УДК 340.132+316.324.8

УХАНОВА Н.С., старший науковий співробітник НДІІП НАПрН України

ВИКЛИКИ І ЗАГРОЗИ ПРАВАМ ТА БЕЗПЕЦІ ЛЮДИНИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Анотація. *У статті проаналізовано вплив загроз інформаційній безпеці. У цьому контексті Доктрина інформаційної безпеки України одним із пріоритетів державної політики в інформаційній сфері визначає розвиток правових інструментів захисту прав людини і громадянина на вільний доступ до інформації, її поширення, оброблення, зберігання та захист. Охарактеризовано принципи забезпечення прав людини в умовах розвитку інформаційного суспільства. Досліджено світовий досвід дотримання прав людини у контексті розвитку інформаційних технологій. Підкреслено переважне значення принципу пропорційності, як однієї з найважливіших гарантій забезпечення прав людини при забезпеченні національної безпеки та інформаційної безпеки держави.*

Ключові слова: *загрози інформаційній безпеці, інформаційна сфера, інформаційні ресурси, інформаційно-телекомунікаційні технології, Доктрина інформаційної безпеки, права і свободи людини і громадянина.*

Summary*. The article analyzes the impact of threats to information security on human rights. In this context, the Doctrine of Information Security of Ukraine,determines the development of legal instruments for the protection of human rights and citizen's free access to information, its dissemination, processing, storage and protection as one of the priorities of the state policy in the information sphere. The principles of ensuring human rights in the conditions of the information societydevelopmentare characterized. The world experience in observing human rights in the context of the development of information technologies has been researched.The overriding importance of the principle of proportionality is emphasized as one of the most important guarantees of ensuring human rights while ensuring the national security and information security of the state.*

Keywords: *threats to information security, information sphere, information resources, information and telecommunication technologies, Doctrine of information security, rights and freedoms of humanand citizen.*

Аннотация. *В статье проанализировано влияние угроз информационной безопасности на права человека. В этом контексте Доктрина информационной безопасности Украины одним из приоритетов государственной политики в информационной сфере определяет развитие правовых инструментов защиты прав человека и гражданина на свободный доступ к информации, ее распространение, обработки, хранения и защиту. Охарактеризованы принципы обеспечения прав человека в условиях развития информационного общества. Исследован мировой опыт соблюдения прав человека в контексте развития информационных технологий. Подчеркнуто преимущественное значение принципа пропорциональности, как одной из важнейших гарантий соблюдения прав человека при обеспечении национальной безопасности и информационной безопасности государства.*

Ключевые слова: *угрозы информационной безопасности, информационная сфера, информационные ресурсы, информационно-телекоммуникационные технологии, Доктрина информационной безопасности, права и свободы человека и гражданина.*

Постановка проблеми. Вільне та безпечне існування особи, суспільства, держави та їх взаємодія залежить від захищеності інформаційної сфери від зовнішніх і внутрішніх загроз. Зокрема, у Доктрині інформаційної безпеки України забезпечення і захист прав людини відносяться до основного напрямку реалізації національних інтересів в інформаційній сфері.

Сучасний стан реалізації прав людини в інформаційній сфері пов'язаний з викликами, обумовленими застосуванням інформаційно-комунікаційних технологій (далі – ІКТ). Розвиток ІКТ призводить до розширення можливостей їх недобросовісного використання, яке створює загрози інформаційній безпеці і може призводити до порушень прав людини. У зв'язку з цим виникає проблема співвідношення інформаційної безпеки і прав людини. Шляхи вирішення означеної проблеми полягають насамперед у необхідності виявлення викликів і загроз правам та безпеці людини в інформаційній сфері, що нині є проблемою надзвичайно актуальною, оскільки Україна, як і всі цивілізовані країни світу, стала на шлях розвитку інформаційного суспільства.

Результати аналізу наукових публікацій. Правові аспекти впливу інформаційних і комунікаційних технологій на розвиток сучасного суспільства знайшли своє відображення в роботах О.А. Баранова, В.М. Брижка, О.Д. Довганя, Г.М. Линника, О.В. Олійника В.Г. Пилипчука, В.Б. Толубка, Є.Л. Ющука та інших дослідників. Розуміння інформаційної безпеки, на нашу думку, має ґрунтуватись на її визначенні з точки зору стану захищеності національних інтересів України в інформаційній сфері, що складається із сукупності збалансованих інтересів особи, суспільства і держави від внутрішніх та зовнішніх загроз. У науковій літературі наводяться подібні судження. Наприклад, О.В. Олійник сформулював теоретичне підґрунтя для подальшої системної характеристики напрямів та ієрархії безпекогенних чинників "ризик", "загроза", "виклик", "небезпека" [6, с. 6]. У той же час науковець справедливо вказує на принципові недоліки цього документу, адже Доктрина, на його думку, не визначає важливі аспекти забезпечення інформаційної безпеки України [6, с. 10]. Крім того, не менш важливим зауваженням щодо змісту зазначеного документу є відсутність принципу дотримання прав людини під час забезпечення інформаційної безпеки. Внесення цього доповнення слугуватиме надійним фундаментом в процесі формування державної політики, що стосується захисту прав людини.

