УДК 32.019.5

НОРМАТИВНО-ПРАВОВІ ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ БАЛАНСУ ПРАЙВЕСІ ТА ДЕРЖАВНОЇ БЕЗПЕКИ НА ПРИКЛАДІ США

Задувайло О. К.

Аспірант відділу інформаційної безпеки та розвитку інформаційного суспільства Національного інституту стратегічних досліджень.

Науковий керівник: кандидат політичних наук, старший науковий співробітник, завідувач відділу інформаційної безпеки та розвитку інформаційного суспільства Національного інституту стратегічних досліджень Дубов Д. В.

Анотація. *У статті представлено науковий огляд можливих наслідків для національної безпеки від несанкціонованого доступу та розголошення секретної інформації на прикладі США. В червні 2013 року в газетах The Washington Post і The Guardian було опубліковано інформацію про надсекретну програму американського уряду PRISM, яка є комплексом адміністративних заходів, що надають можливість для поглибленого спостереження за трафіком користувачів деяких Інтернет-ресурсів. З одного боку, це визвало обурення зі сторони громадськості та поставило під сумнів законність дій уряду. З іншого боку, уряд стверджує що такі заходи є необхідними для запобігання терористичних загроз, а розкриття секретної інформації завдало значної шкоди національній безпеці США.*

Також у статті проаналізовано внесені поправки до нормативно-правових актів, які регулюють діяльність розвідувальних спецслужб США у відповідність до вимог з національною концепцією відкритого управління.

Ключові слова: *витік інформації, національна безпека, Едвард Сноуден, Акт спостереження за іноземною розвідкою.*

Постановка проблеми. Заходи, які вживаються кожною країною світу, щоб зберегти національну безпеку в умовах можливих загроз призводять до постійної діалектичної боротьби, особливо в ліберальних демократіях, між урядом країни і цивільними правами її громадян. Вони є фундаментальною основою у процесі підтримки суверенітету держави в умовах глобалізації та збереженні прав і свобод окремої особи.

Хоча заходи національної безпеки вводяться для захисту суспільства в цілому, багато таких заходів можуть обмежувати права і свободи людей у демократичному суспільстві. Де здійснення законів і повноважень національної безпеки підлягають суворій системі стримувань і противаг, що складає ризик, де національна безпека може просто служити як привід для придушення несприятливих політичних і соціальних поглядів. Заходи, які можуть нібито прийматися в інтересах національної безпеки, такі як масове спостереження, і цензура в засобах масової інформації, у загальному підсумку може привести до антиутопії Оруелла.

Яскравим прикладом є прийнятий у Сполучених Штатах спірній Закон США Patriot та ряд інших урядових дій, які створили загрозу реалізації прав і свобод її громадянин. Серед питань, які виникають головним постає: якою мірою повинні обмежуватися права і свободи громадян заради національної безпеки держави та, як обмеження прав в інтересах національної безпеки можуть бути виправданими за умов відсутності війни.

Мета статті – дослідити нормативно-правові особливості забезпечення балансу прайвесі та захисту національних інтересів на прикладі США.

Аналіз останніх досліджень та публікацій. Концептуальні положення, пов'язані з питаннями забезпечення національної безпеки, містять наукові праці багатьох зарубіжних і вітчизняних вчених. Серед вітчизняних дослідників слід відзначити вагомий внесок у розгляд цього питання І. Бінько, В. Мунтіяна, Г. Почепцова, О. Сосніна, В. Грубова, В. Домарьова, В. Ліпкана, В. Косевцова, О. Литвиненко та інших. Серед зарубіжних вчених широку популярність здобули роботи таких дослідників, як: Г. Кіссінджер, З. Бжезинський, Л. Браун, Ч. Флавін, Х. Френч.

Важливі аспекти для аналізу відкритості політичної влади містяться в роботах Н. Бєляєвої, Т. Єрмилової, В. Міхєєва, А. Сунгурова та інших авторів, що розглядають публічність політики як необхідна умова на шляху становлення її відкритості. Однак при цьому, питання сучасної політики США щодо захисту національних інтересів в процесі забезпечення зваженого балансу між прайвесі та безпекою все ще залишаються не достатньо дослідженими.

