УДК 004
ББК 32.973.2
К36

Understanding the Digital World:
What You Need to Know about Computers,
the Internet, Privacy, and Security, Second Edition
by Brian W. Kernighan.

Керниган, Брайан.

К36 Основы информационных технологий для неспециалистов: что происходит внутри машин / Брайан Керниган ; [перевод с английского Е. В. Жевлаковой]. — Москва : Эксмо, 2024. — 624 с. — (Библиотека ИТ. Главные книги о современных технологиях).

ISBN 978-5-04-184251-2

Компьютеры окружают нас повсюду, включая бытовую технику, автомобили, медицинское оборудование, транспортные системы, электросети и оружие. Однако большинство из них остаются невидимыми, собирая и иногда сливая наши личные данные. Это делает нас уязвимыми для правительств, компаний и преступников, которые могут использовать информацию в своих целях.

Второе издание популярной книги «Цифровой мир» Брайана Кернигана рассматривает принципы работы компьютерного оборудования, программного обеспечения и сетей. Новые разделы посвящены программированию на Python, большим данным, машинному обучению и многому другому.

УДК 004
ББК 32.973.2

ISBN 978-5-04-184251-2

Содержание

Посвящается Мэг

Предисловие

Курс под названием «Компьютеры в нашем мире» я преподаю в Принстоне почти каждую осень начиная с 1999 года. Название курса — размытое до неприличия, но дело в том, что однажды мне пришлось придумать его за пять минут, а поменять с тех пор стало довольно сложно. Впрочем, преподавать этот курс — самая увлекательная часть моей работы, которая и так почти всегда приносит радость.

Факт, что компьютеры и вычислительная техника окружают нас повсюду. Некоторые технологии у всех на виду: у студентов есть ноутбуки, и они намного мощнее компьютера IBM 7094[1], который стоил несколько миллионов долларов, занимал большую комнату с кондиционером и обслуживал весь кампус Принстона, когда я пришел сюда аспирантом в 1964 году. Кроме того, каждый студент пользуется сотовым телефоном, вычислительная мощность которого намного выше, чем у той древней машины IBM. У всех студентов, как и у значительной доли населения земного шара, есть высокоскоростной доступ в интернет. Любой из них может искать информацию в браузере, совершать покупки онлайн, пользоваться электронной почтой, мессенджерами и социальными сетями для общения с друзьями и семьей.

Но это только вершина айсберга вычислительных технологий, бóльшая его часть скрыта в глубине. Мы обычно не думаем о компьютерах, которые незаметно работают

в бытовой технике, машинах, самолетах и вездесущих электронных устройствах вроде умных телевизоров, термостатов и дверных звонков, средств распознавания голоса, фитнес-трекеров, наушников, игрушек и игровых аксессуаров, — и мы воспринимаем их как данность. Мы мало задумываемся и о том, до какой степени от вычислительной техники зависит инфраструктура: телефонная сеть, кабельное телевидение, управление воздушным движением, энергосистема, банковские и финансовые услуги.

Большинство людей напрямую не создают эти системы, но ощущают их сильное влияние — а некоторым предстоит принимать важные решения по поводу их работы. Образованный человек должен знать по меньшей мере основы вычислительных технологий: что делают компьютеры и как, на что они не способны в принципе, а что просто чересчур сложно для них на данный момент, как они общаются между собой и что при этом происходит, какими многочисленными способами технологии и коммуникации воздействуют на мир вокруг нас.

То, что информационные технологии проникают повсюду, влияет на нас неожиданным образом. Хотя нам время от времени напоминают о распространении систем наблюдения, о вторжениях в нашу частную жизнь, угрозах кражи личных данных, мы не всегда осознаем, насколько это все обусловлено технологиями и коммуникациями.

В июле 2013 года Эдвард Сноуден, подрядчик Агентства национальной безопасности (АНБ) Соединенных Штатов Америки, предоставил журналистам 50 000 документов, в которых раскрывалось, что сотрудники АНБ регулярно отслеживали электронные средства связи: звонки, сообщения, письма, интернет — и собирали данные почти по каждому жителю мира. Что примечательно, они следили и за американцами, которые жили в своей стране и не представляли

никакой угрозы ее безопасности. Документы Сноудена показывали, что и другие государства тоже шпионили за своими гражданами. Удивительно, но после первоначального возмущения общественности все вернулось на круги своя, правительства стали еще более масштабно отслеживать, чем занимаются граждане, и шпионить за ними, а люди либо смирились с этим, либо не возражают по неведению.

Нашу деятельность в интернете и реальном мире отслеживают также и корпорации. Бизнес-модели многих компаний основаны на обширном сборе данных, возможностях прогнозировать наше поведение и влиять на него. Доступность громадных объемов данных позволила достичь серьезного прогресса в машинном распознавании речи и образов, а также автоматических переводах. Но она вредит неприкосновенности частной жизни, и теперь сложно сохранять анонимность.