Г.М. Линник обґрунтовано наголошує на наявності потенційних і реальних загроз в інформаційній сфері, які негативно впливають на суспільний розвиток держави та реалізацію її євроінтеграційних прагнень [7, с. 4]. У той же час, авторське розуміння інформаційної безпеки, як "діяльності суб'єктів права щодо задоволення національних інтересів в інформаційній сфері, шляхом управління реальними чи потенційними загрозами", має дискусійний характер, оскільки головний акцент у визначенні способів протидії реальним та потенційним загрозам інформаційній безпеці акцентований на управлінні ними [7, с. 7]. Вчений наводить ґрунтовну періодизацію становлення та розвитку інституту забезпечення інформаційної безпеки. В процесі її формування доходить висновку, що головним недоліком попередніх етапів функціонування системи забезпечення інформаційної безпеки є її недостатня орієнтація на дотримання прав і свобод людини і громадянина.

Є.Л. Ющук, розкриваючи ключові питання забезпечення інформаційної безпеки в мережі Інтернет, справедливо наголошує на всеохоплюючому впливі Інтернет-ресурсів, неможливості забезпечення захисту інформації, причому зазначений вплив, на думку автора, дуже часто має негативний характер [8, с. 5].

В.Б. Толубко розглядає інформаційні ресурси як ефективну зброю, яка використовується конфліктуючими сторонами на міждержавному рівні в процесі вирішення різноманітних конфліктів. Зокрема, вчений класифікує інформаційну зброю "за метою застосування; за об'єктами впливу; за механізмами реалізації впливу; за характером впливу на інформацію та інформаційні процеси; за масштабом вирішуваних завдань; за терміном дії тощо" [9, с. 18]. Окреслені автором завдання та напрями

забезпечення інформаційної безпеки у воєнній сфері мають безсумнівну наукову цінність та чинять безпосередній вплив на дотримання прав і свобод людини.

Заслуговує на увагу позиція О.Д. Довганя, який розглядає об'єкт організації національної інформаційної безпеки через призму трьох її складових компонентів: "основоположної суверенної інформації, національного інформаційного простору використання інформації та інформаційного виробництва" [10, с. 112]. Важливим є висновок автора щодо обов'язкової адекватності структурної організації системи управління інформаційною безпекою загальній системі державного управління.

Системні проблеми захисту приватності, у тому числі пов'язані з використанням новітніх ІКТ, розглядаються у низці праць В.М. Брижка та В.Г. Пилипчука [11, с. 60-70; 12, с. 16-37]. У роботах цих вчених є важлива ідея необхідності *формування інституту "права приватної власності людини на свої персональні дані", як основної складової загальної системи визначення захисту її прав,* яку можна розглядати як новацію в юридичній сфері. В умовах активного розвитку та поширення ІКТ типу Інтернет речей, Хмарних технологій, Великих Даних та їх конвергенції все складніше стає здійснювати захист персональних даних завдяки звичайних юридичних приписів. Сьогодні різноманітні ІКТ, кожна з яких на початку створення передбачала конкретне функціонально-цільове призначення, застосовують можливості інших ІКТ, які інтегруючись стали доповнювати одна одну і у комплексі створювати, так би мовити, надсумарний ефект конвергентності та надавати нову якість результатів від сумісного їх використання, що позначається на умовах реальних можливостей захисту прав людини в сфері персональних даних.

У контексті вищезазначеного, в роботі [13] доволі ґрунтовно розглядаються проблеми застосування сучасної інформаційної зброї в інформаційних війнах, зокрема в Інтернет. Визначено види, зміст, зброя, засоби нападу та захисту. Здійснено аналіз та систематизація наукових досягнень щодо розв'язування деяких техніко-технологічних і правових питань із захисту інформаційних ресурсів та знань, зокрема стосовно створення дієвих умов захисту персональних даних людини.

Метою статті є аналіз проблемних питань сучасного розвитку інформаційного суспільства, виявлення викликів і загроз правам та безпеці людини в інформаційній сфері та окреслення напрямів удосконалення національного законодавства у сфері інформаційної безпеки особи.

Виклад основного матеріалу. Постановка проблеми правового забезпечення інформаційної безпеки особи пов'язана, на нашу думку, перш за все з умовами формування стану її захищеності від внутрішніх і зовнішніх загроз у глобальному інформаційному суспільстві. Під викликами і загрозами інформаційній безпеці особи ми розуміємо актуалізовані та потенційні дії, події, процеси та явища, які чинять деструктивний вплив на психіку і свідомість людини та призводять до завдання шкоди її інтересам в умовах глобального інформаційного суспільства. До сучасних викликів і загроз інформаційній безпеці, на наш погляд, слід віднести:

1) загрози, які переслідують цілі: а) впливу на свідомість людини, на її психологічний стан, на формування екстремістських настроїв серед молоді; б) чинення деструктивного впливу, який шкодить здоров'ю людини (наприклад шляхом поширення заборонених до обігу лікарських засобів, тощо); в) оволодіння особистою інформацією, у тому числі з метою її використання у протиправних цілях; г) поширення ідеології тероризму, радикальних ідей в мережі Інтернет; д) вплив на статеву недоторканність та статеву свободу людини; е) фінансове шахрайство; є) розвиток антигромадських стереотипів поведінки, тощо;

2) навмисне поширення інформації обмеженого доступу, інформації, поширення або подання якої заборонено в Україні. Це: а) матеріали з порнографічним зображенням неповнолітніх та (або) оголошення про притягнення неповнолітніх в якості виконавців та учасників видовищних заходів порнографічного характеру; б) інформація про засоби розробки, виготовлення і використання наркотичних засобів, психотропних речовин та їх придбання, способи і місця культивування нарковмісних рослин; інформація про способи вчинення самогубства, а також заклики до вчинення самогубства;

3) загрози в мережі Інтернет: фішингові сайти, шкідливе програмне забезпечення, спам-розсилки, шахрайські сайти, рекламовані з метою отримання прибутку (фінансові піраміди, фальшиві Інтернет-магазини та ін.), Інтернет-майданчики, що впливають на індивідуальну свідомість молоді (веб-сайти, які сприяють поширенню кіберсуїциду, порносайти, чати і форуми які використовуються педофілами та сексуальними маніяками).

