Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

Шон С. Костиган и Густав Линдстрьом,
Connections QJ 15, № 2 (2016): 9-19
https://doi.org/10.11610/Connections.rus.15.2.01

Рецензированная статья

Политика и Интернет вещей

Шон С. Костиган [a] и Густав Линдстрьом [b]

[a] *Новая школа, Нью Йорк, штат Нью Йорк, http://www.newschool.edu/*

[b] *Женевский центр политики безопасности, http://www.gcsp.ch/*

Резюме: Кибер-безопасность неуклонно продвигается в начало национальной повестки дня в сфере безопасности. В то же время происходит значимое слияние физического и виртуального миров. Сочетание технологий сделало это возможным под наименованием Интернет вещей (ИВ). Это слияние сделает так, что миллиарды датчиков и вычислительных устройств будут связаны в сети, которая не будет требовать вмешательства человека, со всеми проистекающими из этого превозносимыми выгодами, ожидаемыми рисками, неопределенностями и значимыми дилеммами в области безопасности. Используя прошлое как прогноз для будущего поведения, можно ожидать, что огромное увеличение числа устройств, которые можно взломать, породит огромное количество уязвимостей, которые коснутся физического мира. Тем не менее, ИВ даст такие возможности, которые сегодня мы только начинаем себе представлять, сделав по сравнению с самим собой Интернет революцию незначительной. Хотя технологическое развитие, похоже, обгоняет развитие политики, государство сохраняет за собой власть обсуждать эти проблемы и, в итоге, их регулировать. В этой статье рассматривается вопрос, почему политики должны беспокоиться об ИВ, рассматриваются существенные тенденции на следующие пять-десять лет и вероятные последствия для безопасности, проистекающие из этих тенденций. Статья завершается обзором соображений, касающихся политики по данной проблеме.

Ключевые слова: Интернет вещей, Индустриальный Интернет, последствия ИВ для безопасности, машинные коммуникации, критические инфраструктуры.

Введение

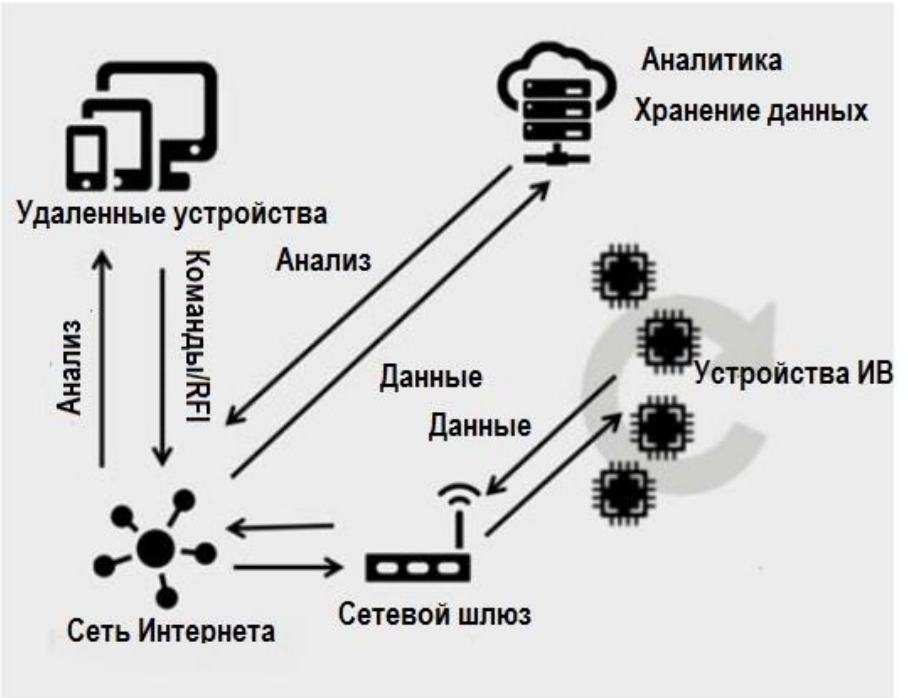
В течение последних десяти лет проблемы кибербезопасности неуклонно продвигались в начало национальной и международной повестки дня в сфере безопасности. Однако, если фокусироваться в основном на политике и стратегии, быстрое технологическое развитие и далее будет подрывать понимание политиками кибер рисков и кибер возможностей. Одним таким развитием технологии является Интернет вещей (ИВ).

