

Наведений перелік показує, що основною передумовою до рішення задачі є наявність достатньо зручного опису процесу  $X(t)$ . При цьому пропонується апроксимувати реальний випадковий процес  $X(t)$  лінійною функцією часу  $X(t)=A+Bt$ , де  $A$  і  $B$  – випадкові коефіцієнти ймовірні, характеристики яких визначаються за допомогою методу найменших квадратів на основі з умови  $M \int_T [X(t) - (A + Bt)]^2 dt = \min$ , при чому  $T$  – інтервал спостереження випадкового процесу  $X(t)$ .

### III Висновки

Проблема прогнозування включає в себе низку труднощів, одні з яких власне зв'язані з прогнозуванням, інші характерні для всіх напрямків автоматичного контролю, треті визначають загальні можливості прогнозування і його місце серед інших видів контролю.

Таким чином в статті досліджено та приведено деякі загальні проблеми прогнозування несанкціонованого доступу в інформаційних системах, досліджено загальні методи прогнозування та представлено етапи вирішення задачі прогнозування в автоматизованих системах контролю, що в свою чергу дозволило отримати подальший розвиток вирішенню проблеми прогнозування НСД.

*Список використаної літератури:* 1. Силин В. Б., Заковряшин А. И. *Автоматическое прогнозирование состояния аппаратуры управления и наблюдения*. Москва. Энергия 1973г. – 336 с. 2. Путінцев Н. Д. *Апаратний контроль цифрових обчислювальних машин*. – М. Сов. радио, 1966. – 236 с. 3. Смирнов Н. В., Душин-Барковский И. В. *Курс теории вероятностей и математической статистики* – М.: Наука, 1968. – 576 с. 4. Тихонов В. И., *Достижение границ марковских процессов // изв. Вузов радиотехника, т. 15, № 4, 1972. – С. 253.* 5. Згуровський М. З., Панкратова Н. Д., *Техническое предвидение* -К.: Политехника, 2005. – 165 с. 6. Демидович Б. П., Марон Н. А., Шувалова Д. З. *Численные методы анализа* –М.: Наука, 1967. – 242 с. 7. Клямко Э. И. *Схемный и тестовый контроль автоматических цифровых вычислительных машин* – М.: Сов. Радио., 1983. – 320 с. 8. Сидоров А. М. *Методы контроля электронных цифровых машин*. – М.: Сов. Радио., 1986. – 342 с. 9. Згуровський М. З. *Основи системного аналізу/ Згуровський М. З., Панкратова Н. Д.* – К:ВНУ, 2007–544 с.

**Олексій Мервінський**

*Національний технічний університет України «Київський політехнічний інститут»*

УДК 35.078.3+340.68

## ЄВРОПЕЙСЬКІ ВИМОГИ ЩОДО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

*Анотація:* Розглядаються нормативно-правові акти Європейського Союзу, пов'язані із захистом і обробкою персональних даних у сфері електронної комерції і спрямовані на захист основоположних прав і свобод людини і громадянина, проведено їх аналіз.

*Summary:* The article reviews normative acts, regulations, constitutive or other documents European Union involving protection and processing of personal data in the field of e-commerce and aim to protect the fundamental rights and freedoms of natural persons, particularly the right to privacy in relation to the processing of personal data and includes statistical analysis.

*Ключові слова:* Електронна комерція, персональні дані, захист персональних даних, захист прав суб'єкта персональних даних.

### I Вступ

Розвиток новітніх технологій та сучасних засобів комунікацій призвів до появи в другій половині ХХ століття нового виду діяльності – електронної комерції («*electronic commerce*» або «*e-commerce*»), яка за своєю сутністю є сферою економіки, що функціонує в електронній формі в електронному середовищі з використанням комп'ютерних мереж, зокрема глобальної мережі Інтернет. Проте створення та забезпечення функціонування таких сфер діяльності супроводжується можливістю виникнення певних ризиків, насамперед для фізичних осіб, які вступають у правові відношення в результаті створення попиту на товари та послуги, укладання договорів в електронній формі, здійсненні електронних платежів, а також обслуговуванні споживачів. Масовий характер використання персональних даних в сфері електронної

комерції створює передумови для виникнення чисельних порушень при їх обробці, особливо при збиранні, накопиченні, зберіганні, оновленні та використанні персональних даних, які суттєво посилюють ризик незаконного втручання третіх осіб у приватне життя людини. Ризики в сфері електронної комерції для людини можуть бути пов'язані з ймовірністю нанесення шкоди через розповсюдження недостовірної або неналежної реклами, а також з порушеннями норм чинного законодавства щодо незаконної обробки даних, у тому числі їх втрати або випадкового знищення, а також від незаконного доступу до них.