4) загрози, спрямовані на трафік віртуальної валюти Bitcoin, загрози конфіденційності персональних даних внаслідок ІКТ он-лайн-реклами Real-TimeBidding (RTB), загрози, які надходять від спеціальних файлів "кукі" (від англ. – cookie).

Як ключові принципи формування державної політики в галузі забезпечення інформаційної безпеки людини можуть бути прийняті: принцип визнання особи як ключового і найбільш уразливого учасника інформаційних відносин, відповідальності держави в інформаційній сфері, відповідності вживання організаційно-правових заходів безпеки реальним викликам і загрозам, а також принцип контролю за забезпеченням інформаційної безпеки людини, в тому числі за рахунок механізму захисту інформаційних прав і свобод громадськими організаціями. З метою реалізації принципу недоторканності приватного життя, неприпустимості збору, зберігання, використання і поширення інформації про приватне життя особи без її згоди, доцільно введення такого механізму, як моніторинг стану захищеності людини від внутрішніх і зовнішніх загроз в інформаційній сфері.

Ключове місце у забезпеченні прав і безпеки людини в інформаційній сфері належить захисту персональних даних. У зарубіжних країнах захист персональних даних заснований на загальних принципах роботи з ними: персональні дані мають збиратися і оброблятися тільки відповідно до закону та наділеними відповідними повноваженнями органами; персональні дані повинні бути адекватними заздалегідь визначеним цілям і розпорядження ними повинно обмежуватися за термінами, відповідним зазначеним цілям; бути точними і оброблятися тільки за згодою суб'єктів цих даних; персональні дані повинні бути доступні суб'єктам цих даних, в тому числі і для внесення в них уточнення; персональні дані повинні бути належним чином захищені.

У Грузії 1 березня 2017 року завершився тривалий процес розробки і прийняття поправок до Закону "Про електронні комунікації" від 20.11.13 р. № 1591. Рішення складного завдання дотримання прав людини і забезпечення безпеки країни завершилося прийняттям норм про створення спеціалізованого оперативно-технічного агентства, яке на підставі оперативної інформації про загрозу безпеці державі буде таємно прослуховувати і записувати телефонні розмови, а також контролювати соціальні мережі, здійснювати приховані відеозйомки, перевіряти поштові посилки [14]. За задумом авторів прийнятого парламентом Грузії закону, новий державний суб'єкт буде працювати за такою схемою: коли спецслужбам знадобиться інформація про громадян особистого характеру, вони спочатку запитають ордер в суді (як визначено законом і зараз), потім нададуть його новому державному відомству, а не провайдерам. Коротко кажучи, правозахисники хочуть, щоб доступ до "чорних скриньок" мали не

спецслужби, а нова структура. Юрист Центру вивчення і моніторингу за правами людини Г. Імнадзе – один з авторів поправок. Ідею створення окремої самостійної структури він назвав know-how грузинських правозахисників: *"Такого досвіду немає у інших країн – це наше know-how. Але у них і не було такого минулого, як у нас. Європейську модель ми не пропонуємо, тому що у нас інша ситуація – у нас провайдери могли знати, які саме дані запитують спецслужби. А це могло відбитися на безпеці країни. Вважаємо, що в Грузії право доступу і обробки особистої інформації має перейти до незалежної державної структури"* [15].

У правовій доктрині США визначення "інформаційна безпека" та "приватність" деталізується через перерахування конкретних елементів інформаційної сфери, на захист яких вона спрямована [16, с. 17]. Правові принципи конфіденційності, цілісності та доступності інформації виступають головною підставою визначення зазначених елементів. Так, при дотриманні принципу конфіденційності ознайомлення з конфіденційною інформацією, її обробка і пред'явлення вимоги про її надання допускаються тільки для особи, яка має право доступу до такої інформації. Роль принципу конфіденційності полягає у запобіганні шкоди, яку може бути заподіяно суспільним відносинам в результаті неправомірного надання та поширення інформації, що зберігається в таємниці в силу її значення для безпеки особи, суспільства та держави. Даному принципу відповідає свого роду право "зберігати у таємниці" інформацію, обмежувати доступ третіх осіб до неї, контролювати її цільове використання тощо.

На відміну від конфіденційності інформації, забезпечення її цілісності, набуло актуальності в процесі розвитку ІКТ та виникнення можливостей несанкціонованого доступу до неї з метою внесення змін або її знищення. Особа, яка володіє інформацією або правом доступу до інформації, має право вимагати забезпечення її цілісності, а також в ряді випадків цілісності носія інформації, тобто збереження їх в оригінальному, незмінному вигляді, забезпечення невтручання в структуру (форму) і зміст інформації. Зазначений принцип спрямований на забезпечення достовірності інформації, яка дозволяє зберігати між учасниками суспільних відносин необхідний рівень довіри і впевненості в тому, що вони мають справу з оригінальною інформацією та її джерелом.

