Глава 1

Цифровые иммигранты и цифровые аборигены

В этой главе мы поговорим о том, чем отличается отношение к цифровым технологиям у взрослых и у молодого поколения, и о том, как учитывать эту разницу в восприятии, чтобы понимать друг друга. Также коротко перечислим возможные неприятности, случающиеся в цифровом мире, которые подробно рассмотрим в следующих главах.

Когда-то, давным-давно, когда нынешние учителя и родители школьников еще сами ходили в школу, никаких айфонов не было и в помине, и далеко не в каждом доме был интернет. Без повсеместного доступа к Всемирной паутине наше детство не слишком сильно отличалось от детства наших бабушек и дедушек, и даже пра-пра-бабушек и пра-пра-дедушек. За книгой нужно было идти в библиотеку, а за редкой книгой иной раз даже ездили в другой город. Чтобы пообщаться с друзьями, мы ходили в гости, а услышав что-то важное по радио, немедленно записывали это, чтобы не забыть. Расплачивались только наличными, а письма писали на бумаге, запечатывали в конверты и опускали их в почтовый ящик.

Мы застали уникальный период в истории цивилизации, когда за короткое время изменилось буквально все. Отсчет новой эры начался с появления айфона в 2007 году. Простота и естественность его интерфейса впервые позволили маленьким детям пользоваться компьютером самостоятельно — без помощи взрослых. А то, что со смартфона можно было еще и позвонить, стало рассматриваться подрастающим поколением лишь в качестве дополнительного бонуса. Телефонные звонки для молодежи — не самая главная функция.

Смартфон стал ключом ко всему, что можно найти в интернете, — а найти в нем можно все. Как явление интернет сравним разве что с изобретением книгопечатания в XV веке, когда каждому образованному человеку стали доступны почти все сокровища, ранее скрытые в монастырских библиотеках.

По средневековым меркам распространение печатных книг произошло практически мгновенно, хотя в действительности

процесс занял довольно продолжительное время. Иоганн Гутенберг изобрел метод книгопечатания около 1450 года. Через 50 лет в Германии работало свыше 50 типографий, в которых трудились 200 печатников. А во всей Европе к тому моменту насчитывалось до 1000 печатников, которые до конца XV века в целом издали около 30 тысяч книг — так называемых инкунабул. Первая же газета в привычном для нас формате появилась лишь в XVII веке. Таким образом, технология книгопечатания достигла зрелости через 150 лет после своего изобретения («Википедия»).

С момента изобретения телефона в 1876 году до массовой телефонизации в XX веке прошло почти сто лет, телевизоры пришли в наши дома в течение полувека. А затем все неимоверно ускорилось. Мобильные телефоны прошли путь от символа высокого статуса до ширпотреба лет за двадцать, доступ в интернет стал массовым явлением в течение десятка лет, iPhone завоевал сердце массового потребителя за год с небольшим, а iPad стал мегапопулярным всего за несколько месяцев. Теперь каждая новинка распространяется по планете со скоростью вируса гриппа, и есть все основания полагать, что так будет продолжаться и впредь.

У наших предков было время приспособиться к переменам, потому что изменения происходили медленно — на протяжении нескольких поколений. Нас же накрыло цифровой волной внезапно. Слова, которые еще совсем недавно могли вызвать, по меньшей мере, недоумение — например, «позвольте я вас сфотографирую на телефон», сегодня всеми воспринимаются как должное. Новые технологии распространяются настолько быстро, что никакие учебники и образовательные программы за ними не поспевают, и нам приходиться учиться на ходу.

«Нужно беспокоиться, когда что-то развивается слишком быстро. Не потому, что рост — это плохо, а потому, что прежние наработки не сохраняются. Если эволюция будет слишком быстрой, то некоторые виды вымрут». Эти слова принадлежат Нассиму Николасу Талебу, почетному профессору Нью-Йоркского университета в области управления рисками.

Да, мы более или менее приспособились к новому миру, но мы все равно в нем чужие. Мы — цифровые иммигранты[1], которые перебрались сюда из своего «теплого лампового» мира. Как известно, базовые навыки восприятия формируются в раннем возрасте, а в нашем детстве гаджетов не было и в помине. Поэтому, как бы мы ни старались стать «цифровыми», нам все равно не достичь такой легкости в пользовании гаджетами, какую мы наблюдаем у детей.

