ТЕМА В ФОКУСЕ: ДИЛЕММЫ КИБЕРБЕЗОПАСНОСТИ

И.А. Шеремет*

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ В УСЛОВИЯХ РАЗВИТИЯ ЦИФРОВОЙ ЭКОНОМИКИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский государственный университет имени М.В. Ломоносова»
119991, Москва, Ленинские горы, 1

Опора на возможности цифровой экономики рассматривается в стратегических документах Российской Федерации в качестве одного из ключевых факторов, способных в современных условиях обеспечить экономический рост и национальный суверенитет, а также стимулировать развитие производства во всех сферах социально-экономической деятельности. В то же время, как отмечает автор, неуправляемый переход на новые принципы организации экономики может резко повысить ее уязвимость для враждебных действий в киберсфере. В этой связи представляется необходимым более подробно осветить вызовы и угрозы, с которыми сопряжен процесс цифровизации в экономической сфере.

В статье рассмотрены основные подходы к определению сущности феномена цифровой экономики, а также наиболее перспективные направления развития глобальной информационной инфраструктуры вообще и ее аппаратно-программных элементов в частности. Автор отмечает, что ключевое значение в этом контексте приобретают проблемы разработки оптимальных механизмов управления социотехническими системами, образующими цифровую экономику. Вместе с тем наблюдается резкое расширение спектра угроз кибербезопасности, реализуемых посредством различных информационно-технологических воздействий. В статье подробно освещены основные виды кибератак и описаны их возможные последствия для опорных инфраструктур цифровой экономики. Автор подчеркивает, что связность ее объектов существенно повышает разрушительность так называемых цепных эффектов кибератак.

* *Шеремет Игорь Анатольевич* — доктор технических наук, профессор, член-корреспондент Российской академии наук, главный научный сотрудник факультета мировой политики МГУ имени М.В. Ломоносова, заместитель директора по науке Российского фонда фундаментальных исследований (e-mail: sheremet@rfbr.ru).

В условиях невозможности достижения полной защищенности цифровой экономики от киберугроз особую роль приобретает устойчивость социотехнических систем. Киберустойчивость предполагает способность системы выполнять свои функции в условиях успешно реализованных кибератак на ее ресурсы (возможно, несколько менее эффективно в течение относительно непродолжительного периода времени, необходимого для нейтрализации кибератак и устранения их последствий).

Обращаясь к проблеме обеспечения киберустойчивости формирующейся цифровой экономики Российской Федерации, автор рассматривает основные виды системоразрушающих кибератак, а также освещает шаги, предпринимаемые правительством России для парирования этих угроз. Автор заключает, что достижение независимости и устойчивости российской информационной инфраструктуры невозможно без создания соответствующего научно-технологического потенциала и подготовки нового поколения научно-технических кадров.

Ключевые слова: Российская Федерация, цифровая экономика, глобальная информационная инфраструктура, социотехническая система, кибератака, кибербезопасность, киберустойчивость.

Сегодня человечество переживает интереснейший и чрезвычайно динамичный период своего развития. Проникновение информационных технологий (ИТ) во все сферы жизни и деятельности людей, формирование целостной глобальной техносферы из взаимосвязанных инфраструктур — энергетической, транспортной, производственной, финансовой и собственно информационной — создают предпосылки для возникновения в планетарном масштабе совершенно нового уклада жизни, основные характеристики которого принято объединять понятием «цифровая экономика» [The new digital economy, 2011: 31].

Говоря о цифровой экономике, как правило, имеют в виду четыре ключевых аспекта:

– гибкие энергоэффективные киберфизические производства на основе аддитивных технологий и глубокой роботизации процессов ассемблирования создаваемых материальных объектов [Lee, 2015];

– интеллектуальную глубоко роботизированную логистику, обеспечивающую максимально быстрое перемещение материальных объектов и ресурсов в материальном пространстве при минимальных затратах энергии на реализацию этих перемещений [Managing the transition to driverless road freight transport, 2017: 74];

– цифровые финансовые технологии, обеспечивающие максимально оперативное и безопасное выполнение финансовых операций [Шеремет, 2018];

– «интернет вещей» [Internet of things, 2017: 311], который, интегрируясь с «интернетом сервисов» и «интернетом людей», постепенно трансформируется в «интернет всего» (internet of everything), т.е. глобальную информационную инфраструктуру (ГИИ) — центр современной цивилизации, объединяющий людей и различные технические объекты, в том числе средства производства, образующие «промышленный интернет вещей» (industrial internet of things).

