Темная сторона технологий

Риски снижают преимущества цифровой эры

Крис Веллиш

ЦИФРОВЫЕ технологии принесли нам удобства, о которых едва ли приходилось мечтать еще поколение назад. Интернет избавляет студентов и ученых от долгих часов утомительного поиска в библиотеках, мгновенно и практически бесплатно обеспечивает визуальное, устное и письменное общение. Любой человек со смартфоном может воспользоваться GPS, чтобы не потеряться в незнакомом городе или найти ближайшую кофейню. Потребители, не выходя из дома, совершают покупки и банковские операции, а врачи проводят компьютерную диагностику. Чудеса цифровой эры впечатляют настолько, что два ученых, Эрик Бринёлфссон и Эндрю Макафи, окрестили ее «вторым веком машин», заявив, что компьютеры делают для нашего интеллекта то же, что паровой двигатель сделал для мышц.

Тем не менее, у прогресса есть и свои недостатки. Некоторые критики цифровой эры сетуют на то, что несколько гигантских социальных сетей способны манипулировать общественным мнением. Другие наблюдатели всерьез обеспокоены такими патологическими явлениями, как киберзапугивание и интернет-порнография. Есть и те, кого волнуют возможная утрата неприкосновенности частной жизни и угроза нарушения гражданских свобод, ведь в наши дни практически любое действие, телефонный звонок и электронное сообщение оставляют цифровой след, которым может воспользоваться любопытный сосед или бесцеремонное правительство.

Все эти опасения обоснованны, однако подвергнуть их количественной оценке невозможно. И все же для компаний и экономических систем некоторые аспекты цифровых технологий связаны с измеримыми издержками, сводящими на нет как минимум часть той эффективности, которую предлагает «второй век машин».

Хакеры могут получить доступ к управлению автомобилями или обесточить электросеть. Киберворы крадут персональные данные и используют их для выкачивания средств с чужих банковских счетов или для совершения покупок онлайн по чужим кредитным картам. Электронная почта, мобильные телефоны и социальные сети, с одной стороны, произвели революцию в общении, а с другой — наносят удар по производительности офисных работников, прикованных к своим лентам в Твиттере или пристрастившихся к обмену мгновенными сообщениями.

Риски в сфере кибербезопасности

Когда несколько бывших сотрудников Подразделения 8200, израильского корпуса радиоэлектронной разведки, решили создать частную компанию по обеспечению кибербезопасности, они пришли к выводу, что настоящим прорывом в современном мире станут автомобили с интернет-соединением.

«Эти люди просто изучили ситуацию на рынках и подумали, что в скором времени на дорогах появятся миллионы подключенных к сети автомобилей», — объясняет Йони Хейлбронн, вице-президент по маркетингу компании Argus Cyber Security Ltd.

Три года спустя тель-авивская Argus открыла отделения в Германии, Японии и США. Компания процветает, благодаря историям о хакерах, захватывающих управление автомобилями (не говоря уже об авариях — правда, связанных не с хакингом, а с функцией автопилота на машинах Tesla Motors), и внимание общественности все чаще привлекает необходимость повышения автомобильной кибербезопасности.

Добро пожаловать в «интернет вещей» — предметов, подключенных к сети, которая позволяет им отправлять и получать данные. Эта система постоянно расширяется, охватывая самые разные устройства, от диагностического оборудования в больницах до кофеварок и других домашних электроприборов. Согласно прогнозам Gartner Inc., ведущей исследовательской и консалтинговой фирмы в сфере информационных технологий, в текущем году число устройств, подключенных к интернету, увеличится на 30 процентов и достигнет 6,4 миллиарда единиц. Общемировые расходы на безопасность «интернета вещей» возрастут на 24 процента, до 348 миллионов долларов США.

Мир, подключенный к сети, открывает все новые возможности для киберпреступников, которые собирают персональные данные, чтобы использовать их для проведения мошеннических сделок, либо внедряют программы-вымогатели — вредоносные программные средства, способные блокировать устройства или шифровать данные и требовать деньги в обмен на ключ для дешифровки.