Основні результати дослідження. В сучасних умовах розвитку системи державного управління і підвищення його ефективності будується на основі новітніх інформаційних технологій, що пропонують цілий комплекс засобів для підвищення якості діяльності органів державної влади, забезпечення прозорості та відкритості у прийнятті управлінських рішень, надання доступу громадянам і інститутам громадянського суспільства до інформації що складає суспільний інтерес.

США та європейські країни в якості стратегічних цілей розвитку механізму відкритого державного управління декларують відкритість і прозорість діяльності органів державної влади перед суспільством, та залучення своїх громадян до участі у прийняті різних політичних рішень в багатьох сферах діяльності держави, в тому числі з питань національної безпеки. В кожній демократичній країні було прийнято законодавчі акти та положення про свободу інформації, в яких закладені основні пріоритети для забезпечення публічності державної влади. Прикладом держав, в яких існують закони про доступ до (свободу) інформації, є: США (Закон про свободу інформації), Великобританія (Закон про свободу інформації), Латвія (Закон про свободу інформації), Естонія (Закон про свободу інформації), Словаччина (Закон про вільний доступ до інформації), Болгарія (Закон про доступ до публічної інформації), Словенія (Закон про доступ до публічної інформації), Угорщина (Закон про захист інформації) і т. д. На прикладі загальнодержавної концепції відкритого правління США, до таких пріоритетів відносяться:

- органи державної влади зобов'язані бути більш прозорими на кожному рівні, для цього слід надавати максимально повну інформацію про діяльність уряду і при цьому, зробити її легкодоступною для кожного охочого;
- максимально залучати своїх громадян до процесів прийняття управлінських рішень, адже завдяки цьому уряд стає більш ефективним і відповідальним;
- реалізовувати вищі стандарти чесності, тому що ті, хто знаходяться у владі, повинні служити народу, а не самим собі;
- розширювати доступ до користування сучасними технологіями, тому що в існуючому цифровому столітті доступ до інформації стає відкритим для всіх [1].

За таких умов суспільство має доступ до архівних даних, що стосуються діяльності органів державної влади, та існують ряд виключень згідно яких держава має право не надавати громадянам відомості про результати своєї роботи, в першу чергу це стосується національної безпеки, оборони і зовнішньої політики [1]. В контексті національної без-

пеки в будь якій країні розглядається питання по забезпеченню і захисту його інформаційної складової, яка включає в себе з одного боку забезпечення якісного інформування громадян та вільного доступу до різних джерел інформації, а з іншого – контроль за непоширенням таємної інформації, сприяння цілісності суспільства, захисту від негативних інформаційних впливів тощо [2]. Інформаційна політика охоплює широке коло урядових заходів: спрямованих на створення інформаційних технологій та управління ними; пов'язаних з потоками інформації; пов'язаних із впливом інформаційних технологій і потоків інформації на конкретні установи чи сферу суспільної діяльності [3].

Парадоксальним є факт, що обмеження прав необхідних для збереження свободи слова яскраво ілюструє неминучий конфлікт в будь-кому демократичному суспільстві між інтересами національної безпеки і конституційними свободами громадян країни. Залишатися захищеним від внутрішніх і зовнішніх загроз, зобов'язує націю бути здатною зберігати державні таємниці про плани національної безпеки та військові операції. Враховуючи постійний розвиток інформаційно-комунікаційні технології нарівні з проблемами надійності і стійкості їх функціонування, виникає проблема забезпечення безпеки циркулюючої у ній секретної інформації. Витік, порушення її цілісності та блокування інформації, яка становить законом таємницю, що є власністю держави – це одна з основних можливих загроз національній безпеці в інформаційній сфері [5].

Однак вимоги секретності суперечать демократичним поняттям необмеженого публічного обговорення і підзвітності уряду перед суспільством труднощі в збалансуванні національної безпеки й інтересів свободи слова посилюються у випадку витоку інформації, що відноситься до державних таємниць у сфері національної безпеки. Прийняття законопроектів, які знижують ризик можливого несанкціонованого розповсюдження секретної інформації завжди буде натикатися на гарячу критику в правових і академічних колах.

Витік секретної інформації може задовольняти демократичні інтереси, але не в тому випадку, коли суспільний інтерес від оприлюднення такої інформації не переважає потенційної шкоди від її розкриття. Витік інформації не завжди має позитивні наслідки для забезпечення національних інтересів, забезпечення прозорості і підзвітності влади, а може завдати значної шкоди зовнішній політиці та здатності держави вчасно реагувати на реальні загрози національній безпеці країни.