Современные дети — цифровые аборигены, родившиеся со смартфоном в руке. Они не представляют, зачем ехать в кассу, чтобы купить билет на поезд или самолет. Они не верят авторитетам и ставят под сомнение любые ваши слова. А пока вы напрягаете память, чтобы вспомнить дату Ледового побоища (1242 год, если кто забыл) или количество хромосом у морского ежа (на всякий случай, их 42), они успевают посмотреть все ответы в Сети и приготовиться поймать вас на любой неточности. Иногда это раздражает, иногда удивляет — но это совершенно другой способ познания мира, к которому нам трудно привыкнуть.

---

1 Термины «цифровые аборигены» и «цифровые иммигранты» были введены организацией Electronic Frontier Foundation в 1996 году в рамках Декларации независимости киберпространства (https://www.eff.org/cyberspace-independence) и популяризированы консультантом по образованию Марком Пренски в статье «Аборигены и иммигранты цифрового мира».
Digital Natives, Digital Immigrants. // On The Horizon (MCB University Press, Vol. 9 № 5, октябрь 2001 г.) © 2001 Marc Prensky.

В этом свете вечная проблема отцов и детей заиграла миллионами цифровых оттенков. Герои Тургенева спорили о путях развития страны, о материализме и идеализме, о знании науки, понимании искусства и отношении к народу. Но жизнь их от поколения к поколению мало менялась: они учились по одним и тем же учебникам, читали газеты, ездили на лошадях. К сегодняшнему же дню конфликт поколений изрядно помолодел, усложнился и сместился практически на уровень начальных классов. Несомненно, первоклашек еще не волнуют высокие материи, но зато у них уже есть собственное представление о том, как добывать информацию. А школа все еще пытается научить их методам, которые использовались в XIX веке.

> *«Школьники и студенты стали совсем другими, — писал Марк Пренски в 2001 году. — Сегодняшние учащиеся — больше не те люди, для которых была создана наша система образования. Мы родились до цифровой эпохи, но впоследствии были очарованы новым миром и многое в нем приняли. Тем не менее, по сравнению со школьниками мы навсегда останемся «цифровыми иммигрантами».*

Может быть, автор излишне драматизирует? Конечно, тонким перышком в тетрадь уже никто не пишет — мы давно перешли на авторучки, но все остальное-то не изменилось: про глагол и про тире, и про дождик на дворе, к четырем прибавить два — и так далее. Да, но где же про интернет и про смартфон, про YouTube и про Питон[1]? Сайты нужные любить, на плохие не ходить? Крепко-накрепко дружить, но внимательными быть — мало ли кто там? Школа считает цифровые

---

1 *Python — язык программирования, который одним из первых рекомендуют для изучения детям. Правильно произносится «пайтон», но в русском языке прижилось произношение «питон».*

технологии чем-то очень сложным, что следует изучать в рамках отдельного предмета, потому что для большинства учителей цифровые технологии действительно сложны. И вроде бы учителей они не касаются напрямую. Про острова и города мы говорим на географии, а в Google Earth ученики как-нибудь сами разберутся. В результате цифровая жизнь детей фактически изгоняется из школы, и они оказываются с ней один на один — вместе со всеми опасностями, которые существуют в интернете.

Марк Пренски обратил внимание на эту проблему еще двадцать лет назад. Но и сегодня нельзя сказать, что за прошедшие годы ситуация кардинально изменилась:

> *«Единственной проблемой становления нового формата образования является то, что наши преподаватели — цифровые иммигранты. Они говорят на архаичном языке доцифровой эпохи, изо всех сил старясь учить поколение, говорящее на совершенно новом языке. Цифровые аборигены часто воспринимают школу именно так: к местным жителям пришел невразумительный иностранец с сильным акцентом и собирается их чему-то научить. Вот аборигены часто и не понимают, что им говорит иммигрант».*

Наверное, можно было бы воспользоваться идеей Льва Толстого, который объединил в своей «Азбуке» все, что было нужно для обучения детей начальной грамотности — чтение, письмо и арифметику. Первое издание «Азбуки» вышло в 1872 году. А через три года доработанный вариант под названием «Новая Азбука» был рекомендован Министерством народного просве-

щения в качестве учебника для народных школ России. Еще при жизни автора пособие было переиздано 28 раз. Правда, под давлением критиков из новой редакции была исключена арифметика — во времена Толстого школа тоже была очень консервативной и отвергла его новаторскую идею.

