УДК 346.7:004
DOI https://doi.org/10.32837/npnuola.v26i0.657

М. Д. Василенко, Н. С. Киреєва

ЕЛЕКТРОННА КОМЕРЦІЯ У ПРОЯВАХ ЮРИСПРУДЕНЦІЇ (ЗАКОНОДАВСТВА) ТА КІБЕРБЕЗПЕКИ (НЕСАНКЦІОНОВАНИХ ВТОРГНЕНЬ): МІЖДИСЦИПЛІНАРНЕ ДОСЛІДЖЕННЯ

Постановка проблеми. Відомо, що електронна комерція є сферою цифрової економіки, яка включає всі торгові та фінансові транзакції, що проводяться з використанням комп'ютерних мереж, а також бізнес-процеси, які пов'язані з проведенням таких транзакцій [1]. Це все сталося завдяки використанню інформаційних технологій, що, у свою чергу, призвело до принципових змін традиційних способів ведення бізнесу та виникнення нового виду економічної діяльності, який можна кваліфікувати як електронний бізнес. Активний розвиток мережі Інтернет продовжує сприяти формуванню комп'ютерних мереж, які суттєво впливають на сферу товарного обігу та інших видів господарської діяльності.

Розвиток електронної комерції відбувається досить швидкими темпами, суттєво випереджаючи як законодавство, так і безпекові заходи щодо до неї. Сьогодні доступ до ресурсів інформаційних мереж відкрив нові можливості для електронної комерції. Саме функціонування інформаційних мереж зумовлює правові, економічні та безпекові можливості електронній комерції. Дослідженням електронної комерції займалися такі науковці-економісти, як М. Возний, Т. Дубовик, Д. Легеза, С. Маловичко, О. Мельник, Н. Гринів, Л. Третьякова та ін. (див., наприклад [2, 3]). Серед зарубіжних авторів варто звернути увагу на праці Ф. Котлера, Р. Уілсона, А. Хартмана, У. Хенсона, В. Холмогорова, Т. Кеглера, М. Ліндстрома тощо. Правові питання використання інтернет-технологій вивчали П. Біленчук, В. Гаєнко, Л. Борисова та М. Козир [4], а на правове удосконалення електронної комерції звертали увагу в своїх роботах такі науковці, як В. Брижко, М. Швець, А. Новицький та В. Цимбалюк [5], а також Н. Киреєва [6; 7]. Один із співавторів цієї роботи є як фахівцем-юристом з господарського та міжнародного права з великим дослідницьким стажем, так і інженером електронної техніки з великим досвідом дослідника в минулому, вченим із проблем кібербезпеки, що відповідним чином відображається в теперішній час у його публікаціях (див., наприклад [8–10]).

Метою статті є встановлення та дослідження проявів можливостей права у поєднанні з можливостями кібербезпеки та їх значення для розвитку електронної комерції.

Виклад основного матеріалу. Досліджуючи електронну комерцію в проявах юриспруденції перш за все слід звернути увагу на законодавче визначення даного поняття, закріплене в Законі України «Про електронну комерцію», згідно зі ст. 3 якого електронною комерцією є «відносини, спрямовані на отримання прибутку, які виникають у ході вчинення правочинів щодо набуття, зміни або припинення цивільних прав та обов'язків, здійснені дистанційно з використанням інформаційно-телекомунікаційних систем, у результаті чого в учасників таких відносин виникають права та обов'язки майнового характеру» [11].

Електронна комерція включає в себе цілий ряд галузей господарської діяльності, які об'єднані ознаками дистанційності та використання інформаційно-телекомунікаційних систем. Комісія ООН з права міжнародної торгівлі (ЮНСІТРАЛ), яка є одним з основних суб'єктів нормотворчості у сфері електронної комерції, відносить до неї:

1) електронний рух капіталу (Electronic Funds Transfer, EFT);
2) електронні гроші (e-cash);
3) електронний банкінг (e-banking);
4) електронні страхові послуги (e-insurance);
5) електронний обмін інформацією (Electronic Data Interchange, EDI);
6) електронну торгівлю (e-trade);
7) електронний маркетинг (e-marketing) [12].

