УДК 330.34.014–026.23:338.22:336.565.2:005.334 *DOI: 10.5281/zenodo.1245578*

А.В. КОЛОДІЙЧУК

Політично–правові ризики впровадження ІКТ в національній економіці

У статті розглянуто зміст і структуру законодавчих суспільно–політичних ризиків впровадження інформаційно–комунікаційних технологій, а також класу політичних загроз від проведення інформатизації. Зокрема, серед законодавчих ризиків розглянуто нормативно–правові, інтегративні ризики, ризики законотворчого процесу, порушення суміжних прав і свобод громадянського суспільства, ефективізації боротьби з комп'ютерною злочинністю. У розрізі політичних ризиків ІКТ виділено революційні, терористичні, ризики е–урядування, політичного переслідування інтернет–активістів, впливу ІКТ на виборчий процес, ризики зміни політичних режимів.

Ключові слова: *законодавство, ризики, комп'ютерна злочинність, інформаційно–комунікаційні технології, дезінформація, криптовалюта, кібератаки на біржі, електронне урядування.*

А.В. КОЛОДИЙЧУК

Политическо–правовые риски внедрения ИКТ в национальной экономике

В статье рассмотрены содержание и структура законодательных общественно–политических рисков внедрения информационно–коммуникационных технологий, а также класса политических угроз от проведения информатизации. В частности, среди законодательных рисков рассмотрены нормативно–правовые, интегративные риски, риски законотворческого процесса, нарушение смежных прав и свобод гражданского общества, эффективизации борьбы с компьютерной преступностью. В разрезе политических рисков ИКТ выделены революционные, террористические, риски е–правительства, политического преследования интернет–активистов, влияния ИКТ на избирательный процесс, риски изменения политических режимов.

Ключевые слова: *законодательство, риски, компьютерная преступность, информационно–коммуникационные технологии, дезинформация, криптовалюта, кибератаки на бирже, электронное управление.*

A. KOLODIYCHUK

Political–legal risks of the introduction of ICT in the national economy

The article deals with the content and structure of legislative sociopolitical risks of the introduction of information and communication technologies, as well as the class of political threats from the conduction of informatization. In particular, regulatory risks, integrative risks, risks of the lawmaking process, violations of related rights and freedoms of civil society, and the effectiveness of the fight against computer crime are considered among legislative risks. In the context of the political risks of ICT, there are revolutionary, terrorist, e–governance risks, political persecution of online activists, the impact of ICT on the electoral process, and the risks of changing political regimes are highlighted.

Keywords: *legislation, risks, computer crime, information and communication technologies, misinformation, cryptology, cyberattacks on the exchange, electronic government.*

Постановка проблеми. В останні два десятиліття процес бурхливої інформатизації охопив різні сфери суспільного життя та економічної діяльності. Не оминув він і таку важливу сферу суспільних та соціокультурних взаємин, як політичну. Проте це породило велику різноманітність можливих ризиків, яким приділена недостатня увага, оскільки, як правило, побутує думка, що виробники ІКТ–продукції все передбачили наперед, а різноманітні політтехнологи в комерційно–політичних цілях і кіберзловмисники в злочинних цілях цим вдало користуються.

Аналіз останніх досліджень та публікацій. Питанням вивчення політичних ризиків присвятили свої праці такі зарубіжні та вітчизняні учені, як Т. Вахненко, В. Горбатенко, І. Івченко, Ч. Кеннеді, О. Кіндратець, Б. Краснов, Б. Ліві, Л. Нагорна, М. О'Лірі, Дж. Саймон, В. Тихомиров, Д. Хінен

та ін. Вищезгадані дослідники вивчали не лише природу політичних ризиків, але економічні наслідки настання останніх, подавали своє бачення щодо пошуку шляхів усунення таких ризиків. Однак, системно проблема політичних ризиків інформатизації та інших аспектів функціонування ІКТ–сектора не досліджувалася і тому їй присвячена наша увага.

Мета статті – окреслити суспільно–трансформаційні та політично–правові ризики впровадження інформаційно–комунікаційних технологій.

