УДК 347.77:(007:004.056)

М. Василенко,
доктор юридичних наук, доктор фізико-математичних наук, професор,
академік Академії наук вищої освіти України,
професор кафедри права міжнародного та європейського права
Національного університету «Одеська юридична академія»

ЯКІСТЬ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ (ІКС) ТА ДЕЯКІ ЗАКОНОДАВЧІ ПИТАННЯ ЩОДО ЇЇ ПІДВИЩЕННЯ

Широке використання інформаційно-комунікаційних технологій (далі – ІКТ) в усіх сферах суспільного життя спонукає до вирішення питань кібербезпеки, передусім питань, пов'язаних із підвищенням її якості. Однак до останнього часу питання підвищення якості кібербезпеки в спеціальній літературі практично не розглядалося. Вперше це питання було поставлено та обговорено автором (М. Василенко) у роботі «Підвищення стану кібербезпеки інформаційно-комунікаційних систем: якість в контексті удосконалення інформаційного законодавства» [1]. Розуміючи складність поєднання знань із різних галузей науки, автор вважає за необхідне розглядати існуючу проблему всебічно, з різних сторін.

Метою статті є дослідження питання впливу якості та її складників на кібербезпеку ІКС з урахуванням колізій чинного законодавства та деякого світового досвіду.

Питання, що обговорюються, мають певні припущення, обмежені законодавчим, часовим та іншими чинниками. Безумовно, що кібербезпека пов'язана з інформаційною безпекою, доповнюючи залежність та вплив одна на одну. Так, можна погодитися із законодавцем, який визначає, що інформаційна безпека представляє собою стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [2]. Однак таке визначення має суттєве припущення, що, в решті-решт, не сприяє підвищенню якості кібербезпеки ІКС. Наприклад, до прийняття Закону України «Про основні засади забезпечення кібербезпеки України» (05.10.2017 р.) (чинний від 09.05.2018 р.) [3] в інформаційному законодавстві було відсутнє визначення не тільки поняття «кібернетична безпека (кібербезпека)», а й таких понять, як «кібернетичний простір (кіберпростір)», «кібернетична загроза (кіберзагроза)», «кібернетична атака (кібератака)», «кібернетичний захист (кіберзахист)», «кіберзлочинність» тощо. Вказаний Закон визначає засади національної системи кібербезпеки як сукупності політичних, соціальних, економічних та інформаційних відносин разом з організаційно-адміністративними і техніко-технологічними заходами державного і приватного секторів та громадянського суспільства. Фактично ним визначено правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, повноваження й обов'язки державних органів,

підприємств, установ, організацій, осіб та громадян, основних засад координації їхньої діяльності, а також базових термінів у сфері кібербезпеки. Отже, згідно із задекларованими у преамбулі цього Закону положеннями встановлюються засади, можливість та регулювання за допомогою норм вітчизняного права у кіберпросторі з метою забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, а також національних інтересів України. Водночас, не дивлячись на удосконалення чинного законодавства, реальні прояви кібератак стали мало прогнозованими, а їх результатом, як правило, стають значні фінансово-економічні збитки або непередбачувані наслідки порушень функціонування інформаційно-телекомунікаційних систем, які безпосередньо впливають не тільки на стан фінансової та економічної безпеки, а й на стан національної безпеки та оборони [4].

Проблеми кібербезпеки виникали разом зі становленням ІКС. У зв'язку з цим вони неодноразово розглядалися на різних міжнародних та національних рівнях, постійно шукаючи рішень у контексті розвитку самих ІКС. Так, ще за рік до проведення І етапу Всесвітнього саміту з питань інформаційного суспільства (Женева, грудень 2003 року) Генеральною Асамблеєю (ГА) ООН було прийнято Резолюцію, зміст якої пов'язаний саме з питаннями забезпечення кібербезпеки. Зокрема, в Резолюції йшлося про конкретні заходи: про необхідність створення системи глобальної культури кібербезпеки. ГА ООН пропонувала державам-членам відповідно віднестися до створення глобальної культури кібербезпеки, зокрема в межах їхніх зусиль щодо розвитку у своїх суспільствах культури кібербезпеки під час застосування і використання інформаційних технологій. У Резолюції відзначалося також важливе значення міжнародного співробітництва з метою досягнення кібербезпеки шляхом підтримки національних зусиль, спрямованих на укріплення людського потенціалу, розширення можливостей у плані навчання і зайнятості, покращення державних послуг і підвищення якості життя за рахунок використання передових, надійних та безпечних ІКТ і мереж, а також сприяння забезпеченню загального доступу [5]. У Женевській декларації зазначалося, що необхідно формувати, розвивати і впроваджувати глобальну культуру кібербезпеки в співробітництві з усіма заінтересованими сторонами і компетентними міжнародними органами. Ці зусилля повинні спиратися на все ширше міжнародне співробітництво. У межах цієї глобальної культури кібербезпеки важливо підвищувати безпеку і забезпечувати захист даних і недоторканності приватного життя (п. 35) [6]. Для її реалізації була розроблена міжнародна програма (Туніська програма для інформаційно—го суспільства), де наголошувалося на прагненні підвищувати довіру і безпеку під час використання ІКТ шляхом зміцнення основи для довіри, необхідність далі просувати, розвивати і впроваджувати у співробітництві з усіма заінтересованими сторонами глобальну культуру кібербезпеки, як це викладено в Резолюції 57/239 ГА ООН та в інших відповідних регіональних основоположних документах. Далі було відзначено, що ця культура потребує національних дій та активізації міжнародного співробітництва для зміцнення безпеки за підвищення захисту особової інформації, недоторканності приватного життя і даних (п. 39) [7].

