УДК 338:339.9 DOI: 10.14451/1.233.373

Трансформация системы экономической безопасности под влиянием высоких технологий

© 2024 **Уметбаев Ильшат Шарифуллович**
Генеральный директор. ООО Опытный завод НЕФТЕХИМ-СЕРВИС.
E-mail: lctak@mail.ru

Ключевые слова: экономическая безопасность, высокие технологии, инструменты нейтрализации угроз, неопределенность внешней среды, неэкономические последствия регулирующих мер.

В статье рассмотрен процесс трансформации системы экономической безопасности на макро- и микроуровнях в результате разработки и внедрения высоких технологий во все сферы жизнедеятельности общества. Представлены атрибутивные признаки детерминистского и эссенциалистского подходов к трактовке роли технологий в жизни общества, доказана ограниченность познавательного потенциала данных подходов для разработки действенных мер по обеспечению безопасности в условиях цифровой трансформации общества. Выявлены особенности современного этапа обеспечения технологической безопасности; представлен анализ технологических угроз и определен их глобальный характер, что обусловливает необходимость межгосударственного взаимодействия для их нейтрализации. Определена роль предпринимательского сектора в решении задач обеспечения экономической безопасности; проанализированы последствия внедрения высоких технологий в сферу безопасности для ценностных представлений, этических норм и образа жизни населения.

Четвертая промышленная революция и внедрение сквозных цифровых технологий во все сферы жизнедеятельности современного общества, с одной стороны, создали предпосылки для роста производительности факторов производства и более полного удовлетворения растущих потребностей населения, с другой стороны, стали причиной новых вызовов для человеческого сообщества, что нашло отражение в техногенных катастрофах и обострении геополитических проблем. Это предопределило необходимость выделения технологической безопасности как нового явления и самостоятельного объекта исследования, а также инициировало поиск инструментов ее обеспечения. Решение задачи формирования целостной системы технологической безопасности, представленной микро-, мезо- и макроуровнями, предполагает переосмысление теоретических и методологических подходов к представлениям о взаимосвязи между технологиями и безопасностью, о роли государства во внедрении технологий безопасности, и об инструментах нейтрализации технологических рисков и угроз. Это определяет выбор темы исследования, его теоретическую и практическую значимость

Наука рассматривает технологию как совокупность представлений о методах воздействия человека на природу во взаимосвязи с фундаментальными науками, а также о политических, социальных, символических и этических последствиях их развития, о влиянии на общественные отношения и окружающую среду. В повседневной действительности под технологией подразумеваются способы соединения факторов производства и производственные процессы, направленные на получение конечной продукции. Другой ключевой категорией теории технологической безопасности выступает понятие «устройство», которое определяется как совокупность разнородных взаимосвязанных элементов, включающих машины, процессы, правила их использования, окружающую среду, а также символические и реляционные средства, которые моделируют индивидуальное и социальное поведение. Подобная трактовка отражает связь между технологией, внешней средой и человеком, а также позволяет выявить последствия внедрения принципов технологической безопасности в повседневную жизнь людей, формах их участия в моделировании их поведения и общественных отношений.

Анализ предпосылок формирования технологий и последствий их внедрения в процессы воспроизводства позволяет сделать вывод, что они не сводятся к созданию устройств, а существуют во взаимосвязи со средой. Это, в частности, проявляется в том, что внедрение технологий идентификации, наблюдения и отслеживания, используемых в целях обеспечения безопасности на предприятии, на автотрассах и на улицах городов и др. необходимо изучать во взаимосвязи с растущей турбулентностью и рисками нарушения границ личного пространства. При этом взаимосвязь технологических и социальных процессов проявляется не только во внешних эффектах, которые сопровождают внедрение новых технологий в процессы жизнедеятельности общества, но и в составе факторов, которые инициируют подобные нововведения. Так, например, технологизация безопасности была обусловлена множеством факторов, среди которых террористические акты играли важную роль, но не исчерпывали их состав полностью. Этот тезис подтверждается тем, что внедрение высоких технологий в сферу безопасности началось в мире в 1980-х годах и было направлено на предупреждение распространения наркотиков и нелегальной миграции. Серия терактов в различных государствах в начале 2010 годов привела к формированию межгосударственных взаимодействий и одновременно превратила международные организации, субъектов предпринимательства, некоммерческие организации, отраслевые ассоциации, экспертное сообщество и др. в самостоятельные субъекты технологической безопасности. При этом государство сохранило за собой роль субъекта институционального проектирования системы технологической безопасности и координатора действий иных участников данного многоуровневого образования.

