Information security of the state in the national legislation of European countries

Інформаційна безпека держави в національному законодавстві європейських країн

Taras Tkachuk

Key words:

information security, defense of information, cybersecurity, Europe.

Ключові слова:

інформаційна безпека, безпека інформації, кібербезпека, Європа.

Постановка проблеми. Безпека особи, суспільства і держави, зокрема й інформаційна, становить складне, багаторівневе явище, яке водночас може розглядатися як процес і показник стану реалізації національних інтересів. Велике значення для ефективного функціонування національної системи гарантування інформаційної безпеки має досвід європейських країн, з огляду на національні пріоритети й ускладнену ситуацію в досліджуваній сфері у зв'язку з військовими діями на Сході нашої держави.

Стан дослідження. Питання гарантування інформаційної безпеки України досліджувалися в наукових працях таких вітчизняних і закордонних авторів, як: А. Гальчинський, О. Голобуцький, Я. Жаліло, О. Зощенко, Р. Калюжний, А. Колодюк, Б. Кормич, В. Ліпкан, А. Марущак, Н. Марчук, С. Чукут та інші.

Постановка завдання. Метою статті є вивчення досвіду окремих європейських країн із гарантування інформаційної безпеки держави та розроблення на цій основі відповідних пропозицій для коригування національної політики.

Виклад основного матеріалу. Активну політику у сфері гарантування інформаційної безпеки проводить не лише НАТО, але й Європейський Союз (далі – ЄС), який сьогодні об'єднує високо розвинуті країни, що відчутно впливають на міжнародні відносини, встановлюючи норми і стандарти поведінки держав у політичній, економічній, соціальній, інформаційній та інших сферах.

Ще 1991 р. країнами Європи розроблено «Європейські критерії безпеки інформаційних технологій»[1], якими, зокрема, визначені завдання досягнення інформаційної безпеки: захист інформаційних ресурсів від несанкціонованого доступу з метою забезпечення конфіденційності; забезпечення цілісності інформаційних ресурсів шляхом їх захисту від несанкціонованої модифікації або знищення; забезпечення працездатності систем за допомогою протидії загрозам відмови в обслуговуванні. 1996 р. стандарти європейської інформаційної безпеки втілено в «Єдиних критеріях безпеки інформаційних технологій»[2], згідно з якими для характеристики основних критеріїв інформаційної безпеки застосовується модель тріади CIA (CIA Triad), яка передбачає три основні характеристики інформаційної безпеки: конфіденційність, цілісність і доступність[3].

2001 р. Європейською комісією було представлено документ «Мережева та інформаційна безпека: європейський політичний підхід», в якому окреслено сучасний підхід ЄС до проблеми інформаційної безпеки. У документі вживається термін «мережева та інформаційна безпека», який трактується як здатність мережі або інформаційної системи чинити опір випадковим подіям або зловмисним діям, які становлять загрозу доступності, автентичності, цілісності та конфіденційності даних, що зберігаються або передають-

[1] Information Tecnhology Security Evaluation Criteria. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ Zertifizierung/ITS icherheitskriterien/itsec-en_pdf.pdf.

[2] Common Criteria for Information Technology Security Evaluation. URL: https://www.commoncriteriaportal.org/files/ccfiles/CCPART 2V3.1R4.pdf.

[3] Нестеряк Ю. Міжнародні критерії інформаційної безпеки держави: теоретико-методологічний аналіз. URL: http://visnyk.academy.gov.ua/wp-content/uploads/2014/02/2013-3-8.pdf.

ся, а також послуг, що надаються через ці мережі і системи[4]. Документ визначає такі основні напрями європейської політики інформаційної безпеки: підвищення обізнаності користувачів щодо можливих загроз під час користування комунікаційними мережами; створення європейської системи попередження й інформування про нові загрози; забезпечення технологічної підтримки; підтримка ринково орієнтованої стандартизації та сертифікації; правове забезпечення, пріоритетами якого є захист персональних даних, регламентація телекомунікаційних послуг ы протидія кіберзлочинності; зміцнення інформаційної безпеки на державному рівні шляхом впровадження ефективних і сумісних засобів гарантування інформаційної безпеки та заохочення використання країнами-членами електронних підписів під час надання державних онлайн-послуг тощо; розвиток міжнародного співробітництва з питань інформаційної безпеки.