Принцип доступності відіграє важливу роль у формуванні гарантій права людини на доступ до інформації. Вказаний принцип спрямований на запобігання обмеження і створення умов доступу до соціально-значимої інформації, перш за все під час взаємодії людини з органами влади, а також до іншої інформації, надання якої вона має право вимагати. Цей принцип лежить в основі реалізації заходів щодо забезпечення доступу до інформації про діяльність державних органів і органів місцевого самоврядування, екологічної інформації, в тому числі шляхом розміщення інформації на офіційних сайтах органів і організацій.

В свою чергу Доктрина інформаційної безпеки України одним із пріоритетів державної політики в інформаційній сфері визначає розвиток правових інструментів захисту прав людини і громадянина на вільний доступ до інформації, її поширення, оброблення, зберігання та захист [17]. Крім того, доступ до публічної інформації, відповідно до статті 4 Закону України "Про доступ до публічної інформації", здійснюється на принципах: прозорості та відкритості діяльності суб'єктів владних повноважень; вільного отримання, поширення та будь-якого іншого використання інформації, що була надана або оприлюднена відповідно до Закону, крім обмежень, встановлених законом; рівноправності, незалежно від ознак раси, політичних, релігійних та інших переконань, статі, етнічного та соціального походження, майнового стану, місця проживання, мовних або інших ознак [18]. Зміст цих положень яскраво

демонструє, що допустимі згідно з Конституцією України [19] та міжнародними документами про права людини обмеження повинні відповідати за змістом та обсягом цілям обмежень, що вводяться, і можуть застосовуватися тільки для захисту інших рівнозначних правових цінностей.

На додаток до принципів конфіденційності, цілісності і доступності, в правовій доктрині вироблені спеціальні правові принципи захисту права на недоторканність приватного життя, в яких визначаються межі й умови здійснення даного права. У зв'язку з принципом конфіденційності такі спеціальні правові принципи визначають можливість збору персональних даних лише законними засобами і для конкретно визначених цілей за умови попереднього повідомлення або попередньої згоди суб'єкта персональних даних, забезпечення їх захисту від таких ризиків як втрата або несанкціонований доступ, знищення, використання, зміна або розкриття даних. Поряд з принципом цілісності застосовується принцип, при дотриманні якого персональні дані повинні відповідати цілям їх використання і відповідно до таких цілей мають бути точними, повними й актуальними. Принцип доступності доповнюється принципами, які створюють умови для доступу суб'єкта персональних даних до інформації про наявність у оператора і характер оброблюваних ним персональних даних такого суб'єкта, основні цілі їх використання, місце знаходження оператора, а також наділяють суб'єктів персональних даних додатковими правами, включаючи можливість знищення, виправлення, доповнення або зміни своїх персональних даних. Зазначені принципи наразі відображені в багатьох міжнародних актах, початок визначення яких було надано Конвенцією Ради Європи "Про захист осіб у зв'язку з автоматизованою обробкою персональних даних" від 28 січня 1981 року № 108 [20].

Конфіденційність особистої інформації забезпечується шляхом надання доступу або можливості збору і обробки такої інформації тільки тим особам, які отримали відповідну згоду її власника. Якщо доступ або можливості збору і обробки надаються на підставі закону, то обов'язковим є повідомлення власника про обробку персональних даних. Повідомлення також обов'язково при інших випадках, визначених суб'єктом персональних даних або встановлених законодавством, наприклад, при порушенні конфіденційності або цілісності персональних даних. Зазначені механізми надають суб'єкту персональних даних правові можливості контролю за їх використанням і, відповідно, гарантії недоторканності його приватного життя.

Зазначимо, що з розвитком мережі Інтернет та Інтернет-сервісів, створенням потужних колекцій інформації, вказані механізми виявляються недостатніми для дотримання права людини на недоторканність приватного життя. Фактично користувач поступово втрачає контроль над використанням та поширенням персональних даних про себе. Так, при використанні Хмарних технологій процес передачі та обробки даних стає для користувача невизначеним і на практиці може полягати у клонуванні інформації та її розміщенні на серверах, розташованих в різних національних юрисдикціях. Крім того, більшість користувачів дає згоду на обробку їх персональних даних, належним чином не ознайомившись з її умовами, не розуміючи правових наслідків такої згоди і не передбачаючи подальшого використання своєї особистої інформації. В результаті механізм надання згоди користувача на обробку його особистої інформації виявляється недосконалим та неефективним, а відтак, не забезпечує конфіденційності особистої інформації і реального захисту права на недоторканність приватного життя.

Для сучасної електронної комерції попередня згода і подальше повідомлення суб'єкта персональних даних можуть інколи створювати перешкоди розвитку бізнесу та впровадження інновацій. У зв'язку з цим обмеження свободи підприємницької

діяльності в Інтернеті, зумовлені використанням традиційних механізмів захисту права на недоторканність приватного життя, стають надлишковими.