Як відзначалося в наступних Доктринах інформаційної безпеки (2009, 2014, 2017 рр.), що були розроблені вже в Україні, інформаційний складник набуває дедалі більшої ваги і стає одним із найважливіших елементів забезпечення національної безпеки. Інформаційний простір, інформаційні ресурси, інформаційна інфраструктура та інформаційні технології значною мірою впливають на рівень і темпи соціально-економічного, науково-тех-

нічного і культурного розвитку [8; 9]. Після цього в переважній більшості провідних країн світу були прийняті відповідні законодавчі акти щодо діяльності в галузі кібербезпеки. Незважаючи на це, за оцінками експертів у сфері кібербезпеки все ж таки відмічається посилення тенденції до значного зростання кількості та розширення спектра кібератак з метою порушення конфіденційності, цілісності і доступності державних інформаційних ресурсів, зокрема тих, що циркулюють на об'єктах критичної інформаційної інфраструктури. Таке зростання свідчить про недостатню якість не тільки кібербезпеки, а також того, як і що треба захищати. І це не дивно, оскільки в законодавстві України тлумачення терміна «кіберзахист» з'явилося нещодавно [8; 9]. І хоча згаданий Указ Президента України [8] вже не є чинним, він залишається цікавим в історичному плані, бо до його прийняття існувала правова невизначеність, яка означала порушення принципу верховенства права, закріпленого у ст. 8 Конституції України. На необхідності додержання цього принципу в діяльності державних органів неодноразово наголошено у рішеннях Європейського суду з прав людини, у документах Ради Європи, а також Венеціанської комісії. Невизначеність створювала умови до можливості існування плутанини, що сприяло постійному (додатковому) виникненню умов для кіберзагроз. На нашу думку, в цьому контексті важливо розібратися з розумінням питання якості в кібербезпеці та його зв'язком з законодавчими приписами.

Автор свого часу займався проблемами підвищення якості критичних технологій і має певні уявлення про неї. Відомо і не викликає сумнівів те, що якість представляє собою комплексне поняття, яке характеризує ефективність усіх сторін діяльності: розробка стратегії, організація виробництва, маркетинг тощо. Важливо усвідомлювати, що категорія якості є всеохоплюючою. Крім продукції та послуг, вона поширюється на підприємства, організації, установи, їхній персонал і системи менеджменту, законодавство. З філософсько-правових позицій якість притаманна будь-якій діяльності людини, взаєминам між людьми, ставленню людей до навколишнього світу. Якість включає в себе одночасно і мету, і засіб її досягнення. Більшість людей говорять про якість і економіку, якість і культуру, якість і духовність, якість і законодавство, а зрештою, все це створює якість життя. Саме з цих позицій слід підходити до розв'язання комплексу проблем якості кібербезпеки.

Оновлений варіант стандарту ISO (стандарти Міжнародної організації по стандартизації) розглядає якість як ступінь, до якого сукупність власних характеристик задовольняє вимоги. Як продукт праці якість визначається як категорія, що нерозривно пов'язана як із вартістю, так і зі споживчою вартістю. Адже споживача цікавить не природа продукту праці як такого, а йому важливо те, що продукт має необхідні властивості, які є об'єктом споживання. Предметом споживання можуть бути продукти діяльності, які є різними за способом споживання, конструкцією, призначенням. Один і той самий продукт може мати безліч різноманітних властивостей і бути придатним для різних способів використання. У свою чергу сукупність властивостей, притаманних окремому продукту, вирізняє його з безлічі аналогічних предметів. Тому з економічної точки зору якістю товару може виступати його спроможність задовольняти ту чи іншу потребу. Сам предмет споживання становить ніщо інше, як сукупність корисних властивостей продукту праці. І лише сукупність певних властивостей робить продукт предметом споживання. За наявності суто конкретної потреби кожний предмет споживання, крім її спроможності задовольняти, характеризується ще й тим, наскільки вчасно і повно він це робить, що має пряме відношення до якості кібербезпеки.