По-перше, у випадку оприлюднення секретної інформації подальше обговорення питань у сфері національної безпеки інститутами громадського суспільства може бути завідома помилковими та призвести до небажаних наслідків, адже інформація, яка стала загальнодоступною не завжди є достовірною і повноцінною, адже лише частково пояснює природу діяльності держави або її інтересів.

По-друге, уряд в більшості випадках не в змозі протистояти наслідкам таких розсекречень, що змушує його, або повністю оприлюднити секретну інформацію, що може нанести значної шкоди національній безпеці, та при цьому задовольнивши суспільний інтерес, або відмовитися, оперуючи вимогами закону про доступ до секретної інформації.

По-третє, та найголовніше, несанкціоновані розкриття ставлять під загрозу ефективність перебігу військових операцій, захист національних інтересів, безпеку громадян держави. На загальному рівні, витік секретної інформації погіршує здатність уряду розробляти і здійснювати політику національної безпеки, знищивши необхідну атмосферу конфіденційності та довіри. Крім того, може заподіяти шкоду інтересам співробітництва між країнами-партнерами і союзниками, та потенційно загрожує глобальній безпеці світу.

Останній гучний випадок витоку секретної інформації відбувся в 2013 році в США. Едвард Джозеф Сноуден колишній співробітник Агентства Національної Безпеки США (АНБ) та Центрального розвідувального управління (ЦРУ), скачав досі невідомий масив інформації про секретні програми стеження розвідувального відомства та передав їх для опублікування в газети The Guardian і The Washington Post. В цих матеріалах було розкрито подробиці таємних операцій АНБ, включаючи відомості про проект PRISM, а також X-Keyscore і Tempora. Спецслужби мали дозвіл на зібрання та зберігання метаданих з усіх систем електронного зв'язку, включаючи соціальні мережі Інтернету, якими користуються громадяни США і не лише. Уся ця діяльність здійснювалася з секретного дозволу таємного суду стеження за закордонною розвідкою (Foreign Intelligence Surveillance Court), що мав на меті виявляти й моніторити можливі зв'язки з терористичною діяльністю. Опубліковані документи включали також «чорний бюджет» американських розвідувальних відомств, секретні урядові схеми, що ілюстрували, як діють програми стеження АНБ, правничі меморандуми, рішення таємного суду, що становлять основу програм [6].

За даними закритої доповіді Пентагону, Е. Сноуден викрав 1,7 мільйона секретних файлів, більшість документів стосується «життєво важливих даних про військовий потенціал, про операції, тактику, техніку та методи роботи американської армії, флоту, морської піхоти і військово-повітряних сил» [7]. У зв'язку з цим, у США Е. Сноудену заочно були пред'явлені звинувачення в шпигунстві та викраденні державної власності, оголошено в міжнародний розшук [8].

За результатами національного опитування проведеного Quinnipiac University: 55% американських виборців вважають колишнього консультанта Агентства національної безпеки Е. Сноудена вважають інформатором, який виявив зловживання і віддав їх гласності, 34% – зрадником. Це продемонструвало суттєві зміни в громадській думці щодо діяльності спецслужб, за всю історію це вперше, коли американці вважають, що уряд зайшло занадто далеко в порушенні їхнього приватного життя, навіть серед прихильників АНБ [9].

Також суттєво розуміти поняття «інформатор» – це федеральний службовець, який виявив шахрайство, розтрату, зловживання, незаконність чи небезпека для здоров'я і безпеки населення і вважає, що його докази досить вагомі. В Законі про інформаторів (The Whistleblower Protection Act) йде мова про адресовані «будь-якому службовцю, який володіє повноваженнями вжити, наказати іншим зробити, рекомендувати або схвалити якунебудь дію кадрового характеру» [10]. Такий службовець не повинен «вживати або, навпаки, не вжити, погрожувати вжити або, навпаки, не почати дію кадрового характеру відносно іншого чиновника або претендента на посаду чиновника, якщо останній розкриває інформацію, яка як він обґрунтовано вважає свідчить: по-перше, про порушення закону, норми або регламенту; по-друге, про некомпетентне виконання своїх обов'язків, значну розтрату фондів, зловживання владою, істотну або особливу загрозу охороні здоров'я та громадської безпеки». Але той факт, що виток служив інтересам суспільства, виставляючи уряду незаконність і зловживання не означає, Е. Сноуден захищений законом, тому що розвідувальне співтовариство не підпадає під дію Закону захисту інформаторів [11].

