Industry 4.0, IoT, облака и перспективы информационной безопасности

Р.М. Гусейнов (Компания Digital Complianc)

Рассмотрена эволюция современных информационных технологий и общие риски, которые следуют из этой эволюции. Сделана попытка обобщить отдельные тренды в области ИТ и спрогнозировать проблематику информационной безопасности на ближайшие несколько лет.

Ключевые слова: IoT, Industry 4.0, сервис-провайдеры, облачные технологии, цифровизация, информационная безопасность.

Введение

Чем сложнее система, тем менее она надежна. Рост числа элементов системы усложняет контроль за качеством отдельных элементов, увеличивает число возможных взаимодействий, создает новые точки отказа. Поэтому при проектировании высоконадежных систем люди часто отдают предпочтение простым решениям и минимизируют число составных элементов. Другое дело системы, которые эволюционируют естественным образом. Например, организм человека настолько сложный, что без современной медицины значительная часть людей рискует умереть до 20 лет или не родиться вообще. Современные технологии очень похожи на эволюционирующий организм: хотя теоретики ИТ [1] еще в 40-е годы XX века описывали современный Internet, облачные технологии, голосовых помощников и прочие компоненты IoT, никто не проектировал Internet заранее. С момента своего возникновения в виде первых, маленьких и медленных сетей, которые соединяли мейнфреймы в научных и государственных учреждениях, и до сегодняшнего дня, когда эти сети образовали Internet, к которому подключаются миллионы пользовательских устройств, прошло более 50 лет. И все эти годы Internet развивался ситуативно, при участии различных субъектов и под влиянием нужд текущего момента, без мыслей о том, с чем придется столкнуться системе в будущем. Не было единого генерального плана, не было общего to do листа. Но были компании, люди и государства, которые решали конкретные задачи. История отдельных технологических компаний когерентна истории развития Internet как целого. Думал ли Джефф Безос, создавая on-line магазин книг Amazon в 1994 г., о том, какая судьба уготована его компании? Эволюционная природа технологий и Internet вызывает множество следствий, в частности, трудности прогнозирования будущего состояния сложной системы, ее возможностей, угроз ее развитию и существованию, а также угроз развитию и существованию людей, которая эта система несет внутри себя. И хотя попытка точно предсказать будущее - занятие в целом бесперспективное [2], понимание существующих тенденций позволяет немного заглянуть вперед и подготовиться к возможным сценариям.

Целью настоящей статьи является анализ сложившейся в области информационных технологий ситуации с тем, чтобы понять, чем это грозит с точки зрения информационной безопасности, и какой мир может ожидать нас через 10-15 лет.

Развитие инновационных технологий

Начнем с предистории. В журнале РБК (№6(141), 2018) приведена отраслевая статистика на основе исследований, которые посвящены индустрии будущего. Согласно данным журнала, рост рынка в таких отраслях, как облачные сервисы, распознавание (нейросети), беспилотные автомобили, голосовые ассистенты, искусственный интеллект и виртуальная реальность в период 2017- 2025 гг. составит от 214 % для облачных технологий до 3490 % для голосовых ассистентов. История рынка и ценообразования всегда туманна, но обратимся к фактам. Последние несколько лет сводки новостей из мира технологий похожи на прелюдию к научно-фантастическому триллеру. Выборочно просмотрим последние новости: Московский центр Карнеги сообщает о китайском эксперименте с системой контроля за населением в неспокойных провинциях (https://carnegie.ru/commentary/75492); в США Национальное бюро экономических исследований публикует научную статью о способах прогнозирования благонадежности заемщика по его поведению в Internet и метаданным сессии в браузере (http://www.nber.org/papers/w24551); компания Яндекс запускает собственный гаджет из категории умный дом (http://www.nber.org/papers/w24551). И рядом с этими сообщениями: утечка данных о 340 млн. физических и юридических лицах от американской маркетинговой компании Exactis, которая забыла ограничить доступ к базе данных в облаке Amazon (https://www.wired.com); сотрудник был ошибочно уволен из компании «искусственным» интеллектом из-за невозможности отменить решение автоматизированной кадровой системы (Metro № 78 (123/4001)). А сообщений об очередных уязвимостях IoT и ботнетах, которые паразитируют на умных устройствах, так много, что их просто не успеваешь читать. Даже если отбросить маркетинговый хайп и вспомнить об инерции в вопросах внедрения технологических новшеств, складывается интересная картина. По мере развития технологии получают более широкое распространение, возникают новые сервисы и услуги, но вместе с предполагаемой пользой возникают неочевидные, часто крайне опасные следствия. Рассмотрим некоторые из них.