Хотя Интернет вещей не является предметом обширной дискуссии в политических кругах, тем не менее он, вероятно, начнет оказывать влияние на то, как личности, институции и общества будут взаимодействовать в будущем. В двух словах, ИВ касается взаимосвязи типа «машина-машина» уникально идентифицируемых устройств через Интернет. Относительно широко известным примером такой связи является использование устройств радиочастотной идентификации (УРЧИ) в розничной торговле для определения местоположения и инвентаризации товаров.

По некоторым оценкам, в настоящее время имеется около 9 миллиардов устройств, связанных с Интернетом. Ожидается, что это число – которое уже больше, чем численность всего населения в мире – в следующие десять лет драматически будет расти. По последним подсчетам, каждую секунду к Интернету подсоединяется 127 новых устройств.[1] По прогнозам реномированных институтов предполагается, что к 2025 году с Интернетом будут связаны приблизительно от 50 миллиардов до 1 триллиона устройств, что окажет влияние на ведение дел в разных областях – от здравоохранения до политики безопасности. В настоящее время это порождает такие новые концепции, как переход к «Интернету всего» (Cisco) или «Промышленному Интернету» (General Electric). По оценкам General Electric, в следующие 20 лет «Промышленный Интернет» увеличит мировой ВВП на 10-15 триллионов долларов США. При таком масштабе роста ИВ приведет к новой эре распределенных вычислений, по сравнению с которой изменения, порожденные Интернетом, будут казаться маленькими.

В этой статье рассматривается вопрос, почему политики должны быть озабочены ИВ, рассматриваются важные тенденции на следующие пять-десять лет и возможные последствия для безопасности, проистекающие из этих тенденций. Статья заканчивается обзором соображений, касающихся политики по этой проблеме.

[1] “127 devices added to the Internet each second, but Congress is clueless about IoT,” *NetworkWorld*, 1 July 2015, доступно на http://www.networkworld.com/article/2942596/microsoft-subnet/127-devices-added-to-the-internet-each-second-but-congress-is-clueless-about-iot.html.



Фигура 1: Экосистема ИВ.
(Источник: Business Insider, www.businessinsider.com)

Почему Интернет вещей имеет значение

Мы полагаем, что существуют три основные причины, по которым субъекты, определяющие политику, должны считаться с ИВ. Во-первых, у Интернета вещей имеется потенциал для способствования существенному экономическому росту. Нынешнее развитие ситуации в этой области, например, постепенное внедрение интеллигентных измерителей (для повышения энергетической эффективности) и беспилотных автомобилей (для транспорта и логистики) является всего лишь небольшим примером возможностей, предоставляемых ИВ. Применение ИВ возможно во многих областях, что открывает дверь для экономического роста в основном через повышение эффективности и предоставление новых услуг, которые не требуют участия человека. Согласно одному исследованию консалтинговой компании Accenture, ИВ может увеличить на 10.6$ триллионов суммарный ВВП 20 стран с развитыми и развивающимися экономиками, дающими 75 % миро-

вого объема производства.[2] Согласно другому докладу Мирового института им. Мак-Кинси, экономическое влияние ИВ к 2025 году оценивается от 2.7$ до 6.2$ триллионов в год.[3]