В свою очередь механизмы использования возможностей ГИИ эволюционируют по следующим основным направлениям:

– реализация парадигмы «больших данных» (big data) [Magoulas, Lorica, 2009], в рамках которой пользователям ГИИ доступны огромные массивы ретроспективной и текущей информации, необходимой для принятия различных решений и оптимизации повседневной деятельности субъектов глобальной экономики;

– развитие информационно-технологических инструментов для оперирования «большими данными» (data mining) [Lescovec et al., 2014: 511], обеспечивающих поиск логических и статистических закономерностей, которые проявляются в накапливаемых массивах сведений;

– повсеместное внедрение средств и технологий искусственного интеллекта, в первую очередь самообучения (machine learning) [Alpaydin, 2004: 400], для решения широкого спектра управленческих и аналитических задач.

Аппаратно-программную поддержку перечисленных средств обеспечивает развитие вычислительной и коммуникационной основы ГИИ в следующих областях:

– реализация парадигмы «облачных вычислений» (cloud computing) [Cloud computing law, 2013: 448], в рамках которой индивидуальные и корпоративные пользователи, по сути, передают на аутсорсинг функции накопления «больших данных» и обработки потоков сообщений от устройств, включенных в ГИИ, оставляя за собой формирование запросов (заказов) и обращение с ними к центрам обработки данных (ЦОД), или дата-центрам (data centers), доступным посредством соответствующего языково-программного интерфейса с пользовательских терминалов (настольных рабочих станций и мобильных устройств типа смартфонов);

– дополнение возможностей «облачных вычислений» «повсеместными вычислениями» (ubiquitous computing) [Kang, 2007], или «туманными вычислениями» (fog computing) [Perera et al., 2017: 32], реализуемыми на миллиардах вычислительных средств пользователей и устройств «интернета вещей»;

– создание коммуникационной инфраструктуры, обеспечивающей максимально высокую при достигнутом уровне развития технологий скорость трафика между элементами ГИИ.

Дата-центры представляют собой сети высокопроизводительных стационарных компьютеров (в том числе суперкомпьютеров), архитектура которых позволяет максимально распараллелить процессы обработки входящих информационных потоков. Принципиальной особенностью ЦОД являются наращиваемые поля памяти, обеспечивающие хранение «больших данных» и оперативный доступ к ним. С помощью программных средств ЦОД реализуются самые разные «облачные вычисления», необходимые для решения широкого круга задач, тем самым корпоративные и индивидуальные клиенты избавляются от затрат на поддержание вычислительной базы и обеспечение ее надежного функционирования.

При этом в качестве альтернативного подхода к организации массовых вычислений в последние годы активно прорабатываются упомянутые «туманные вычисления», суть которых состоит в использовании огромных ресурсов вычислительных средств, работающих «на земле» (от смартфонов до видеокамер и транспортных «беспилотников») и включенных в ГИИ. Термин «туманные вычисления» отражает реальность в том смысле, что приближение облака к земле порождает туман. Использование вычислительных ресурсов «тумана» позволяет снизить нагрузку на дата-центры и соответственно радикально уменьшить время обработки входных потоков. Коммуникационной основой «туманных вычислений» в настоящее время выступает сотовая инфраструктура 5G, обеспечивающая максимально быстрый обмен между различными устройствами (device-to-device, D2D), в первую очередь «интернета вещей».

Совместное использование современных парадигм вычислений позволяет оптимизировать затраты на собственно информационно-технологическую основу цифровой экономики и переместить центр тяжести работ по ее развитию на создание математических основ и алгоритмики оптимального (рационального) управления образующими ее социотехническими системами (СТС).

Однако обратной стороной этого процесса являются существенное расширение спектра угроз кибербезопасности СТС — различных информационно-технологических воздействий (ИТВ), или кибератак, на их ресурсы, а также последствия реализации этих угроз.

* * *

Несмотря на централизованную реализацию функций защиты информационных и программно-аппаратных ресурсов СТС на основе самых совершенных технологий обеспечения кибербезопасности, каждая из опорных инфраструктур цифровой экономики постоянно подвергается кибератакам, описание разрушительных результатов и способов совершения которых составляет один из наиболее интересных и читаемых разделов новостных лент [Жуков и др., 2014: 184]. Действительно, деструктивные, системоразрушающие последствия кибератак на СТС и используемые ими инфраструктуры трудно переоценить [Шеремет, 2017: 480].