Если бы Лев Николаевич писал «Азбуку» в наши дни, наверняка включил бы в нее и азы цифровой грамотности, ведь он задумывал свой учебник как минимальный набор знаний, необходимый человеку для нормального существования в современном ему обществе. И, наверное, точно также нашлись бы критики, требующие строго научного подхода в ущерб цельности. Что, в общем-то, мы и имеем.

Цифровизация школы, вне всякого сомнения, неизбежна. Но очевидно, что это случится еще нескоро. Поэтому пока в вопросах кибербезопасности нужно полагаться на свои силы и строить свою собственную цифровую крепость.

Родители и дети в цифровую эпоху

В начале нулевых годов на волне всеобщей эйфории от взрывного распространения интернета бытовало мнение, что дети — цифровые аборигены — обладают некими врожденными навыками и способны освоить цифровые технологии без помощи взрослых. Как и следовало ожидать, это была иллюзия. То, что дети безвылазно находятся в онлайне, еще не означает, что у них есть реальное представление о том, как применять цифровые инструменты наилучшим образом.

То, что дети безвылазно находятся в онлайне, еще не означает, что у них есть реальное представление о том, как применять цифровые инструменты наилучшим образом.

В большинстве своем они пользуются интернетом для решения самых примитивных задач — для общения в социальных сетях, просмотра видео и многого другого. Чуда не произошло. Одного только рождения в цифровую эпоху оказалось недостаточно для овладения ее технологиями, и мы встали перед фактом, что цифровых аборигенов тоже необходимо учить.

Строго говоря, цифровые аборигены и иммигранты — всего лишь красивая метафора, а не научная теория. К тому же, как нетрудно догадаться, в силу естественных причин существующее положение вещей не будет сохраняться вечно. После того, как первые цифровые аборигены повзрослеют и обзаведутся собственными детьми (что уже происходит), непонимание между поколениями уменьшится. А когда они станут бабушками и дедушками, то круг и вовсе замкнется — цифровых иммигрантов не останется.

Означает ли это, что проблема компьютерной грамотности и цифровой гигиены решится сама собой? Вовсе нет. Как и во всех других аспектах воспитания, в том, что касается «цифры», ключевую роль играет семья. Какой пример показывают родители, такую модель и воспроизводят дети, — яблоко от яблони недалеко падает.

Какой пример показывают родители, такую модель и воспроизводят дети, — яблоко от яблони недалеко падает.

Взрослые — цифровые иммигранты — адаптировались к внезапным изменениям очень по-разному. Одни были творцами и активными участниками цифровой революции. Другие отнеслись к происходящему с пассивным принятием, без глубокого интереса, и стали простыми потребителями. Нашлись и неолуддиты, которые отвергают технические новинки и видят в распространении цифровых технологий только зло. Все они транслировали свои воззрения детям, а их дети — своим детям и так далее.

По данным исследования Александры Самюэль, проведенного в 2015 году среди десяти тысяч американских семей[1], три указанные выше категории родителей оказались примерно равными по численности. И важно отметить, что они отличаются не только в вопросе отношения к технологиям, но также и в вопросах ограничения детей в пользовании этими технологиями или, наоборот, помощи в их освоении.

Первую категорию можно назвать **наставники (digital mentors)**. Они активно помогают отпрыскам осваивать компьютер и смартфон, записывают их на занятия по программированию и робототехнике, беседуют о правилах ответственного и безопасного поведения в киберпространстве. В результате их дети, которых Александра Самюэль называет **цифровыми наследниками (digital heirs)**, со школьной скамьи умеют создавать сайты, мон-

---

1 *Александра Самуэль — технический стратег (tech strategist), исследователь, писатель и докладчик. Автор книги «Работай умнее с социальными сетями» («Work Smarter with Social Media», Harvard Business Review Press, 2015), регулярно пишет для The Wall Street Journal и The Harvard Business Review, а также выступает в качестве обозревателя по цифровым технологиям для JSTOR Daily.*
Alexandra Samuel. Parents: Reject Technology Shame. // The Atlantic, 4 ноября 2105.

тировать видео, писать программы, быстро находить нужный контент и адекватно вести себя в социальных сетях. Иными словами, эти детишки оказываются вполне подготовленными, чтобы в будущем занять хорошие рабочие места в цифровой экономике.