У країнах ЄС значна увага приділяється також проблемі кібербезпеки. З 1999 р. ЄС реалізує програми «Безпечніший Інтернет» ("Safer Internet"), у межах яких здійснюються заходи, спрямовані на боротьбу не лише зі шкідливим контентом, але й з небезпечною поведінкою в мережі[5]. 2007 р. Європейською комісією представлено документ «На шляху до загальної політики у сфері боротьби з кіберзлочинністю», в якому кіберзлочинність визначається як кримінальні дії, вчинені з використанням електронних комунікаційних мереж та інформаційних систем або проти таких мереж і систем, і охоплює: традиційні форми злочину (шахрайство та підробки в електронних комунікаційних мережах та інформаційних системах); публікацію незаконного контенту в електронних медіа; специфічні злочини в електронних мережах (атаки на інформаційні системи, хакерство тощо)[6]. 2009 р. опубліковано Повідомлення Європейської комісії «Захист Європи від широкомасштабних кібератак та руйнувань: посилення рівня підготовленості, безпеки та стійкості», в якому визначено основні виклики/проблеми, які потребують негайного реагування з боку країн ЄС, а також окреслено основні заходи, необхідні для посилення безпеки та здатності європейської критичної інформаційної інфраструктури протистояти зовнішнім впливам[7]. Згідно із цим документом, основними викликами безпеці інформаційних інфраструктур країн ЄС є некоординовані національні підходи до безпеки інформаційних інфраструктур, що знижує ефективність національних заходів; відсутність на європейському рівні партнерства між державним і приватним секторами; обмежені можливості щодо раннього попередження та реагування на безпекові інциденти, зумовлені нерівномірністю розвитку систем моніторингу і сповіщення про інциденти в країнах-членах, нерозвиненістю міждержавного співробітництва й обміну інформацією щодо цих проблем; відсутність міжнародного консенсусу щодо пріоритетів у реалізації політики захисту критичної інформаційної інфраструктури.

Основоположною тезою для країн-членів ЄС у сфері інформаційної відкритості органів державної влади є така: «Загальновизнано, що демократична система може функціонувати найбільш ефективно лише тоді, коли громадськість повністю поінформована»[8]. Водночас у рекомендації Ради Європи № R(81)19 «Про доступ до інформації, яка знаходиться в розпорядженні державних органів» зазначено, що для адекватної участі всіх у суспільному житті необхідно забезпечити, з урахуванням неминучих винятків і обмежень, доступ громадськості до інформації, що перебуває в розпорядженні державних органів усіх рівнів[9]. Отже, європейські стандарти інформаційної діяльності органів державної влади передбачають їхню максимальну інформаційну відкритість за винятком обмежень, пов'язаних із дотриманням конфіденційності інформації з обмеженим доступом. Передусім це стосується безпеки персональних даних.

Зокрема, у резолюції Генеральної Асамблеї Організації Об'єднаних Націй (далі – ООН) «Право на приватність у цифрову епоху» від 18 грудня 2013 р. підкреслено глобальну і відкриту природу Інтернету і швидкий розвиток у сфері інформаційних і комунікаційних технологій як рушійної сили для прискорення прогресу на шляху до розвитку в різних формах. У документі підтверджено, що «ті ж права, що люди мають

[4] Communication from the European Commission: Network and Information Security: Proposal for a European Policy Approach. COM (2001) 298. URL: http://ec.europa.eu/information_society/eeurope/2002/ news_library/pdf_files/netsec_en.pdf.

[5] Safer Internet Programme. URL: http://ec.europa.eu/information_society/activities/sip/policy/programme/current_prog/index_en.htm.

[6] Communication from the Commission: Towards a general policy on the fight against cybercrime. COM (2007). URL: http://eurlex.europa.eu/LexUriServ/site/en/com /2007/com2007_0267en01.pdf

[7] Communication from the Commission on Critical Information Infrastructure Protection: Protecting Europe from larges cale cyberattacks and disruptions: enhancing preparedness, security and resilience. COM (2009) 149. URL: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ ciip/index_en.htm.