Наразі в Україні розпочато імплементацію європейського законодавства у сфері електронної комерції. Розглянемо Закон України «Про електронну комерцію» [1], проаналізуємо, чому він не врегулює всі відносини, які пов'язані із захистом персональних даних під час їх обробки у цій сфері згідно з вимогами законодавства в сфері захисту персональних даних і потребує подальшого розвитку та удосконалення, спеціалізованого правового регулювання цієї сфери.

## II Основна частина

Діяльність суб'єктів господарювання в сфері електронної комерції повинна відповідати вимогам законодавства в сфері захисту персональних даних. Оскільки спеціальні питання, пов'язані із захистом персональних даних при здійсненні процедур електронної торгівлі, наразі не відображені в українському законодавстві, до сфери електронної торгівлі застосовуються загальні положення законодавства в сфері захисту персональних даних, насамперед Закону України «Про захист персональних даних» [2].

Правові відносини у сфері електронної комерції під час вчинення електронних правочинів повинні також чітко врегулювати відносини, пов'язані із захистом даних відповідно до проведеної класифікації економічної діяльності в мережі Інтернет з урахуванням всіх суб'єктів електронної комерції.

Сутність електронної комерції полягає у відносинах, спрямованих на отримання прибутку, що виникають під час вчинення правочинів щодо набуття, зміни або припинення цивільних прав та обов'язків, здійснених дистанційно з використанням інформаційно-телекомунікаційних систем, внаслідок чого в учасників таких відносин виникають права та обов'язки майнового характеру [1]. Таким чином сфера електронної комерції має дві складові: взаємовідносини суб'єктів господарювання та фізичних осіб і внутрішню взаємодію різних суб'єктів господарювання (див. рис. 1).

При класифікації економічної діяльності враховуються всі залучені до неї суб'єкти, що можуть мати доступ до персональних даних при їх обробці: B2B (продавець-продавець), B2C (продавець-покупець), C2B (покупець-продавець), а також C2C (покупець-покупець).