Розвиток гарантій даного права здійснюється шляхом створення додаткових по відношенню до згоди суб'єкта персональних даних та його повідомлення механізмів захисту конфіденційності, які виражені в пред'явленні специфічних вимог до осіб, які здійснюють збір і обробку особистої інформації. Такі вимоги можуть полягати у встановленні спеціального правового режиму так званих чутливих даних, обмеження збору певної особистої інформації в цифровій формі, в тому числі геолокаційних і біометричних даних, обмеження автоматичного прийняття юридично значущих рішень. Формою правового захисту персональних даних також є обмеження їх передачі в національні юрисдикції, де не забезпечуються необхідні гарантії права на недоторканність приватного життя. Одночасно зростають вимоги до технічного захисту персональних даних для запобігання несанкціонованого доступу до них, усунення наслідків їх розкриття або компрометації.

У Європейському Союзі право на недоторканність приватного життя розглядається як фундаментальне право. Його захист гарантується ст. 8 Європейської Конвенції про захист прав людини і основоположних свобод 1950 року [21] і конституціями держав-членів ЄС. Пріоритет повного контролю особи щодо своїх персональних даних перед традиційними демократичними свободами (свободою підприємницької діяльності та свободою слова) лежить в основі кількох поколінь національних законів у сфері захисту недоторканності приватного життя, нормативних правових актів ЄС та рішень Європейського суду з прав людини, див., зокрема [22; 23].

На відміну від ЄС, в США спеціальні вимоги в сфері обробки персональних даних встановлені тільки в найбільш чутливих сферах. В інших сферах держава віддає пріоритет саморегулюванню, в основі якого знаходиться свобода підприємницької діяльності, свобода договору, свобода слова та друку. Держава впливає на суспільні відносини шляхом видання різного роду рекомендацій та політичних заяв.

В час бурхливого розвитку науково-технічного прогресу і стрімкого зростання цифрової економіки європейські законодавці проходять нову важливу віху в регулюванні захисту персональних даних. Європейський Парламент і Рада 27 квітня 2016 року прийняли Регламент (ЄС) 2016/679 "Про захист фізичних осіб у зв'язку з обробкою персональних даних та про вільне переміщення таких даних, а також про скасування Директиви 95/46/ЄС (Загальні Положення про захист даних)" [24 – 27]. Цей Регламент покликаний уніфікувати норми в європейських країнах щодо захисту персональних даних громадян ЄС і забезпечити їх надійніший захист. Нові правила стали відповіддю на громадське занепокоєння щодо стану справ захисту прав на приватність.

Метою Регламенту (ЄС) 2016/679 є:

- гармонізація законодавства про захист даних по всьому ЄС;
- модернізація законів про захист даних у світлі технологічних змін;
- посилення прав громадян;
- збільшення вимог до відповідальності й обов'язків контролерів даних та обробників даних;
- вдосконалення процесу створення облікових записів користувачів, а також контроль за дотриманням законів про захист даних;
- забезпечення більшої прозорості того, як використовуються дані, ким і для чого.

Регламент (ЄС) 2016/679 застосовується до компаній (незалежно від їхнього членства в ЄС), які обробляють особисті дані осіб, що проживають у ЄС, включаючи особисті дані клієнтів Global Logic, а також їх кінцевих замовників та працівників.

Згідно з Регламентом (ЄС) 2016/679, не можна просто так взяти і використовувати персональну інформацію, прикриваючись чекмарком на згоду про конфіденційність. Для цього необхідний, щонайменше реальний дозвіл суб'єкта даних і прозорий для нього механізм використання даних компанією. Компаніям, які мають справу з обробкою персональних даних, – а це всі компанії, що мають справу з кінцевим споживачем, доведеться облікувати все, починаючи з дати, коли клієнт надав чи відредагував інформацію, і закінчуючи тим, коли дані будуть видалені зі сховищ. І найголовніше, на запит власника потрібно буде в повному обсязі і в зрозумілій формі надавати йому всі ці дані, а також видаляти їх зі сховища за його бажанням.

За запитом користувачів, Інтернет-компанії зобов'язані, зокрема, надати інформацію, з якою метою використовуються персональні дані, чи не передані вони до третіх країн і т.д. Якщо компанія, наприклад, передає персональну інформацію до іншої країни, не маючи законних підстав для цього (в регламенті вони також указані) то штраф за такі дії буде ще більшим.

На нашу думку, багато людей досить безтурботно ставляться до своїх персональних даних. Особливо це небезпечно в авторитарних державах, що використовують Інтернет як засіб контролю над громадянами (приклад Китаю). Однак і в демократичних державах Європи використання зайвої інформації, викладеної в Інтернеті, може мати негативні наслідки.

У кращому випадку користувач отримує величезну кількість непотрібної реклами, в гіршому, вся інформація про нього, включаючи сексуальні вподобання, стає надбанням третіх осіб. Регламент (ЄС) 2016/679 гарантує користувачу конфіденційність. Обов'язки з захисту інформації регулюються статтями 6, 25, 28 та 32 [25; 26].

Експерти, політики і підприємці по-різному оцінюють запровадження нових норм. Як і будь-яке інше нововведення, нове положення про захист даних містить ще багато відкритих питань. На нашу думку, новиною Регламенту (ЄС) 2016/679 є введення таких понять, як "контролер", "оператор" та "співробітник захисту даних", які мають створити умови технічного та організаційного забезпечення, котре буде гарантувати відповідність вимогам з приводу дотримання прав суб'єкта даних.

