Библиографические ссылки

1. Жилкин О. Н., Манцуров К. Б. Интеграция телематических инструментов в деятельность страховых компаний. Проект «умное страхование» // Вестник Университета. – № 7–8. – 2016. – М. : Издательский дом ГОУВПО ГУУ. – С. 202–207.

2. Индикаторы умных городов. – Москва, НИИТ : http:/www. niitc.ru/publications/SmartCities.pdf (дата обращения 15. 01.2020).

3. Финансы в цифровой экономике : сохранение традиций и новые горизонты / монография под общей ред. А. Н. Жилкиной. – М. : ГУУ, 2018.

4. Smart Communities Guidebook: How California's Communities Can Thrive in Digital Age. – San Diego, 1997.

5. Global B2C e-commerce sales 2012-2018 URL : https://www.statista.com/statistics/261245/b2c-e-commerce-sales-worldwide/ (дата обращения 16.12.2018).

6. Anna N. Zhilkina, Vladimir K. Krylov Financial and Economic and Information Aspects of Smart City – AI at Citizens' Service // Financial and Economic and Information Aspects of Smart City – AI at Citizens' Service. In : Popkova E., Sergi B. (eds) Artificial Intelligence : Anthropogenic Nature vs. Social Origin. ISC Conference – Volgograd 2020. Advances in Intelligent Systems and Computing, vol 1100. Springer, Cham. P. 148–155.

УДК 338.45:334.72

ИНДУСТРИЯ 4.0: ВЫЗОВЫ И УГРОЗЫ БЕЗОПАСНОСТИ

М. Ю. Завгородняя

Кандидат экономических наук, научный сотрудник отдела промышленной политики ГУ «Институт экономики и прогнозирования НАН Украины», г. Киев (Украина)

В статье определены вызовы безопасности, связанные со становлением цифровой экономики и распространением Индустрии 4.0. Проанализированы вызовы для экономики и промышленности, которые стремительно меняют приоритетность, усиливают существующие угрозы и сопровождаются обострением противоречий между инновационными и традиционными связями производительных отношений стейкхолдеров. Очерчены возможные направления обеспечения безопасности государства.

Ключевые слова: Индустрия 4.0; вызовы; угрозы; кибербезопасность; промышленность.

INDUSTRY 4.0: CHALLENGES AND THREATS TO SECURITY

M. Zavgorodnia

PhD in Economics, Researcher of the Department of Industrial Policy Institute of Economics and Forecasting of National Academy of Science, Kyiv (Ukraine)

The paper identifies the security challenges connected with the development of the digital economy and the proliferation of Industry 4.0. Challenges for the economy and industry are analyzed, which are rapidly changing priority, reinforce existing threats and are accompanied by an exacerbation of the contradictions between the innovative and traditional ties of productive relations of stakeholders. Possible directions of ensuring state security are outlined.

Key words: Industry 4.0; challenges; threats; cybersecurity; industry.

Цифровизация в экономике и, в частности, промышленности дает возможность различным субъектам хозяйствования, органам власти и населению повысить эффективность использования финансовых, трудовых и других ресурсов, внедрять инновационные технологии, улучшить доступность продукции и услуг для потребителей. Разви-

тие цифровой экономики характеризуется: трансформацией бизнес-моделей; появлением новых инструментов делового сотрудничества – социальных сетей и моделей предоставления ИТ-услуг; Mobile ID, IoT; изменением деятельности институтов; преобразованием производственных циклов в электронные формы и информационно-производственные; формированием сетевых и кластерных структур; возникновением новых производств в промышленности и секторов экономики; упрощением взаимоотношений потребителя и производителя из-за исключения посредников; повышением прозрачности ведения предпринимательства и государственного регулирования экономики; экономией трансакционных издержек; расширением международного сотрудничества и его форм. Особой приоритетностью выделяются тренды по технологическим секторам: развитие промышленного Интернета вещей, коботов, автономных вещей и производство новых материалов, наносящих минимальный вред окружающей среде.

В то же время, информатизация порождают новые угрозы безопасности для страны, предприятий и населения. От масштабов и уровня охвата цифровой экономикой страны зависит темпы развития, характер проявлений, последствия угроз для безопасности страны. К тому же становиться необходимостью сменить традиционную практику пассивной адаптации к внешним и внутренним угрозам на превентивное реагирование и их предотвращение.

В Украине вызовы цифровой экономики накладываются на противоречия инновационных и традиционных производственных отношений, между формирующимися сетевыми объектами и иерархическими структурами, на структурный дисбаланс между производством и экспортом отечественного производства и внутреннего спроса промышленности, в том числе ИТ-товаров и ИТ-услуг. Под влиянием информационных факторов экономического развития происходит трансформация угроз безопасности к которым можно отнести:

- значительное отставание от передовых стран Украины в производстве продукции и предоставлении услуг с помощью информационно-коммуникационных технологий;
- социальную и экономическую нестабильность вследствие высвобождения работающих в традиционных отраслях;
- острый кадровый дефицит ИТ-специалистов на внутреннем рынке; качественный разрыв в развитии отечественного образования;
- существенная зависимость от производителей и поставщиков программного обеспечения, комплектующих и материалов компьютеров и оборудования;
- увеличение вероятности кибератак, технологических сбоев; разрушающее влияние киберпреступности и информационного влияния конкурентов;
- утрата контроля за частью налоговых поступлений по причине виртуализации трансакций[1];
- невозможность обеспечения эффективного государственного контроля и финансового мониторинга финансовых потоков;
- затруднение налогообложения из-за мобильности факторов производства и перетока капиталов.