Перелічені галузі становлять основу електронної комерції, яка з розвитком науки та техніки дедалі більше поширює свій вплив також на інші галузі господарювання.

У зв'язку з тим, що вплив електронної комерції як на економіки окремих держав, так і на світову економіку в цілому став беззаперечним, на сучасному етапі електронна комерція стала одним із найперспективніших напрямів нормотворчої діяльності. При цьому правове регулювання даної сфери має поєднувати у собі гнучкість, що дозволить попередити гальмування подальшого розвитку, та жорсткість, яка зробить можливим гарантування належного рівня безпеки операцій у електронній сфері.

Проаналізувавши нормотворчість міжнародних організацій та національних законодавчих органів, можна виділити кілька основних напрямків правового регулювання електронної комерції.

По-перше, нормативно-правові акти в даній сфері покликані сприяти зниженню бар'єрів у галузі торгівлі товарами інформаційних технологій, до яких належать комп'ютери, програмне забезпечення, телекомунікаційне обладнання, мікропроцесори та інше аналогічне устаткування. Якщо вони не будуть доступними для широкого кола осіб, розвиток електронної комерції буде значною мірою обмежений.

По-друге, існує нагальна потреба у розробці та подальшому вдосконаленні таких правових аспектів електронної торгівлі, як захист конфіденційної інформації, ідентифікація підписів, якими скріплюються електронні документи, встановлення ідентичності інформації та документів, що ство-

рюються з використанням інформаційно-телекомунікаційних систем. Вагомим аспектом є також забезпечення ідентичності товарів та послуг. Крім того, не варто забувати про необхідність захисту авторських прав та інших об'єктів права інтелектуальної власності, вразливість яких у сфері електронної комерції посилюється. У даному аспекті правового регулювання має проявитися згадана вище жорсткість, адже забезпечення безпеки суб'єктів, які здійснюють господарську діяльність або є споживачами у сфері електронної комерції, має бути пріоритетом.

Наступним важливим аспектом правового регулювання у сфері електронної комерції є митні та податкові питання. Тут йдеться, насамперед, про оподаткування товарів та послуг, що передаються через мережу Інтернет або іншими електронними способами. Наразі контроль за такими операціями є недостатнім, внаслідок чого державний бюджет втрачає значні суми грошових коштів.

Також у якості перспективного з точки зору нормотворчості можна відзначити напрямок обслуговування електронним шляхом класичних торгівлі товарами та надання послуг. Йдеться про складання та передачу всіх необхідних документів та інформації електронним шляхом, укладання електронних договорів з контрагентами та споживачами, дистанційне узгодження змін до них тощо. Особливо цікавий даний підхід для зовнішньоекономічної діяльності. Таке обслуговування звичайних комерційних операцій посідає дедалі більш вагоме місце в електронній комерції поряд з власне електронною торгівлею, тобто переданням інформації, товарів або послуг за допомогою використання інформаційно-телекомунікаційних систем [13, с. 140].

До «класичної» ж електронної торгівлі можна віднести, наприклад, придбання та відчуження електронних книг, програмного забезпечення, звуко- та відеозаписів тощо. Не менш вагоме місце посідають також послуги, що надаються електронним шляхом, як от консультаційні, окремі медичні, бронювання номерів в готелях, придбання електронних квитків для проїзду у транспорті або відвідування тих чи інших заходів тощо.

Таким чином, з розширенням сфери електронної комерції збільшується кількість напрямів її правового регулювання.

Вагоме значення для правового забезпечення електронної комерції має діяльність міжнародних та регіональних організацій, які поряд із власне правовими створюють також організаційні та адміністративні правила електронної комерції та електронного документообігу. Провідну роль серед таких організацій, крім згаданої вище ЮНСІТРАЛ, відіграють Світова організація торгівлі (СОТ), Комісія ООН з торгівлі та розвитку (ЮНКТАД), Організація економічного співробітництва та розвитку (ОЕСР), Всесвітня митна організація (ВМО), Всесвітня організація інтелектуальної власності (ВОІВ) та інші. Безумовно, вагомим є внесок Європейського Союзу [13, с. 139].