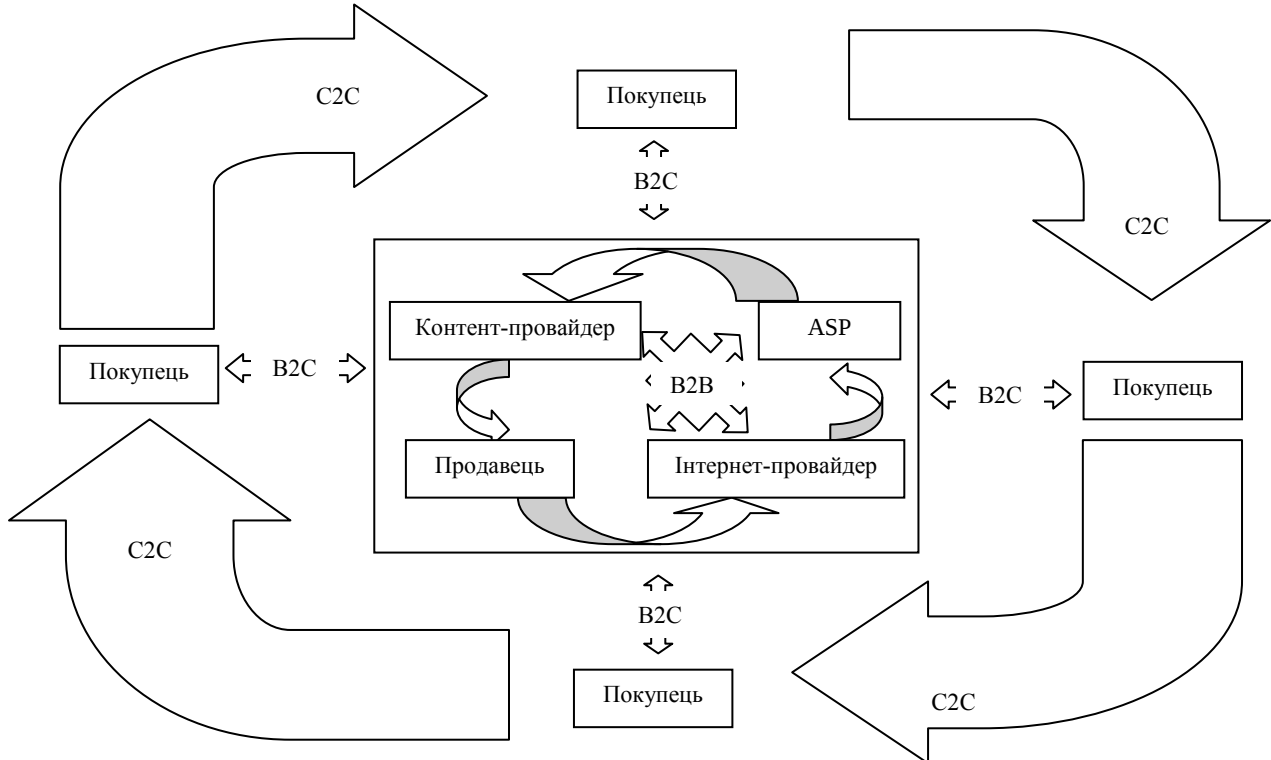


Рисунок 1 – Схема електронної комерції

Крім того при класифікації процесів на рівні B2B (продавець-продавець) повинні обов'язково враховуватися суб'єкти господарювання, що пропонують певний обсяг інформації (контенту) для розташування на дисковому просторі мережевого серверу комп'ютера (контент-провайдери), надають контент-провайдеру дисковий простір або виділений сервер для розміщення інформації (Інтернет-провайдери), послуги Інтернет-провайдера контент-провайдеру щодо надання дискового простору та каналу зв'язку для розміщення інформації на мережевому сервері або надання контент-провайдеру виділеного серверу (хостинг), а також суб'єкти господарювання, що надають контент-провайдеру або покупцю технічний доступ до мережі Інтернет (ASP, access server provider). Таким чином схема електронної комерції повинна змінюватися з урахуванням матриці віртуальних відносин суб'єктів, пов'язаних з персональними даними.

Таблиця – Матриця віртуальних відносин суб'єктів, пов'язаних з персональними даними в сфері електронної комерції

	Покупці	Продавці	Треті сторони
Покупці (C)	C2C	C2B	C2N
Продавці (B)	B2C	B2B	B2N
Треті сторони (N)	N2C	N2B	N2N

Важливо наголосити на тому, що електронну комерцію не можна розглядати як автоматизацію існуючих процесів комерційної діяльності або дублювання в електронному вигляді офф-лайнної діяльності. Надання електронних послуг завжди розглядається як створення нових процесів і формування нових взаємовідносин між суб'єктами господарювання та суб'єктами персональних даних.

Виникнення цілого комплексу нових суспільних відносин вимагає відповідного правового врегулювання. Необхідність такого врегулювання визначається тим, що з одного боку правова невизначеність суб'єктів цих відносин призводить до їх незахищеності, а по-друге, неповне правове врегулювання створює «правовий вакуум».

Крім того, зважаючи на транскордонний характер сфери електронної комерції, розробка вітчизняних нормативно-правових актів повинна відбуватися з урахуванням вимог відповідних актів міжнародного права. Наразі організації, що входять в структуру ООН та Європейського союзу ухвалили цілу низку міжнародних нормативних актів (модельні закони UNITRAL, директиви Європейського союзу тощо) і відпрацювали відповідні рекомендації, спрямовані на надання допомоги країнам щодо удосконалення національних законодавств, які за своєю сутністю представляють узгоджену позицію світової спільноти з проблем та перспектив правового врегулювання відносин, що виникають в сфері електронної комерції.

Важливість врахування норм міжнародного права при імплементації законодавства в сфері електронної комерції також обумовлена глобальною доступністю електронних послуг, а також тим, що відносини суб'єктів відносин, пов'язаних з персональними даними, набувають транскордонного характеру.