Успех или неудача технологических инноваций в значительной степени зависит от эффективности взаимодействий между различными участниками данного сетевого образования. В условиях растущего числа участников отношений по поводу обеспечения технологической безопасности возникают многочисленные социальные и этические проблемы, влияние которых возрастает по мере внедрения инноваций в повседневную жизнь. В данном контексте ключевым остается вопрос о том, что выступает первопричиной развития системы технологической безопасности — технологии, которые инициируют поиск новых инструментов нейтрализации угроз и рисков, или потребность в безопасности, способствующая разработке и реализации проектов по внедрению инноваций. Для решения данной проблемы необходимо учитывать, что субъектный состав системы безопасности представлен разнородными факторами, что вызывает перманентные конфликты интересов, требующие изучения и принятия во внимание при принятии решений. Кроме того, анализ эффективности инструментов обеспечения технологической безопасности предполагает учет не только экономических последствий их использования, но и социальных,

политических, этических и др. эффектов. Тем самым, традиционно используемые детерминистские и эссенциалистские подходы к изучению технологий в жизни общества не могут быть использованы для исследования технологической безопасности современного государства, предприятий и отдельных индивидов, поскольку подобные подходы трактуют технологию как деконтекстуализированное и трансисторическое явление.

Согласно детерминистскому подходу, технология является отражением поступательного развития общества и экономического роста, а также источником прироста валового продукта. Это обусловливает необходимость адаптации институциональной среды к императивам технологических нововведений. Другим следствием детерминизма в отношении технологий выступает тезис о технологической универсальности, предполагающий примат науки над политикой и индивидуальным выбором на уровне отдельного государства и мирового сообщества. Идеи технологического детерминизма были сформулированы в 1920-х годах в работах Т. Веблена [3] под влиянием активного развития массового производства и получили развитие во второй половине XX века в трудах разработчиков постиндустриального общества (Д. Белл [2], М. Кастельс [7], Й. Масуда [17] и др.). В то же время техносферные катастрофы, экологические угрозы, пандемии и др. события планетарного масштаба доказывают несостоятельность идеи инструментальной рациональности как единственного способа достижения прогресса. Сторонники эссенциализма (К. Леви-Строс [6] и др.) в свою очередь исходят из признания онтологического различия между технологией и смыслом, отдавая предпочтение рациональности и эффективности первого и отказываясь принимать второе во внимание. При таком подходе техника представляется относительно самостоятельным феноменом и развивается в соответствии с внутренними законами, не связанными с опытом человеческого сообщества. В реальной действительности технологии не являются автономным явлением и связаны со всеми секторами жизнедеятельности общества, выполняя множество функций и, в частности, они формируют образ жизни и культуру, порождают ограничения и моделирует поведение индивидов, а также определяют их отношение к технологическим инновациям, включая отношение сопротивления.

В условиях обострения геополитических угроз и распада глобальных цепочек создания стоимости в Российской Федерации была разработана Концепция технологического развития на период до 2030 года [12], которая определила роль технологической безопасности в обеспечении и технологического суверенитета государства. Однако до принятия данного документа в России уже действовал комплекс законов и подзаконных актов, определяющих необходимость внедрения технологических новаций в различные области жизнедеятельности общества для предупреждения и нейтрализации угроз. Так, например, безопасность на дорогах обеспечивалась в соответствии с Приказом МВД России от 23.08.2017 N 664 [11], а с 1 сентября 2024 года вступят в силу единые положения стационарных, передвижных и мобильных камер для автоматической фиксации нарушений правил дорожного движения (ПДД). Соблюдению общественного порядка способствуют нормы российского законодательства (статья 152.2 Гражданского кодекса РФ [5]), которые легитимизируют введение видеонаблюдения в общественных местах и др. Понимание того, что развитие технологий приводит к формированию новых угроз, включающих, в частности, угрозы информационной безопасности, привело к принятию Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ [16] и др.