[8] Костенко О. Європейські стандарти правового регулювання обігу інформації з обмеженим доступом у роботі органів прокуратури. Науковий вісник Ужгородського національного університету. Серія «Право». Випуск 34. Том 3. 2015. С. 109–114.

[9] Про доступ до інформації, яка знаходиться в розпорядженні державних органів: рекомендації Ради Європи № R (81)19. URL: http://medialaw.org.ua/library/rekomendatsiya-r-81-19-pro-dostup-do-informatsiyi-shho-znahodytsya-u-rozporyadzhenni-derzhavnyh-organiv.

в оффлайн-режимі також повинні бути захищені онлайн, у тому числі право на приватність»[10]. Засади захисту персональних даних у правовій практиці країн ЄС зводяться до такого: пріоритетним є право особи розпоряджатися своїми персональними даними, а їх використання без дозволу володільця призводить до відповідальності згідно із законодавством; для будь-кого, хто здійснює користування персональними даними фізичних осіб з їхнього дозволу, встановлено відповідальність у разі умисного розголошення цих даних третім особам (крім випадків, коли на це надано дозвіл)[11].

Отже, варто констатувати, що країни ЄС мають «у певному сенсі злагоджену систему захисту інформації», але водночас кожна країна має свої закони, положення, інструкції щодо врегулювання питань інформаційної безпеки. Зокрема, для законодавства Німеччини характерне детальне розроблення системи різних видів інформації з обмеженим доступом, чіткі формулювання їх визначень у федеральному законодавстві. Так, відповідно до Закону «Про перевірку безпеки»[12], секретною інформацією є факти, вироби та відомості незалежно від форми їх представлення, які в державних інтересах повинні зберігатися в таємниці та яким наданий державним органом чи за його дорученням ступінь секретності, що відповідає необхідному рівню захисту: «цілком таємно», «таємно», «конфіденційно» чи «для службового користування». У систему секретної інформації входить державна таємниця (відомості ыз грифом «цілком таємно» і «таємно») та відомча таємниця (відомості ыз грифом «конфіденційно» і «для службового користування»), охорона яких, на відміну від інших видів таємниць, що стосуються конфіденційної сфери приватних осіб, зумовлена інтересами зовнішньої безпеки держави. Зокрема, особливо важливою та такою, що підлягає особливому захисту, вважається конфіденційна інформація про етнічне походження, політичні погляди, релігійні і філософські переконання, членство в об'єднаннях, здоров'я й статеве життя фізичних осіб.

Нарощування потенціалу для ведення кібервійн свідчить про перехід Німеччини до принципу «активної оборони», адже раніше основна увага приділялася тільки питанням гарантування безпеки інформації. Виділення наступального складника інформаційного протиборства в окрему структуру, за оцінками німецьких експертів, є адекватною відповіддю на наявні загрози інформаційній безпеці, а також підкреслює прагнення Німеччини забезпечити відповідність можливостей бундесверу сучасним реаліям.

Національна інформаційна політика Республіки Польща зорієнтована на побудову вільного відкритого суспільства, забезпечення прав людини, впровадження концепції вільного транскордонного обігу інформації, створення незалежних і плюралістичних масмедіа. Її правовим підґрунтям є ухвалені в 90-і рр. минулого століття «Закон про пошту і телекомунікації», «Закон про телебачення і радіомовлення», «Закон про державні відносини з римською католицькою церквою в Республіці Польща», в яких визначаються напрями інформаційної політики, встановлюються технологічні стандарти інформаційного зв'язку, форми залучення іноземних інвестицій (від 33% –49% іноземного капіталу), ліцензування інформаційної діяльності. Окремо визначаються права церкви на інформаційну діяльність, з огляду на значний вплив клерикальної інформації на політичні пріоритети та моральність польського суспільства[13].