Уточнюючи термін «якість» у 1994 р., з його попередніх визначень було виключено термін «властивості». Якщо розмістити терміни за спільністю понять про якість, то отримаємо ряд: споживання – властивості – якість.

Математично споживання характеризує зв'язок між залежними й незалежними змінними, вираженими у вигляді тексту, таблиць, математичних формул, графіків.

Властивість, як і якість, теж представляє філософську категорію, що виражає такий бік предмета, який зумовлює його відмінність або спільність з іншими предметами та виражається його відношенням до них. Зазвичай вона узагальнює низку характеристик об'єкта, наприклад властивість безпеки.

У визначенні якості є ще два терміни, що потребують пояснення, якими виступають потреба і об'єкт.

Потреби виникають у разі незадоволеності вимог суспільства, необхідних для його нормальної життєдіяльності, і спрямовані на усунення цієї незадоволеності. Частина потреб суспільства, для задоволення яких необхідна економічна діяльність, носить назву економічних потреб. Ринок орієнтований не просто на задоволення потреб споживачів, а на задоволення попиту покупців, що випливає з їхніх потреб.

У визначенні якості поняття потреби є вихідним, а їхні характеристики мають відповідати характеристикам якості об'єкта. У неконкретних ситуаціях на ринку важливу роль відіграє суб'єктивне поняття і сприйняття якості, тобто це може бути і «ступінь задоволення потреби», або «якість представляє те, за що платять гроші». Поняття якості доволі змінне, виходячи з потреби його новизни, надійності, реклами тощо. З часом уява про якість змінюється, вона залежить від рівня інформації про об'єкт.

Недолік якості кібербезпеки полягає те тільки в будь-якій невідповідності продукції вимогам нормативно-правових актів і нормативних документів або вимогам, пред'явленим до неї, а і в необхідності своєчасних опереджувальних інноваційних змін. Можливий істотний недолік виступає як недолік, який робить неможливим чи неприпустимим використання продукту відповідно до його цільового призначення, що виникає з вини виробника. Після його усунення може виявитися знову з незалежних від споживача причин.

Отже, безпека безпосередньо залежить від якості, представляє собою стан, за якого ризик шкоди обмежений допустимим рівнем. При цьому контроль якості у вигляді перевірки відповідності кількісних та якісних характеристик продукції або технологічного процесу, від якого залежить якість продукції, встановленим технічним нормам у кібербезпеці практично суттєво обмежений. Низький рівень якості кібербезпеки сприяє створенню сприятливого середовища для хакерських атак. Об'єктом уваги зловмисників стають не тільки провладні об'єкти та установи держави, а й компанії державного і приватного сектора різних розмірів, причому атаки можуть бути як масовими, так і націленими на конкретну організацію. Хакери навчилися добре маскуватися, і щоб ефективно протистояти їхнім атакам, необхідно мати на озброєнні такі якісні засоби кібербезпеки, які здатні розпізнати загрозу, навіть коли вона не помітна на загальному фоні.

У ситуації, що склалася, необхідно оцінити стійкість установ (компаній) до загроз, які умовно можна поділити за типами кібератак. До звичайних атак відносяться атаки з боку «пересічних непрофесійних» хакерів, які, знаючи про слабкі місця в тій або іншій системі захисту, намагаються зламати її за допомогою стандартних хакерських утиліт. Для успішного проведення подібного роду атак не потрібен особливий досвід та навички. Складні атаки виконують професійні хакери, озброєні передовими технічними засобами і методиками. Вони знають про критичні точки уразливості в системі