Во-вторых, ИВ окажет влияние на множество разных областей, обеспечивая прогресс и повышение эффективности по разным направлениям, а не в одной или в двух сферах. Имея это в виду, областями, которые больше всего выиграют от ИВ, наиболее вероятно, будут здравоохранение, инфраструктура и сектор общественных услуг.[4] С учетом нынешних тенденций, возможные применения ИВ будут широко охватными, и в некоторых случаях будут ограничиваться только нашим воображением. Перспективы охватывают спектр от «умных городов» до «персонализированного здравоохранения». В число конкретных примеров может входить более эффективное управление транспортного потока, при котором дорожные знаки и светофоры будут коммуницировать между собой и с автомобилями поблизости. Датчики ИВ могут быть расположены на такой инфраструктуре, как мосты, для идентификации микротрещин, что позволит предпринимать профилактические меры для увеличения их срока службы. В секторе обороны ИВ можно использовать для улучшения логистики и транспорта. ИВ может также играть определенную роль и в автономных системах вооружения, в частности, если речь идет об автоматических системах.

В-третьих, субъекты, принимающие решения, должны интересоваться ИВ потому, что существуют недостатки и нежелательные последствия, некоторые из которых имеют значение для общества, критических услуг и критических инфраструктур. Как минимум, зависимость общества от ИВ и увеличивающаяся «поверхность, подверженная нападениям», будут иметь далеко идущие и трудно прогнозируемые последствия. Эти проблемы будут рассмотрены более подробно в разделе о потенциальных последствиях для безопасности.

---

[2] Mark Purdy and Ladan Davarzani, “The Growth Game-Changer: How the Industrial Internet of Things can drive progress and prosperity” (Accenture Strategy, 2015), доступно на https://www.accenture.com/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_18/Accenture-Industrial-Internet-Things-Growth-Game-Changer.pdf.

[3] James Manyika, Michael Chui, Jacques Bughin, Richard Dobbs, Peter Bisson, and Alex Marrs, “Disruptive Technologies: Advances that Will Transform Life, Business, and the Global Economy,” Report (McKinsey Global Institute, May 2013), доступно на http://www.mckinsey.com/business-functions/business-technology/our-insights/disruptive-technologies.

[4] Для дополнительной информации об экономическом влиянии ИВ, смотри Charles Saidu, Adamu Usman, and Peter Ogedebe, “Internet of Things: Impact on Economy,” *British Journal of Mathematics & Computer Science* 7:4 (2015): 241–251.

Тенденции будущего развития ИВ

Заглядывая вперед, можно выявить три взаимосвязанные тенденции, касающиеся ИВ. Первая, это ускоряющийся темп распространения ИВ, которое, хотя и находится на самой начальной стадии, заметно и сегодня. В качестве иллюстрации можно указать на факт, что с 2014 по 2015 год число вещей, связанных с Интернетом, увеличилось на 30 %. Таблица 1, показанная ниже, иллюстрирует тенденции в разных секторах.

Как показано в таблице, общий процентный рост по всем четырем рассматриваемым категориям составляет примерно 500 %, причем наибольший рост проникновения ИВ ожидается в автомобильной промышленности. Если эти траектории развития хотя бы приблизительно точны, общество столкнется с существенными изменениями в том, как собирается, подвергается мониторингу и обрабатывается информация. Эта тенденция поддерживается двумя другими четко различимыми тенденциями развития: 1) Продолжающееся развитие протоколов коммуникации (в том числе беспроводной), методов хранения энергии (например, батареи), микро электромеханических систем (МЭМС) и вычислительной мощи и 2) Развитие в областях, которые могут оказать влияние на применение ИВ, например, нанотехнологии, искусственный интеллект и науки о данных.[5]