Міжнародні та регіональні нормативно-правові акти, що регулюють відносини у сфері електронної комерції, є основою для законотворчості на національному рівні.

Фактично першим кроком до правового врегулювання електронної комерції в Україні стало прийняття Закону України «Про Національну

програму інформатизації», який визначив загальні принципи формування, реалізації та коригування стратегії вирішення проблеми забезпечення інформаційних потреб та інформаційної підтримки соціальної, економічної, наукової, технічної, екологічної, оборонної, національно-культурної та іншої діяльності на всеукраїнському рівні [14].

Ще одним із ключових нормативно-правових актів у досліджуваній сфері є Закон України «Про електронні документи та електронний документообіг». Цей Закон розкрив поняття електронного документа та електронного документообігу, закріпив міжнародні тенденції з визнання юридичної сили електронного документа, визначив права і обов'язки учасників електронного документообігу, встановив відповідальність тощо [15].

Наступним важливим документом є Закон України «Про електронні довірчі послуги», який було спрямовано на гармонізацію національного законодавства з положеннями Регламенту (ЄС) № 910/2014 Європейського Парламенту та Ради від 23 липня 2014 року про електронну ідентифікацію та довірчі послуги для електронних транзакцій в межах внутрішнього ринку та про скасування Директиви 1999/93/ЄС. Цей Закон визначив основні засади надання електронних довірчих послуг, права та обов'язки суб'єктів правовідносин у цій сфері, правові та організаційні основи здійснення електронної ідентифікації [16].

Та, безумовно, основним нормативно-правовим актом в Україні, що регулює сферу електронної комерції, є власне Закон України «Про електронну комерцію». Даний Закон визначив організаційно-правові основи діяльності в галузі електронної комерції в Україні, закріпив чіткий порядок вчинення правочинів із застосуванням інформаційно-телекомунікаційних систем (електронних правочинів), а також та визначив права та обов'язки суб'єктів правовідносин у сфері електронної комерції [11].

Незважаючи на наявність нормативної бази, в Україні існує ряд факторів, що істотно перешкоджають розвитку електронної комерції, а саме недобросовісна та протиправна поведінка учасників цієї сфери. Серед найбільш поширених випадків можна виділити фіктивні магазини, які створюються для того, щоб зібрати інформацію про картки клієнтів; магазини або суб'єкти надання послуг, які зникають із ринку після того, як отримають гроші клієнтів; шахрайство з викраденими реквізитами карток; крадіжка персональних даних тощо. Особливо небезпечним шахрайство є у сфері електронних фінансових послуг і в сучасних умовах. Так, як пише BBC з посиланням на дані агентства Muso, на фоні коронавірусної пандемії у світі відбувся різкий стрибок піратства в електронній сфері та хакерських атак [17].

Сучасні тенденції свідчать про те, що викорінити такі явища практично неможливо, адже технічний розвиток та хакерська майстерність завжди йдуть на крок попереду законодавства та способів протидії їм. У цьому світлі очевидним стає зв'язок електронної комерції та кібербезпеки.

Більше того, в умовах дедалі більшої складності інформаційних систем питання кібербезпеки електронної комерції набуває все більшого значення. З одного боку, потрібна побудова єдиного кібербезпекового простору. З іншого боку, крайня нерівномірність розвитку IT-служб та інфраструктури і різнорідність експлуатованих систем перешкоджають забезпечен-

ню необхідного рівня кібербезпеки. Навіть із найдосконалішим захистом комп'ютерні системи не можна назвати абсолютно невразливими. Актуальне значення набула проблема виявлення аномалій у роботі мережевих пристроїв, які є результатом як мережевих атак хакерів, так і збоїв у роботі апаратури і програмного забезпечення.

Кібербезпека за своєю сутністю є комплексним та стратегічним питанням для кожної держави. Вона стосується, в першу чергу, економіки та електронної комерції, розвитку інфраструктури електронних комунікацій, розробки технологій кіберзахисту інформаційних систем та ресурсів, запровадження заходів, спрямованих на боротьбу з кіберзлочинами тощо [18, с. 14].