Вывод из строя сегментов энергетической инфраструктуры представляется наиболее опасным для всех использующих ее СТС, так как лишает электроэнергии все их элементы и приводит к обездвижению электрозависимого транспорта (в первую очередь железнодорожного и подземного), остановке производственно-технологических процессов, параличу жилищно-коммунальной инфраструктуры (отключению освещения, водоснабжения и канализации, лифтового хозяйства, холодильного оборудования, нагревательных приборов и систем регулирования микроклимата внутри помещений), а также информационной инфраструктуры (средств и систем передачи, накопления, обработки и отображения информации). Прекращение функционирования автозаправочных станций и систем навигации и управления движением останавливает автомобильный, воздушный и водный транспорт. Прерывание электроснабжения служит триггером деструктивных социальных процессов. Выключение охранных систем торговых центров и хранилищ готовой к реализации продукции в сочетании с параличом лишенной мобильности правоохранительной системы провоцирует массовые безнаказанные грабежи. Органы государственной и муниципальной власти де-факто перестают выполнять свои функции, и ставший объектом кибератаки на его энергетическую инфраструктуру мегаполис в короткие сроки превращается в территорию хаоса и анархии.

Как можно видеть, подобное широкомасштабное системоразрушающее воздействие на городскую агломерацию по своим последствиям вполне сопоставимо с ударом по ней оружием массового поражения.

Столь же опасны кибератаки на элементы транспортной инфраструктуры, особенно в условиях насыщения транспортных систем беспилотными средствами. Находясь под управлением субъекта ИТВ, каждое такое средство (автомобиль, летательный аппарат, морское или речное судно) может стать препятствием для функционирования других транспортных средств либо даже инструментом кинетического воздействия на материальные объекты любого рода (так, по некоторым оценкам, самолеты, врезавшиеся в небоскребы 11 сентября 2001 г., вскоре после взлета были переведены истинными организаторами этого преступления в режим автопилотирования с заранее введенными траекториями, запрограммированными на встречу со зданиями; как впоследствии отмечали компетентные эксперты, для наведения по короткой глиссаде тяжелого и габаритного пассажирского «Боинга» на узкий небоскреб требуется квалификация опытного летчика палубной авиации, которой люди, названные впоследствии террористами и прошедшие курсы пилотирования для пилотов-любителей, заведомо не обладали).

Кибератаки на объекты производственной инфраструктуры способны, в простейшем случае, остановить выпуск продукции, жизненно важной для населения (в первую очередь продовольственных товаров), или, что гораздо более опасно, привести к нарушению производственно-технологических процессов и выводу из строя сложного и дорогостоящего оборудования, выполняющего уникальные функции. Результатом может стать остановка целой кооперации, производящей конкурентоспособные изделия, вследствие чего кооперация понесет многомиллионные (если не миллиардные) убытки. В тех случаях, когда речь идет о производстве продукции военного назначения, под угрозу могут быть поставлены планы переоснащения вооруженных сил и поддержания военно-технического паритета с потенциальными противниками. Однако еще более опасно так называемое отложенное воздействие, в основе которого лежит производство дефектоносных комплектующих: их отказ в условиях боевого применения образцов и систем оружия может привести к массовому выходу последних из строя.

Результатом ИТВ на производственные объекты химической и микробиологической промышленности становится загрязнение

окружающей среды вредными веществами и микроорганизмами, что не менее опасно, чем применение химического и биологического оружия.

Тем не менее наиболее распространенными и результативными являются кибератаки на объекты финансового сектора [Кузнецов и др., 2017]. С повсеместным внедрением технологий мобильного банкинга объем средств, похищенных путем реализации ИТВ на автоматизированные банковские системы, вырос на несколько порядков. Если в 2007 г. он составлял лишь 2% всех украденных за год денежных средств, то в 2017 г. эта цифра увеличилась до 98%, а в абсолютном выражении она приблизилась к 300 млрд долл. США в год. Опасность кибератак на финансовый сегмент цифровой экономики заключается в том, что, не затрагивая техносферу как таковую, они могут способствовать полному разрушению системы взаимных расчетов субъектов глобальной либо любой национальной экономики и, таким образом, привести ее в состояние полного хаоса и последующего коллапса.

Следует отметить, что связность различных инфраструктур цифровой экономики и их отдельных объектов между собой существенно повышает результативность кибератак на основе так называемых каскадных, или цепных, эффектов (chain effects) [Sheremet, 2018]. При этом результат ИТВ на какой-либо объект (например, искаженный радиосигнал, превышенное значение электрического тока или недостаточное количество материального ресурса на выходе производственного комплекса) становится самостоятельным воздействием на физически и/или информационно связанные с ним объекты, и «волны» таких производных воздействий могут в течение короткого времени распространиться по территориям мегаполисов и целых регионов, вызвав описанные ранее фатальные последствия.