Вторую категорию составляют **потакающие родители (digital enablers)**. Эти папы и мамы пускают цифровое воспитание своих детей на самотек. Они позволяют детишкам сколько угодно времени проводить за экранами гаджетов, но при этом нисколько им не помогают в освоении этих устройств, поскольку сами не слишком в них разбираются. Поэтому их детей называют **цифровыми сиротами (digital orphans)**. Несмотря на отсутствие контакта с родителями, они могут вырасти достаточно подкованными в техническом плане, но, скорее всего, будут лишены коммуникативных навыков и знаний, необходимых для того, чтобы использовать онлайн-инструменты для решения реальных жизненных проблем.

Третья категория — **запрещающие родители (digital limiters)**. А их дети — **цифровые изгнанники (digital exiles)**. Из опасения, что цифровые устройства могут причинить ребенку вред, запрещающие родители жестко ограничивают детей в пользовании гаджетами, а некоторые сторонники ограничений доходят до крайности — вообще не позволяют детям пользоваться гаджетами до достижения подросткового возраста. И это чревато, ведь подростки в гораздо меньшей степени склонны слушать советы старших, и как только им представится возможность, они могут уйти в онлайн-жизнь с головой, пренебрегая опасностями этой жизни. Возможен и такой вариант, что они по примеру родителей станут добровольными изгоями в цифровом мире — и он тоже

грозит неприятностями. Современное общество еще может понять, если люди старшего возраста не разбираются в компьютерах, но когда в них не разбирается молодой человек, он рискует элементарно остаться без работы.

Исследование, которое в 2015 году провели EU Kids Online и Лондонская школа экономики (LSE)[1], выявило пять основных видов взаимодействия родителей с детьми в возрасте от 9 до 16 лет:

- *активное посредничество: обмен и обсуждение онлайн-деятельности;*
- *обеспечение безопасности: консультирование и руководство по управлению рисками;*
- *ограничения: правила и запреты;*
- *технический подход: использование фильтров, родительский контроль;*
- *мониторинг: проверка компьютера, социальных сетей, телефонов и прочего после использования.*

Также исследование обнаружило зависимость между моделью поведения родителей и их социально-экономическим статусом. Например, в семьях с низким доходом и низким об-

1 *Livingstone, S., Mascheroni, G., Dreier, M., Chaudron, S. and Lagae, K. (2015) How parents of young children manage digital devices at home: The role of income, education and parental style. London: EU Kids Online, LSE.*

разовательным уровнем дети сравнительно хорошо разбираются в цифровых устройствах. Но очень заметно, что они гораздо лучше владеют технологиями, чем родители. Особенно отчетливо поколенческий разрыв проявляется в семьях иммигрантов (обычных — нецифровых). Как правило, главы этих семейств ограничивают детей в пользовании гаджетами, хотя среди них встречаются и те, кто достаточно амбивалентен в этом вопросе.

В более образованных семьях, но также имеющих низкий доход (часто это неполные семьи), родители в вопросах цифровых технологий скорее взаимодействуют с детьми, нежели что-то им запрещают. Но все же и они нередко прибегают к ограничениям.

Что же касается семей, где высоки и доходы, и образовательный уровень, то в них принято рассматривать права и возможности ребенка с позиций этики. Родители, само собой, используют различные способы контроля за цифровой жизнью своих чад. Но, как правило, стараются обходиться без строгих запретов. А чтобы отвлечь детей от гаджетов, для них, например, организовывают различные офлайн-активности.

Суммируя, можно сделать вывод, что уровень образования родителей — определяющий фактор в выборе ими модели регулирования интернет-активности своих детей.

Вместе с тем стоит обратить внимание, что низкий уровень доходов не является барьером для вхождения в цифровой мир. Это значит, что дети из небогатых семей потенциально имеют шансы стать

цифровыми профессионалами. Они вполне могут построить карьеру, если школа даст им недостающие навыки рационального и ответственного использования технологий, которые они не смогли перенять от родителей. В противном случае они рискуют остаться всего лишь потребителями примитивного контента или перейдут на темную сторону: пополнят ряды киберпреступников, если «прокачают» свой технический уровень.

Необязательно быть мишенью, чтобы стать жертвой

«У меня нет миллионов в швейцарском банке, заводов и яхт, в политику я не лезу. Разве я интересен киберпреступникам?»

На первый взгляд может показаться, что среднестатистическому гражданину действительно не о чем беспокоиться, ведь преступная деятельность требует организованных усилий, вовлечения большого числа высококвалифицированных специалистов, а все это обходится весьма дорого. Вспомните любой добротный фильм про ограбление — хотя бы историю про друзей Оушена. Сколько сил и энергии тратят герои, чтобы завладеть сокровищами! Никто же специально не планирует ограбление квартиры простого служащего, живущего на скромную зарплату.