Демцов А. та Добржанська О. влучно відзначають, що в сучасних реаліях досягти суспільного та економічного процвітання в державі можливо виключно в разі забезпечення безпеки у кіберпросторі, адже саме кібербезпека повинна сприяти належному та ефективному функціонуванню мережевих інформаційних інфраструктур та попередити завдання шкоди користувачам кіберпростору [19, с. 112]. Для України таке твердження вчених є актуальним, оскільки в економіці нашої держави інформаційно-комунікаційні технології займають вагоме місце. За даними Global Innovation Index, у 2019 році Україна посіла 47 місце і ввійшла до трійки країн з економічної групи з доходом нижче середнього (lower-middle income) [20]. Отже, кібербезпека є вагомим чинником розвитку економічного потенціалу держави, тому що зарубіжні інвестиційні кошти вливаються в економіку країни лише за наявності сприятливого інвестиційного клімату, для якого забезпечення кібербезпеки відіграє важливу роль.

Сучасний етап розвитку кібербезпеки характеризується новими тенденціями, які пов'язані з переходом від кількісного до якісного зростання стану технічного забезпечення самої інформаційної технології. Водночас сама кібербезпека реалізує стан захищеності інтересів як держави і суспільства в цілому, так і кожного окремого індивіда від кіберзагроз. Фактично це правове, організаційне, науково-технічне, інформаційне забезпечення мережевої і комп'ютерної безпеки. Кібербезпека спрямована на забезпечення ефективного захисту кіберпростору та включає, зокрема, криптографічний захист інформації, адміністративну та інформаційну безпеку інформаційно-телекомунікаційних систем, безпеку веб-сайтів.

Слушною є думка Лук'янчува Р., який зауважив, що сфера правовідносин, які у сучасних реаліях складаються в мережі Інтернет, є доволі інноваційною. Дана обставина суттєво ускладнює правозастосовчу практику. Інтернет-відносини за своєю сутністю є новим типом суспільних відносин, які виникають, змінюються і припиняються в кіберпросторі (віртуальному просторі) – середовищі, яке дає можливості здійснювати комунікації і реалізувати суспільні відносини, утвореному шляхом функціонування сумісних комунікаційних систем та забезпечення електронних комунікацій з застосуванням мережі Інтернет. З огляду на наведене Інтернет-відносини не можна вважати правовими відносинами в чистому вигляді, адже вони являють собою соціальні зв'язки особливої правової, технічної та інформаційної природи [18, с. 66].

Правове регулювання кібербезпеки забезпечується, насамперед, Законом України «Про основні засади забезпечення кібербезпеки України», який закріпив організаційні та правові засади забезпечення інтересів особи, держави та суспільства, національних інтересів України в кіберпросторі, визначає цілі та принципи політики держави в кіберпросторі, повноваження органів державної влади в цій сфері, а також права та обов'язки фізичних та юридичних осіб, основи координації їх діяльності.

З юридичної точки зору об'єктами кібербезпеки є:

1) основоположні права та свободи людини й громадянина;

2) сталий розвиток цифрового комунікативного середовища та інформаційного суспільства;

3) конституційний лад, суверенітет, територіальна цілісність держави та недоторканність її кордонів;

4) загальнонаціональні інтереси, а також інтереси особи, суспільства та держави [18, с. 202].

Суб'єктів суспільних відносин, що пов'язані із забезпеченням кібербезпеки (Інтернет-відносин), можна розділити на три групи:

1) суб'єкти, що створюють, розширюють, розвивають програмно-технічну частину інформаційної інфраструктури Інтернету, а також забезпечують її експлуатацію. До таких суб'єктів належать розробники транскордонних інформаційних мереж, програмних засобів тощо;

2) суб'єкти, які створюють та розповсюджують інформацію в мережі Інтернет, а також забезпечують підключення до мережі Інтернет. Це спеціалісти, які формують інформаційні ресурси і надають інформацію з них споживачам, а також підключають споживачів до Інтернету;

3) споживачі інформації та послуг в мережі Інтернет. Вони, у свою чергу, поділяються на споживачів інформації, що виконують пошук і отримання інформації в Інтернеті; споживачів послуг за хостингом, тобто тих, хто розміщує інформацію в Інтернеті на серверах; та споживачів послуг інформаційної пошти [18, с. 68].