захисту організації, про які їй самій не завжди відомо. До третього типу відносять такий тип атак, який можна назвати інноваційними. Це принципово новий тип атак, які проводяться з прицілом на уразливості в ІКС і зумовлені появою нових технологій. Як правило, на подібні атаки йдуть найбільш технічно підковані зловмисники, які наперед проводять ретельну підготовчу роботу, щоб мати можливість визначити слабкі ланки в системі захисту і скористатися ними. Не виключено, що незабаром на багато організацій обрушиться ціла хвиля хакерських атак, охоплюючи діапазон від найпростіших до найбільш витончених. Подібним атакам потрібно вміти давати відсіч, а без якісних засобів захисту це неможливо. У відповідь необхідно вживати рішучих заходів у всіх можливих випадках, починаючи з протистояння найбільш поширеним атакам і закінчуючи застосуванням «тонших» підходів для протидії просунутим і принципово новому інноваційному типу атак. Оскільки повністю захиститися від атак неможливо, і яка-небудь з них неодмінно знайде слабке місце в захисті, слід насамперед зосередитися на тому, як оперативно виявити таку атаку і ефективно подолати її наслідки. У цьому випадку доречні такі поради.

1. Захиститися від звичайних атак означає вміти тримати свою «межу» на замку. Ключовими складниками стійкості організації до подібних видів атак є такі традиційні засоби, як антивірусні програми, системи виявлення і запобігання вторгненням (IDS і IPS), регулярне оновлення програмного забезпечення, а також технології шифрування, що забезпечують цілісність даних навіть у тому випадку, якщо зловмисникам вдасться одержати до них доступ. Важливим елементом вибудовування надійної системи захисту також є інформування співробітників на всіх рівнях організаційної ієрархії з метою формування відповідального відношення до питань кібербезпеки, включаючи забезпечення неухильного дотримання вимог парольної політики.

2. Захиститися від складних атак означає визнати, що несанкціоноване проникнення може відбутися в будь-який момент, і бути здатним якомога раніше його виявити. Знаковим для ефективного виявлення кіберзагроз може стати створення центру забезпечення інформаційної безпеки (SOC), який повинен відігравати роль центрального штабу, що координує всю роботу в цьому напрямі. Сьогодні все частіше можна спостерігати трансформацію функцій SOC від пасивного захисту до активної оборони, ретельно спланованої, безперервної, націленої на виявлення і нейтралізацію прихованих зловмисників. Це забезпечить якість заходів у боротьбі з вірогідними загрозами за збереження найбільш важливих активів організації.

3. Захиститися від нових інноваційних атак означає визнати, що у ряді випадків походження загроз буде невідомим. Не дивлячись на всю невизначеність, найбільш інноваційно просунуті установи (компанії) можуть сформувати для себе контур майбутніх загроз і виробити такий підхід, що дозволить ужити оперативні заходи реагування в потрібний момент. Установи, що володіють надійною системою корпоративного управління, можуть розробити системи та засоби, здатні ефективно реагувати на несподівані ризики і загрози, взявши на озброєння принципи «проектованої безпеки».

На наш погляд, слід розробити програму і план дій на випадок порушення кібербезпеки, усвідомлюючи, що рано чи пізно та або інша атака зловмисників завершиться успіхом. Попередня підготовка до таких атак разом із наявністю плану дій на випадок порушення кібербезпеки (cyber breach response plan, CBRP), який автоматично виконується в разі виявлення кіберпорушень, є найкращим засобом для зведення до мінімуму їх наслідків. Варто відзначити, проте, що подібну програму порушення кібербезпеки необхідно реалі-

зовувати в масштабах усієї установи (закладу, компанії). Керівником такої програми повинен бути фахівець, що володіє належним досвідом і знаннями в області операційного і стратегічного реагування.

Зауважимо, що не слід нехтувати програмами стримування загроз. Сьогоднішні програми стримування шкідливих програм автоматично розпізнають і зупиняють шкідливі програми перш, ніж ті поширяться. Програми стримування загроз указують браузерам запускати найбільш часті адресні програми у віртуальному середовищі. Отже, навіть у разі відвідування сторінки, яка містить шкідливу програму, ця програма не може спрацювати і атакувати власника операційної системи. Крім того, ці системи можуть визначити шкідливі атаки, ґрунтуючись на поведінкових факторах, а не на підписах, тому компанія може зупинити поширення атак шкідливих програм, проти яких ще не розроблені захисні механізми.

Зауважимо, що законодавство є необхідною, але недостатньою складовою частиною розвитку кібербезпеки, де не менш важливим стає забезпечення її якості. Більше того, зусилля тільки законодавця, як і зусилля тільки розробників і користувачів ІКС, не вирішують проблемних питань. Необхідно забезпечити створення спільної приватно-державної платформи для функціонування якісної кібербезпеки в різних секторах, таких як енергетика, охорона здоров'я, транспорт та фінанси, а також самої держави та її інститутів. Це потребує включення в цей процес не тільки органів влади, а й сторони, яка б розвивала дослідницький та інноваційний потенціал сектору платформи. Однак це реально реалізувати за існування довіри щодо державно-приватної співпраці в цьому секторі діяльності.