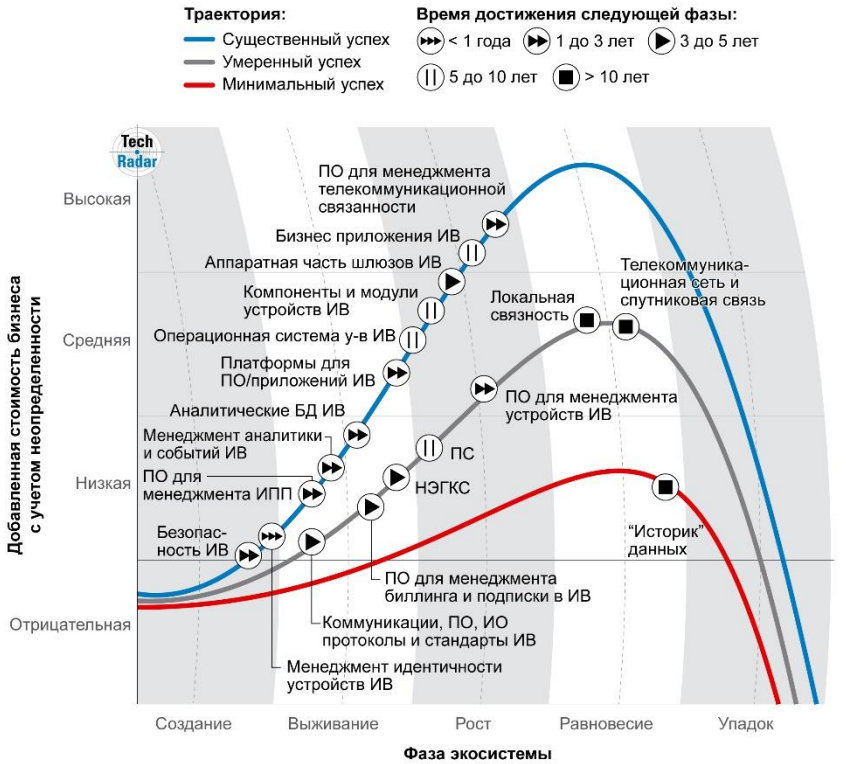
В сочетании эти две дополнительные тенденции расширят как охват, так и спектр приложений ИВ в ряде областей.

Таблица 1. Проникновение ИВ по секторам в миллиардах устройств (2015-2020).

Категория	2015	2020	Увеличение в процентах
Автомобили	372	3511	944 %
Потребление	2,875	13,173	458 %
Основной бизнес	624	5,159	827 %
Вертикально интегрированный бизнес	1,009	3,164	314 %
В целом	**4,880**	**25,007**	**512 %**

Источник: Gartner, “4.9 Billion Connected ‘Things’ will be in use in 2015,” November 2014.

[5] Для сведения, имеется множество протоколов, которые обеспечивают коммуникацию между устройствами. Оно охватывает такие беспроводные существующие протоколы как ZigBee, Bluetooth, и BACnet, а также разрабатываемые стандарты RPL, CoAP, и 6LoWPAN.



Фигура 2: Добавленная стоимость от ИВ за период в 10 лет
Источник: Forrester Research, www.zdnet.com/article/internet-of-things-security-years-away-from-being-fully-baked-says-forrester.

Второй основной тенденцией является быстрый рост машинных коммуникаций (M2M). По мере расширения проникновения ИВ будет расширяться и прямая коммуникация между устройствами, которые связаны через Интернет в проводной или беспроводной форме. По одной оценке прогнозируется, что общее число устройств, связанных по типу M2M, увеличится к 2018 году от 196 миллионов до 361 миллиона – рост на 184 % за три года.[6] Эта тенденция очень важна, поскольку мы не можем полностью предвидеть последствия, проистекающие из роста M2M коммуникаций. В мире, в котором коммуникации осуществляются или между человеком и

[6] The Statistics Portal, Statista, 2016. Доступно на www.statista.com/statistics/295635/total-number-m2m-connections-worldwide.

устройством, или между двумя устройствами, результат предсказать легче. В мире ИВ данные и коммуникации станут всеохватными.