Очевидним стало те, що значущим елементом забезпечення кібербезпеки є розвиток технологій кіберзахисту, створення його надійної та ефективної системи, яка включає, зокрема, впровадження апаратної, змістовної безпеки, безпеки сервісів та додатків. У зв'язку із цим під кіберзахистом слід розуміти систему правових, організаційних та технічних заходів, метою яких є виявлення та усунення кіберінцидентів та кібератак, запобігання їм, нейтралізація їх наслідків та поновлення стабільності і надійності роботи інформаційних, інформаційно-телекомунікаційних мереж, технологічних систем і мереж.

Разом із тим ще раз підкреслимо, що комп'ютерні системи є вразливими навіть за умови застосування найдосконалішого захисту. Виявлення невизначеностей у роботі мережевих пристроїв, очевидно, ще довгий час буде залишатися основною проблемою.

Зазначаємо і акцентуємо увагу на тому, що захист, який забезпечується за допомогою фаєрволу, вже не є таким ефективним проти мережевих атак. Саме система виявлення та запобігання вторгнень (IDS / IPS) дозволяє реагувати на атаки зловмисників, що використовують відомі уразливості, а також розпізнавати шкідливу активність всередині мережі.

Таким чином, IDS / IPS системи стали і залишаються основними та найбільш ефективними системами для виявлення вторгнень і захисту мереж компанії від атак, неавторизованого проникнення в мережу. Рішення в них можуть обривати сумнівні з'єднання і автоматично налаштовувати міжмережевий екран, який блокує подальші атаки, а також інформують службу інформаційної безпеки компанії. При цьому важливим стає виявлення неполадок і несанкціонованих вторгнень у мережу підприємства та сканування системи на наявність «дірок», використовуючи насамперед IDS. Однак слід пам'ятати, що IDS – лише один із засобів гарної архітектури забезпечення безпеки мережі та багаторівневої стратегії її захисту.

IDS / IPS системи мають свої переваги і недоліки. Розвинути перші і згладити останні можна, застосовуючи IDS в комплексі з іншими засобами забезпечення безпеки електронної комерції. У IDS є деякі перекриття виконуваних функцій, особливо з міжмережевими екранами, які вже виконують деякі обмежені функції виявлення вторгнень, піднімаючи тривогу, коли «спрацьовує» відповідне правило (сигнатура). IDS унікальні в тому, що на відміну від міжмережевих екранів, які можуть виконувати велику кількість різних функцій (фільтрація пакетів, аутентифікація користувачів, кешування та інші), в них реалізована лише одна функція, але реалізована добре та ефективно. Виявлення вторгнень у реальному масштабі часу, особливо на високих мережевих швидкостях, вимагає значної кількості виділених ресурсів, яких не може забезпечити жоден з мережевих екранів, крім складних, які мають значну вищу вартість і порівнянні з іншими, а тому є менш доступними для кінцевих споживачів.

Підсумовуючи вищенаведене, відзначимо, що для забезпечення повноцінної діяльності у сфері електронної комерції, яка є однією з перспективних галузей сучасної економіки, необхідне поєднання двох основних чинників: ефективного правового регулювання та забезпечення належного рівня кібербезпеки. При цьому необхідно забезпечити одночасну реалізацію правових, організаційних, адміністративних та науково-технічних заходів, які можуть бути ефективними лише у їх сукупності.

Отже, враховуючи наведене вище, стає постулованим те, що, оскільки науково-технічний прогрес та дії хакерів і шахраїв у сфері електронної комерції завжди випереджають можливості кібербезпеки і, особливо, правове регулювання, подальші дослідження окресленої проблематики зберігають свою актуальність та перспективність.

Література

1. Мельник О.В. Електронна комерція як складова частина електронного бізнесу. URL : http://intkonf.org/melnik-ov-elektronna-komertsiya-yak-skladova-chastina-elektronnogo-biznesu/ (дата звернення: 07.05.2020).

2. Возний М.І. Міжнародна електронна торгівля. Проблеми та перспективи розвитку в Україні. *Зб. наук. праць Буковин. ун-ту. Економічні науки*. 2014. Вип. 7. С. 243–252.