Джеселін Радак адвокат з прав людини у «Проекті підзвітності уряду», яка також захищає інтереси Е. Сноудена та інших держслужбовців, які виступають із подібними викриттями, зазначає у своєму зверненні: «Згодна, що є речі, які потрібно тримати в секреті. Але ідея, що можна класифікувати незаконне поведінку, аморальна і суперечить положенню про класифікацію. Ви не можете приховати незаконні дії, класифікуючи їх як сек-

ретні, а потім звинувачувати людей, що намагаються їх викрити, у тому, що вони порушують закон. Незалежно від незначних адміністративних правопорушень, які викривачі могли вчинити, порушивши угоду про секретності, злочини уряду (шахрайство, розбазарювання коштів, зловживання і порушення законності), як у випадку Е. Сноудена, набагато переважають все, що він міг переступити». Її програма спрямована на інформаторів, які організували витік секретних урядових даних; це означає, що більша частина її роботи пов'язана зі стеженням і тортурами [12].

Інформація про діяльність американських спецслужб та уряду США гостро поставила питання про принципи демократії та свободи особистості в сучасному світі, при цьому ряд держав піддали різкій критиці програми АНБ, зазначивши, що агентство безпосередньо порушує права людини. Адміністрація президента США Барака Обами зреагувала, вперше пояснивши юридичне обґрунтування, виконання та контроль за програмами АНБ таємного стеження. Також було розсекречено і оприлюднено чимало раніше таємних урядових доповідей, судових рішень та інших документів, зокрема загальну кількість щорічних наказів про стеження для телекомунікаційних компаній [77].

Також у Вашингтона виникла необхідність внести зміні до Акту спостереження за іноземною розвідкою (FISA) з метою обмеження сфери діяльності програми PRISM і замінити масовий збір метаданих на точковий, що вимагало в свою чергу суспільство. Цей закон був прийнятий в 1978 році та визначав процедури збору інформації про американців, що підтримують контакт зі співробітниками іноземних спецслужб і членами зарубіжних неурядових організацій, діяльність яких визнана в Америці «ворожої». Згідно з вимогами FISA, спецслужби з тих пір були зобов'язані отримувати санкцію спеціально створеного суду на ведення спостереження за громадянином США протягом 72 годин після того, як цей громадянин потрапив у їх поле зору за чітко прописаними ознаками шпигунської або підривної діяльності. Невиконання спецслужбами цієї умови тягло за собою кримінальне переслідування винних у порушенні американської Конституції.

У 2001 році цей документ був доповнений Патріотичним актом США (USA Patriotic Act), у зв'язку з терористичними атаками 11 вересня та неспроможністю спецслужб ефективно боротися з ісламськими терористичними угрупованнями. Це дозволило американським спецслужбам без всяких санкцій контролювати протягом року контакти будь-якого громадянина США з іноземцями по електронних системах зв'язку, якщо виникла підозра, що він замішаний у підготовці терористичного акту. Тобто для отримання прав на стеження за особою АНБ дозволялося обходитися без санкції спеціального суду у справах FISA [13].

Наступна поправка була внесена в 2008 році – Акт захисту Америки (Protect America Act), в якому акцентували увагу на протидії організаціям, що використовують терор як засіб досягнення своїх політичних цілей [14]. Також цього року Конгрес схвалив поправки до Закону про нагляд за іноземними розвідками, який розширив можливості уряду в плані ведення тотальної електронного стеження за людьми (для потенційних розслідувань у зв'язку з тероризмом), що знаходяться за межами США, а також за тими американцями, з якими вони спілкувалися за допомогою засобів зв'язку [15].

