сфері. Наприклад, йдеться про рішення ЄСПЛ у справі «Компанія «Регент» проти України», численні рішення Верховного Суду.

Така множинність правових та правозастосовних актів вимагає спеціального розуміння єдності правових норм для цілей їх послідовної інтерпретації й найбільш ефективного застосування з урахуванням самої логіки арбітражного розгляду, обумовленого потребами інституційного сприяння розвитку бізнесу в країні та покращення іміджу України як держави, здатної формувати міжнародні юрисдикційні інституції, яким довіряють іноземні інвестори й ТНК. При цьому, глибоко опанувати питання міжнародного комерційного арбітражу, як і будь-якої іншої спеціальної сфери, можна лише якщо перейнятися духом відповідного регулювання, тонкою гранню взаємодії саморегулівних засад арбітражу й публічного правопорядку у державі.

Ключові слова: міжнародний комерційний арбітраж, правовий кластер, ЮНСІТРАЛ.
Ключевые слова: международный коммерческий арбитраж, правовой кластер, ЮНСИТРАЛ.
Key words: international commercial arbitration, legal cluster, UNCITRAL.

БОЙКО ВІКТОР ДМИТРОВИЧ

Національний університет «Одеська юридична академія»,
доцент кафедри кібербезпеки

ВАСИЛЕНКО МИКОЛА ДМИТРОВИЧ

Національний університет «Одеська юридична академія»,
професор кафедри господарського права і процесу

КІБЕРБЕЗПЕКА ЯК СКЛАДОВА ЦИФРОВОГО СУСПІЛЬСТВА В КОНТЕКСТІ РОЗВИТКУ ГОСПОДАРСЬКО-ПРАВОВИХ ВІДНОСИН

Сьогодні одним із засобів забезпечення державою своїх інтересів на міжнародній арені є завоювання інформаційного простору. Останнє досягається шляхом розвитку сучасних національної телекомунікаційної інфраструктури й інформаційних технологій і створення на їхній основі глобальної інформаційно-телекомунікаційної системи. Інформатизація як явище сучасності призвела до переходу людства в інформаційне (цифрове) суспільство, в якому були створені інформаційно-комунікаційні технології та інформаційно-комунікаційні системи. Вони стали важливим ресурсом та рушійною розвитку сучасної цивілізації. Однак використання комп'ютерних технологій, особливо у сукупності із телекомунікаційними мережами, породило особливий (вірусний) клас кіберзагроз. Ситуація набувала загострення разом з поширенням вико-

ристання мережі Інтернет, тобто існуючі кіберзагрози розв'язуються через забезпечення саме кібербезпеки і її постійного покращення. Слід відзначити, що широких масштабів проблема кібербезпеки набула тоді, коли можлива шкода від реалізації загроз у сферах, де використовувались комп'ютерні системи та телекомунікаційні мережі, стала досягати великих обсягів. Сьогодні практично всі національні стратегії щодо забезпечення кібербезпеки пов'язані з використанням у процесі людської діяльності комп'ютерних систем і телекомунікаційних мереж (до останніх належить і мережа Інтернет). Кібербезпека має забезпечувати захист інформаційно-комунікаційних технологій та захист інформаційно-комунікаційні систем в економіці, інших галузях господарства. Це в повній мірі стосується і господрсько-правових відносин в таких галузях як виробництво, транспорт, енергетика, рух цінних паперів, аудиторська діяльність, фінансові послуги, в бізнесі, в торгівлі тощо. Так, наприклад, в господарсько-правовому регулюванні широко поширились такі дефініції як «електронний бізнес», «електронна торгівля» та «електронна комерція». Перша здійснює розмежування електронної торгівлі на «електронну торгівлю», «електронну комерцію» чи «електронний бізнес». Під поняттям «електронний бізнес» часто розуміють будь-яку ділову активність із використанням глобальних інформаційних мереж для модифікації внутрішніх та зовнішніх зв'язків фірми з метою одержання прибутку, та зазначає, що основною складовою електронного бізнесу є електронна комерція. Так, під електронною комерцією І. О. Шалева розуміє комерційну взаємодію суб'єктів бізнесу з приводу купівлі-продажу товарів та послуг (матеріальних та інформаційних) з використанням інформаційних мереж (Internet, мережа стільникового зв'язку, внутрішні локальні мережі фірм), та відносить до неї електронний обмін інформацією (Electronic Data Interchange, EDI), електронний рух капіталу (Electronic Funds Transfer, EDF), електронну торгівлю [E-trade), обіг електронних грошей [E-cash), електронний маркетинг (E-marketing), електронний банкінг (E-banking), електронні страхові послуги [E-Insurance) тощо [1, с. 9-10]. Отже, І. О. Шалева встановлює схематичний взаємозв'язок: електронний бізнес – електронна комерція – електронна торгівля. Фактично ту ж саму схему наводить і Р. Ю. Царьов, який під електронною комерцією розуміє будь-яку транзакцію, яка здійснюється через комп'ютерну мережу, внаслідок якої право власності або право використання товаром або послугою було передано від однієї особи до іншої. Електронна комерція, на думку Р. Ю. Царьова, є складовою електронного бізнесу, тобто будь-якого процесу, який будь-яка організація проводить за допомогою мережі пов'язаних між собою терміналів (комп'ютерів, телефонів) [2, с. 10-11]. Такої ж думки дотримується і І. Б. Федишин, який розмежовує електронну комерцію та електронний бізнес. На його думку, електронний бізнес – це вид економічної діяльності компаній через комп'ютерні мережі, зокрема, Internet, з метою отримання прибутку. Це електронна економічна діяльність, яка здійснюється за допомогою інформаційно-комунікаційних технологій з метою отримання прибутків. Електронна комерція є такою, що становить е-бізнес, це один із способів його здійс-