Зважаючи на значну кількість ймовірних загроз приватності фізичній особі як суб'єкту персональних даних, найбільш доцільно вивчити досвід країн Євросоюзу, які у цьому питанні вже перейшли від стадії «впровадження» до стадії «становлення».

Загалом, аналіз законодавства країн Європейського Союзу показує, що питання застосування електронних технологій регулюються такими типами законодавчих актів:

- Закони про електронну комерцію (торгівлю), які охоплюють найбільш широке коло суспільних відносин;
- Закони про електронний документ, що мають значно вужчий спектр нормативного врегулювання;
- Закони про електронний цифровий підпис, що сконцентровані тільки на одному з реквізитів електронного документу – ЕЦП;
- Закони про електронні платежі, що майже не перетинаються з названими, оскільки мають специфічний предмет врегулювання.

Проте, за усталеною практикою, всі названі акти щодо електронної комерції обов'язково розглядаються насамперед на відповідність вимогам щодо захисту основоположного права на недоторканість приватного життя і отримують відповідні висновки уповноважених органів з питань захисту персональних даних.

Єдиним визнаним міжнародним договором з захисту свободи, безпеки та прав людини в мережі Інтернет залишається Будапештська конвенція про злочинність в кіберпросторі [3], яка була розроблена Радою Європи в 2001 році і ратифікована Верховною Радою України в 2005 році. Відповідно до Конвенції будь-який незаконний доступ до комп'ютерних даних, їх перехоплення або втручання в них повинні вважатися

протизаконними діями. До комп'ютерних даних Конвенцією віднесено персональні дані фізичних осіб або конфіденційні дані юридичних осіб, що розміщуються в комп'ютерних мережах.

Резолюція Парламентської Асамблеї Ради Європи від 2011 року про захист особистого життя та персональних даних в Інтернеті [4] сформулювала такі загальні принципи захисту особистого життя при використанні інформаційно-комунікаційних технологій:

- захист особистого життя є необхідним елементом життя людини та існування людини в демократичному суспільстві; там де не поважається приватне життя людини і її гідність, там виникає загроза для свободи та безпеки;

- право на захист приватного життя і персональних даних є одним з основних прав людини, яка накладає на державу обов'язок сформулювати належну правову базу такого захисту від втручання з боку органів державної влади, а та також сторонніх осіб та структур;

- кожен повинен мати можливість контролювати використання своїх персональних даних іншими особами, включаючи будь-який доступ, збирання, зберігання, розкриття, маніпулювання, використання.

В 2000 році Європейським парламентом та Радою ЄС було ухвалено Директиву про деякі правові аспекти інформаційних послуг на внутрішньому ринку, зокрема про електронну комерцію (Директива про електронну комерцію), метою якої є наближення окремих національних нормативно-правових актів до сформованих єдиних вимог до суб'єктів відносин, що пов'язані з наданням інформаційних послуг на внутрішньому ринку ЄС, вимог до сервіс-провайдерів, вимог до засобів комерційної комунікації (електронних засобів, засобів зв'язку тощо), які використовуються у зазначеній сфері, а також загальні вимоги щодо відповідальності посередників та положення щодо розроблення кодексів поведінки. Також Директива містить основні положення щодо організації співробітництва між країнами-членами ЄС в сфері електронної комерції.

Перед ухваленням Директиви про електронну комерцію всі її положення були ретельно опрацьовані Робочою групою із захисту фізичних осіб при обробці персональних даних, створеною відповідно до Статті 29 Директиви 95/46/ЄС [6] і яка є незалежним консультативним органом ЄС з питань захисту фізичних осіб при обробці персональних даних. У розробленому та представленому Робочою групою Висновку 1/2000 «Щодо певних аспектів захисту даних в світлі електронної комерції» [7] звертається особлива увага на важливість захисту персональних даних в процесі здійснення електронної комерції, наводиться європейський досвід щодо врегулювання цього питання на законодавчому рівні, а також наголошується на тому, що правова структура захисту основоположного права на недоторканість приватного життя та захист особистих даних, в тому числі і у сфері електронних комунікацій, повинна відповідати принципам захисту даних, що визначені Директивою 95/46/ЄС [6] та Директивою 2002/58/ЄС [8], яка доповнює їх щодо сфери телекомунікацій і містить чітке пояснення стосовно повного та належного застосування до Інтернет-послуг законодавства про захист даних.