Персонально вы, скорее всего, неинтересны жуликам, и в аналоговом мире крайне маловероятно, что именно вас выберут мишенью. Но цифровой мир устроен не так. Здесь можно автоматизировать не только полезные процессы — скажем, запись

ребенка в школу или на прием к врачу. Ограбление тоже можно автоматизировать. Ваши деньги и персональные данные украдут вместе с деньгами и данными миллионов других пользователей, «за компанию».

Способов почти незаметного воровства денег, а также причинения другого вреда, существует довольно много, и мы в этой книге о них еще поговорим. Но сначала вам стоит уяснить одну вещь: сегодня скромные доходы не спасают от внимания криминальных структур. Поэтому о своей безопасности, равно как и о безопасности своих близких, нужно заботиться вне зависимости от уровня ваших доходов.

Пожалуй, наибольшее число неприятностей, в которые попадают обычные граждане, включая детей, связаны с неперсонализированными атаками, когда кибержулики ловят широким неводом, загребая любую мелкую рыбешку, какая встречается им на пути. Чтобы миновать их сети, необходимо стать чуть более умной рыбой. И это вполне возможно — просто нужно научиться соблюдать хотя бы элементарные правила цифровой гигиены.

Под прицелом

Совершенно иная ситуация, когда именно вы — или, того хуже, ваш ребенок — по каким-то причинам становитесь чьей-то мишенью. Чем скорее вы поймете, что находитесь под прицелом, тем лучше.

Чем скорее вы поймете, что находитесь под прицелом, тем лучше.

Ведь полагаться на пассивные методы защиты из области цифровой гигиены в этом случае уже бесполезно — нужно переходить к активным действиям, потому что вам грозят серьезные опасности. Например, это могут быть:

- травля в соцсетях;
- попытки вербовки в преступные организации;
- вовлечение в деструктивные сообщества;
- вымогательство, шантаж или преступления на сексуальной почве.

Экономические мотивы тоже могут присутствовать, но по сравнению с вышеперечисленным попытка обчистить ваши карманы выглядит сравнительно мелкой проблемой. А вот если ваш ребенок ввязался в переписку с маньяком (они, к сожалению, существуют не только в кино), то вы рискуете узнать об этом, когда будет уже поздно.

Вашим противником может оказаться как профессионал, который специально подготовлен к ведению преступной деятельности в киберпространстве, так и обычный преступник, который выискивает свои жертвы через интернет. В обоих случаях вам неизвестна его личность и истинное местонахождение. При этом первый умеет ловко заметать цифровые следы, что затрудняет его поиск и поимку, а второй бывает достаточно наивен в способах цифровой маскировки, вследствие чего с большей вероятностью может быть обнаружен и задержан. Тем не менее уровень опасности в обоих случаях очень высок.

Рассказывает Константин Игнатьев, «Лаборатория Касперского»:

«Пятнадцатилетняя старшеклассница из Барнаула познакомилась в соцсети с мужчиной 30 с лишним лет. У них завязался диалог. Потом они встретились в реальности, он за ней ухаживал и, в конце концов, уговорил вступить с ним в половую связь. Более того, снял этот процесс на видео, сделал множество фотоснимков девочки в обнаженном виде, а затем начал ее шантажировать. Две недели она скрывала произошедшее от родителей, но потом все-таки призналась. Родители обратились в полицию, преступника нашли и осудили. Правда, срок он получил условный — 5 лет. Через какое-то время семья девочки переехала в Москву — они это давно планировали, а происшествие только ускорило переезд.

Но на этом история не закончилась. Мужчина снова попытался выйти с девочкой на связь и для этого создал в соцсети «ВКонтакте» ее фейковый аккаунт с фотографиями. Староста класса, в котором училась девочка, нашел этот якобы ее аккаунт и добавил его в группу класса. В результате злоумышленник узнал, где она учится, и снова начал ей угрожать. Но, к счастью, у него ничего не получилось.

Благодаря тому, что героиня этой истории тесно и доверительно общалась с родителями, которые ее всячески поддерживали, она прошла это испытание, хотя и не без травм, но все же сохранив здравый рассудок. Я общался с ней и вполне могу это засвидетельствовать.

Но бывают и трагедии. Встречаются авторитарные родители, особенно отцы, которые говорят: «Интернет — это помойка, я это запрещаю — и все!» В итоге они теряют контакт с ребенком. А если ребенок перестает доверительно общаться с родителями, это всегда не к добру.