нення. Електронна комерція (e-commerce) – вид електронної комерційної діяльності з використанням інформаційних комунікаційних технологій. Електронна комерція передбачає: відкриття Web-сайтів компанії і віртуальної крамниці в Internet; наявність автоматизованої системи управління компанією; використання електронної реклами і маркетингу; використання певної моделі бізнес-взаємодії [3, с. 8-9]. А. А. Маєвська зазначає, що електронна комерція є окремим випадком електронного бізнесу та вважає, що це широкий набір інтерактивних методів ведення діяльності з надання споживачам товарів та послуг. Загалом же А. А. Маєвська під електронною комерцією розуміє використання електронних комунікацій та технологій обробки цифрової інформації для встановлення та змін відносин створення вартості між організаціями та між організаціями і індивідами [4, с. 16]. Д. Д. Євтушенко пропонує визначити електронний бізнес як вид підприємництва, який здійснюється на основі інформаційних технологій для перетворення зв'язків підприємства з постачальниками, партнерами і клієнтами, з метою поліпшення загальної ефективності бізнесу та вдосконалення бізнес-процесів (виробництва, управління запасами, розробки продукту, управління ризиками, фінансів, управління знаннями та людськими ресурсами). Електронну комерцію науковець пропонує визначити як сукупність всіх операцій між підприємством і всіма контрагентами, здійснених за допомогою інформаційних технологій з метою автоматизації бізнес-процесів для оптимізації витрат і збільшення економічної ефективності бізнесу. Електронна комерція охоплює відносини управління персоналом; оформлення, виконання та оплати замовлень; співпрацю з постачальниками, фінансовими установами, державними та місцевими органами влади [11, с. 185-187]. Однак жоден із зазначених вище поділів не впливає на силу кібернетичних атак, нанесених в цій та інших галузях господарювання. Це стосується усіх галузей, що регулюються нормами господарського права. Від неї залежать загрози на господарські об'єкти щодо їх безпеки, тому влучно поділити їх на кількатипів (прості, складні та інноваційні). Захиститися від звичайних атак означає уміти тримати свою «межу» на замку. Ключовими складовими 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 в 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. Захиститися від складних атак означає визнати, що несанкціоноване проникнення може відбутися у 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 в боротьбі з вірогідними загрозами за збереження найбільш важливих активів організації. Захиститися від 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 вжити 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». Сучасні програми стримування шкідливих програм автоматично розпізнають і зупиняють шкідливі програми перш, ніж ті поширяться. Програми стримування загроз вказують браузерам запускати найбільш часті адресні програми у віртуальному середовищі. Отже, навіть при відвідуванні сторінку, 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 програми, проти яких ще не розроблені захисні механізми.

Отже, враховувати ступень (силу) кіберзагроз для електронних засобів господарювання цифровому суспільстві, що формується в контексті розвитку господарсько-правових відносин, а також конкретних галузевих напрямів господарського права.

Список використаної літератури:

1. Шалева І. О. Електронна комерція : Навч. посіб. К. : Центр учбової літератури. 2011. 216 с.
2. Царьов Р. Ю. Електронна комерція : навчальний посібник з підготовки бакалаврів. Одеса : ОНАЗ ім. О. С. Попова, 2010. 112 с.
3. Федишин І. Б. Електронний бізнес та електронна комерція (опорний конспект лекцій для студентів напрямку «Менеджмент» усіх форм навчання). Тернопіль : ТНТУ імені Івана Пулюя, 2016. 97 с.
4. Електронна комерція і право. Уклад. А. А. Маєвська. Х. 2010. 256 с.
5. Євтушенко Д. Д. Електронний бізнес, електронна комерція, Інтернет-торгівля: сутність та взаємозв'язок понять . БІЗНЕСІНФОРМ. 2014. № 8. С. 184-188.

Ключові слова: кібербезпека, інформаційні технології, господарське право, галузь, електронний бізнес, електронна комерція.

Ключевые слова: кибербезопасность, информационные технологии, хозяйственное право, отрасль, электронный бизнес, электронная коммерция.

Key words: cybersecurity, information technologies, economic legal law, e-business, e-commerce, e-trade.