В этой связи в последнее время стало актуальным понятие «устойчивости» СТС, цифровой экономики и в целом техносферы к кибератакам, или, для краткости, киберустойчивости [Gvishiani et al., 2018]. Данное понятие (в англоязычной литературе слову «устойчивость» применительно к рассматриваемой области соответствуют «sustainability» и «resilience») является более широким по отношению к давно применяемому термину «кибербезопасность» (cybersecurity). Последняя понимается как защищенность от угроз, т.е. невозможность их успешной реализации вследствие использования адекватных мер защиты. Однако практика последних 30 лет показывает, что огромное количество СТС, удовлетворявших априори всем критериям кибербезопасности,

оказывались уязвимыми для новых видов ИТВ, разработанных с учетом возможностей и ограничений применяемых средств защиты. При этом, однако, часть таких систем, несмотря на относительно успешно проведенные кибератаки на их ресурсы, продолжали функционировать с минимальным ущербом для их эффективности, тогда как другие выходили из строя на весьма продолжительное время и несли значительный материальный и репутационный ущерб. В этой связи киберустойчивость СТС (и в целом цифровой экономики) трактуется как способность системы выполнять свои функции в условиях успешно реализованных кибератак на ее ресурсы (возможно, несколько менее эффективно в течение относительно непродолжительного периода времени, необходимого для нейтрализации кибератак и устранения их последствий).

* * *

С точки зрения возможности достижения и поддержания киберустойчивости информационной инфраструктуры России и создаваемой на ее базе цифровой экономики особое значение приобретает анализ основных разновидностей и особенностей системоразрушающих кибератак.

Наиболее часто применяется «штурмовое» ИТВ, называемое также кибератакой типа «распределенный отказ в обслуживании» (distributed denial of service, DDoS). Ее сущность заключается в генерации массового потока сообщений на интернет-узел (адрес), являющийся объектом атаки, вследствие чего штатные обращения к нему для реализации с его помощью тех или иных функций практически не доходят до обработки, и информационный процесс, развитие которого зависит от данного узла, замедляется до недопустимых пределов и в итоге разрушается. Генерация потока, как правило, реализуется так называемой бот-сетью, содержащей заблаговременно скрыто установленные на пользовательских компьютерах, смартфонах и устройствах «интернета вещей» специальные программные модули («операционные мины», ОМ). Группировка ОМ, управляемая по скрытым коммуникационным сетям, использующим в качестве носителя команд естественный трафик интернета, способна сгенерировать поток сообщений плотностью десятки и сотни терабайт в секунду, который в свою очередь может парализовать или по крайней мере серьезно замедлить работу любой СТС, функционирующей в реальном времени (единицы секунд на сообщение).

DDoS-атаки, однако, представляют собой достаточно примитивное «силовое» воздействие, парируемое и контролируемое на основе не очень сложных архитектурно-программных решений.

Гораздо более опасными являются кибератаки типа «человек посередине» (man-in-the-middle, MITM), в основе которых лежит использование специальных программных или аппаратно-программных модулей, способных перехватывать трафик между двумя взаимодействующими объектами интернета и модифицировать этот трафик, приводя к изменению функционирования его получателей (людей и устройств). Результатом реализации таких кибератак могут быть любые самые опасные ситуации: аварии транспортных средств, техногенные катастрофы любого масштаба, отключения электроэнергии в целых регионах, массовые хищения денежных средств и т.п. Во время боевых действий применение MITM-кибератак по интегрированным автоматизированным системам управления войсками и оружием противника может привести к искажению координат объектов поражения, передаваемых от его командных пунктов на огневые средства, и в итоге — к бесполезному расходованию им боезапаса и целому ряду других последствий, которые могут решающим образом сказаться на ходе и исходе вооруженной борьбы.

Традиционный подход к предотвращению MITM-атак предполагает закрытие трафика между удаленными объектами системы криптостойкими методами шифрования и их взаимное опознавание на основе имитостойких методов аутентификации.

Наиболее совершенные специальные информационные технологии (СИТ), обеспечивающие нейтрализацию эшелонированных систем обеспечения кибербезопасности и осуществления разнообразных ИТВ на защищенные ресурсы СТС, объединяют под общим названием «глубоко разработанные длительно реализуемые угрозы» (advanced persistent threats, APT).