Виклад основного матеріалу. Досить широким за вмістом є клас законодавчих суспільно–політичних ризиків імплементування нових ІКТ–процесів. Це клас всіх загроз, які пов'язані з відсутністю, недосконалістю державної законодавчої системи у сфері регулювання процесів впровадження ІКТ–технологій в національній економіці. Зокрема, сюди входять (класифікація за особливостями законотворчої технології): 1) нормативно–правові ризики ІКТ; 2) інтегративні загрози нового цифрового законодавства в існуючу нормативну базу держави (тобто ризики, пов'язані з кодифікаційними змінами у законодавстві); 3) ризики законотворчого процесу у сфері нових інформаційних та комунікаційних технологій; 4) ризики невиконання або неправильної імплементації законодавства, яке регулює впровадження ІКТ; 5) загрози, пов'язані з можливим порушенням суміжних прав та свобод громадянського суспільства в результаті прийняття законодавчих норм, що регламентують функціонування цифрової сфери в Україні; 6) ризики ефективізації (технології виконання рішень і запобігання неправомірних кібердій) боротьби з комп'ютерною злочинністю. Зупинимось детальніше на кожній із складових цього класу. Перші пов'язані зі змістом законодавчих і нормативно–правових актів, котрі регулюють сферу ІКТ в Україні. Другі – ризики, які зв'язані з питаннями систематизації законодавчої бази, яка стосується питань розвитку інформаційних технологій, можливою невідповідністю нових законів, указів, розпоряджень раніше прийнятим регулюючим нормам. Треті виникають через порушення процедур законотворчого і законодавчого процесів, зокрема через можливі регламентні порушення, відсутність належного громадського обговорення, належної професійної оцінки і т.д. Четверті заключаються в дуже частих прогалинах законодавства, які дають змогу зловмисникам через опрацьовані «темні схеми» здійснювати різноманітні махінації, в тому числі і через кіберпростір, а також можливому «тихому» саботажі виконання державних нормативно–правових актів стосовно інформатизації органами влади на місцях. П'яті також надзвичайно актуальні у демократичному суспільстві і правовій державі, оскільки дуже часто державна влада в різних країнах для захисту своїх власних політичних інтересів вводить різні інтернет–обмеження, закриває суспільно–популярні ресурси, обґрунтовуючи це боротьбою з піратством, навіть екстремізмом; звісно, подібні випадки не сприяють захисту прав і свобод людини і громадянина. Одним з найбільш яскравих прикладів в недавній історії України стало прийняття т.зв. «законів 16 січня» у січні 2014 року, серед яких поміж інших обмежень і покарань вводились кримінальна відповідальність за втручання в роботу державних інформаційних ресурсів, розміщення закликів в Інтернеті до повалення тодішньої влади в Україні і т.п., що в сукупності призвело до каталізації силового протистояння в ході Євромайдану 2013–2014 рр. Шості полягають у всіх можливих порушеннях і прогалинах в ході законотворчого процесу, які сприяють росту кіберзлочинності і криміналізації інтернет–простору.

Головними проблемами і «вузькими місцями» українського ІТ–законодавства, які виступають джерелами утворення ризиків впровадження ІКТ–технологій, є: його фрагментарний характер; поверховість; хронічна запізнілість рішень; повна відірваність від сучасних комп'ютерно–комунікаційних трендів і пов'язаних з ними загроз, українське ІТ–законодавство в основному орієнтоване на комп'ютерні технології середини 90–х років попереднього століття; дуже часте неврахування інтересів юзерів та інтернет–спільноти, а іноді – повне їм протиріччя, превалювання «методу батога» над «методом пряника»; держава майже не присутня як повноцінний суб'єкт процесу впровадження ІКТ в макроекономічній системі, що безумовно гальмує розвиток електронної економіки в Україні; відсутність взаємовигідної, належно закріпленої на нормативно–правовому рівні, кооперації з авторитетними міжнародними організаціями у сфері ІТ та комунікацій; відсутність державного стимулювання розвитку ІКТ–сфери, яка розвивається в основному особистими ініціативами ІТ–бізнесу, розширен–