На підставі викладеного ми дійшли висновку, що Регламент (ЄС) 2016/679 дозволить створити міцнішу законодавчу базу із захисту персональних даних для громадян ЄС і, як наслідок, такий захист буде мати вплив на світову систему захисту інформації.

Більшість держав відреагувала на підвищені останнім часом загрози національній безпеці шляхом розширення повноважень органів влади щодо доступу до особистої інформації, її збирання й опрацювання, які наразі не обмежені якимись окремими категоріями інформації. Все це загострює проблему забезпечення інформаційної безпеки людини і робить її виключно злободенною та актуальною. В контексті даного завдання посилюється необхідність найширшого залучення соціологічної науки, адже інформаційна агресія – це, перш за все, руйнування позитивних соціальних установок, базових цінностей, орієнтацій, відносин, зміна їх відповідно до інтересів, які властиві тим чи іншим антисоціальним елементам і силам. При цьому в різних державах підходи до забезпечення пропорційності вжитих заходів щодо забезпечення національної безпеки також можуть відрізнятися.

Міжнародна практика свідчить, що чим менше значення демократичних цінностей у політичному режимі, тим більшу роль відіграє забезпечення національної безпеки для збереження існуючого порядку управління державою, наслідком якого є встановлення різних обмежень прав людини, включаючи право на недоторканність приватного життя. Згідно з позицією Європейського суду з прав людини, вираженою в справі "Клас та інші проти Німеччини": …*"право таємного спостереження за громадянами, яке характерно для поліцейської держави, терпимо відповідно до Конвенції тільки тоді, коли воно суворо необхідно для збереження демократичних інститутів"*; держави *"не можуть в ім'я боротьби проти шпигунства і тероризму робити будь-які дії, які вони вважають потрібними"* [23].

На нашу думку, в структурі інформаційної безпеки слід інституціоналізувати систему засобів, методів та способів протидії. Вона має передбачати оптимальний (найбільш дієвий в сформованих умовах) підбір суб'єктів задля обмеження або блокування негативних інформаційних потоків і каналів. Суб'єкти мають володіти достатньою дієздатністю і правоздатністю у "відсіканні" деструктивної інформації. Важливо, щоб координація та взаємодія були налагодженими в часі та просторі, були оперативні і рухливі, володіли достатнім ступенем гнучкості. Система засобів, методів, способів протидії має враховувати особливості сприйняття інформації тими чи іншими соціальними групами населення, їх віковий, освітній, професійний, сімейний цензи, національність, загальний фон національної культури.

Необхідно, щоб система протидії керувалася рядом принципів, таких як:

1) соціальної значущості і доцільності, забезпечення інтересів більшості населення країни;

2) принцип найширшої гласності і демократії на основі об'єктивності і адекватності інформації сучасної дійсності;

3) принцип дотримання прав людини;

4) принцип гуманності;

5) принцип збереження соціальної стабільності;

6) принцип загальноприйнятої людської моралі і моральності;

7) принцип всебічного духовного, культурного і інтелектуального розвитку людини як головного творця історичного прогресу.

Серед конкретних напрямів реалізації принципів слід виділити: контрінформацію, деідеологізацію, правове, організаційне блокування негативної інформації, парламентський, громадський і громадянський контроль за інформацією, що надається людині на змістовному і інституціональному рівні.

Зазначимо, що в нашій країні питання забезпечення інформаційної та інформаційно-психологічної безпеки вже почало опрацьовуватись. Так, Українським центром економічних досліджень в 2011 році проведений системний аналіз ситуації у сфері інформаційної безпеки України. До основних загроз інформаційної безпеки України експерти віднесли: обмеження свободи слова та доступу громадян до інформації; руйнування системи цінностей, духовного та фізичного здоров'я особи, суспільства, негативні зміни їх цільових настанов; маніпулювання громадською думкою з боку державної влади, фінансово-політичних кіл; низький рівень інтегрованості України у світовій інформаційний простір тощо [27, с. 29]. Проте такі дослідження мають здійснюватися на регулярній основі.

Висновки.

Підсумовуючи зазначене, можна констатувати, що інформаційна безпека – це такий стан соціуму, в якому забезпечений надійний і всебічний захист людини,

суспільства та держави від впливу особливого виду загроз, які виступають в формі організованих або стихійно виникаючих інформаційних потоків, що здійснюються в інтересах регресивних, реакційних або екстремістські налаштованих політичних і соціальних сил і спрямованих на усвідомлену деформацію суспільної та індивідуальної свідомості, наслідком чого виступає девіантна поведінка особи, посилення соціально-політичних, економічних і духовних колізій, наростає психологічна напруженість соціуму тощо.

Якісне правове забезпечення інформаційної безпеки можливе тільки тоді, коли воно буде побудоване на сукупності наукових принципів, до яких можна віднести:

1. Законність і правова забезпеченість. Реалізуючи цей принцип, важливо домогтися невідворотної адміністративної та судової відповідальності за неправдиву інформацію.

2. Баланс інтересів особи, суспільства та держави. Даний принцип має бути спрямований на забезпечення оптимального співвідношення конфіденційної інформації та інформації, що викриває антисоціальні елементи суспільства.

3. Об'єктивність, науковість – з метою об'єктивного відображення існуючих реалій.

4. Інтеграція з міжнародними системами безпеки, чого нагально вимагають закономірності глобальної інтеграції та розвиток міжнародних комунікацій.