К примеру, если некий датчик осуществляет мониторинг температуры в определенном месте и запрограммирован на отправку предупреждения человеку или другому устройству, когда температура достигнет определенного порога, направление движения информации ясное и простое. В устройствах, во все большей степени коммуницирующих мгновенно в процессе управления или мониторинга, взаимоотношения становятся многомерными, комплексными и возможно более стохастическими или случайными. С учетом этой тенденции способность контролировать конкретные отношения между устройствами может стать более сложной и непредсказуемой.

И последнее, расширение ИВ и M2M коммуникаций будет создавать все большее количество машинно-генерируемых данных. Согласно исследованию корпорации IDC «Цифровая вселенная» от 2012 года количество машинно-генерируемых данных к 2020 году увеличится в 15 раз.[7] Далее IDC отмечает, что к 2020 году около 40 % всех данных будут генерированы машинами. Эта тенденция будет иметь влияние на разные области, в частности на то, как накапливаются, обрабатываются, сохраняются и распространяются данные. И здесь политика по вопросу отстает от развития ситуации.

Потенциальные последствия для безопасности

Возможно, революция ИВ будет иметь два важных последствия для безопасности. В первую очередь, это устранение отсутствия функций безопасности в большинстве датчиков и приводов, которые составляют хребет ИВ. В частности, поскольку компании выбрасывают на рынок минимально жизнеспособные продукты с тем, чтобы удовлетворить спрос, дешевые датчики и приводы для сбора данных, осуществления мониторинга и оптимизации процессов будут оставаться без соответствующих встроенных в них функций безопасности. Безопасность, как правило, остается дорогостоящим запоздавшим соображением.

Более того, сенсоры, как правило, страдают ограниченной памятью и вычислительной мощью, что еще больше уменьшает возможность производить ИВ устройства с соответствующими протоколами, обеспечивающими безопасность (которые в схеме мышления разработчиков не являются первостепенной целью). Этот внутренне присущий недостаток в ИВ превращается в возможные общественные уязвимости, поскольку компрометирует устройства, используемые в разных областях, варьирующих от здравоохранения до сельского хозяйства.

[7] John Gantz and David Reinsel, “The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East” (IDC, December 2012), доступно на www.emc.com/leadership/digital-universe/2012iview/index.htm.

Эта уязвимость ИВ уже связывается с защитой критической инфраструктуры, для которой есть опасения, что такие системы промышленного контроля как «Диспетчерское управление и сбор данных» (ДУСД) могут быть скомпрометированы до такой степени, что это заблокирует работу критических услуг или критической инфраструктуры. При подключении миллиардов устройств онлайн поверхность современного общества, которая может подвергнуться нападению, неимоверно увеличивается, причем все эти неизбежные уязвимости, которые мы видим сегодня, будут присутствовать уже в гораздо более широком масштабе. Весьма вероятно каскадное нарастание проблем, поскольку одни системы будут контролировать другие. Системы управления, не связанные с Интернетом, доступ к которым раньше в принципе происходил с использованием систем собственной разработки, сейчас доступны через готовые коммерческие программы, к которым есть онлайн доступ.

Эта уязвимость привлекает все больше внимания после конкретных атак на иранские ядерные центрифуги (через вирус Stuxnet) и на саудовские рабочие станции компании Aramco (через вирус Shamoon). Иначе говоря, ИВ в потенциале сделает Интернет еще менее безопасным для всех.

Второй проблемой, порожденной ИВ, является баланс между индивидуальным правом на конфиденциальность и требованиями безопасности. Как недавно сформулировал это Брюс Шнайер, «бизнес моделью Интернета яв-

Фигура 3: Вызовы перед ИВ.
Источник: Information is Beautiful, http://www.informationisbeautiful.net.