ням споживчого ринку комп'ютерної продукції, який, щоправда, зазнав негативного впливу від кризових явищ в українській економіці з точки зору падіння купівельної спроможності населення; державні програми та регіональні проекти інформатизації носять здебільшого декларативний або однобокий характер, вони носять точковий характер, а тому не цілком відповідають потребам розвитку національної економіки; відсутні дієві реальні механізми захисту прав інтелектуальної власності в інтернет–просторі, що пов'язано з тим, що провайдери телекомунікаційних послуг не несуть відповідальності за зміст інформації, що циркулює їх мережами; держава не бере поки що на себе відповідальність за кіберзахист комп'ютерно–активного населення України і не здатна ще його технічно забезпечити; відсутність Інформаційного кодексу України, який би цілісно регулював відносини у сфері інформатизації української економіки; проблеми, пов'язані з так званим національним контентом в інтернет–середовищі, зокрема його захисту, підвищення рівня його якості і конкурентоспроможності серед вітчизняної інтернет–аудиторії; законодавчо не закріплена роль Інтернет–мережі як інструменту демократизації пострадянського суспільства в Україні; надзвичайно слабка адаптація українського законодавства до умов ведення і потреб захисту інтересів держави і громадянського суспільства в рамках протікання сучасної інформаційної війни; відсутність належного державного планування у розвитку інформаційного сектору макроекономічної системи, ІКТ–інфраструктура дуже часто розвивається стихійно, через місцеві ініціативи і за рахунок місцевих та зарубіжних приватних спонсорів та зацікавлених інвесторів; держава законодавчо не створила умови для покращення інвестиційного клімату в цілях залучення інвестицій в інформаційно–комунікаційну сферу в Україні; відсутність системності нормативно–правового поля до питань розбудови системи електронного урядування, незважаючи на прикладені в останні роки значні зусилля, вона все–таки розвивається не системно, а за ініціативами місцевих і регіональних органів влади, крім того, спостерігається значна диференціація якості електронного урядування в різних регіонах України, що стало можливим в тому числі і за рахунок недосконалості вітчизняної нормативно–правової бази, що присвячена цим питанням; законодавчо не прописано і не врегульовано питання функціонування і обороту сучасних електронних фінансових інструментів (як міжнародних, так і регіональних), таких як, наприклад, криптовалюти (біткоїни, лайткоїни, неймкоїни, піркоїни, NXT–валюта [8] з міжнародних, венесуельська «ель–петро», польська «PLNCoin», іспанська «SpainCoin», російська «SibCoin», ісландська «AuroraCoin», китайська «NEO Coin», грецька «GreekCoin», шотландська «ScotCoin» з регіональних тощо), електронних фідуціарних (фіатних) грошей, а також новітніх електронних фінансових операцій типу майнінгу, форжингу, криптовалютних ICO–операцій, функціонування різноманітних онлайн–сервісів з обміну віртуальних валют на реальні активи (електронних криптовалютних бірж, в Україні це – біржа «UA–BIT» [5], яка працює як з «криптою», так і з електронними фіатними грошима, тобто нічим не підкріпленими електронними грошовими засобами, номінальна вартість яких гарантується певними державами, наприклад, передоплачені банківські картки «Visa Cash», гонконгські картки «Octopus», електронні гроші на базі голландських смарт–карток «Chipknip», електронні мережі «PayPal» тощо), що загрожує ризиками перетворення нашої держави в офшор–зону для різноманітних фінансових махінацій передусім у кіберпросторі, курсовими втратами, розбалансуваннями національної фінансової системи (на тлі вже існуючих глибоких макрофінансових проблем цим загрозам уваги, на жаль, не приділяють), ризиками кібератак по е–біржах криптовалют через їх недостатню технічну захищеність і відсутній законодавчий захист; ще донедавна державна система тендерних закупівель для інформаційного сектору економіки в Україні була непрозорою і корумпованою, а тому про ефективність розбудови інформаційної економіки з боку державних органів влади не могло бути й мови; недостатньо врегульовано питання функціонування в Україні нефіатних електронних грошей, частина з яких на сьогодні заборонена Нацбанком України («Webmoney», «QIWI Wallet», «Яндекс.Деньги», «Wallet one / Единый кошелек»); в українському законодавстві не врегульовано питання функціонування ігрових грошових одиниць, тобто електронних привілеїв у соцмережах чи віртуальних онлайн–іграх, які практично неможливо поки що обмінювати на національну валюту чи іноземні валюти, до прикладу це онлайн–валюта мережі «Фейсбук» – «facebook–credits» [7], т.зв. «голоси» забороненої в Україні мережі «ВКонтакте», «жжетони» блогосервісу «LiveJournal» [6] і так да–