Крім того, Робоча група в ході проведеного дослідження приділила серйозну увагу питанням захисту персональних даних щодо трьох важливих питань, які відносяться до характерних особливостей новітніх інформаційних технологій, і зробила відповідні Висновки щодо інформації публічного сектору та захисту персональних даних 3/99 [9], Рекомендації стосовно невидимої та автоматизованої обробки персональних даних в Інтернеті 1/99 за допомогою програмних і апаратних засобів [10] та Рекомендації стосовно збереження Інтернет-провайдерів інформації про трафік з метою забезпечення правопорядку 3/99 [11].

В контексті електронної комерції Робочою групою також було додатково опрацьовано питання щодо надання роз'яснення із застосування Європейських правил захисту даних до обробки даних для цілей електронної розсилки і наголошувалося на тому, що перед початком рекламної кампанії чи комерційної розсилки, організації чи установі, яка здійснює розсилку, необхідно мати докладний та відповідний список адрес електронної пошти потенційних споживачів, які можуть бути одержаними з мережі Інтернет шляхом збирання безпосередньо від споживачів або відвідувачів веб-сайтів; через списки, підготовлені третіми особами, або шляхом пошуку у відкритих джерелах, таких як загальнодоступні каталоги, групи новин та дискусійні групи [7].

До особливостей електронних комерційних розсилок, які створюють передумови для виникнення ризиків, відносять низьку вартість практичної реалізації цієї процедури для відправника, порівняно з традиційними методами прямого маркетингу, а також мінімальний час, необхідний для її реалізації, що є стимулом для широкомасштабного використання цього засобу маркетингу та ігнорування питань захисту даних та проблем, які спричиняє електронна розсилка.

При цьому з позиції фізичної особи як суб'єкта персональних даних маємо потрійну проблему. По-перше, це отримання адрес електронної пошти без їхньої згоди або дозволу, по-друге, це одержання величезної кількості небажаних з боку користувача рекламних матеріалів, по-третє – зайві витрати на оплату інтернет-трафіку.

Ключовим питанням щодо забезпечення приватності фізичних осіб при функціонуванні електронної комерції є спам. Спам – це неодноразове надсилання великої кількості незапитуваних повідомлень електронної пошти, зазвичай комерційного характеру, особам, з якими відправник до цього не контактував. Як правило, спам має місце тоді, коли адреси електронної пошти були зібрані в загальнодоступних місцях в мережі Інтернет. У зв'язку з цим європейськими фахівцями також була окреслена проблема з точки зору внутрішнього ринку (між країнами-членами ЄС), яка може виникнути у зв'язку з розбіжностями в національних регуляторних актах щодо регулювання електронної комерційної комунікації, і яка у подальшому може призвести до створення торгових бар'єрів [7]. Обидві ці проблеми вплинули на розвиток національних законодавчих актів Європейської спільноти.

Робоча група із захисту фізичних осіб при обробці персональних даних, створена відповідно до Статті 29 Директиви 95/46/ЄС [6] і яка є незалежним консультативним органом ЄС з питань захисту фізичних осіб при обробці персональних даних в Робочому документі WP 16 (5013/99) «Обробка персональних даних в мережі Інтернет» наголошує на тому, що європейське законодавство у сфері захисту персональних даних застосовується до сфери електронної комерції [12]. При цьому питання електронної розсилки є характерним прикладом того, як проблеми захисту даних, які створює електронна комерція, можна вирішити завдяки використанню тих правових принципів, які містять відповідні директиви Євросоюзу.

Відповідно до Директиви 95/46/ЄС «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» [6] персональні дані повинні збиратися для встановлених, чітких і законних цілей, і оброблятися чесно і законно у спосіб, сумісний з цими цілями; обробка персональних даних повинна здійснюватися на законних підставах, таких як згода, контракт, закон чи баланс інтересів; суб'єкт персональних даних повинен бути проінформований про обробку даних, і мати право на заперечення проти обробки своїх персональних даних, зокрема для цілей прямого маркетингу.