Так случилось с девочкой, которой отец строго-настрого запрещал пользоваться социальными сетями. Но какой же подросток сегодня не «зависает» в соцсетях! Поскольку девочке приходилось скрывать это от родителей, она завела несколько аккаунтов со смартфонов друзей и через один из них познакомилась с мужчиной. Как потом оказалось, он планировал не просто шантаж, а изнасилование и убийство. Трагедии можно было бы избежать, расскажи она все родителям. Но несчастный ребенок боялся признаться самым близким людям, что тайком пользуется соцсетями...

В жизни случается, что угроза исходит от известных вам людей, действующих из мстительных побуждений или по каким-то другим личным мотивам. По личным мотивам, как правило, организовывается и травля в интернете (кибербуллинг). Чаще всего агрессоры — это кто-то из ближайшего окружения, например, одноклассники. Как от них скроешься? Они же все равно достанут в реальной жизни. Выход один: организовывать поддержку со стороны родителей и друзей, объяснять, что не нужно реагировать на агрессивные выпады. Делать это необходимо: кибертравля часто приводит к самоповреждениям и суицидам, потому что дети еще не способны выходить из сложных ситуаций самостоятельно, а рассказывать о них родителям стесняются или боятся».

Примечательно, кстати, что кибербуллинг в наибольшей степени распространен в детской и подростковой среде, а к старшим классам практически сходит на нет. Причина проста: когда дети становятся старше, они начинают понимать, что за свои действия им придется отвечать.

Когда некого винить, кроме себя

Третья группа киберпреступлений — те, которые становятся возможны вследствие неразумных или неосторожных действий пользователей. То есть когда жертва сама преподносит злоумышленникам свои данные, ключи и пароли. Типичный пример — школьные компьютеры, на которых дети регулярно оставляют открытые сессии в соцсетях или электронной почте, а в браузере — логины и пароли. Стоит ли потом удивляться, что кто-то украл их данные?

Можно вспомнить и неразумные посты в соцсетях, которые оборачиваются условными, а иногда и реальными сроками — просто потому, что ребенку не рассказали об ответственности за его публикации и о том, как работает правоохранительная система.

Если родители старательно внушали юному пользователю мысль, что честному человеку нечего скрывать, и не научили его заботиться о своих секретах, тогда этот пользователь, выйдя на работу, будет также беззаботно относиться и к секретам своей компании, из-за чего может нажить себе крупные неприятности.

Короче говоря, цифровой мир дает множество возможностей, чтобы наделать глупостей.

Цифровой мир дает множество возможностей, чтобы наделать глупостей.

И если каждую минуту не отдавать себе отчет в том, что и зачем ты делаешь, то неприятные последствия фактически гарантированы. Зашел в интернет через публичный wi-fi, ввел логин и пароль от почты, на которую завязаны регистрации на всех сервисах, — и только успевай расхлебывать. Поленился сменить пароль по умолчанию на роутере — под твоим IP-адресом кто-то ограбил банк.

Понятное дело, стопроцентной защиты от всех рисков не существует, но можно хотя бы свести их к минимуму. И для этого даже не нужны какие-то специальные средства. Нужно лишь приучить себя соблюдать простые правила, и, разумеется, приучить к этому детей — чем раньше, тем лучше.

Ребенок как угроза

Обычно родители озабочены тем, как защитить ребенка от нехороших людей и недетского контента в Сети, но редко думают, как обезопасить самих себя от своего дитяти. Помните эту песенку?

В каждом маленьком ребенке,
И мальчишке, и девчонке,
Есть по двести грамм взрывчатки
Или даже полкило!

Должен он бежать и прыгать,
Все хватать, ногами дрыгать,

А иначе он взорвется, трах-бабах!
И нет его!

Каждый новенький ребенок
Вылезает из пеленок
И теряется повсюду,
И находится везде!

Он всегда куда-то мчится,
Он ужасно огорчится,
Если что-нибудь на свете
Вдруг случится без него![1]

Все именно так! А еще дети страшно любят хватать разные гаджеты, нажимать на все кнопки, удалять фотографии, отправлять странные сообщения вашим знакомым, устанавливать приложения-игрушки в промышленных количествах, находить и открывать сайты 18+++ (которые останутся в вашей истории просмотров), кликать на рекламные ссылки, цепляя кучу вирусов, и вообще творить бог знает что.