ляется наблюдение»[8], и в мире ИВ эта проблема будет сильно разрастаться. Ее влияние, скорее всего, в краткосрочном и среднесрочном плане будет недооценена, особенно с учетом того, что развитие ИВ сопровождается развитием и в других областях. К примеру, встраивание датчиков в материалы для одежды – что облегчается прогрессом в нанотехнологиях – открывает дверь к мониторингу информации о местонахождении личности и, возможно, некоторых жизненных показателей. Заглядывая вперед, если использование встроенных датчиков для мониторинга состояния здоровья станет более распространенным, это может привести к широкомасштабному сбору данных о состоянии здоровья отдельного человека. Такое развитие уже происходит с так называемым движением носимых датчиков, но вероятно, уже в следующем десятилетии оно неимоверно усилится по глубине и охвату. Хотя от более персонализированной системы здравоохранения может быть много пользы, она может создать определенные проблемы в отношении индивидуального доступа к пакетам медицинского страхования и способности гарантировать возможности для найма на работу.

Уже сейчас сложный вопрос о балансировании прав на конфиденциальность и на безопасность станет еще более колючим. При перспективе использования миллиардов датчиков и устройств ИВ субъекты, определяющие политику, будут обязаны более тщательно проанализировать способы, с помощью которых можно скомпрометировать данные. Поэтому, кроме понимания проблем со сбором данных, будет нужно большее понимание уязвимостей на других этапах; к примеру: как собирается и используется информация в ИВ (к примеру, как она распространяется по отношению к третьей стороне?); существует ли опасность, что третья сторона получит доступ к чувствительным данным в ИВ; и как изменяется ценность данных, когда они сочетаются с другими данными.[9]

Соображения о политике по данной проблеме

Движение к Интернету вещей выдвигает перед субъектами, определяющими политику, несколько соображений, касающихся политики по этой проблеме. Самый главный вопрос, это как лучшим образом позиционировать национальную политику и стратегию с тем, чтобы воспользоваться выгодами ИВ в то же время минимизируя риски, ассоциируемые с увеличением числа устройств, связанных с Интернетом. Очень немногие страны (Чешская Республика, Объединенное Королевство и Австралия) и организации провели такой анализ на национальном уровне, тогда как другие страны восприняли подход наблюдения и выжидания, или вообще не имеют никакого подхода.

---

[8] Bruce Schneier, “The Internet of Things Talks About You Behind Your Back,” 13 January 2016, доступно на https://www.schneier.com/blog/archives/2016/01/the_internet_ of.html.

[9] Rolf Weber, “Internet of Things: Privacy Issues Revisited,” *Computer Law & Security Review* 31 (2015): 618–627.

Во-вторых, субъекты, определяющие политику, должны знать узкие места, которые могут отрицательно сказаться на возможностях, предоставляемых ИВ. В настоящее время имеется ряд существенных проблем, которые будут оказывать влияние на то, как развивается ИВ, начиная от технических вопросов – например, достижение согласия по конкретным стандартам для сетевой коммуникации в ИВ, – и заканчивая стратегическими соображениями, касающимися применимости ИВ в сфере безопасности.

В-третьих, субъекты, определяющие политику, должны попытаться лучше понять непреднамеренные последствия, проистекающие из революции ИВ. К примеру, как пострадают занятость и национальные экономики, когда определенные наборы умений станут лишними? С юридической точки зрения, как может ИВ оказать влияние на законодательные и нормативные гарантии? С технической точки зрения важно, каковы последствия расходящихся позиций по вопросу о конфигурировании и управлении устройств в ИВ (например, должны ли устройства заявлять о себе? Как будет осуществляться их аутентикация? Должны ли IP-адресы устройств в ИВ генерироваться автоматически системой или самим устройством?). Нет нужды говорить, что решения, касающиеся технической организации, могут иметь множество нежелательных последствий в разных областях.