«Это новый способ доступа для мошенников, — говорит Брэдли Дж. Вискирхен, генеральный директор Kount, фирмы по обеспечению интернет-безопасности с головным офисом в Бойсе, штат Айдахо. — Им вовсе не обязательно взламывать мой компьютер, если они могут взломать мой принтер или холодильник и узнать обо мне все необходимое».

Попытку взлома бытовых электроприборов, подключенных к интернету, нередко облегчает один простой фактор: слабость, а то и полное отсутствие, встроенной системы безопасности. Исключением становятся продукты таких компаний, как Nest Labs из Пало-Альто, Калифорния, производителя интеллектуальных устройств со сложными механизмами безопасности.

«Многие просто покупают программное обеспечение с открытым исходным кодом и устанавливают его на устройстве, то есть практически не задумываются о безопасности», — говорит Крис Кинг, аналитик по вопросам уязвимости в координационном центре CERT при Институте по разработке программного обеспечения университета Карнеги-Меллон. Взломать можно что угодно, в том числе игрушки вроде подключенной к Wi-Fi куклы Hello Barbie.

По мере расширения сетевого мира увеличивается и перечень уязвимых устройств. По словам Кинга, чтобы получить выкуп, хакеры отключают даже диагностические системы в больницах. В прошлом году хакеры обесточили электросеть на западе Украины, оставив без света более 200 000 человек. В Германии атаке кибервандалов подвергся прокатный стан, что нанесло колоссальный ущерб сталелитейному заводу.

Особенно пугает перспектива взлома автомобилей, который может привести к смертельным ДТП. По оценкам компании Gartner, к 2020 году порядка 250 миллионов автомобилей во всем мире будут оснащены тем или иным видом бортовых терминалов для беспроводного подключения к сети.

Почти все элементы современного автомобиля — тормоза, рулевое управление, датчики давления в шине, освещение — контролируются с помощью компьютеризованных приборов, соединенных друг с другом через коммуникационную систему, или «шину», которая была изобретена 30 лет назад, еще до наступления эпохи интернета. Сама по себе шина ничем не защищена, как и многие другие устройства автомобиля.

«Систему, которую никогда не планировалось использовать в режиме онлайн, подключили к интернету, и она внезапно стала уязвимой для всего того, о чем ее создатели и представления не имели», — говорит Кинг.

Производители автомобилей и комплектующих со всей серьезностью отнеслись к этой угрозе и после пары нашумевших взломов начали усиливать меры безопасности.

Исследователи из компании Argus взломали устройство под названием Zubie, которое отслеживает технические характеристики автомобиля, а затем по беспроводной связи через удаленный сервер передает на смартфон водителя актуальные данные — наряду с уведомлениями о техническом обслуживании и советами по улучшению навыков вождения. После взлома исследователи смогли контролировать рулевую систему, тормоза и двигатель автомобиля. Специалисты Argus сообщили Zubie об этой уязвимости, и она, по словам представителей компании, была устранена.

В прошлом году, после того как журнал *Wired* сообщил, что исследователи сумели захватить контроль над автомобилем Jeep Cherokee, проникнув в его бортовой компьютер с помощью ноутбука, компания Fiat Chrysler Automobiles объявила об отзыве 1,4 миллиона машин.

«Если ваши автомобили подключены к сети, они должны быть защищены», — говорит Хейлбронн из компании Argus. ■

Киберкражи

Магнус Карлссон стоял у окна в своем кабинете на восьмом этаже и наблюдал за людьми на оживленной улице в Бетезде, штат Мэриленд, когда на экране его компьютера появилось электронное сообщение. Его боссу, исполнительному директору Ассоциации профессиональных финансистов, потребовалась помощь в переводе средств.

Но когда Карлссон нажал кнопку ответа, в окне приложения Outlook появился незнакомый адрес. По словам Карлссона, он с самого начала понял, что это классическое мошенничество. Ему ли не знать, что как менеджер отдела кассовых операций и платежей в глобальной отраслевой группе, представляющей интересы финансовых директоров, он обязан предупреждать членов группы по всему миру об источниках финансового мошенничества, включая интернет-махинации.

Тактика, о которой он рассказал, известна как «компрометация коммерческой электронной почты». Она быстро набирает

Киберкражи *(окончание)*

популярность среди киберпреступников, заставляющих сотрудников компаний — как правило, путем подделки электронного распоряжения от начальства, — совершать безналичные банковские переводы фальшивым поставщикам или кредиторам. В ходе опроса 64 процента участников ассоциации сообщили, что сталкивались с компрометацией коммерческой электронной почты.