3. Дубовик Т.В. Інтернет-торгівля в Україні. *Вісн. Київ. нац. торг.-екон. ун-ту*. 2015. № 1. С. 20–28.

4. Біленчук П.Д., Гаєнко В.І., Борисова Л.В., Козир М.В. Правовий аспект використання інтернет-технологій в Україні. *Право і безпека*. 2002. № 3. С. 14–16.

5. Брижко В., Швець М., Новицький А., Цимбалюк В. Електронна комерція: правові засади та заходи удосконалення. Київ : НДЦПІ АПрН України, 2008. 149 с.

6. Kyreieva N. Foreign Experience of Economic-Legal Regulation of Electronic Financial Services. *Юридичний вісник*. 2018. № 1. С. 103–107.

7. Киреєва Н. Електронний підпис як засіб забезпечення безпеки на ринку фінансових послуг. *Юридичний вісник*. 2018. № 3. С. 73–78.

8. Василенко М.Д. Підвищення стану кібербезпеки інформаційно-комунікаційних систем: якість в контексті удосконалення інформаційного законодавства. *Юридичний вісник*. 2018. № 3. С. 17–34.

9. Бойко В.Д., Василенко М.Д. Кібербезпека як складова цифрового суспільства в контексті розвитку господарсько-правових відносин. *Правові та інституційні механізми забезпечення розвитку України в умовах європейської інтеграції*: матеріали Міжнродн. наук.-практ. конф. (м. Одеса, 17 трав. 2019 р.). Одеса, 2019. С. 637–640.

10. Василенко М.Д. Деякі питання щодо місця кібербезпеки в забезпеченні стабільного розвитку економіки. *Правові умови сприятливого бізнес-клімату: досвід Німеччини та України*: матеріали міжн. наук.-практ. конф. (Одеса, 27 черв. 2019). Одеса, 2019. С. 35–39.

11. Про електронну комерцію : Закон України від 03.09.2015 р. № 675-VIII. Дата оновлення: 19.04.2020. URL : https://zakon.rada.gov.ua/laws/show/675-19 (дата звернення: 10.05.2020).

12. UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998. United Nations publication. URL : https://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf (дата звернення: 07.05.2020).

13. Крегул Ю., Батрименко В., Батрименко В. Правове регулювання міжнародної електронної комерції. *Зовнішня торгівля: економіка, фінанси, право*. 2018. № 2. С. 136–147.

14. Про Національну програму інформатизації : Закон України від 04.02.1998 № 74/98-ВР. Дата оновлення: 01.08.2016. URL : https://zakon.rada.gov.ua/laws/show/675-19 (дата звернення: 10.05.2020).

15. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 № 851-IV. Дата оновлення: 07.11.2018. URL : https://zakon.rada.gov.ua/laws/show/851-15 (дата звернення: 10.05.2020).

16. Про електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII. Дата оновлення: 13.02.2020. URL : https://zakon.rada.gov.ua/laws/show/675-19 (дата звернення: 10.05.2020).

17. В мире резко увеличилось количество пиратства. URL : https://internetua.com/v-mire-rezko-uvelicsilos-kolicsestvo-piratstva (дата звернення: 11.05.2020).

18. Лук'янчук Р.В. Державне управління у сфері забезпечення кібербезпеки України : дис. ... канд. наук з держ. упр. : 25.00.01 / Інститут законодавства Верховної Ради України. Київ, 2017. 250 с.

19. Добржанська О.Л., Демцов А.А. Кібербезпека як феномен міжнародних відносин на прикладі Федеративної Республіки Німеччини. *Актуальні проблеми міжнародних відносин*. Київ, 2011. Вип. 102(1). С. 111–116.

20. Global Innovation Index 2019. URL : https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2019.pdf (дата звернення: 13.05.2020).

Анотація

Василенко М. Д., Киреєва Н. С. **Електронна комерція в проявах юриспруденції (законодавства) та кібербезпеки (несанкціонованих вторгнень): міждисциплінарне дослідження.** – Стаття.