Эффективность APT-атак относительно достигнутого уровня развития средств и систем кибербезопасности есть результат противостояния в духе «снаряд–броня», спроецированного на киберпространство. При этом, однако, указанная эффективность мультиплицируется соотношением возможностей противоборствующих сторон по реальному управлению фрагментами ГИИ и национальных информационных инфраструктур.

Так, в 2013 г. достоянием гласности стало наличие ОМ в семействе средств сетеобразования, производимых американской фирмой CISCO. Только на территории Российской Федерации функционировало 9121 такое средство (в Нидерландах — 1053,

КНР — 1285, Австралии — 1530, в самих США — 2751), что позволяло Агентству национальной безопасности США, имплантировавшему эту ОМ, практически полностью контролировать внутрироссийский трафик интернета и при необходимости осуществлять DDoS-, MITM- и APT-атаки на субъекты российской экономики, использующие российский сегмент Всемирной сети.

Другим системным недостатком этого сегмента является прохождение интернет-трафика, обеспечивающего обмен между российскими пользователями, через средства сетеобразования, расположенные на территории зарубежных стран (на конец 2018 г. подобный трафик составлял до 10% всего внутрироссийского трафика). Это обстоятельство также делает интернет-зависимые субъекты российской экономики уязвимыми для широкого спектра кибератак.

Третий весьма серьезный недостаток российского сегмента интернета и в целом российской информационной инфраструктуры — ее перенасыщенность программными и вычислительными средствами зарубежного производства (упомянутый пример с оборудованием CISCO — одна из многих возможных иллюстраций этого обстоятельства). Все такие средства в общем случае могут быть носителями ОМ, создающих угрозу нормальному функционированию всей техносферы Российской Федерации. Каждая из этих «мин» может использоваться как для деструктивного воздействия, так и для расширения контролируемой области киберпространства посредством скрытой установки новых ОМ на ранее не подконтрольных объектах.

Однако еще более уязвимой для кибератак российская экономика может стать вследствие неуправляемого перехода на упомянутые ранее «облачные технологии» и тесно связанные с ними хранилища «больших данных», физически располагающиеся на территории зарубежных стран. В настоящее время крупнейшие мировые игроки на рынке ИТ-сервисов (в первую очередь Amazon и Facebook) активно инвестируют в создание дата-центров, которые позволят им в обозримом будущем захватить устойчивые конкурентные позиции в глобальной цифровой экономике. Это означает перемещение огромных массивов данных, чувствительных для СТС различных стран, из-под национальной юрисдикции. Фактически на территории этих государств могут остаться примитивные терминалы (уровня смартфонов) для обращения к упомянутым сервисам и устройства «интернета вещей», а все программные средства и массивы данных, необходимые для обработки этих обращений, будут находиться в дата-центрах

под полным контролем их владельцев. Иными словами, любая национальная (в том числе российская) информационная инфраструктура при успешной реализации подобного сценария может полностью виртуализироваться и в реальности стать собственностью зарубежных политико-экономических акторов.

* * *

Как можно судить по шагам, предпринимаемым российской законодательной и исполнительной властью, рассмотренные угрозы руководством страны глубоко осознаны и меры, необходимые для их парирования, достаточно быстро реализуются.

В программе «Цифровая экономика Российской Федерации», утвержденной распоряжением Правительства Российской Федерации от 28 июня 2017 г. № 1632-р[1], присутствует специальный раздел «Информационная безопасность», и центром компетенции по этому разделу определен Сбербанк, обладающий наиболее эффективной в России службой кибербезопасности. С 2015 г. активно ведутся работы по созданию интегрированной сети связи (ИСС) для нужд обороны, безопасности и правоохранительной системы. Наличие такой сети, проект которой был разработан еще в 1990-е годы бывшим Федеральным агентством правительственной связи и информации, позволит изолировать от общедоступных коммуникационных ресурсов наиболее критичную для обороноспособности и безопасности страны часть российской информационной инфраструктуры. Со временем ИСС может охватить не только силовые ведомства, но и предприятия оборонно-промышленного комплекса, а затем и системообразующие субъекты российской экономики.

Наиболее серьезным вкладом законодательной власти России в решение рассматриваемых проблем следует считать принятие в 2017 г. Федерального закона № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[2]. Этим документом определены ключевые направ-

---

[1] Программа «Цифровая экономика Российской Федерации», утв. распоряжением Правительства Российской Федерации от 28 июня 2017 г. № 1632-р // Официальный сайт Правительства Российской Федерации. Доступ: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (дата обращения: 03.05.2019).

[2] Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Российская газета. 31.07.2017. Доступ: https://rg.ru/2017/07/31/bezopasnost-dok.html (дата обращения: 03.05.2019).