лі. Цю всю масу недопрацювань частково покриває лише визнання віднедавна криптовалютного майнінгу окремим видом економічної діяльності і внесення його у вітчизняний КВЕД [4], а точніше в клас 63.11 «Оброблення даних, розміщення інформації на веб–вузлах і пов'язана з ними діяльність» у 2018 р., чому сприяло входження України до двадцятки країн світу з розвинутою криптоекономікою; це було спрямовано на легалізацію криптовалютного бізнесу в Україні, запровадження над ним фіскального контролю, проте держава на вчинила так і жодних дій заради стимулювання законодавчими та нормативно–правовими інструментами розвитку різних сегментів ІТ–діяльності. Що ж до конкретних ризиків, які з цих проблем витікають, то їх можна звести до ряду наступних груп за змістом загроз: 1) гальмівні ризики, тобто уповільнення розвитку ІКТ–сектору; 2) ризики загострення кіберзлочинності; 3) інтегративні ризики, тобто загрози інтегрування інформаційного сектору України у світовий інформаційний простір; 4) соціально–культурні ризики від стану ІКТ–законодавства; 5) фінансово–економічні ризики від стану ІКТ–законодавства. Перші полягають у посиленні відставання вітчизняної сфери інформаційних технологій й комунікацій від глобальних ІКТ–трендів, в першу чергу через відсутність ефективно діючого механізму ІКТ–регуляції, реальних стимулів для розвитку цієї галузі. Друга група загроз пов'язана з слабкістю державного механізму в Україні протистояти сучасним кібервикликам, вираженим різноманітними кіберзлочинами через відсутність відповідних підготовлених і наділених відповідними повноваженнями структур, крім того це технічно складно і фінансово затратно. Третя група викликів полягає насамперед в тому, що в Україні не створено належних законодавчих передумов щодо гармонійного інтегрування ІКТ–сектору економіки України у глобальну електронну й інтернет–економіку. Четверта група загроз пов'язана передусім з тим, що інтернет–технології (соцмережі, екстремістські веб–сайти) через законодавчі недопрацювання все частіше стають інструментом для вчинення різних кримінальних дій. П'ята група загроз охоплює збитки, понесені від фінансових махінацій, реалізованих за допомогою ІКТ, що стали можливими через законодавчі промахи.

Все частіше з розгортанням різних сценаріїв політичної конкуренції на різних ієрархічних рівнях, загостренням міжнародних та внутрішньодержавних політичних конфліктів з одного боку, та розвитком науково–технічної революції та її комп'ютерної складової з іншого боку, спостерігається урізноманітнення сукупності політичних ризиків впровадження ІКТ. До даного класу загроз належать такі: 1) революційні; 2) терористичні; 3) ризики електронної демократії (електронного урядування); 4) ризики впливу ІКТ на волевиявлення виборців; 5) ризики зміни політичних режимів; 6) ризики політичного переслідування інтернет–активістів.

Висновки

На сьогоднішній день Українська держава не готова протистояти всій палітрі різноманітних кіберзагроз, що великою мірою пояснюється величезними прогалинами у її законодавстві, що регулює ІТ–сектор національної економіки, нерівномірністю протікання політичного процесу в державі, а також перетіканням історичних та етнокультурних суперечок в цифрову площину. Це спонукає не лише реагувати на вже існуючі загрози, котрі постійно диверсифікуються, але й вибудовувати політико–правовий механізм, здатний адекватно боротися з відповідними загрозами, попереджати їх появу. Дуже часто відсутність такого спеціалізованого механізму пояснюється високими затратами (фінансовими, часовими, матеріальними) на фахово–експертний аналіз таких загроз, низьким рівнем технологічності національного ІКТ–сектора, його кустарним в певній мірі характером, а також високою динамічністю розвитку світової комп'ютерної індустрії, частою зміною різних трендів і тенденцій у ній. Однак, такого роду аргументи та слідування ним з часом можуть призвести до того, що цілі галузі національної економіки та сфера державного управління можуть опинитися паралізованими в результаті масштабних кібератак із застосуванням сучасних інструментів кібератаження, що, в підсумку, здатне призвести до цілковитого макрогосподарського хаосу.