IoT и Industry 4.0

Обычные люди склонны экономить энергию и среди любителей пошутить ходит анекдот, что материю технического творчества является не изобрета-

тельность, а самая обычная лень. Идеи отказа от рутинного труда и делегирования части задач «умному» прибору, а еще лучше полная автоматизация повседневности были популярны среди людей испокон веков. Мир, в котором свободные от поденщины люди занимаются только интересными и творческими вещами, лежал в основе многих утопий, но упирался в отсутствие материальной базы. Но сегодня, на наших глазах мечты прошлого воплощаются в реальность. Не будем говорить о бытовых приборах – они стали возникать задолго до этого. Изменения идут дальше, и в таких странах как Германия или Япония роботизированные производства, лишенные простых рабочих, уже не являются редкостью. Автоматизированное производство требует минимального числа офисных работников - операторов, техников и программистов и почти не нуждается в синих воротничка. Подробно о прогнозируемых изменениях можно почитать в популярной литературе [3], но даже поверхностный анализ позволяет заметить одну вещь. Даже в продуктах самых известных ИТ корпораций, которые годами совершенствуют свои системы, обнаруживаются опасные уязвимости [4]. Даже самые крупные компании, несмотря на внедренные средства защиты или контроль со стороны независимых организаций, становятся жертвами инцидентов [5]. А теперь представим худший сценарий, к которому может привести повсеместное распространение “умных” устройств, когда отдельное домохозяйство превращается в целую информационную систему, со множеством хитро связанных компонент. Ведь эти компоненты нужно не только правильно спроектировать и разработать, но еще и правильно внедрить, учитывая особенности окружения и лучшие практики работы с соответствующими системами. Как это могут сделать обычные люди, которые просто хотят иметь дома умный телевизор или скачать на рабочий компьютер музыку с любимого телефона? Вопрос возможности решить подобную задачу – дискуссионный. Но проблема осложняется тем, что в реальной жизни мы боремся не только с техническими сбоями или непреднамеренными ошибками эксплуатации систем. В реальной жизни есть атакующая сторона — злоумышленник, который пытается целенаправленно использовать недостатки системы. И этот злоумышленник тоже не стоит на месте. Уже сейчас существуют различные способы автоматизации атак, в частности, с использованием популярного поискового ПО Shodan (https://xakep.ru), которое позволяет любому желающему находить публично доступные в Internet IoT-устройства. А знаменитая история с Иранскими центрифугами и вирусом Stuxnet показывает, что может сделать группировка профессионалов, если она задалась целью совершить таргетированную атаку.

Облака

Другим массовым трендом современности являются облачные технологии. Amazon, Microsoft, Google и множество компаний помельче стремительно развивают свою инфраструктуру и сервисы, чтобы отвоевать долю рынка побольше. Облачные технологии предлагают клиентам большой спектр услуг, существенно упрощают процессы технического обслуживания, обеспечивают высокую надежность и масштабируемость, но также не являются панацеей. Несмотря на то, что все крупные провайдеры уделяют большое внимание информационной безопасности, проходят сертификации на предмет соответствия требованиям различных стандартов по информационной безопасности (например, PCI DSS) и регулярно выпускают новые features, проблем не становится меньше. Облака не способны защитить от человеческого фактора. Получая доступ к облачным сервисам и с легкостью создавая ИТ-инфраструктуру, клиенты облачных провайдеров часто забывают об элементарных правилах безопасности. Выше упоминалась история компании, которая открыла публичный доступ к базе данных, где хранились персональные данные клиентов. И это не единичный случай, но распространенная ситуация. Согласно материалам той же статьи исследователю удалось обнаружить 7000 баз данных в облаке Amazon, владельцы которых оставили их публичными. И это только один облачный провайдер, и только одна проблема.

Если отойти от узкого определения облаков как облачных провайдеров, которые продают организациям услуги IaaS, PaaS, SaaS и т.п., и рассмотреть их в широком контексте, возникает еще одна интересная проблема. Обычно, когда мы заполняем профиль в социальных сетях, пользуемся браузером или делаем покупки в on-line-магазине, мы не задумываемся о том, что происходит на другой стороне. А между тем собранные данные накапливаются, формируется наш поведенческий профиль, и для таких компаний, как Google и Facebook главным активом являются их пользователи, которые незаметно оставляют в Сети детальный слепок самих себя. В свою очередь агрегированная таким образом информация может продаваться третьим, не всегда благонадежным сторонам [6]. И хотя в рамках государственного регулирования возникают такие инициативы, как GDPR[1], есть большие сомнения в действенности такого подхода. У государственных органов, призванных контролировать работу с персональными данными, не хватает ресурсов, чтобы охватить даже малую часть контролируемой области. Кроме того, оказывается под вопросом право личности на забвение. Если раньше даже самый тяжелый преступник мог рассчитывать на новую жизнь с чистого листа, то в мире, где как гласит лозунг одной поисковой системы: «найдется все!», такого права может не оказаться.