При цьому до процедур захисту персональних даних в сфері електронної комерції висуваються також вимоги, спрямовані на захист прав споживачів. Директива 97/7/ЄС «Про захист прав споживачів в дистанційних контрактах» [13] зі змінами, які були внесені Директивою Європейського Парламенту та Ради №2002/65/ЄС [14] вимагає, зокрема, щоб фізичним особам не тільки як суб'єктам персональних даних, а також як споживачам, як мінімум надавалося право заперечувати проти використання електронної пошти як засобу дистанційного зв'язку.

Директива стосовно електронної комерції чітко визначає такі технічні аспекти: зобов'язання ідентифікувати комерційну електронну пошту як таку, зобов'язання звірятися та поважати реєстри відмов від розсилок там, де вони передбачені національними нормами. Проте декларативна частина та стаття 1(4)(b) дають чітко зрозуміти, що ця Директива в жодній мірі не ставить за мету зміну правових принципів та вимог, які передбачає вищезазначена існуюча законодавча база. Оскільки законодавство про захист даних в повній мірі застосовується до електронної комерції, впровадження Директиви стосовно електронної комерції має повністю відповідати сформульованим принципам захисту даних. Це означає, по-перше, що в питаннях, що стосуються захисту даних, в ЄС до відповідальної за обробку персональних даних компанії продовжує застосовуватися національне законодавство тієї країни, де така компанія була заснована [6]. Це також означає, що Директива стосовно електронної комерції не може державам-членам ЄС вимагати від компаній запитувати попередню згоду на комерційні комунікації [8], ані перешкодити анонімному користуванню Інтернетом [6].

Зазначені норми врегульовують питання невтручання в особисте життя, а також визначають права і обов'язки всіх учасників. Зазначається також, що необхідно розрізняти дві ситуації.

Якщо компанія отримала адресу електронної пошти безпосередньо від суб'єкта даних в цілях здійснення такою компанією електронної розсилки, або від третьої особи, якій були розголошені дані, перша компанія повинна повідомити суб'єкта персональних даних щодо цілей збирання цих даних в момент збирання адрес [6]. До того ж, на момент збору і в будь-який час після суб'єкту персональних даних як мінімум має бути надане право на заперечення за допомогою простих електронних засобів, як то шляхом натискання на призначене для цього відповідне віконце, проти використання його даних першою компанією та подальшого використання компаніями, які отримали дані від першої компанії [6]. Деякі національні законодавства країн-членів ЄС, які впроваджують відповідні директиви, навіть вимагають від компаній отримувати згоду суб'єкта персональних даних на обробку цих даних. Вимоги Директиви стосовно електронної комерції щодо незапитуваних комерційних комунікацій доповнюють ці норми на технічному рівні шляхом встановлення, по відношенню до постачальника послуг, обов'язку звірятися з реєстром, але вони жодним чином не обмежують зобов'язання володільців чи розпорядників персональних даних.

Інша ситуація виникає у разі отримання адреси електронної пошти з публічного простору, зокрема в мережі Інтернет. Вважається, що її використання для цілей електронної розсилки буде суперечити вимогам Директиви «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» [6] з трьох причин. По-перше, це може розцінюватись як «нечесна» обробка персональних даних. По-друге, це суперечитиме принципу цілей збору даних в тому сенсі, що суб'єкт персональних даних міг зробити свою адресу електронної пошти загальнодоступною з дещо іншої причини, наприклад, з метою участі в групі новин. По-третє, враховуючи вартісний дисбаланс та порушення щодо одержувача, така розсилка не може вважатися такою, що необхідна в цілях законних інтересів, переслідуваних володільцем персональних даних, крім випадків, коли над такими інтересами переважають інтереси основних прав і свобод суб'єкта даних стосовно дотримання балансу інтересів.

Основним питанням захисту приватності в сфері електронної комерції залишається розуміння способу реалізації прав суб'єктів персональних даних, що обумовлена специфічними особливостями використання технічних засобів та наданих механізмів для реалізації прав. До специфічних особливостей відносять насамперед віртуальність (існування тільки за умови використання спеціального програмного і технічного забезпечення в штучно створеному комп'ютерному середовищі) та існування у невизначеному фізичними межами просторі, що може призводити до відсутності дійового механізму правового врегулювання. Крім того, відносини суб'єктів, пов'язаних з персональними даними, ускладнюються неможливістю чіткої ідентифікації учасників таких відносин, а також наявністю як учасника таких відносин провайдера телекомунікацій. А в деяких випадках обмін інформацією може відбуватися навіть не фізичною особою, а комп'ютерною програмою.