5. Економічна ефективність – результати від заходів інформаційної безпеки мають перевищувати сукупні витрати на них.

6. Комплексність, системність – тісний зв'язок всіх видів безпеки, засобів, методів і способів її забезпечення у часі та просторі.

Ключовими принципами формування державної політики у сфері забезпечення інформаційної безпеки людини мають стати:

- визнання особи як ключового і найбільш уразливого учасника інформаційних відносин;

- відповідальність держави в інформаційній сфері;

- відповідність вжиття організаційно-правових заходів безпеки реальним викликам і загрозам;

- недоторканність приватного життя (неприпустимість збору, зберігання, використання і поширення інформації про приватне життя особи без її згоди, обмеження доступу третіх осіб до інформації, контроль її цільового використання тощо);

- достовірність та цілісність інформації (особа, яка є суб'єктом права на інформацією або правом доступу до інформації, має право вимагати забезпечення її цілісності, тобто перебування в незмінному вигляді, забезпечення невтручання в структуру (форму) і зміст інформації;

- прозорість, відкритість та доступність інформації про діяльність суб'єктів владних повноважень (державних органів, органів місцевого самоврядування тощо). Можуть бути введені обмеження цього принципу, які мають відповідати за змістом та обсягом цілям обмежень і застосовуватися тільки для захисту інших рівнозначних правових цінностей;

- контроль за забезпеченням інформаційної безпеки людини. При цьому доцільно введення такого механізму, як моніторинг стану її захищеності від внутрішніх і зовнішніх загроз в інформаційній сфері.

Щодо захисту персональних даних людини, ми погоджуємось з думкою вчених щодо необхідності належного захисту даних, при якому необхідно дотримуватись таких принципів:

- персональні дані мають збиратися і оброблятися тільки відповідно до закону та тільки наділеними відповідними повноваженнями органами;

- персональні дані повинні бути адекватними відповідним зазначеним цілям, розпорядження ними має бути обмежено за термінами, бути точним і оброблятися тільки за згодою суб'єктів цих даних;

- персональні дані повинні бути доступні суб'єктам цих даних, у тому числі і для внесення уточнення в ці дані та ін.

У період посилення загроз національній безпеці зазвичай розширюються повноваження органів влади щодо доступу до особистої інформації, її збирання й опрацювання, які сьогодні не обмежені якимись окремими категоріями інформації, що у свій час загострює проблему забезпечення інформаційної безпеки людини. У цьому випадку, на наш погляд, юридична наука покликана виявити відхилення соціуму від позитивних соціальних установок, базових цінностей та орієнтацій відповідно до інтересів, які властиві тим чи іншим антисоціальним елементам чи силам, адже інформаційна агресія – це, перш за все, руйнування зазначених стереотипів.

В структурі інформаційної безпеки слід інституціоналізувати систему засобів, методів та способів протидії. Вона має передбачати оптимальний підбір суб'єктів задля обмеження або блокування негативних інформаційних потоків і каналів. Суб'єкти мають володіти достатньою дієздатністю і правоздатністю у "відсіканні" деструктивної інформації. Важливо, щоб координація та взаємодія були налагодженими в часі та просторі, були оперативні і рухливі, володіли достатнім ступенем гнучкості. Система засобів, методів, способів протидії має враховувати особливості сприйняття інформації тими чи іншими соціальними групами населення, їх віковий, освітній, професійний, сімейний цензи, національність, загальний фон національної культури.

Необхідно, щоб система протидії керувалася рядом принципів, таких як: соціальна значущість і доцільність; забезпечення інтересів більшості населення країни; гласність і демократія на основі об'єктивності і адекватності інформації сучасній дійсності; дотримання прав людини, гуманність; збереження соціальної стабільності; принцип загальноприйнятої людської моралі і моральності, всебічного духовного, культурного і інтелектуального розвитку людини як головного творця історичного прогресу.

Перспектива подальших досліджень. Останнім часом дедалі дослідників і практиків звертають увагу на необхідність активної розробки проблематики інформаційно-психологічної безпеки особи, суспільства та держави. Логіка суспільного розвитку висуває ці проблеми до числа першочергових. Розгляд проблеми з науково-юридичної точки зору представляється особливо важливим, оскільки в основі більшості сучасних ІКТ і систем лежать суспільні процеси, а об'єктом їх впливу виступає конкретна особа в реальних історичних умовах.

Використана література

1. Про національну безпеку: Закон України від 21.06.18 р. № 2469-19. URL: http://zakon2.rada.gov.ua/laws/show/2469-19

2. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України": Указ Президента України від 01.05.14 р. № 449/2014. *Офіційний вісник України*. 2014. № 37. Ст. 28.

3. Стратегія забезпечення кібернетичної безпеки України / Національний інститут стратегічних досліджень, 2013 р. URL: http://www.niss.gov.ua/public/File/2013 _nauk_an_rozrobku/kiberstrateg.pdf

4. Проект Концепції інформаційної безпеки України / Міністерство інформаційної політики України. URL: http://mip.gov.ua/documents/30.html

5. Про внесення змін до деяких законів України щодо захисту інформаційного телерадіопростору України: Закон України від 05.02.15 р. № 159-VIII. *Відомості Верховної Ради України*. 2015. № 18. Ст. 131.