Ребенок — пользователь, который очень высоко мотивирован на достижение своих личных целей (играть или смотреть мультики), и ради этого готов пренебречь любыми правилами. С точки зрения специалиста по информационной безопасности, это — портрет типичного нарушителя. Поэтому следует предпринять меры, чтобы активность ребенка не привела к ущербу.

О чем нам говорят сказки? О том, что дети постоянно нарушают правила и попадают в разные нехорошие ситуации. Козлята

1 *Песня на стихи Григория Остера из мультфильма «Осторожно, обезьянки!» (1987 год).*

забыли все, что им говорила мама-коза, и открыли дверь волку. Красная Шапочка не послушалась маму и тоже угодила в лапы к волку, да еще вместе с бабушкой. Старшая сестра заигралась, и гуси-лебеди утащили ее братика. Буратино разговорился с незнакомцами и выдал им все персональные данные. В общем, полагаться на разумное поведение маленького пользователя не стоит.

В 2018 году организация EU Kids Online[1] при поддержке Министерства юстиции и общественной безопасности Норвегии провела исследование среди детей и подростков в возрасте 9-15 лет, которое показало, что существует большой разрыв между тем, что они знают об основных концепциях интернета, и их способностью применять эти знания на практике. Также исследователи отмечают, что детям не хватает целостного понимания рисков и возможностей, которые могут быть связаны с их действиями.

То есть детишки кое-что знают, но далеко не все умеют. По-хорошему, таким неопытным путешественникам по цифровому миру стоило бы давать специальный значок, наподобие знака «У» для водителей-новичков, чтобы другие участники движения были с ними поосторожнее. Но таких знаков не существует. Поэтому, прежде чем подпустить ребенка к своим цифровым устройствам, необходимо обезопасить свои цифровые активы.

Прежде чем подпустить ребенка к своим цифровым устройствам, обезопасьте свои цифровые активы.

1 *Ní Bhroin, N. and Rehder, M. M. (2018). Digital Natives or Naïve Experts? Exploring how Norwegian children (aged 9-15) understand the Internet. EU Kids Online.*

Понятно, что лучший выход из этой ситуации — покупка ребенку собственного гаджета. Но не всякий семейный бюджет это выдержит, особенно если семья — многодетная. С другой стороны, даже если у детки будет свой телефон, это еще не гарантия того, что он не заинтересуется вашим — вдруг у вашего экран побольше и поярче. Так что расслабляться нельзя. Ни в коем случае не привязывайте к детскому телефону ни свою банковскую карту, ни даже карту ребенка, если таковая у него уже имеется, и настройте резервное копирование в облако: если юный исследователь цифровых миров все-таки угробит ваш девайс, вам будет проще восстановить данные.

Как обезопасить свои гаджеты от любимых детишек

- *Установите на телефон и компьютер пароль или пин-код. Не стоит считать это признаком недоверия к ребенку, это самая обычная мера безопасности — как мы ставим заглушки на розетки и блокираторы на ящики и дверцы шкафов, когда в доме есть маленькие дети. Теоретически можно попытаться договориться с детьми, чтобы они не брали без спроса ваш телефон, но искушение бывает столь велико, что лучше подстраховаться.*

- *Не привязывайте к телефону (точнее, к учетной записи Apple ID или Google для обладателей Android-телефонов) свою основную банковскую карту. Это, в принципе, полезно, вне зависимости от наличия детей. Если у детей есть свои телефоны, то тем более. Лучше всего будет выпустить виртуальную карту (обычно это бесплатно) и положить на нее небольшую сумму — тогда ваш основной счет будет в большей безопасности. Если вы привыкли платить с помощью телефона, то есть пользуетесь сервисами Apple Pay*

или Google Pay, то к ним придется привязать настоящую карту для покупок.

- *Настройте копирование в облако фотографий, контактов, заметок и другой ценной информации. Помните: телефон, попавший в детские ручки, может вернуться к вам совсем не таким, каким вы его знали раньше.*

- *Установите приложение-контейнер. Это специальное приложение, которое из одного телефона «делает» два — как на компьютере могут быть отдельные профили для разных пользователей. Обычно это применяется для разделения рабочего и личного пространств, но для разделения взрослого и детского тоже подойдет. На телефонах Samsung это приложение называется Secure Folder (раньше это был Knox), есть аналоги и у других производителей. Secure Folder позволяет быстро и легко защищать любые папки на смартфонах Android. С этим приложением вы сможете создать пин-код или пароль, чтобы защитить файлы от любопытных глаз, перемещать их в защищенную папку и из нее. В эту папку можно поместить и приложения — например, для социальных сетей, сайтов знакомств и другие, доступ к которым вы хотите оградить от посторонних.*