Останні та найбільш очікуванні зміни в даному законі відбулися 1 червня 2015, по закінченню терміну, втратили силу одразу три положення Патріотичного акту, найбільш обговорюваною і суперечливою з яких є стаття 215 – «Доступ до записів та іншим даними». Згідно зі статтею, директор ФБР або уповноважена ним особа має право подати запит на будь-які дані, які допомогли б в боротьбі з тероризмом або диверсіями іноземних розвідників. Інші дві статті, стосуються конкретних випадків розслідування, а не масового збору

даних. Перша стаття 206 надавала дозвіл на постійне прослуховування передбачуваного терориста, який часто змінює засоби зв'язку – без цього положення спеціальним агентам доведеться запитувати ордер для кожного нового пристрою підозрюваного. Друга стаття 6001(а) передбачала можливість використовувати весь арсенал спецслужб для стеження за терористом-одинаком, чия зв'язок з великими угрупованнями не доведена [16].

Також конгресом було прийнято Закон про свободу, який прокладає шлях для телекомунікаційних компаній взяти на себе відповідальність за зберігання зібраних телефонних записів спецслужбами та посилити захист приватного життя, коли йдеться про дозвіл, згідно з Патріотичним актом, на здійснення програм АНБ. У розгляді справ у таємному суді, що скеровує програму розвідувального відомства, де раніше був представлений тільки уряд, відтепер братиме участь і адвокат, що захищатиме приватні права кожного підозрюваного [16].

На додаток до реєстру урядових інформаційних сайтів президент оголосив, що 16 відомств розвідувального співтовариства США запускають власний сайт «IC on the Record» [17]. Який був створений для того, щоб швидко і оперативно надавати прямий доступ до фактичної інформації, пов'язаної із законними формами стеження, якими користуються розвідувальні співтовариства США.

Президент підписав ухвалений конгресом Закон про інформаторів (Whistle-Blower Act of 2012) разом із президентською політичною директивою, спрямованою на захист від покарання всіх державних інформаторів, однак не контрактників спецслужб [17]. Втім, адміністрація домоглася ухвалення апеляційним судом рішення, що позбавляє багатьох федеральних службовців, які обіймають посади, пов'язані з чутливими сферами національної безпеки, оскаржувати «персональні дії в їхніх відомствах», що можуть включати покарання за донесення. Адміністрація наполягла на тому, щоб урядові інформатори спочатку порушували свої проблеми у відомствах радше, аніж зі сторонніми особами, зокрема з журналістами.

Висновки. Вище сказане дозволяє зробити висновок що необхідний рівень національної безпеки держави забезпечується цілим комплексом політичних, військових, організаційних та інших заходів, які допомагають реалізувати права та інтереси держави і її суспільства. Розгляд проблем витоку інформації на прикладі США демонструє, з одного боку, подальші небажанні наслідки для реалізації національних задач поставлених перед урядом держави. З іншого, бажання держави контролювати своє населення шляхом масового прослуховування приватних телефонів та інших засобів комунікації, спираючись на боротьбу з терористичними угруповання в інтересах національної безпеки.

Створення розумного механізму захисту різних видів таємниць і встановлення рамок дій інститутів таємниць дозволить як захистити інтереси суспільства і держави, так і сприяти реалізації права громадян на отримання повноцінної та якісної інформації.

Список використаної літератури

1. The White House. The open government partnership [Електронний ресурс] / The White House – Режим доступу: https://www.whitehouse.gov/sites/default/files/docs/us_national_action_plan_6p.pdf.
2. U. S. Department of State Freedom of Information Act // [Електронний ресурс] – Режим доступу: http://foia.state.gov.
3. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. – М. : Академический Проект; Фонд «Мир», 2003. – 640 с.