ления деятельности федеральных органов исполнительной власти в данной сфере. Важнейшим из этих направлений является создание под руководством ФСБ России государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).

Дальнейшее развитие законотворчество в рассматриваемой сфере получило в законопроекте № 608767-7 «О внесении изменений в Федеральный закон "О связи" и Федеральный закон "Об информации, информационных технологиях и защите информации" (в части обеспечения безопасности и устойчивого функционирования сети "Интернет" на территории Российской Федерации)»[3]. Документ одобрен Государственной Думой и Советом Федерации Федерального Собрания РФ. В случае его подписания Президентом Российской Федерации закон вступит в силу в ноябре 2019 г. Как указано в пояснительной записке к этому документу, он подготовлен «с учетом агрессивного характера принятой в сентябре 2018 года стратегии национальной безопасности США» и «в целях реализации защитных мер для обеспечения долгосрочной и устойчивой работы сети Интернет в России, повышения надежности работы российских интернет-ресурсов»[4]. Функции по координации обеспечения устойчивого и безопасного функционирования российского сегмента интернета возлагаются на Роскомнадзор. В указанном документе впервые в российской законодательной практике определены такие понятия, как «трансграничные линии связи» и «точки обмена трафиком», и предусматривается возможность установки на сетях связи специального оборудования для определения источника передаваемого трафика. Законопроектом предусмотрено создание инфраструктуры, обеспечивающей работоспособность российского сегмента интернета в условиях невозможности подключения российских операторов связи к зарубежным серверам. Документ содержит целый ряд принципиальных положений, реализация которых должна существенно повысить устойчивость создаваемой российской цифровой экономики к возможным системоразрушающим ИТВ, т.е. ее киберустойчивость. В частности,

---

[3] Законопроект № 608767-7 «О внесении изменений в Федеральный закон "О связи" и Федеральный закон "Об информации, информационных технологиях и защите информации" (в части обеспечения безопасности и устойчивого функционирования сети "Интернет" на территории Российской Федерации)» // Система обеспечения законодательной деятельности. Доступ: https://sozd.duma.gov.ru/bill/608767-7 (дата обращения: 03.05.2019).

[4] Там же.

с 2021 г. государственные органы и учреждения будут обязаны перейти на программные средства российского производства.

При этом, однако, следует понимать, что разработка российскими специалистами программного обеспечения с использованием информационно-технологических инструментариев зарубежного производства не снимает проблему, а лишь переносит ее на более глубокий системотехнический уровень вплоть до общесистемного программного обеспечения (систем управления базами данных, трансляторов с языков высокого уровня и т.п.), операционных систем и элементной базы вычислительных и коммуникационных средств. Таким образом, о полной независимости российской информационной инфраструктуры можно будет говорить только тогда, когда в нашей стране будет создан научно-технологический потенциал, способный разрабатывать и выпускать в требуемом количестве элементную базу с характеристиками, достаточными для реализации всех необходимых ИТ-сервисов.

Более того, в условиях постоянного повышения сложности и объемов создаваемых программных средств существенно возрастает опасность появления в них непреднамеренных дефектов (эксплойтов), которые, в отличие от ОМ, могут стать причиной выхода из строя целых сегментов СТС и запуска разрушительных процессов без участия каких бы то ни было противоборствующих субъектов. Последний яркий пример, иллюстрирующий это обстоятельство, — катастрофа пассажирского авиалайнера Boeing-737 MAX, причиной которой стал выявленный впоследствии эксплойт в бортовом программном обеспечении.

* * *

Можно заключить, что киберустойчивость цифровой экономики в широком смысле определяется не только ее защищенностью от кибератак и наличием в ней ресурсов, позволяющих функционировать в условиях их успешной реализации, но и качеством программного обеспечения образующих ее СТС. При таком понимании киберустойчивость есть проекция на техносферу качества программного обеспечения СТС, т.е. как минимум качества организации его создания и отладки в компаниях-производителях, а в более широком смысле — качества и результативности научных исследований в сфере ИТ и в областях знаний, на которых базируются соответствующие сегменты техносферы. Таким образом, в самом широком понимании киберустойчивость цифровой экономики есть функция качества

интеллектуального ресурса, обеспечивающего ее создание и функционирование, т.е. в конечном счете — нового класса, именуемого «кибертариатом». В данном контексте представляет несомненный интерес исследование вопросов классовой структуры общества будущего, основанного на цифровой экономике, равно как и самого понятия собственности в ее реалиях.