Это лишь одна из многочисленных нитей разрастающейся глобальной паутины кибермошенничества, которая охватывает тактические приемы и методы с причудливыми, а порой даже зловещими названиями: «программы-вымогатели», «целевой фишинг», «троянские кони». День ото дня киберпреступники становятся все более изобретательными, активными и дерзкими: сначала они преследуют крупную «дичь», включая компании JPMorgan Chase & Co., British Airways, избирательную комиссию Филиппин и Налоговое управление США, а затем, после того как крупнейшие организации выделят на кибербезопасность дополнительные ресурсы, спускаются по корпоративной пищевой цепи к более легкой добыче.

«Расширение масштабов киберпреступлений объясняется простотой их совершения, поэтому все новые страны и компании, выходящие в сеть с самыми примитивными средствами обеспечения кибербезопасности, становятся легкой мишенью для злоумышленников, — утверждает Джеймс Эндрю Льюис, старший вице-президент Центра стратегических и международных исследований в Вашингтоне (округ Колумбия) и автор многих работ о кибермошенничестве. — Правоохранительный контроль в мире крайне неоднороден. Умный хакер найдет способы обойти законы любой страны».

По оценке Льюиса, глобальный ущерб от действий киберпреступников превышает 500 миллиардов долларов США в год, а это больше, чем валовой внутренний продукт такой страны, как Швеция. Этот показатель включает стоимость похищенных наличных средств и интеллектуальной собственности, затраты на возмещение убытков, а также урон, который киберпреступность наносит инновациям, торговле и экономическому росту.

Особо привлекательной целью для преступников становятся финансовые фирмы, о чем свидетельствует кража 81 миллиона долларов из Центрального банка Бангладеш, совершенная в этом году. В ходе атаки хакеры воспользовались идентификационными данными сотрудника банка, отправив с их помощью почти сорок поддельных распоряжений о переводе денежных средств в Федеральный резервный банк Нью-Йорка.

Для такой страны, как Бангладеш, это были огромные финансовые потери, однако регулирующие органы беспокоит гораздо более серьезный риск: киберпреступники, задавшиеся целью посеять хаос, способны вывести из строя всю глобальную финансовую систему, что вызовет экономический коллапс, сопоставимый с кризисом 2007–2008 годов.

«Все это может привести к тому, что участники рынка лишатся доступа к основным элементам рыночных механизмов, — говорит Грег Медкрафт, председатель Австралийской комиссии по ценным бумагам и инвестициям. — Похоже, что кибератаки несут новую, беспрецедентную угрозу мировому порядку».

Опрос, проведенный компанией Depository Trust & Clearing Corporation, показал, что большое число респондентов, 25 процентов, считают киберпреступность основным источником риска для мировой финансовой стабильности. Этот показатель ниже, чем в прошлом году (46 процентов), — отчасти потому, что финансовые учреждения выделяют дополнительные средства на принятие защитных мер. Кроме того, на первый план выходят другие риски, такие как замедление экономического роста в Азии.

И все же регуляторы не спешат делать обнадеживающие выводы. В руководстве, выпущенном в июне Банком международных расчетов и Международной организацией комиссий по ценным бумагам, говорится, что системы платежей и проведения расчетов — ключевые компоненты глобальной финансовой системы — должны принять планы по защите и реагированию на киберпроникновения и назначить ответственных за контроль исполнения этих планов.

Согласно результатам исследования, проведенного компанией PwC, кибермошенничество вышло на второе место по распространенности среди бизнес-преступлений (после незаконного присвоения средств). 61 процент генеральных директоров компаний заявили о том, что обеспокоены проблемами кибербезопасности, однако всего 37 процентов организаций сообщили о наличии плана реагирования.

Интернет-преступления можно условно разделить на две широкие категории. Первая — это взломы, ущерб от которых можно оценить в денежной форме. К ним относятся кражи персональных данных и данных платежных карт. Вторая категория — кибершпионаж: хищение секретов производства, переговорных стратегий и сведений о продукте.