Четвертое, государствам обязательно следует поощрять активное обсуждение по вопросу встраивания безопасности в производимые продукты. Все яснее становится, что производители устройств ИВ имеют мало стимулов для интегрирования протоколов безопасности в свои продукты. С другой стороны, становится все более очевидным, что отсутствие или недостаточность мер безопасности может привести к ужасным последствиям. В число примеров от последнего времени входят продемонстрированная возможность получить доступ к функциям управления скоростью и направлением полета через бортовую систему развлечений,[10] успешные попытки взломать такие медицинские устройства, связанные с ИВ, как инсулиновые насосы,[11] поисковые машины, которые позволяют подсматривать через незащищенные камеры для наблюдения за младенцами,[12] и уязвимости автомобилей и других беспилотных средств передвижения.[13] По мере того, как

[10] Dylan Tweney, “FBI Says This Hacker Took Over a Plane through Its In-flight Entertainment System,” *VentureBeat*, 17 May 2015, доступно на venturebeat.com/2015/05/17/fbi-says-this-hacker-took-over-a-plane-through-its-in-flight-entertainment-system/.

[11] Eric Basu, “Hacking Insulin Pumps and Other Medical Devices,” *Forbes*, 13 August 2013, доступно на www.forbes.com/sites/ericbasu/2013/08/03/hacking-insulin-pumps-and-other-medical-devices-reality-not-fiction.

[12] J.M. Porup, “How to Search the Internet of Things for Photos of Sleeping Babies,” *ArsTechnica*, 19 January 2016, доступно на http://arstechnica.co.uk/security/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies/.

[13] Andy Greenberg, “Hackers Remotely Kill a Jeep on the Highway – With Me in It,” *Wired*, 21 July 2015, доступно на http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

эти уязвимости будут лучше изучаться и обозначаться, для промышленности и кругов, определяющих политику, все труднее будет оставлять их без внимания.

И последнее, государство располагает полномочием призывать к ответу и, в конечном итоге, регулировать. Поэтому государство обязано быть на переднем фронте кривой рисков безопасности и использовать свою власть для поощрения принятия новых технологий и стандартов, которые принесут существенную пользу обществу. В качестве начала улучшения ситуации с безопасностью и улучшения процесса утверждения более безопасных устройств, государство должно профинансировать исследования на экспертном уровне, которые можно будет использовать для инициирования применения здравого «системного подхода» к безопасности и ИВ. Такой подход принесет свои дивиденды в следующие десятилетия.

О авторах

Шон С. Костиган является консультантом и аналитиком по вопросам технологий, риску и безопасности. Он старший советник по Новым вызовам безопасности Консорциума инициативы «Партнерство ради мира» военных академий и институтов, изучающих вопросы безопасности, также является лектором в Новой школе, Нью-Йорк сити. Он руководит совместной разработкой академиями обороны НАТО/ПРМ программы по кибер-безопасности. В последнее время он был представителем Министерства внутренней безопасности США и Канцелярии директора национальной разведки в Программе для частного сектора аналитиков разведывательного сообщества и консультировал федеральное правительство США по вопросам информационных технологий, кибер безопасности, экологической безопасности и прогнозам. Его последняя книга *Киберпространства и глобальные дела* вышла на английском и на китайском языках.
E-mail: costigs@newschool.edu.

Густав Линдстрьом является руководителем Программы по новым вызовам безопасности Женевского центра политики безопасности (ЖЦПБ). До этого он возглавлял Программу ЖЦПБ евроатлантической безопасности и был директором Европейского курса обучения по этим вопросам. В настоящее время он представляет ЖЦПБ в Исполнительном академическом совете Европейского колледжа безопасности и обороны и является сопредседателем Рабочей группы Консорциума ПРМ по новым вызовам безопасности. Доктор Линдстрьом защитил докторскую диссертацию в Высшей школе корпорации RAND и получил степень магистра по исследованиям в сфере международной политики в Стэндфордском университете. До занятия должности в ЖЦПБ он был старшим научным сотрудником в Институте исследований по вопросам безопасности ЕС (ИИБЕС). В сферу его интересов и его компетентности входят Общая европейская политика безопасности и обороны (ОПБО), новые вызовы безопасности, нераспространение и разоружение и кибер-безопасность.
E-mail: g.lindstrom@gcsp.ch.