В целом проблема киберустойчивости в условиях цифровизации глобальной техносферы и реализации целым рядом государств таких амбициозных проектов, как «умный город» (smart city) и «умная нация» (smart nation), становится все более актуальной. В этой связи рассмотрение всего спектра научных, технологических, юридических, образовательных и иных задач, подлежащих решению в рамках данной проблемы, должно стать одним из приоритетов российской науки.

СПИСОК ЛИТЕРАТУРЫ

1. Жуков И.Ю., Михайлов Д.М., Шеремет И.А. Защита автоматизированных систем от информационно-технологических воздействий. М.: МИФИ, 2014.

2. Кузнецов С.К., Лебедь С.В., Шеремет И.А. Противодействие угрозам кибербезопасности банковско-финансовой сферы Российской Федерации // Вестник Академии военных наук. 2017. № 2. С. 41–45.

3. Шеремет И.А. Борьба с инфраструктурами как форма противоборства в условиях глобальной техносферы // Влияние технологических факторов на параметры угроз национальной и международной безопасности, военных конфликтов и стратегической стабильности / Под ред. А.А. Кокошина. М.: МГУ, 2017.

4. Шеремет И.А. Цифровая экономика и кибербезопасность ее финансового сегмента // Научные труды Вольного экономического общества. 2018. Т. 210. № 2. С. 23–34.

5. Alpaydin E. Introduction to machine learning. London: MIT Press, 2004.

6. Cloud computing law / Ed. by C. Millard. Oxford: Oxford University Press, 2013.

7. Gvishiani A.D., Roberts F.S., Sheremet I.A. On the assessment of sustainability of distributed sociotechnical systems to natural hazards // Russian Journal of Earth Sciences. 2018. Vol. 18. ES4004. DOI: 10.2205/2018ES000627.

8. Internet of things: Novel advances and envisioned applications / Ed. by D.P. Acharjya, M. Kalaiselvi Geetha. New York: Springer, 2017.

9. Kang B.-H. Ubiquitous computing environment threats and defensive measures // International Journal of Multimedia and Ubiquitous Engineering. 2007. Vol. 2. No. 1. P. 47–60.

10. Lee E.A. The past, present and future of cyberphysical systems: A focus on models // Sensors (Basel). 2015. Vol. 15. No. 3. P. 4837–4869. DOI: 10.3390/s150304837.

11. Lescovec J., Rajaraman A., Ullman J.D. Mining of massive datasets. Cambridge: Cambridge University Press, 2014.

12. Magoulas R., Lorica B. Introduction to Big Data. Sebastopol: O'Reilly Media, 2009.
13. Managing the transition to driverless road freight transport. Paris: OECD/ITF, 2017.
14. The new digital economy. How it will transform business (White paper). Oxford: Oxford Economics, 2011.
15. Perera C., Qin Y., Estrella J.C. et al. Fog computing for sustainable smart cities: A survey // ACM Computing Surveys. 2017. Vol. 50. No. 3. P. 32. DOI: 10.1145/3057266.
16. Sheremet I. Multiset analysis of consequences of natural disasters impacts on large-scale industrial systems // Data Science Journal. 2018. Vol. 17. No. 4. P. 1–17. DOI: 10.5334/dsj-2018-004.

I.A. Sheremet

ENSURING CYBERSECURITY IN THE CONTEXT OF DIGITAL ECONOMY DEVELOPMENT

Lomonosov Moscow State University
1 Leninskie Gory, Moscow, 119991

Strategic documents of the Russian Federation consider opportunities created by digital economy as one of the key factors capable of ensuring economic growth and national sovereignty as well as of stimulating production in all spheres of social and economic activities. However, the author stresses, that uncontrolled digitalization of economy can drastically increase its vulnerability to cyberthreats. In that context, it is necessary to address more specifically challenges and threats associated with the digitalization process in the economic sphere.

The paper examines key approaches to the definition of the phenomenon of 'digital economy' as well as the most promising directions for global information infrastructure development in general and its hardware/software elements in particular. The author notes that in this context the quest for the most effective management mechanisms of sociotechnological systems (STS) that make up the digital economy, is of special importance. At the same time one can observe a rapid expansion of cyberthreats realized by means of various infotechnological impacts. The paper provides a detailed analysis of the main types of cyberattacks and outlines their potential impact on critical infrastructures of the digital economy. The author emphasizes that the high level of interdependence of its elements significantly increases destructiveness of the so called chained effects of cyberattacks. In view of the impossibility of reaching complete protection of the digital economy from the cyberthreats resilience of the sociotechnological systems is of particular importance. Cybersustainability implies the ability of a system to perform its functions under successful attacks on its resources (prob-

ably less effectively within in a short period of time necessary to neutralize cyberthreats and their impacts).