Почему детей так тянет к смартфонам? Цифровой мир дает ребенку неограниченный простор для исследования — гораздо больший, чем мир реальный, который для него на самом деле ограничен пределами квартиры, двора, школы и нескольких других мест, куда его водят на занятия. Попасть в какие-то действительно новые места ребенку удается редко — только во время семейных походов в развлекательный центр по выходным, поез-

док в отпуск или к бабушке на дачу. Большую же часть времени перед глазами ребенка проплывают одни и те же, уже знакомые картины. Поэтому неудивительно, что виртуальные миры обладают для него притягательной силой, — там в полной мере реализуется его природная функция все изучать и пробовать, причем при почти полном отсутствии риска.

Само собой разумеется, ребенок не думает об угрозах, его ведут азарт и любопытство. И, увидев кнопку с призывной надписью или картинкой, он непременно на нее нажмет, сколько бы ему не рассказывали об опасных ссылках, вирусах, хакерах и мнимых виртуальных друзьях.

Случаи из жизни

— Хватило всего нескольких секунд в детских руках, чтобы айфон моего знакомого намертво завис. В итоге знакомому пришлось дожидаться, когда сядет аккумулятор, чтобы затем попытаться оживить смартфон.

— Раньше у меня на телефоне было приложение «Сити-Мобил». С его помощью ребенок несколько раз вызвал такси. Для этого всего-то и нужно — два нажатия. И всякий раз такси приезжало. В конце концов приложение пришлось удалить.

— Когда моему сыну было пять лет, он однажды накупил кучу платных игр в AppStore — за один вечер потратил около тысячи долларов. Действовал он следующим образом. Покупал сразу несколько игр, но если какие-то из них казались ему неинтересными, тут же удалял, а вместо них заказывал новые. Я обратился в Apple, описал ситуацию, и они вернули мне деньги.

Жизненные ситуации

«Если раз за разом пытаться потрогать раскаленную докрасна кочергу, то, в конце концов, обожжешься; если посильнее полоснуть по пальцу ножом, из пальца обычно идет кровь; если разом осушить пузырек с наклейкой «Яд!», рано или поздно почти наверняка почувствуешь недомогание», — рассудительно говорила Алиса. В наши дни она наверняка продолжила бы список: если заходить на все сайты подряд, непременно подцепишь вирус; если установить слишком простой пароль, его, весьма вероятно, взломают; если твой друг в соцсети просит у тебя фото кредитной карточки твоей мамы, это на 100% мошенник.

Давайте рассмотрим наиболее часто встречающиеся ситуации, связанные с нарушением кибербезопасности.

Что может случиться:

- Потерялся пароль;
- Взломали аккаунт;
- Пропали файлы или фотографии;
- Подцепил вирус;
- Украли (потерял) телефон;
- Нашел флешку;
- Надоела навязчивая реклама;

- Ребенок смотрит взрослый контент;
- Украли деньги с карты;
- Появились лишние подписки на сервисы;
- Утекли персональные данные;
- Кто-то угрожает ребенку или вам;
- Ребенок решил стать хакером;
- Похоже, у ребенка развилась зависимость от интернета;
- В Сеть попали фотографии, которые вы не хотели бы публиковать.

Наверное, список можно дополнить. Часть этих неприятностей будет связана с угрозами непосредственно вашему ребенку или вам, другая может нанести урон вашим цифровым ценностям. Об этом — в нашей следующей главе.

Контрольные вопросы

1. Кто такие цифровые аборигены и цифровые иммигранты?
2. К какой категории вы себя относите?
3. Может ли ребенок освоить цифровую грамотность только интуитивно?

4. Кого называют цифровыми сиротами, изгнанниками и наследниками?

5. К какой категории родителей вы себя относите — наставники, потакающие или запрещающие? Устраивает ли вас эта роль?

6. Почему преступники решают кого-то взломать или ограбить?

7. Что такое кибербуллинг?

8. Какие правила кибербезопасности вы нарушали?

9. На какие три группы можно разделить опасные ситуации?

10. Как защитить свои данные от нечаянных действий ребенка?

11. В каких жизненных ситуациях, перечисленных в этой главе, вы оказывались?

12. Можете ли добавить к этому списку что-то еще?

13. Что значит «бояться интернета правильно»?