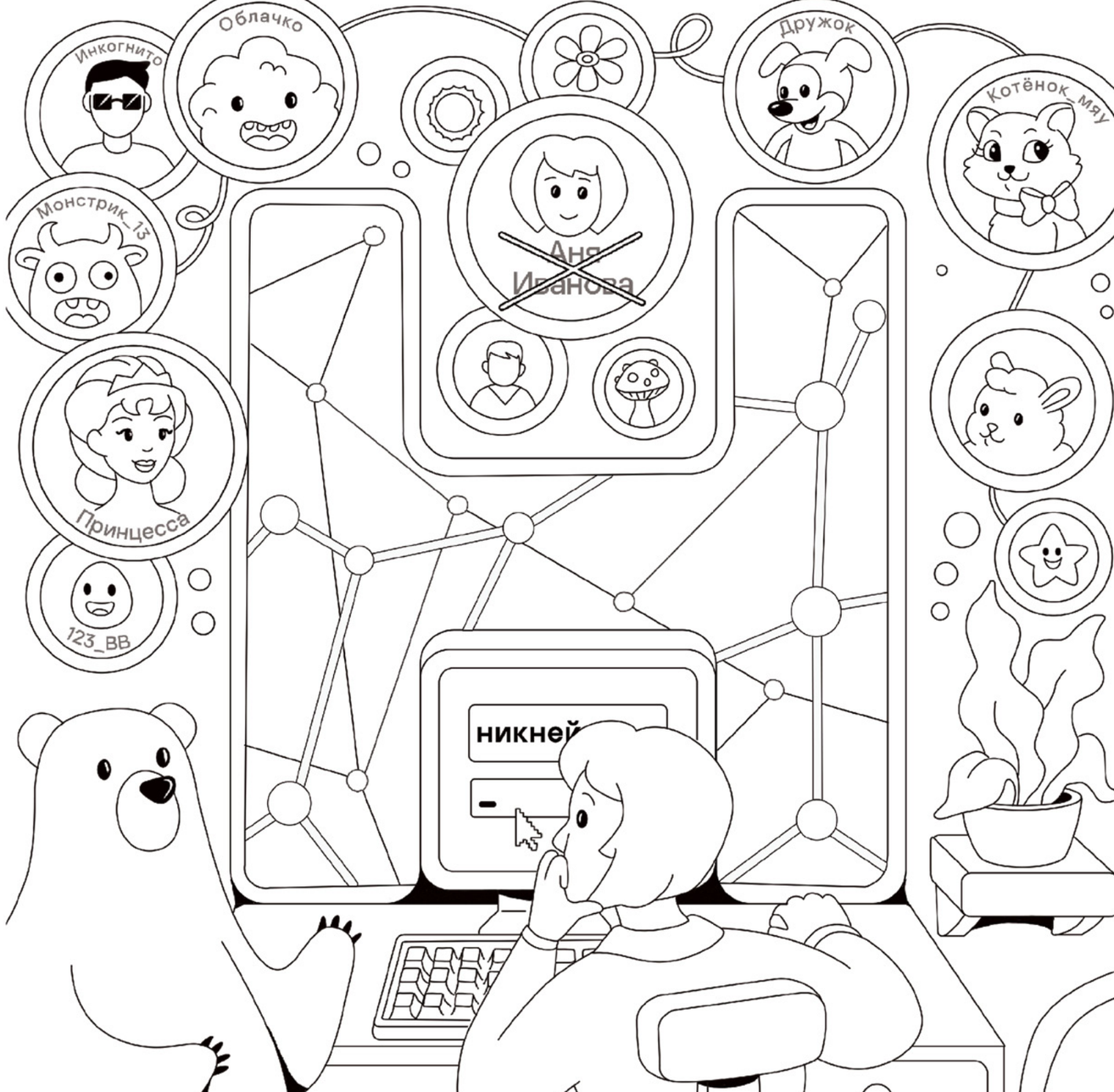
Язык программирования — это язык, который используется для написания программ.