6. Олійник О.В. Інформаційна безпека України: доктрина адміністративно-правового регулювання: автореф. дис. …док. юрид. наук: 12.00.07 - адміністративне право і процес; фінансове право; інформаційне право / Інститут законодавства Верховної Ради України. Київ, 2013. – 34 с.

7. Линник Г.М. Адміністративно-правове регулювання інформаційної безпеки України: автореф. дис. … канд. юрид. наук: 12.00.07 - адміністративне право і процес; фінансове право; інформаційне право / Національний університет біоресурсів і природокористування України. Київ, 2013. 27 с.

8. Ющук Е.Л. Интернет-разведка: руководство к действию. Москва-Санк-Петербург: Вершина, 2007. 249 с.

9. Толубко В.Б. Інформаційна боротьба (концептуальні, теоретичні, технологічні аспекти: монографія. Київ: НАОУ, 2003. 320 с.

10. Довгань О.Д. Сучасні інформаційні структури як компоненти інформаційної безпеки. *Інформація і право*. 2015. № 2. С. 111-120.

11. Пилипчук В.Г., Брижко В.М. Інформаційна безпека та приватність у сфері захисту персональних даних. *Інформація і право*. 2016. № 4(19). С. 60-70.

12. Брижко В. Правовий захист та безпека персональних даних: соціальний і комерційний аспекти. *Інформація і право*. № 3(26)/2018. С. 16-37.

13. Брижко В.М., Швець М.Я. е-боротьба в інформаційних війнах та інформаційне право: монографія / за ред. члена-кореспондента АПрН України, д.е.н., професора М. Швеця. Київ: НДЦПІ АПрН України, 2007 р. 236 с.

14. В Грузии приняли закон о “прослушке”. URL: http://www.inter fax.ru/world/551861

15. Кому в Грузии достанутся ключи от “прослушки”? URL: https://digital.report/ komu-v-gruzii-dostanutsya-klyuchi-ot-proslushki

16. Shaw T.J. Information security and privacy: A practical guide for global executives, law technologists. Chicago: American Bar Association. 2011. P. 17. URL: http://faculty.cbpa.drake.edu/ dmr/0101/DMR010113B.pdf

17. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року “Про Доктрину інформаційної безпеки України”: Указ Президента України № 47/2017. URL: https://www.president.gov.ua/documents/472017-21374

18. Про доступ до публічної інформації: Закон України від 13.01.11 р. № 2939-VI. URL: http://zakon3.rada.gov.ua/laws/show/2939-17

19. Конституція України: Закон України від 28.06.96 р. № 254к/96-ВР. URL: http://zakon0. rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80

20. Про захист осіб у зв’язку з автоматизованою обробкою персональних даних: Конвенція Ради Європи від 28 січня 1981 р. № 108 / офіційний переклад. засвідчено МЗС України 01.07.02 р.: у кн. *Системна інформатизація правоохоронної діяльності: європейські нормативно-правові акти та підходи до упорядкування інформаційних відносин у зв’язку з автоматизованою обробкою даних*: посіб. / В. Брижко, М. Швець та ін. Кн. 2. Київ: ТОВ “ПанТот”, 2006. 509 с. С. 66-72.

21. Про захист прав людини і основоположних свобод: Європейська Конвенція від 4 листопада 1950 року / офіційний переклад засвідчено МЗС України 27.01.06 р.: у кн. *Системна інформатизація правоохоронної діяльності: європейські нормативно-правові акти та підходи до упорядкування інформаційних відносин у зв’язку з автоматизованою обробкою даних*: посіб. / В. Брижко, М. Швець та ін. Кн. 2. Київ: ТОВ “ПанТот”, 2006. 509 с. С. 34-59.

22. Пресс-Релиз № 70/14 Суда Европейського Союза (Люксембург, 13 мая 2014 года): Решение по делу С-131/12 “Марио Костея Гонсалес против Google Spain SL, Google Inc. v

Agencia Española de Protección de Datos": (оператор Интернет-поиска несет ответственность за обработку личных данных, которые появляются на веб-страницах, опубликованных третьими лицами). URL: https://curia.europa.eu/jcms/upload/docs/application/pdf/ 2014-05/cp 140070en.pdf

23. Klass and Othersvs Germany, § 56, Series A, № 28. URL: https://www.stewartroom.co.uk/wp-content/uploads/2014/07/Cases-ECHR-Klass.pdf

24. Брижко В. Сучасні основи захисту персональних даних в європейських правових актах. *Інформація і право*. № 3(18)/2016. С. 45-57.

25. Пилипчук В.Г., Брижко В.М., Баранов О.А., Мельник К.С. Становлення і розвиток правових основ та системи захисту персональних даних в Україні: монографія / за ред. В.М. Брижка, В.Г. Пилипчука. Київ: ТОВ "Видавничий дім "АртЕк", 2017. 226 с.

26. Сучасні правові стандарти Європейського Союзу у сфері захисту персональних даних: зб. документів / переклад з англ. В. Брижко, кор. І. Майстренко / за ред. В. Брижко, передмова В. Пилипчука. / НДІ інформатики і права Національної академії правових наук України. Київ: ТОВ "Видавничий дім "АртЕк", 2018. – 180 с.

27. Актуальні проблеми інформаційної безпеки України: аналітична доповідь. *Національна безпека і оборона*. 2001. № 1. С. 2-59.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~