4. О. В. Олійник / Інформаційна безпека США / Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2012. – Вип. 1. – С. 280-288. – Режим доступу: http://nbuv.gov.ua/j-pdf/boz_2012_1_33.pdf.
5. А. В. Олійник, В. М. Шацька – Навчальний посібник – Львів: «Новий Світ-2000», 2006. – 436 с.
6. Leak investigations and surveillance in post-9/11 America [Електронний ресурс]. – Режим доступу: https://www.cpj.org/reports/2013/10/obama-and-the-press-us-leaks-surveillance-post-911.php.
7. Pentagon report: scope of intelligence compromised by Snowden 'staggering' [Електронний ресурс]. – Режим доступу: http://www.theguardian.com/world/2014/may/22/pentagon-report-snowden-leaks-national-security.
8. U.S. vs. Edward J. Snowden criminal complaint [Електронний ресурс] – Режим доступу: http://apps.washingtonpost.com/g/documents/world/us-vs-edward-j-snowden-criminal-complaint/496.
9. Quinnipiac University National Poll. August 1, 2013 – Snowden Is Whistle-Blower, Not Traitor, U.S. Voters [Електронний ресурс] / Quinnipiac University National Poll – Режим доступу: http://www.quinnipiac.edu/news-and-events/quinnipiac-university-poll/national/release-detail?ReleaseID=1930.
10. Banisar D. Whistleblowing. International Standards and Developments // Corruption and Transparency: Debating the Frontiers between State, Market and Society, I. Sandoval, ed., World Bank-Institute for Social Research, UNAM, Washington, D.C. 2011. – P. 3.
11. Michael German, Senior Policy Counsel, ACLU Washington Legislative Office. Edward Snowden is a Whistleblower [Електронний ресурс] / By Michael German, Senior Policy Counsel, ACLU Washington Legislative Office – Режим доступу: https://www.aclu.org/blog/edward-snowden-whistleblower.
12. Whistle-Blower: Protection Act Doesn't Cover Enough People [Електронний ресурс]. – Режим доступу: http://www.npr.org/2013/08/01/207987822/whistleblower-protection-act-doesnt-cover-enough-people.
13. This Is What Section 215 of the Patriot Act Does [Електронний ресурс] – Режим доступу: http://www.slate.com/blogs/weigel/2013/06/07/nsa_prism_scandal_what_patriot_act_section_215_does.html.
14. Protect America Act [Електронний ресурс] – Режим доступу: https://www.govtrack.us/congress/bills/110/s1927/text.
15. Joe Mullin, «Supreme Court kills activists» challenge to FISA spying law [Електронний ресурс] – Режим доступу: http://arstechnica.com/tech-policy/2013/02/supreme-court-kills-activists-challenge-to-fisa-spying-law.
16. Amendments to the Foreign Intelligence Surveillance Act (FISA) Extended Until June 1, 2015 [Електронний ресурс] – Режим доступу: https://www.fas.org/sgp/crs/intel/R40138.pdf.
17. Office of the Director of National Intelligence [Електронний ресурс] – Режим доступу: http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.
18. The Whistleblower Protection Enhancement Act of 2012 [Електронний ресурс] – Режим доступу: http://www.state.gov/s/ocr/205593.htm.

REGULATORY FEATURES OF BALANCE OF THE PRIVACY AND STATE SECURITY IN THE EXAMPLE OF THE USA

Zaduvailo O. K.

PhD student at the National Institute for Strategic Studies.
Supervisor: Ph.D. in political science, senior scientific officer Head of Department of information security and the development of the information society The National Institute for Strategic Studies Dubov D. V.

Abstract. *The article presents scientific review of possible implications for national security from unauthorized access and disclosure of classified information by the example of the United States. In June 2013 in the newspapers The Washington Post and The Guardian published information about the top-secret US government program PRISM, which is a set of administrative measures that provide an opportunity for in-depth observation of traffic of some users of Internet resources. On the one hand, it has caused resentment from the side of the public and challenged the legitimacy of the government. On the other, the Government asserts that such measures are necessary to prevent terrorist threats, and the disclosure of information caused irreparable harm to the national security of the United States.*

And also analyzed amended to the legal acts regulating the activities intelligence security services of US in compliance with the national concept of open government.

Key words: *leak, national security, Edward Snowden, the Foreign Intelligence Surveillance Act.*