Найбільшу складність для регулювання відносин між суб'єктами, пов'язаними з персональними даними в сфері електронної комерції, викликає невизначеність їхнього місця знаходження. Доступ до глобальної мережі мають громадяни з усіх країн світу і будь-хто може стати учасником таких відносин. Згідно Директиви про електронну комерцію [8] особи, що надають послуги з використанням мережі Інтернет, повинні виконувати вимоги законодавства країни свого походження (так званий *state-of-origin principle*).

Мережа Інтернет надає можливість доступу до інформаційних ресурсів під псевдонімом або взагалі анонімно. Тому складність ідентифікації учасників відносин в сфері електронної комерції пов'язана анонімною користувачів Інтернет: суб'єкт може вказувати своє ім'я (назву), достовірність якого складно перевірити. Все це обумовлює необхідність чіткого визначення сторін та однозначної ідентифікації для всіх можливих учасників відносин.

Необхідно особливо наголосити на питаннях залежності суб'єктів відносин, пов'язаних з персональними даними, від відносин з інформаційними провайдерами або провайдерами телекомунікацій, що не тільки забезпечують доступ до мережі Інтернет, а фактично також стають учасниками таких відносин особливо у разі, коли обмін інформацією стає неможливим або ускладнюється. Крім того, участь провайдерів не тільки забезпечує організаційний характер таких відносин, що надає можливість упорядкувати процеси обміну інформацією в мережі, а також обумовлюється можливістю впливати на відносини своїх користувачів. Форми впливу можуть бути самими різноманітними: від блокування можливості інформаційного обміну до незаконної передачі інформації стороннім особам. При цьому слід зазначити, що вплив може бути як навмисний, так і випадковий у разі збою в роботі апаратних та програмних засобів або витоку інформації. Однак відомі способи регулювання відносин в мережі Інтернет не враховують діяльність провайдерів або навпаки, вимоги до забезпечення діяльності провайдерів не враховують особливості відносин, що відбуваються в мережі Інтернет.

Важливе значення має електронний характер документообігу в мережі та використання спеціального програмного і апаратного забезпечення для обробки, зберігання та обміну інформацією в електронному вигляді. Саме ця особливість обумовлює всі інші характеристики відносин в мережі. Абсолютно надійних програм або баз даних не існує, тому відношення в мережі залежать від тих технологій, що використовуються для забезпечення її функціонування. Крім того, збої у функціонуванні мережі можуть бути викликані діями третіх сторін.

### III Висновки

З аналізу Європейських вимог щодо захисту персональних даних у сфері електронної комерції слідує, що практика розвинутих країн Євросоюзу рекомендує при удосконаленні законодавства в сфері електронної комерції дотримуватися принципу так званої «технологічної нейтралізації законодавства», який полягає в тому, щоб виключати розробку нормативно-правових актів під будь-які технічні стандарти (регламенти) або навіть просто прив'язані під певну технологію. Незважаючи на наявність захищених технологій та спеціалізованого програмного забезпечення, впровадження принципів самоврегулювання та

підвищення рівня обізнаності користувачів щодо існуючих ризиків тільки на законодавчому рівні можна захистити право на приватність та захист персональних даних.

Досвід країн Євросоюзу засвідчує, що вирішення проблеми правового врегулювання питань електронної торгівлі є тільки частиною значної низки питань, пов'язаної з електронною комерцією.

Проведений аналіз норм законодавства Євросоюзу у сфері захисту персональних даних, що стосується питань електронної комерції, не відображає всіх питань взаємодії між наданням електронних послуг та забезпеченням приватності фізичної особи як користувача цих послуг. Його мета – підвищити обізнаність щодо питань, які ставить певний тип обробки даних про фізичну особу, який сьогодні є предметом обговорення та дискусії у багатьох колах, а також допомогти зрозуміти європейську нормативно-правову базу електронної комерції з урахуванням вимог законодавства в сфері захисту персональних даних. Окрім проблем, які були окреслені в статті, можуть існувати інші, що потребують відповідного тлумачення або відпрацювання єдиних підходів, починаючи з кібермаркетингу та електронних платежів до технологій підвищення рівня приватності, а також окремого розгляду питань розсилки спаму та перевірку веб-сайтів відповідно до єдиного європейського контрольного переліку на основі директив стосовно захисту даних.