Согласно ежегодному «Отчету об угрозах безопасности в интернете», который выпускает корпорация Symantec, число скомпрометированных идентификаторов в прошлом году возросло на 23 процента и достигло 429 миллионов единиц. Фактический показатель, вероятно, превышает 500 миллионов, поскольку многие компании не сообщают о нарушениях.

Брэдли Дж. Вискирхен, генеральный директор фирмы Kount, ведущего поставщика решений по управлению цифровыми рисками (Бойсе, штат Айдахо), полагает, что после массовой утечки данных в таких организациях, как медицинская страховая компания Anthem Inc. и цифровой рынок eBay Inc., в руки преступников попали сведения почти обо всех гражданах США.

«Скомпрометирован практически каждый из нас», — заявляет Вискирхен. Похищенные персональные данные попадают на процветающий электронный черный рынок, где искушенные международные торговцы продают свой товар на веб-сайтах, способных составить конкуренцию крупнейшим розничным сетям мира, а клиенты получают гарантию возврата денег, скидки с объема и руководства по применению.

По результатам недавнего опроса 383 компаний, проведенного IBM и институтом Понемона в 12 странах мира, средняя стоимость каждого случая нарушения сохранности данных возросла с 3,79 до 4 миллионов долларов США. Кражи данных чаще всего совершались в Бразилии и ЮАР, а реже всего — в Австралии и Германии.

Произошедшая в 2014 году атака на нью-йоркскую компанию JPMorgan Chase & Co. привела к компрометации 83 миллионов клиентских записей, включая имена, адреса обычной и электронной почты и номера телефонов. Это была крупнейшая в истории США атака на финансовое учреждение. После этого банк, не сообщив, какие убытки он понес в связи со взломом, объявил о намерении дополнительно выделять 250 миллионов долларов в год на принятие мер безопасности.

Стоимость кражи интеллектуальной собственности оценить труднее, но экономический ущерб от нее может оказаться еще более серьезным. Хищение интеллектуальной собственности — от формул краски до чертежей ракет — снижает прибыль от внедрения инноваций, заявляет Джеймс Льюис из Центра стратегических и международных исследований. «На новые изобретения людей мотивирует возможность получения дохода, а в случае его отсутствия они переключаются на другие виды деятельности», — говорит Льюис.

Результатом становится недостаток инвестиций в новые технологии, а также потеря рабочих мест и прекращение экономи-

ческого роста. В долгосрочной перспективе проигрывают даже те страны, которые используют краденые технологии, поскольку это мешает им учиться разрабатывать собственные. «Из-за этого рост замедляется во всем мире», — утверждает Льюис.

По оценкам Льюиса, общие издержки, связанные с киберпреступностью, включая кражу интеллектуальной собственности, в среднем составляют порядка 0,5 процента глобального ВВП. В странах с высокими доходами, где инновации играют более значимую экономическую роль, потери могут достигать 0,9 процента ВВП. В развивающихся странах этот показатель ближе к 0,2 процента.

Все это приводит к резкому повышению потребности в услугах по обеспечению кибербезопасности: согласно прогнозам Cybersecurity Ventures, фирмы, занимающейся исследованиями и сбором рыночной информации, к 2020 году их общий объем в стоимостном выражении увеличится с прошлогодних 75 миллиардов долларов США до 170 миллиардов.

Годовой прирост количества сделок в фирме Kount измеряется трехзначными числами. «При этом, — говорит Вискирхен, — мы едва коснулись верхнего слоя безграничных возможностей. К сожалению, я работаю в отрасли с невероятным потенциалом роста». ■

Цифровое отвлечение

Лори Восс вспоминает то время, когда ему, молодому программисту из Кремниевой долины, дали месяц на выполнение исключительно скучного и бесперспективного проекта. «Занятие было крайне неблагодарным, — вспоминает Восс. — В тот месяц я провел немало времени в Твиттере».

Воссу, который сейчас работает главным специалистом по технологиям в собственном стартапе NPM, твиты в рабочее время представляются современной версией древнего, как свитки Мертвого моря, явления — прокрастинации.