Межі такої співпраці підкреслюють особливу важливість інновацій, що з'являються на перетині інтересів учасників ринку приватно-державного партнерства. Одним з інструментів вирішення цієї ситуації є розбудова механізму економічних кластерів, які можна широко визначити як групу економічних суб'єктів та інституцій, територіально розташованих неподалік, і достатніх масштабів для розвитку спеціалізованої експертизи, послуг, ресурсів, умінь та навичок. Співпрацюючи разом, малі та середні підприємства можуть бути більш інноваційними, створювати більше робочих місць та реєструвати більше міжнародних товарних марок та патентів, сприяючи підвищенню якості ІКС, і не тільки в інформаційно-комунікаційній галузі, ніж ті, що працюють окремо. Водночас приналежність до кластеру дозволяє установам і компаніям, що беруть участь в ініціативі, підвищити конкурентоспроможність і таким чином досягти більшої продуктивності, переважно шляхом підвищення продуктивності, завдяки покращенню доступу до спеціалізованих постачальників, технології та інформації і більш високому інноваційному потенціалу установ і компаній, що співпрацюють. Це пов'язано з передачею знань, генерацією нових ідей та акцентуванням на інноваціях, що й потрібно для підвищення якості кібербезпеки. Оскільки кластери в галузі ІКС забезпечують створення нового якісного продукту за новими бізнес-моделями, в тому числі й нового антивірусного програмного забезпечення, логічно говорити про можливості нової якості кібербезпеки та полегшення доступу до виходу на нові ринки підприємствам малого та середнього бізнесу, що працюють у галузі кібербезпеки.

Ключові слова: кібербезпека, інформаційно-комунікаційні системи, якість, інформаційне законодавство, законодавство з кібербезпеки.

Стаття досліджує питання впливу якості та її складників на кібербезпеку інформаційно-комунікаційних систем з урахуванням колізій чинного законодавства та деякого світового досвіду. З позицій кібербез-

пеки обговорено категорію «якість», розвиток якої щодо рівня безпеки регулюється трьома типами кібератак: стандартними, складними та інноваційними. Доведено необхідність використання державно-приватної співпраці в цьому секторі господарської діяльності.

Статья исследует вопрос влияния качества и его составляющих на кибербезопасность информационно-коммуникационных систем с учетом коллизий действующего законодательства и некоторого мирового опыта. С позиций кибербезопасности обсуждена категория «качество», развитие которой по уровню безопасности регулируется тремя типами кибератак: стандартными, сложными и инновационными. Доказана необходимость использования государственно-частного сотрудничества в этом секторе хозяйственной деятельности.

The article examines the impact of quality and its components on the cyber security to information and communication systems, taking into account the conflicts of the current legislation and some world experience. From the standpoint of cyber security discussed the category of «quality», the development of which is regulated by three types of cybersecurity: standard, complex and innovative. The necessity of using public-private cooperation in this sector of economic activity is proved.

Література

1. Василенко М. Підвищення стану кібербезпеки інформаційно-комунікаційних систем: якість в контексті удосконалення інформаційного законодавства. Юридичний вісник. 2018. № 3.

2. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 09 січня 2007 р. Відомості Верховної Ради України. 2007. № 12. Ст. 102.

3. Закон України «Про основні засади забезпечення кібербезпеки України» від 05 жовтня 2017 р. Відомості Верховної Ради України. 2017. № 45. Ст. 403.

4. Указ Президента України про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України» від 27 січня 2016 р. URL: http://zakon.rada.gov.ua/laws/show/96/2016.

5. Резолюція Генеральної Асамблеї ООН «Створення глобальної культури кібербезпеки» від 20 грудня 2002 р. № 57/239. URL: http://www.un.org/ru/ga/second/57/second_res.shtml.

6. Женевська декларація принципів від 12 грудня 2003 р. URL: http://www.rada.gov.ua.

7. Туніська програма для інформаційного суспільства від 18 листопада 2005 р. URL: https://informationsociety.wordpress.com/basics/wsis_outcomes/tp/.

8. Указ Президента України «Про Доктрину інформаційної безпеки» від 08 липня 2009 року № 514/2009. URL: http://zakon.rada.gov.ua/laws/show/514/2009.

9. Указ Президента України Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» від 25 лютого 2017 р. № 47/2017. URL: http://zakon.rada.gov.ua/laws/show/47/2017.