Referances

1. The White House. The open government partnership [Electronic resource] / The White House – Access to the resource: https://www.whitehouse.gov/sites/default/files/docs/us_national_action_plan_6p.pdf.
2. US Department of State Freedom of Information Act // http://foia.state.gov/ [Electronic resource] – Access to the resource: http://foia.state.gov.
3. Yarochkyn V. I. Ynformatsyonnaya Safety: Textbook for high schools students. – M . : Academic Project; Foundation «Myr», 2003. – 640 p.
4. A. V. Oleynik / Information Security USA / Fighting organized crime and corruption (theory and practice). – 2012. – Vol. 1. – P. 280-288. – Access: http://nbuv.gov.ua/j-pdf/boz_2012_1_33.pdf.
5. A. V. Oliynyk, V. M. Shatska – Tutorial – Lviv: «Nonyi Svit-2000», 2006. – 436 p.
6. Leak investigations and surveillance in post-9/11 America [Electronic resource] – Access to the resource: https://www.cpj.org/reports/2013/10/obama-and-the-press-us-leaks -surveillance-post-911.php.
7. Pentagon report: scope of intelligence compromised by Snowden ‘staggering’ [Electronic resource] – Access to the resource: http://www.theguardian.com/world/2014/may/22/pentagon-report-snowden-leaks- national-security.
8. U.S. vs. Edward J. Snowden criminal complaint [ELECTRONIC RESOURCE] – Access to the resource: ttp://apps.washingtonpost.com/g/documents/world/us-vs-edward-j-snowden-criminal-complaint/496/.
9. Quinnipiac University National Poll. August 1, 2013 – Snowden Is Whistle-Blower, Not Traitor, US Voters [Electronic resource] / Quinnipiac University National Poll – Access to the website: http://www.quinnipiac.edu/news-and-events/quinnipiac-university-poll/national/release-detail?ReleaseID=1930.
10. Banisar D. Whistleblowing. International Standards and Developments // Corruption and Transparency: Debating the Frontiers between State, Market and Society, I. Sandoval, ed. – World Bank-Institute for Social Research, UNAM, Washington, DC 2011. P. 3.
11. Michael German, Senior Policy Counsel, ACLU Washington Legislative Office. Edward Snowden is a Whistleblower [Electronic resource] / By Michael German, Senior Policy Counsel, ACLU Washington Legislative Office - Access to the resource: https://www.aclu.org/blog/edward-snowden-whistleblower.
12. Whistle-Blower: Protection Act Does not Cover Enough People [Electronic resource] – Access to the resource: http://www.npr.org/2013/08/01/207987822/whistleblower-protection-act-doesnt- cover-enough-people.
13. This Is What Section 215 of the Patriot Act Does [Electronic resource] – Access to the website: http://www.slate.com/blogs/weigel/2013/06/07/nsa_prism_scandal_what_patriot_act_section_215_does.html.
14. Protect America Act [Electronic resource] – Access to the resource: https://www.govtrack.us/congress/bills/110/s1927/text.
15. Joe Mullin, «Supreme Court kills activists» challenge to FISA spying law [Electronic resource] – Access to the website: http://arstechnica.com/tech-policy/2013/02/supreme-court-kills-activists-challenge-to-fisa-spying-law/.

16. Amendments to the Foreign Intelligence Surveillance Act (FISA) Extended Until June 1, 2015 [Electronic resource] – Access to the resource: https://www.fas.org/sgp/crs/intel/R40138.pdf.
17. Office of the Director of National Intelligence [Electronic resource] – Access to the resource: http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.
18. The Whistleblower Protection Enhancement Act of 2012 [Electronic resource] – Access to the resource: http://www.state.gov/s/ocr/205593.htm.

НОРМАТИВНО-ПРАВОВЫЕ ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ БАЛАНСА ПРАЙВЕСИ И ГОСУДАРСТВЕННОЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ США

Задувайло О. К.

Аспирант отдела информационной безопасности и развития информационного общества Национально института стратегических исследований.

Научный руководитель: кандидат политических наук, старший научный сотрудник, заведующий отделом информационной безопасности и развития информационного общества Национального института стратегических исследований Дубов Д. В.

Аннотация. *В статье представлены научный обзор возможных последствий для национальной безопасности от несанкционированного доступа и разглашения секретной информации на примере США. В июне 2013 года в газетах The Washington Post и The Guardian была опубликована информация о секретной программе американского правительства PRISM, которая представляет собой комплекс административных мер, которые дают возможность для углубленного наблюдения за трафиком пользователей некоторых Интернет-ресурсов. С одной стороны, это вызвало критику со стороны общественности и поставило под сомнение законность действий правительства. С другой стороны, правительство утверждает, что такие меры необходимы для предотвращения террористических угроз, а раскрытие такого рода секретной информации нанесло непоправимый ущерб национальной безопасности США.*

Также в статье проанализировано внесенные поправки в нормативно-правовые акты, регулирующие деятельность разведывательных спецслужб США в соответствии с требованиями национальной концепции открытого управления.

Ключевые слова: *утечка информации, национальная безопасность, Эдвард Сноуден, Акт наблюдения за иностранной разведкой.*