[1] 25 мая 2018 г. вступил в силу Общий регламент по защите персональных данных Европейского союза (англ. General Data Protection Regulation, GDPR).

Заключение

Подобно другим крупным изменениям в истории цивилизации, цифровая революция происходит незаметно. Неолитическая революция не уничтожила всех охотников-собирателей разом. Изобретение пороха не отменило холодное оружие, которое в некоторых нишах используют до сих пор. Любой тренд имеет свою динамику, область распространения и ограничения. Незаметно для нас новые технологии завоевывают место под Солнцем, пока старые продолжают жить рядом. Происходящие изменения порождают неприятную ситуацию, когда скорость изменений оказывается быстрее способности людей приспосабливаться к этим изменениям. Нарастающий поток сообщений об инцидентах, взломах и атаках, расцветающие как грибы после дождя новые продуты и стартапы в информационной безопасности, повышенный интерес государств и отраслевых регуляторов к киберугрозам — все это свидетельства увеличивающегося спроса на безопасность, который судя по отчетам профильных компаний, остается неудовлетворенным. С учетом непрерывно увеличивающейся сложности технологической экосистемы задача обеспечения безопасности становится все более трудно выполнимой. Вероятно в ближайшие годы это приведет к значительному увеличению популярности различных форм аутсорсинга ИБ и ИТ, когда все больше компаний будут отдавать работы по техническому сопровождению бизнеса и его защите сторонним организациям, а сами сосредотачиваться только на профильных задачах, потому что держать собственный штат компетентных специалистов будет непозволительной роскошью. Уже сейчас видны примеры подобных сервисных организаций. В свою очередь это породит вопрос о доверии к подобным организациям и устойчивости такого подхода — ведь тогда безопасность сосредоточится в руках относительно небольшого числа провайдеров услуг, которые могут оказаться наиболее уязвимыми звеньями новой экосистемы и сделать ее хрупкой. Но это совсем другая история [7].

Список литературы

1. *Bush Vannevar.* As We May Think. The Atlantic Monthly. 1945. Http://www.theatlantic.com
2. *Назаретян А.П.* Нелинейное будущее. Мегаистория, синергетика, культурная антропология и психология в глобальном прогнозировании. Инфра-М. 2014. 512 с.
3. *Клаусс Шваб.* Четвертая промышленная революция. Эксмо. 2016.
4. *Hart Jon.* Cisco Smart Install Exposure. 2017. https://blog.rapid7.com
5. *Brian Fung.* Equifax's massive 2017 data breach keeps getting worse. https://www.washingtonpost.com
6. *Brodkin Jon.* Verizon and AT&T will stop selling your phone's location to data brokers. 2018. https://arstechnica.com
7. *Таллеб Н.Н.* Антихрупкость. Как извлечь выгоду из хаоса. КоЛибри. 2016. 768 с.

Гусейнов Рустам Мехтиевич *– аудитор Digital Complianc.*
Контактный телефон +7 (495) 649 -81 -35.

Рикор разработал отечественный аналог BIOS

Российский инновационный холдинг Рикор разработал серверную систему ввода/вывода (BIOS). Это первая отечественная базовая система, принципиальное отличие которой от импортных аналогов заключается в возможности сертификации исходного кода.

Анализ исходного кода и последующая сертификация являются обязательными условиями для применения ПО в российских государственных учреждениях. Они необходимы для поиска "закладок" и прочих недокументированных функций ПО, которые могут привести, например, к утечке данных.

Системой ввода/вывода Рикор теперь будут оснащаться все производимые холдингом сервера и системы хранения данных. Кроме того, на них также будет установлен модуль управления сервером (BMC Рикор), о разработке которого холдинг объявил в мае 2018 г. Разработка BMC Рикор осуществлена на основе проекта с открытыми кодами (openbmc): производитель предоставляет пользователям системы доступ к исходным кодам для дальнейшей сертификации или внесения необходимых изменений.

Возможность сертификации исходного кода системы ввода/вывода и открытый доступ к кодам модуля управления сервером означают, что в серверах и системах хранения данных Рикор гарантированно отсутствуют несанкционированные модули ПО — "закладки".

В целом продукция Рикор ориентирована в первую очередь на компании, заинтересованные в импортозамещении: производство полностью находится на территории РФ, а разработав собственные системы BIOS и BMC, компания увеличила адвалорную долю отечественных компонентов почти до 70%.

Http://rikor.com