Последние два года опросы руководителей глобальных организаций среди стратегических вызовов, влияющих на возможность экономического роста, показывают доминирование экологических / климатических изменений и стремительный рост киберрисков [2, 3]. В 2019 году 69 % респондентов в мире заявили, что создание сильной киберстратегии является критически важным фактором построения доверия со стороны основных стейкхолдеров. 71 % руководителей утверждает, что их организации рассматривают информационную безопасность как стратегическую функцию и источник конкурентных преимуществ. Руководители, которые сделали свои организации более киберстойкими, также больше ориентированы на инновационные прорывные изменения в своей области. Такие руководители смелее используют искусственный интеллект и прогнозируют более высокий рост доходов (рост доходов на 2 % или более) в течение следующих трех лет. Руководители глобальных организаций (68 %) утверждают, что их организации готовы к любой будущей кибератаке. В то же время в Украине их только 39 %, а 31 % отмечает, что им трудно оценить готовность своей организации к кибератакам. То есть организациям необходимо принять надлежащие меры, чтобы эти угрозы не подрывали потенциал цифрового роста.

По оценкам экспертов в сфере кибербезопасности, в большинстве ведущих стран мира отмечается устойчивая тенденция к значительному росту количества и расширение спектра кибератак с целью нарушения конфиденциальности, целостности и доступности государственных информационных ресурсов, в том числе тех, что циркулируют на объектах критической информационной инфраструктуры. Общеизвестно, что основными целями кибератак становятся стратегические инфраструктуры стран (ядерная, химическая или любая другая промышленность, системы жизнеобеспечения крупных мегаполисов, финансовая, продовольственная, энергетическая национальные системы, транспортные сети, деятельность правительства, правоохранительных органов, вооруженных сил и т. д.). Посягательство осуществляются через информационно-телекоммуникационные системы, особенно автоматизированные системы управления, которые необходимы для функционирования повседневной жизни людей, структур экономики или органов государственной власти. Угрозы распространяются через инновационные формы вредоносных программ, путем компрометации глобальных цепочек поставок и скоординированные преступные и враждебные действия частных и государственных групп хакеров.

Динамический характер угрозы требует построить глобальную структуру кибер-сотрудничества. Такое сотрудничество должно включать: более эффективные платформы для обмена информацией внутри и между странами и глобальными цепочками в промышленности, регулярные национальные / региональные кибер-тренировки, обмен нормативно-правовыми документами; формирование рейтинга промышленного оборудования с наименьшим количеством уязвимостей.

Повышение цифровой грамотности граждан и культуры безопасности поведения в киберпространстве, комплексных знаний, навыков и умений, необходимых для поддержания целей кибербезопасности, реализации государственных и общественных проектов по повышению уровня осведомленности общества о киберугроз и киберзащиты.

Обобщение вышеизложенного позволяет определить направления государственного стратегического планирования в сфере обеспечения безопасности: нормативно-правовое регулирование указанной сферы; формирование и развитие системы стратегического планирования обеспечения безопасности; определение полномочий субъектов обеспечения безопасности, в том числе в условиях кризисных ситуаций, природных катастроф, чрезвычайного положения; усиление прогностической функции системы управления безопасности; повышение эффективности мониторинга в сфере обеспечения безопасности с целью своевременного выявления существующих и новых типов внутренних и внешних угроз, разработку действенных мер по их нейтрализации и локализации; информационно-аналитическое обеспечение субъектов безопасности; подготовка отраслевых индикаторов безопасности; определение перечня объектов и порядка отнесения таких объектов критической информационной инфраструктуре.

Библиографические ссылки

1. Наумік-Гладка К. Г. Державне регулювання розвитку сфери комунікаційної діяльності в системі економічної безпеки України / К. Г. Наумік-Гладка // Проблеми економіки. – 2015. – № 2. – С. 87–92.

2. 2019 Global CEO Outlook KPMG International [Электронный ресурс]. – Режим доступа : https://home.kpmg/xx/en/home/campaigns/2019/05/global-ceo-outlook-2019.html/. – Дата доступа : 24.12.2019.

3. Global Risk Report 2020 [Электронный ресурс]. – Режим доступа : http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf. – Дата доступа :7.02.2020.

УДК 338.24

ВЛИЯНИЕ ИНТЕЛЛЕКТУАЛЬНОГО ПОТЕНЦИАЛА НА РАЗВИТИЕ ЦИФРОВОЙ ЭКОНОМИКИ

В. В. Зазерская

Кандидат экономических наук, доцент, заведующий кафедрой менеджмента Брестского государственного технического университета, г. Брест