С момента принятия нормативных правовых актов, регламентирующих процессы обеспечения безопасности, применяемые инструменты вызывали множество критических оценок, связанных с их неэффективностью (например, в отношении организации видеонаблюдения и др.), с низким уровнем координации взаимодействий между осуществляющими управление министерствами

и ведомствами, что, в частности, проявлялось в низкой эффективности взаимосвязи между локальными системами информационной безопасности и др., а также с нарушениями неприкосновенности частной жизни, с несоблюдением личной и семейной тайны в результате утечки персональных данных и др. В то же время в условиях повышения уровня угроз решение государства об использовании разнообразных технологий безопасности для их нейтрализации представляются целесообразными с позиции защиты прав граждан и оптимизации расходов. Многообразие угроз, различающихся по источникам, содержанию и масштабам потенциального ущерба, определяет многоаспектность системы экономической безопасности и делает целесообразным передачу государством субъектам предпринимательства части полномочий по ее обеспечению (например, организация охранной деятельности с участием частных охранных предприятий, размещение государственного заказа на производство специализированного оборудования и программного обеспечения и др.).

Современный этап обеспечения технологической безопасности характеризуется несколькими особенностями, что находит выражение в содержании мероприятий, направленных на предупреждение угроз. Во-первых, системы технологической безопасности не совпадают с границами национальных государств и формируются при участии всего мирового сообщества или стран-членов международных организаций региональной экономической кооперации (например, взаимодействия стран-участниц Евразийской экономической комиссии в области энергосбережения, энергоэффективности, использования возобновляемых источников энергии и охраны окружающей среды [10] и др.). Во-вторых, использование цифровых технологий предопределило взаимосвязанность растущего количества участников системы технологической безопасности и инициировало сетевизацию экономического пространства, что, в частности, инициировало состояние физической, онтологической, когнитивной и реляционной незащищенности. В-третьих, появляются новые риски и повышается уровень неопределенности, что обусловливает необходимость разработки новых защитных технологий, которые, в свою очередь, инициируют новые риски и рост турбулентности. Если традиционная концепция риска основывалась на признании рациональности поведения экономических субъектов, что позволяло применять рациональные вероятностные и математические методы для прогнозирования рискообразующих факторов, то понимание ограниченной рациональности поведения привело к признанию субъективности оценок риска и методик прогнозирования, основанных на вероятностных подходах [15]. Это проявлялось в том, что выводы, полученные экспертами, не решали задачи предоставления объективной информации и стали инструментом манипулирования аудиторией. В этих условиях сформировался новый подход к классификации угроз, согласной которому угрозы экономической безопасности и экологические угрозы определялись как непреднамеренные вторичные последствия преднамеренных действий, тогда как новые террористические акты, в свою очередь, трактовались как «преднамеренно спровоцированные катастрофы» [1]. В этих условиях риск и неопределенность становятся социальными конструкциями, для оценки которых используются культурные суждения, тогда как в рамках традиционного риск-менеджмента предпочтение отдавалось количественным методам. Технологические инновации участвуют в идентификации и нейтрализации рисков, одновременно они являются источником новых рисков, что оказывает негативное влияние на состояние технологической и экономической безопасности.

Третья особенность современного этапа функционирования системы технологической безопасности находит выражение в передаче государством полномочий по предоставлению некоторых государственных услуг субъектом предпринимательства. Это является следствием ограниченности бюджетных ресурсов, используемых для финансирования процесса оказания государственных услуг, а также стремлением

повысить качества последних за счет использования преимуществ рыночной конкуренции. Решению этих задач способствовало определение функций по охране, видеонаблюдению, аудиту и оказанию консалтинговых услуг по вопросам управления рисками, выполняемых субъектами предпринимательства в качестве деятельности, обеспечивающей коллективную безопасность. Это привело к развитию производства специализированного оборудования с использованием биометрических технологий и методов наблюдения для защиты объектов государственной и частной собственности. Использование технологий дистанционного наблюдения и программного обеспечения для обнаружения признаков противоправного поведения способствовало превращению новых технологий в важный инструмент предотвращения рисков и угроз для экономической безопасности. Применение данных инструментов способствовало повышению эффективности функционирования правоохранительных органов. Привлечение предпринимательского сообщества к решению вопросов обеспечения безопасности привело к быстрому росту рынка технологий наблюдения и защиты, оборот которого увеличился вдвое с 1990-х годов. Эксперты полагают, что мировой рынок оборудования для видеонаблюдения будет расти на 10,55% в год в период с 2024 по 2029 гг. К середине августа 2023 года в России насчитывалось более 550 тыс. камер видеонаблюдения по всей стране [4]. Согласно официальным данным, около 199 тыс. устройств наделены функциями биометрического распознавания, а 11 тыс. камер могут сообщать о тех или иных инцидентах. В то же время следует учитывать межрегиональную дифференциацию в размещении подобного оборудования: 56% обзорных камер расположены в трех субъектах РФ: Москве, Санкт-Петербурге и Республике Татарстан [9; 13; 14]. В девяти регионах правоохранительный сегмент аппаратно-программный комплекс АПК «Безопасный город» вообще отсутствует, а в 26 регионах не установлено ни одной видеокамеры» [8]. Представители Министерства внутренних дел РФ полагают, что это снижает эффективность деятельности правоохранительных органов.