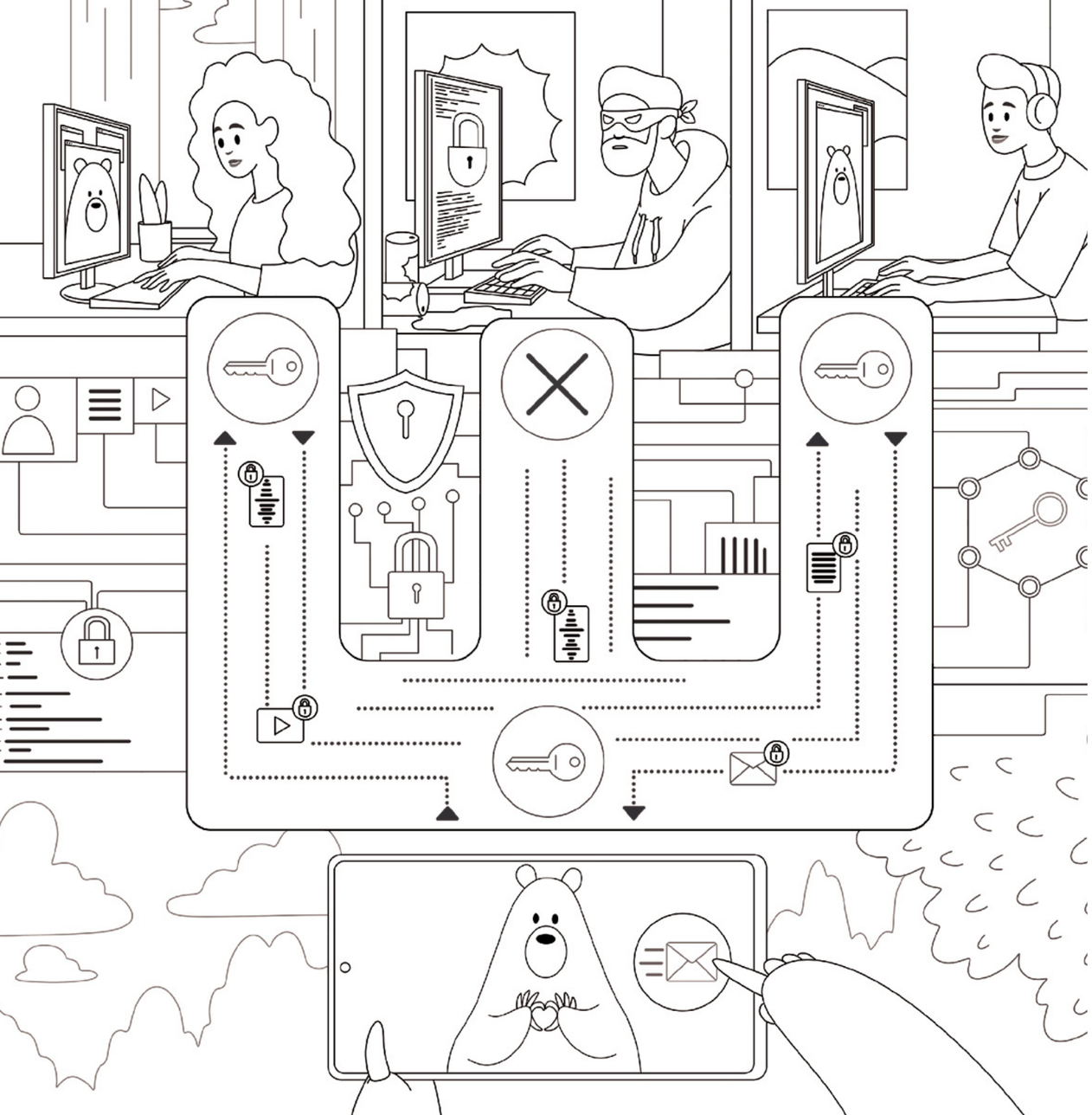
Программы, игры, приложения и сайты, которые мы используем каждый день, создаются именно с помощью таких языков. Человечество придумало уже более 8 тысяч языков программирования. Среди самых популярных на сегодняшний день можно выделить, например, Java, JavaScript, Kotlin, C/C++, C#, Golang, Python.