Хакеры всех мастей стали особенно изощренными в своих атаках на хранилища данных. В государственных службах и на предприятиях почти ежедневно происходят электронные взломы; данные о клиентах и сотрудниках похищают в больших количествах и часто используют в целях мошенничества и кражи личной информации. Обычными стали атаки на отдельных лиц. Раньше считалось, что для защиты от онлайн-мошенников достаточно игнорировать письма от мнимых нигерийских принцев или их родственников. Но сейчас целевые атаки стали куда более хитроумными, и это один из наиболее распространенных способов взлома корпоративных компьютеров.

Социальные сети вроде Facebook*, Instagram*, X (Twitter), Reddit и других изменили способы общения между

---

* Принадлежат компании Meta, признанной экстремистской и запрещенной на территории РФ.

людьми. С одной стороны, это полезно: мы можем поддерживать связь с друзьями и семьей, просматривать новости и всевозможные развлекательные посты. Соцсети могут и помочь, как в середине 2020 года, когда движение Black Lives Matter привлекло всеобщее внимание благодаря «вирусным» видеороликам о жестокости полиции.

Но через социальные сети также распространялось множество дурных идей. Расисты, участники групп ненависти, сторонники теорий заговора и другие безумцы, независимо от их убеждений и политических взглядов, могут легко находить друг друга в интернете, координировать свои действия и усиливать свое влияние. Сдержать разгул ненависти и бреда мешают щекотливые вопросы свободы слова, а также технологические сложности модерирования контента.

В мире с обширным взаимодействием через интернет сложно решать вопросы юрисдикции. В 2018 году Европейский союз ввел в действие Общий регламент по защите персональных данных, который позволил жителям ЕС контролировать сбор и использование своих данных и запретил компаниям отправлять или хранить данные за пределами ЕС. Коллегия присяжных еще не определила, насколько Общий регламент оказался полезным для конфиденциальности. К тому же эти правила применяются только в ЕС, а в других частях мира действуют иные законы.

Еще одна сложность появилась после быстрого внедрения облачных вычислений, когда отдельные лица и компании стали хранить данные и обрабатывать их на серверах, принадлежащих Amazon, Google, Microsoft и т. д. Данные теперь хранятся не только у их владельца, но и у третьих лиц, у которых есть свои цели, обязанности, уязвимые места и неразрешенные проблемы с взаимоисключающими требованиями разных юрисдикций.

Быстро развивается «интернет вещей», в котором все виды устройств подключаются к сети. Смартфоны — это очевидный пример, но, кроме них, онлайн-доступ получают автомобили, камеры слежения, бытовая техника и средства управления домом, медицинское оборудование и бóльшая часть инфраструктуры — например, управление воздушным движением и энергосети. Эта тенденция соединять все с интернетом будет продолжаться, потому что преимущества такого соединения неоспоримы. К сожалению, здесь есть и серьезные риски: некоторые устройства контролируют жизненно важные системы, а не только развлечения, и часто их защита намного слабее, чем у более зрелых технологий.

Криптография — одно из немногих эффективных средств защиты, поскольку она обеспечивает конфиденциальность и безопасность как коммуникации, так и хранения данных. Но надежная криптография подвергается постоянным атакам. Правительствам не нравится идея, что люди, компании или террористы получат возможность общаться по-настоящему тайно, поэтому они часто призывают внедрить в криптографические алгоритмы лазейки, которые позволили бы госслужбам взломать шифрование — разумеется, с «надлежащей страховкой» и только «в интересах национальной безопасности». Какими бы благими ни были их намерения, это очень плохая идея. Даже если вы верите, что правительство всегда будет вести себя достойно и не позволит утечь секретной информации (забудем о Сноудене), ослабленная криптография поможет не только вашим союзникам, но и противникам. А плохие парни все равно не будут ее применять.

Это лишь некоторые проблемы и вопросы, которые должны беспокоить обычных граждан на улицах,

вроде студентов моего курса или, как говорится, «людей просвещенных», независимо от их происхождения и образования.

Студенты моего курса — не технические специалисты. Они не инженеры, не физики, не математики. Они — бакалавры английского языка и политологии, историки, классицисты, экономисты, музыканты и артисты. Превосходная выборка по гуманитарным и общественным наукам. К окончанию курса эти одаренные люди должны научиться читать и понимать новостные статьи на компьютерную тематику, узнавать из них что-то новое и, возможно, находить неточности. В более широком смысле я хочу, чтобы мои студенты и читатели разумно и скептически относились к технологиям, понимали, что они полезны, но вовсе не панацея. И наоборот, понимали, что, хотя технологии иногда приводят к плохим последствиям, они вовсе не абсолютное зло.

Ричард Мюллер в своей прекрасной книге «Физика для будущих президентов»[2] пытается объяснить научно-техническую подоплеку, лежащую в основе проблем, с которыми сталкиваются лидеры: ядерная угроза, терроризм, энергетические кризисы, глобальное потепление и так далее. Эрудированные люди, хоть и не претендующие на пост президента, тоже должны разбираться в этих темах. Если опираться на подход Мюллера, то и мое направление работы можно определить схоже: «Компьютеризация для будущих президентов».

Что будущий президент должен знать о компьютеризации? Что должен знать об этом эрудированный человек — например, вы?[3]

Я выделяю четыре основные технические области: аппаратное обеспечение, программное обеспечение, коммуникации и данные.