Важной характеристикой современного состояния системы технологической безопасности общества выступает распространение новых моделей поведения, нового образа жизни и ограничений. Это приняло форму вторжения «технологической парадигмы» в повседневную жизнь. Названный «эффектом диффузии» этот феномен возникает, по мнению М. Кастельса [7], за на основе связности и гибкости, свойственных новым технологиям, что привело к сетевизации общества.

Проведенное исследование показывает, что внедрение новых технологий в систему обеспечения экономической безопасности приводит к возникновению этических, правовых, философских, социологических и политических вопросов, которые приобретают особое значение в контексте рисков и неопределенностей. Целесообразно исследовать технологические угрозы и инструменты по их нейтрализации во взаимосвязи с экономическими и неэкономическими явлениями и процессами, что позволяет повысить объективность прогнозов.

Библиографический список

1. *Бек У.* Общество риска. На пути к другому модерну / пер. с нем. В. Седельника, Н. Федоровой. — М. : Прогресс-Традиция, 2000. — 384 с.
2. *Белл Д.* Грядущее постиндустриальное общество. — М. : Academia, 2004. — 944 с.
3. *Веблен Т.* Теория праздного класса. — М. : Прогресс, 1984. — 183 с.
4. Видеонаблюдение / TAdviser. — URL: https://www.tadviser.ru/index.php/Видеонаблюдение.
5. Гражданский кодекс Российской Федерации (ГК РФ) (Часть I) от 30.11.1994 г. № 51-ФЗ. — URL: https://www.consultant.ru/document/cons_doc_LAW_5142 (дата обр. 02.04.2024).
6. *Леви-Строс К.* Первобытное мышление. — М. : Республика, 1994. — 384 с.
7. *М. К.* Информационная эпоха: экономика, общество и культура : пер. с англ. — М. : ГУ-ВШЭ, 2000. — 383 с.
8. МВД назвало число камер видеонаблюдения в России. Регионы-лидеры / TAdviser. — URL:

https://www.tadviser.ru (дата обр. 31.03.2024).
9. Москва / TAdviser. — URL: https://www.tadviser.ru/index.php/Москва.
10. Официальный сайт Евразийской экономической комиссии. Взаимодействие государств – членов ЕАЭС в области энергосбережения, энергоэффективности, использования возобновляемых источников энергии и охраны окружающей среды. — URL: https://energy.eaeunion.org/Documents/energy_efficiency.pdf (дата обр. 31.03.2024).
11. Приказ МВД России от 23.08.2017 № 664 (ред. от 21.12.2017) «Об утверждении Административного регламента исполнения Министерством внутренних дел Российской Федерации государственной функции по осуществлению федерального государственного надзора за соблюдением участниками дорожного движения требований законодательства Российской Федерации в области безопасности дорожного движения» (Зарегистрировано в Минюсте России 06.10.2017 № 48459) (утратил силу). — URL: https://www.consultant.ru/document/cons_doc_LAW_280037 (дата обр. 23.02.2024).
12. Распоряжение Правительства РФ от 20.05.2023 N 1315-р «Об утверждении Концепции технологического развития на период до 2030 года». — URL: https://www.consultant.ru/document/cons_doc_LAW_447895 (дата обр. 23.02.2024).
13. Санкт-Петербург / TAdviser. — URL: https://www.tadviser.ru/index.php/Санкт-Петербург.
14. Татарстан / TAdviser. — URL: https://www.tadviser.ru/index.php/Татарстан.
15. *Туфетулов А. М., Бакулина Л. Т., Хамидуллина Ф. И.* Трансформация инструментария управления национальной экономической безопасностью с учетом «новых социальных рисков» // Горизонты экономики. — 2023. — 4(77). — С. 22—27.
16. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (последняя редакция). — URL: https://www.consultant.ru/document/cons_doc_LAW_61801 (дата обр. 02.04.2024).
17. *Masuda Y.* The information Society as Post-Industial Society. — Washington, 1981.