Список використаних джерел

1. Альгин А.П. Риск и его роль в общественной жизни / А.П. Альгин. – М.: Мысль, 1989. – 188 с.

2. Важинський Ф.А. Маркетингові дослідження в системі управління конкурентоспроможністю підприємств / Ф.А. Важинський, А.В. Колодійчук // Науковий вісник НЛТУ України. – 2009. – Вип. 19.1 – С. 129–130.

3. Важинський Ф.А. Механізм регулювання інвестиційної діяльності в регіоні / Ф.А. Важинський, А.В. Колодійчук // Науковий вісник НЛТУ України : зб. наук.–техн. праць. – Львів: РВВ НЛТУ України. – 2010. – Вип. 20.7. – С. 138–143.

4. Класифікація видів економічної діяльності на сайті Державної служби статистики [Електронний ресурс]. – Режим доступу: http://kved.ukrstat.gov.ua/index.html

5. Офіційний сайт української біржі Bitcoin «UA–BIT» [Електронний ресурс]. – Режим доступу: https://dou.ua/forums/topic/12948/

6. У LiveJournal з'явилися власні гроші nicely [Електронний ресурс]. – Режим доступу: https://tsn.ua/nauka_it/

7. How will sir pay? Facebook credits, that'll do nicely [Електронний ресурс]. – Режим доступу: http://www.theregister.co.uk/2009/06/03/facebook_payments/

8. Nxt (NXT) : криптовалюта – обзор [Электронный ресурс]. – Режим доступа: https://inp.one/cryptoworld/nxt–nxt–kriptovalyuta–obzor

References

1. Algin, A. P. (1989). Risk i yego rol' v obshchestvennoy zhizni [Risk and its role in public life]. Moscow: Thought. [in Russian].

2. Vazhynskyy, F. A., & Kolodiychuk, A. V. (2009). Marketynhovi doslidzhennya v systemi upravlinnya konkurentospromozhnistyu pidpryyemstv [Marketing research in the system of competitiveness management of enterprises]. In Naukovyy visnyk NLTU Ukrayiny [Scientific Bulletin of National Forestry University of Ukraine]: Vol. 19.1 (pp. 129–130). [in Ukrainian].

3. Vazhynskyy, F. A., & Kolodiychuk, A. V. (2010). Mekhanizm rehulyuvannya investytsiynoyi diyal'nosti v rehioni [Mechanism for regulation of investment activity in the region]. In Naukovyy visnyk NLTU Ukrayiny [Scientific Bulletin of National Forestry University of Ukraine]: Vol. 20.7 (pp. 138–143). [in Ukrainian].

4. State Statistical Service of Ukraine (2018). Klasyfikatsiya vydiv ekonomichnoyi diyal'nosti [Classification of types of economic activity]. Retrieved from http://kved.ukrstat.gov.ua/index.html [in Ukrainian].

5. Ukrainian exchange Bitcoin «UA–BIT» (2018). Retrieved from https://dou.ua/forums/topic/12948/ [in Ukrainian].

6. «U LiveJournal z'yavylysya vlasni hroshi [LiveJournal has its own money]» (2018). Retrieved from https://tsn.ua/nauka_it/ [in Ukrainian].

7. «How will sir pay? Facebook credits, that'll do nicely» (2009, June 3). Retrieved from http://www.theregister.co.uk/2009/06/03/facebook_payments/ [in Ukrainian].

8. Website Nxt (2018). Kryptovalyuta – obzor [Cryptography – review]. Retrieved from https://inp.one/cryptoworld/nxt–nxt–kriptovalyuta–obzor [in Russian].

Дані про автора

Колодійчук А.В.,

к.е.н., доцент, Ужгородський торговельно–економічний інститут Київського національного торговельно–економічного університету

e–mail: info@utei–knteu.org.ua

Данные об авторе

Колодийчук А.В.,

к.э.н., доцент, Ужгородский торгово–экономический институт Киевского национального торгово–экономического университета

e–mail: info@utei–knteu.org.ua

Data about authors

Kolodiychuk A.

PhD, Associate Professor of Uzhgorod Trade and Economic Institute of the Kyiv National Trade and Economic University

e–mail: info@utei–knteu.org.ua