Turning to the issue of ensuring cybersustainability of the emerging digital economy of the Russian Federation, the author examines the main types of system-destructing cyberattacks and highlights the steps taken by the Russian government to tackle these threats. The author concludes that it will impossible to achieve independence and resilience of the Russian information infrastructure without relevant capacity-building in science and technology as well as without training a new generation of S&T personnel.

Keywords: Russian Federation, digital economy, global information infrastructure, sociotechnological system, cyberattack, cybersecurity, cybersustainability.

About the author: *Igor A. Sheremet* — Doctor of Sciences (Engineering), Professor, Corresponding Member of the Russian Academy of Sciences, Chief Research Fellow at the School of World Politics, Lomonosov Moscow State University; Deputy Director for Science of the Russian Foundation for Basic Research.

REFERENCES

1. Zhukov I.Yu., Mikhailov D.M., Sheremet I.A. 2014. *Zashchita avtomatizirovannykh sistem ot informatsionno-tekhnologicheskikh vozdeystvii* [Protection of automated systems from information-technological impacts]. Moscow, MEPhI Publ. (In Russ.)

2. Kuznetsov S.K., Lebed' S.V., Sheremet I.A. 2017. Protivodeystvie ugrozam kiberbezopasnosti bankovsko-finansovoi sfery Rossiiskoi Federatsii [Countering cybersecurity threats to the banking and financial sector of the Russian Federation]. *Vestnik Akademii voennykh nauk*, no. 2, pp. 41–45. (In Russ.)

3. Sheremet I.A. 2017. Bor'ba s infrastrukturami kak forma protivoborstva v usloviyakh global'noi tekhnosfery [Infrastructure warfare as a form of confrontation in a global technosphere environment]. In Kokoshin A.A. (ed.). *Vliyanie tekhnologicheskikh faktorov na parametry ugroz natsional'noi i mezhdunarodnoi bezopasnosti, voennykh konfliktov i strategicheskoi stabil'nosti* [The impact of technological factors on parameters of national and international security, military conflicts, and strategic stability]. Moscow, Moscow University Press. (In Russ.)

4. Sheremet I.A. 2018. Tsifrovaya ekonomika i kiberbezopasnost' yeyo finansovogo segmenta [The digital economy and the cybersecurity of its financial segment]. *Nauchnyye trudy Vol'nogo ekonomicheskogo obshchestva*, vol. 210, no. 2, pp. 23–34. (In Russ.)

5. Alpaydin E. 2004. *Introduction to machine learning.* London, MIT Press.

6. Millard C. (ed.). 2013. *Cloud computing law.* Oxford, Oxford University Press.

7. Gvishiani A.D., Roberts F.S., Sheremet I.A. 2018. On the assessment of sustainability of distributed sociotechnical systems to natural hazards. *Russian Journal of Earth Sciences*, vol. 18, ES4004. DOI: 10.2205/2018ES000627.

8. Acharjya D.P., Kalaiselvi Geetha M. (eds.). 2017. *Internet of things: Novel advances and envisioned applications.* New York, Springer.

9. Kang B.-H. 2007. Ubiquitous computing environment threats and defensive measures. *International Journal of Multimedia and Ubiquitous Engineering*, vol. 2, no. 1, pp. 47–60.

10. Lee E.A. 2015. The past, present and future of cyberphysical systems: A focus on models. *Sensors (Basel)*, vol. 15, no. 3, pp. 4837–4869. DOI: 10.3390/s 150304837.

11. Lescovec J., Rajaraman A., Ullman J.D. 2014. *Mining of massive datasets*. Cambridge, Cambridge University Press.

12. Magoulas R., Lorica B. 2009. *Introduction to Big Data*. Sebastopol, O'Reilly Media.

13. *Managing the transition to driverless road freight transport*. 2017. OECD/ITF. Paris, OECD Publishing.

14. *The new digital economy. How it will transform business (White paper)*. 2011. Oxford, Oxford Economics.

15. Perera C., Qin Y., Estrella J.C. et al. 2017. Fog computing for sustainable smart cities: A survey. *ACM Computing Surveys*, vol. 50, no. 3, pp. 32. DOI: 10.1145/3057266.

16. Sheremet I. Multiset analysis of consequences of natural disasters impacts on large-scale industrial systems. *Data Science Journal*, vol. 17, no. 4, pp. 1–17. DOI: 10.5334/dsj-2018-004.