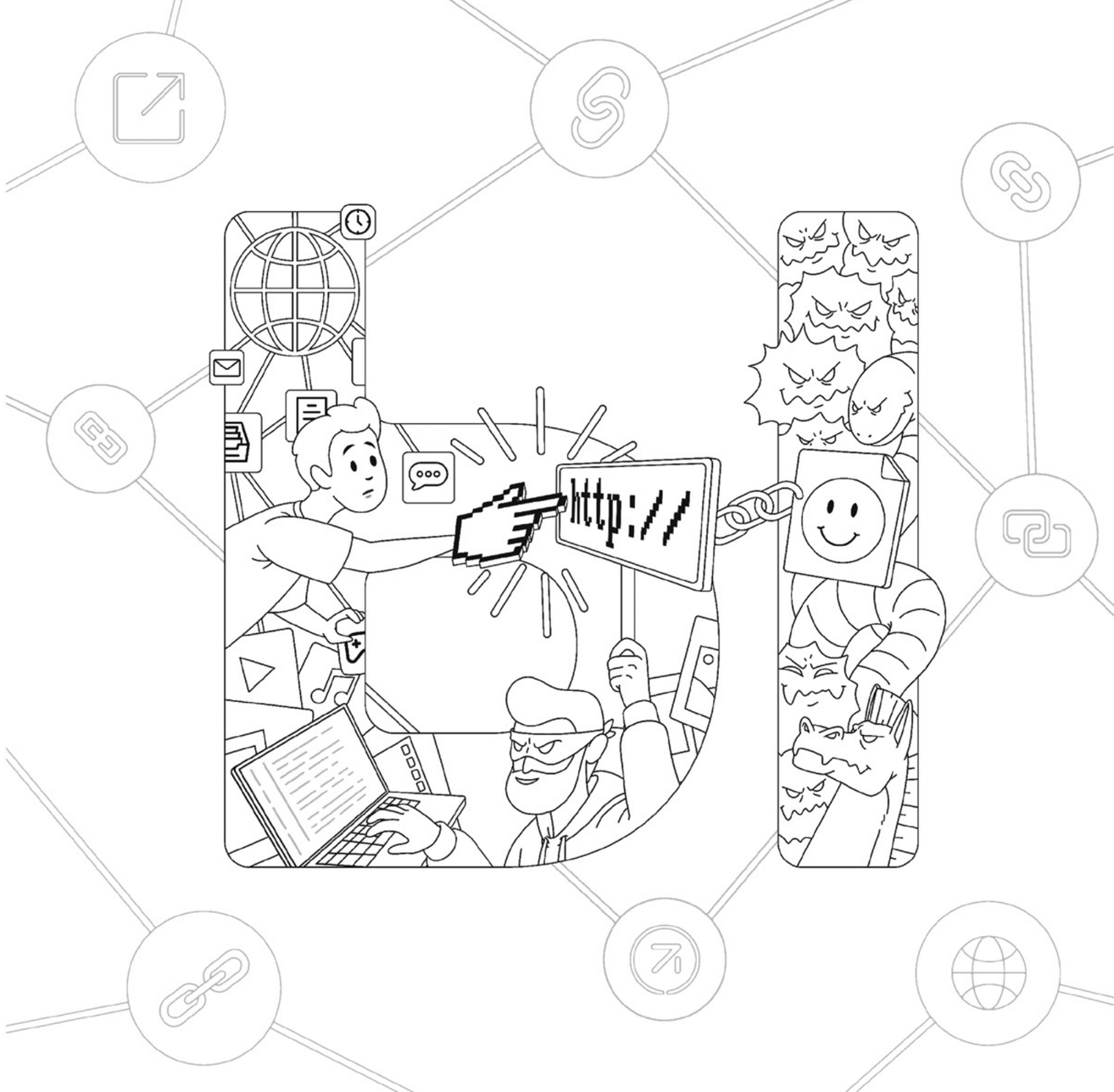

НОВОСТИ
МЕДВЕДЬ
ОК


WWW
.RU
.COM
.NET
.COM
1 ТБ




Инкогнито
Облачко
Дружок
Котёнок_мяу
Монстрик_13
Аня Иванова
Принцесса
123_ВВ
никней




http://

Заметки

Дорогой кибериссследователь,
надеемся, тебе было интересно читать эту необычную азбуку. Впереди тебя ждет ещё много открытий, ведь твои приключения в цифровом мире только начинаются. Задавай вопросы, проси старших помочь разобраться с непонятным, читай азбуку вместе с друзьями и перечитывай её с родителями.
И помни о важных правилах цифровой безопасности:

- старайся не рассказывать о себе, своей семье и друзьях в интернете слишком много;
- придумывай сложные длинные и уникальные пароли, в которых есть и цифры, и буквы, и специальные символы;
- скачивай приложения только с официальных сайтов или из официальных магазинов приложений;
- несколько раз подумай, стоит ли перейти по ссылке из сообщения, даже если там обещают что-то очень интересное.

Дизайн книги выполнен в студии Мыслеформа: www.behance.net/Thoughtform
Арт-директор и менеджер проекта: Илья Калимулин.
Иллюстраторы: Евгений Паненко, Наталья Ермолаева, Дмитрий Коротченко, Роман Шипунов, Наталья Шилова, Андрей Лебединский, Юрий Волкович, Мария Фадеева, Даниил Шубин, Марк Никитин, Ольга Терехова, Алексей Крапивин, Маргарита Солианова, Ольга Марковская