Список використаної літератури: 1. Закон України «Про електронну комерцію». [Електронний ресурс]. – Режим доступу: <http://zakon0.rada.gov.ua/laws/show/675-19> 2. Закон України «Про захист персональних даних». <http://zakon3.rada.gov.ua/laws/show/2297-17> 3. Будапештська конвенція про злочинність в кіберпросторі. [Електронний ресурс]. – Режим доступу: [http://zakon0.rada.gov.ua/laws/show/994\\_575](http://zakon0.rada.gov.ua/laws/show/994_575) 4. Резолюція Парламентської Асамблеї Ради Європи від 2011 року про захист особистого життя та персональних даних в Інтернеті [Електронний ресурс]. – Режим доступу: <http://www.khpg.org/index.php?id=1329990005> 5. Директива Європейського Парламенту та Ради ЄС 2000/31/ЄС від 08.06.2000 року про деякі правові аспекти інформаційних послуг на внутрішньому ринку, зокрема про електронну комерцію (Директива про електронну комерцію) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). [Електронний ресурс]. – Режим доступу: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:HTML> 6. Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року, Європейський Союз; Директива, Міжнародний документ від 24.10.1995 №95/46/ЄС. [Електронний ресурс]. – Режим доступу: [http://zakon4.rada.gov.ua/laws/show/994\\_242](http://zakon4.rada.gov.ua/laws/show/994_242) 7. Висновок 1/2000 Робочої групи із захисту фізичних осіб при обробці персональних даних, створеної відповідно до Статті 29 «Щодо певних аспектів захисту даних в світлі електронної комерції», прийнятий 3-го лютого 2000 року: WP 28 (5007/00/EN/final). [Електронний ресурс]. – Режим доступу: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp28\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp28_en.pdf) 8. Директива №2002/58/ЄС Європейського Парламенту і Ради ЄС в отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи (Директива о конфиденциальности и электронных средствах связи), Директива, Міжнародний документ від 12.07.2002 №2002/58/ЄС. [Електронний ресурс]. – Режим доступу: [http://zakon4.rada.gov.ua/laws/show/994\\_243](http://zakon4.rada.gov.ua/laws/show/994_243) 9. Висновок 3/99 щодо Інформації публічного сектору та захисту персональних даних, прийнятий 3 травня 1999 року: WP 20 (5055/99). [Електронний ресурс]. – Режим доступу: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp28\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp28_en.pdf) 10. Рекомендація 1/99 стосовно невидимої та автоматизованої обробки персональних даних в Інтернеті за допомогою програмних і апаратних засобів, ухвалена 23 лютого 1999 року: WP 17 (5093/98). [Електронний ресурс]. – Режим доступу: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp17\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp17_en.pdf) 11. Рекомендація 3/99 стосовно збереження Інтернет-провайдерів інформації про трафік з метою забезпечення правопорядку, ухвалена 7 вересня 1999 року: WP 25 (5085/99). [Електронний ресурс]. – Режим доступу: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp25\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp25_en.pdf) 12. Робочий документ Робочої групи із захисту фізичних осіб при обробці персональних даних, створеної відповідно до Статті 29: Обробка персональних даних в мережі Інтернет. Прийнятий 3 лютого 1999 року, WP 16 (5013/99). [Електронний ресурс]. – Режим доступу: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1999/wp16en.pdf> 13. Директива 97/7/ЄС Європейського Парламенту та Ради «Про захист прав споживачів в дистанційних контактах» від 20 травня 1997 року. [Електронний ресурс]. – Режим доступу: [http://zakon1.rada.gov.ua/laws/show/994\\_245](http://zakon1.rada.gov.ua/laws/show/994_245) 14. Директива №2002/65/ЄС Європейського Парламенту і Ради ЄС о дистанционном маркетинге потребительских финансовых услуг и о внесении изменений в Директиву Совета №90/619/ЕЭС и Директивы № 97/7/ЕС и 98/27/ЕС от 23 сентября 2002 года. [Електронний ресурс]. – Режим доступу: [http://zakon1.rada.gov.ua/laws/show/994\\_b31](http://zakon1.rada.gov.ua/laws/show/994_b31)