Новейшие приложения и гаджеты предлагают новые и, несомненно, крайне заманчивые способы пустой траты времени. Сидя в своих кабинетах по всему миру, офисные сотрудники подвергаются настоящей бомбардировке: с мобильных телефонов, компьютеров и планшетов на них без конца сыплются сообщения. По мере распространения в мире новых технологий и расширения экономики знаний цифровое отвлечение и сопутствующая ему информационная перегрузка наносят все больший ущерб производительности.

Три из четырех работодателей в США указывают на то, что ежедневно не менее двух часов проходят впустую из-за отвлекающих факторов, которые действуют на сотрудников. Об этом свидетельствуют данные исследования, опубликованные в июне чикагской компанией по кадровому консалтингу CareerBuilder.

На первое место среди причин непродуктивной траты времени работодатели поставили разговоры по мобильному телефону и обмен текстовыми сообщениями. Далее следуют интернет, офисные сплетни и социальные сети. Все это приводит к снижению качества работы, ослаблению морального духа сотрудников, которые вынуждены доделывать задания за нерадивых коллег, а также к несоблюдению сроков.

Натан Зелдес, консультант по организационным вопросам из Иерусалима, считает электронную почту основной причиной потерь рабочего времени и винит работодателей в неспособности ограничить ее использование. По его словам, сотрудник офиса может ежедневно получать от 50 до 300 сообщений, связанных с работой.

«Внимательно прочитать и обработать такой объем информации невозможно, — говорит Зелдес. — А письма все приходят и приходят».

Бесполезные электронные сообщения и ненужные задержки отнимают у работника умственного труда один день в неделю в результате снижения производительности, утверждает Зелдес, ссылаясь на исследование, которое он провел в 2006 году, когда работал инженером в компании по производству компьютерных чипов Intel Corporation. Для компании, в которой занято 50 000 человек, это ежегодно означает потерю 1 миллиарда долларов США.

С электронной почтой бороться непросто, считает Зелдес. Сотрудники чувствуют себя обязанными читать сообщения и отвечать на них в любое время дня и ночи — из опасения упустить важную информацию либо из желания произвести благоприятное впечатление на коллег или начальство.

«Я вижу в этом подобие дилеммы узника, — говорит Зелдес. — Всем хотелось бы отправлять поменьше электронных сообщений и пораньше уходить домой. Тем не менее никто не решается стать в этом деле первым».

Чтобы описать условия, вынуждающие людей использовать электронную почту, Глория Марк, доктор психологических наук, преподающая на факультете информатики Калифорнийского университета в Ирвайне, проводит аналогию с азартными играми.

«Я называю это лас-вегасским феноменом», — говорит она. Человек, сидящей за игровым автоматом, через случайные промежутки времени выигрывает деньги. Перспективы следующего выигрыша достаточно, чтобы заставить игрока тянуть за ручку.

«Случайным образом подкрепляемое поведение труднее всего поддается искоренению», — утверждает Марк.

В ходе исследования, проводившегося в 2012 году, Марк установила, что в среднем работники способны сосредоточить внимание на экране компьютера всего на 75,5 секунды — после этого они переключаются на другие задачи. К прошлому году этот показатель снизился до 47 секунд.

Работники и их начальники применяют целый ряд стратегий по борьбе с отвлечением и перегрузкой. Многие отводят специальное время для проверки электронной почты, а в оставшуюся часть дня просто игнорируют все входящие сообщения.

«Я трачу немало времени на оптимизацию своей жизни в электронной почте», — говорит Восс из NPM. Принятое им решение заключается в том, чтобы «безжалостно отфильтровывать» любое сообщение, «которое повторяется из раза в раз, касается какого-то повседневного вопроса, всего, что вам не нужно знать и с чем не нужно иметь дела».

«Отключите все уведомления. Не позволяйте сообщениям всплывать у вас перед носом», — рекомендует Клифф Уильямс, старший дизайнер Nextdoor, компании из Сан-Франциско, называющей себя «частной социальной сетью для вашего района».

Вместе с тем Уильямс признает, что избегание отвлекающих факторов — это «постоянная борьба».

«Это похоже на попытки похудеть, — говорит он. — На чем-то ты теряешь, а на чем-то набираешь вдвойне». ■

Крис Веллиш работает финансовым журналистом в Вашингтоне, округ Колумбия.