У статті досліджено поняття електронної комерції, визначено основні її галузі та напрямки розвитку, проаналізовано тенденції її розвитку на території України, зокрема, відмічено постійне збільшення значення електронних операцій. Встановлено, що правове регулювання електронної комерції, головним чином, має забезпечувати сталий та вільний розвиток електронної комерції і одночасно гарантувати безпеку суб'єктів у цій сфері. Проаналізовано основні національні нормативно-правові акти у сфері електронної комерції та визначено коло правовідносин, що вони регулюють, зокрема, щодо формування та реалізації стратегії у сфері інформатизації, визнання юридичної сили електронних документів та діяльності у сфері електронного документообігу, електронної ідентифікації, вчинення електронних правочинів тощо. Відзначено, що головними перешкодами на шляху розвитку електронної комерції є шахрайство, хакерські атаки, комп'ютерне піратство та інші подібні загрози в кіберпросторі, на підставі чого зроблено однозначний висновок про нерозривний

зв'язок електронної комерції та кібербезпеки. Кібербезпека, з одного боку, є станом захищеності держави, суспільства та особи від кіберзагроз, а з іншого – організаційно-правовим, науково-технічним, інформаційним забезпеченням мережевої і комп'ютерної безпеки. З'ясовано коло суб'єктів та об'єктів правовідносин у сфері кібербезпеки, визначено основи нормативно-правового регулювання даної сфери в України. Здійснено аналіз сучасних тенденцій кібербезпеки, що пов'язані з переходом від кількісного до якісного зростання стану технічного забезпечення інформаційної технології. Акцентовано увагу на тому, що у сучасних реаліях ефективність «фаєрволів» значно зменшилася, тому для забезпечення кібербезпеки перспективнішими стають системні рішення класу IDS / IPS, проте здійснено застереження, що навіть використання найдосконаліших систем захисту не гарантує невразливість комп'ютерних систем. Автори підкреслили, що науково-технічний прогрес та можливості зловмисників у кіберпросторі завжди випереджають законодавство та можливості заходів забезпечення кібербезпеки, що робить окреслену сферу перспективною для подальших досліджень.

Ключові слова: інформаційно-комунікаційні технології, електронна комерція, електронна торгівля, кібербезпека, інтернет-технології, кіберпростір, захист, інформаційна безпека.

S u m m a r y

Vasilenko M. D., Kyreieva N. S. **E-commerce in the aspects of jurisprudence (legislation) and cybersecurity (unauthorized intrusions): an interdisciplinary study.** – Article.

In this article the concept of e-commerce is examined, its main industries and directions of development are identified, and main trends of its development in Ukraine are analyzed, in particular, the constant increase of the importance of electronic transactions is noted. It is established that the legal regulation of e-commerce, above all, should ensure the sustainable and free development of e-commerce and at the same time guarantee the safety of entities and individuals in this area. The main national regulations in the field of e-commerce are analyzed and the range of legal relations that they regulate is determined, in particular, on the formation and implementation of strategy in the field of informatization, recognition of legal force of electronic documents and activities in the field of electronic document management, electronic identification, electronic transactions, etc. It is noted that the main difficulties for the development of e-commerce are fraud, hacking, computer piracy and other similar threats in cyberspace, which led to a clear conclusion about the inextricable link between e-commerce and cybersecurity. Cybersecurity, on the one hand, is a state of protection of the state, society and the individual from cyberthreats, and, on the other hand, it is organizational and legal, scientific and technical, informational support of network and computer security. The range of subjects and objects of legal relations in the field of cybersecurity is clarified, the bases of normative-legal regulation of this sphere in Ukraine are determined. An analysis of current trends in cybersecurity, related to the transition from quantitative to qualitative growth of technical support of information technology, is made. It is emphasized that in modern realities the efficiency of "firewalls" has significantly decreased, so IDS / IPS class system solutions are becoming more promising for cybersecurity, but it is cautioned that even the use of the most advanced protection systems does not guarantee invulnerability of computer systems. The authors emphasized that scientific and technological progress and the capabilities of criminals in cyberspace are always ahead of the law and the possibility of cybersecurity measures, which makes the outlined area promising for further research.

Key words: information and communication technologies, e-commerce, e-trade, cybersecurity, Internet technologies, cyberspace, protection, information security.