На відміну від Польщі, Угорщина адаптувала до вимог НАТО чинне раніше законодавство про захист державних і офіційних секретів. Зокрема, 1995 р. Угорщина ухвалила закон про державні й офіційні секрети, який 2001 р. доповнений і виправлений, виходячи із практики Альянсу. Загалом угорська політика у сфері інформаційної безпеки налаштована переважно на впровадження обмежень. Так, закон про засоби масової інформації, ухвалений 2010 р., піддався критиці з боку світових засобів масової інформації (далі – ЗМІ) та ЄС – Угорщину звинуватили в запровадженні тотального контролю за ЗМІ, разом із Інтернетом, у ліквідації свободи слова й навіть у прагненні встановити тоталітарний режим[14].

У Хорватії із 2007 р. діє Акт про інформаційну безпеку, що визначає поняття інформаційної безпеки, її заходи й стандарти, а також сфери інформаційної безпеки та компетентні органи для ухвалення й реалізації рішень у сфері гарантування інформаційної безпеки, а також нагляду за дотриманням стандартів

[10] The right to privacy in the digital age: General Assembly Resolution, A/RES/68/167. URL: http://www.ohchr.org/EN/Issues/ DigitalAge/Pages/DigitalAgeIndex.aspx.

[11] Размєтаєва Ю. Приватність в інформаційному суспільстві: проблеми правового розуміння та реегулювання. Науковий вісник Ужгородського національного університету. Серія «Право». Випуск 37. Том 1. 2016. С.44

[12] Gesetzüber die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen (Sicherheitsüberprüfungsgesetz – SÜG. URL: http://www. gesetze-im-internet.de/s_g/BJNR086700994.html.

[13] Chappell Laura, Palgrave Macmillan. Germany, Poland and the Common Security and Defence Policy: Converging Security and Defence Perspectives in an Enlarged EU. 29 august 2012. P. 61–67.

[14] Затинайко О., Павленко В., Бочарніков В., Свєшніков С. Політика безпеки і воєнно-політичні відносини Угорщини. Наука і оборона. 2014. № 1. С. 11.

інформаційної безпеки. Зокрема, інформаційна безпека визначена як стан конфіденційності, цілісності й доступності інформації, що досягається шляхом реалізації політики заходів і стандартів і організаційної підтримки робочих місць, планування, реалізації, оцінки й відновлення заходів і стандартів. Крім того, 2015 р. в Хорватії ухвалено Національну стратегію кібербезпеки[15].

Варто зазначити, що досягнення інформаційної безпеки, зокрема й шляхом активних інформаційних операцій, наприкінці минулого століття стало важливим компонентом боротьби Хорватії за свої тимчасово окуповані території, на яких понад чотири роки існувала сепаратистська «Республіка Сербська країна». За оцінками експертів, якщо в мілітарному значенні боротьба за повернення вказаних територій закінчилася в серпні 1995 р. під час операції «Буря», у дипломатичному – на початку 1998 р., водночас із мирною реінтеграцією хорватського Подунав'я, то в інформаційному сенсі війна закінчилася лише через 15 років зі дня закінчення бойових дій[16] [17], і запорукою перемоги в цій інформаційній війні була постійна боротьба за «вуха, очі та розум» населення окупованих територій, а також протидія інформаційній агресії супротивника.

В Австрії, Фінляндії та Ірландії, як і в інших країнах ЄС, значна увага приділяється проблемам кібербезпеки, висвітленим у документі Європейської комісії «На шляху до загальної політики у сфері боротьби з кіберзлочинністю», в якому кіберзлочинність визначається як кримінальні дії, вчинені з використанням електронних комунікаційних мереж та інформаційних систем або проти таких мереж і систем, і охоплює: традиційні форми злочину (шахрайство та підроблення в електронних комунікаційних мережах та інформаційних системах); публікацію незаконного контенту в електронних медіа; специфічні злочини в електронних мережах (атаки на інформаційні системи, хакерство тощо).

Стратегія національної безпеки Фінляндії передбачає, що критична інфраструктура країни стає все більше залежною від інформаційних систем і мереж, тому мінімізація відповідних ризиків має стати завданням гарантування всеосяжної безпеки. Концепція всеосяжної безпеки, окрім традиційного сценарію протидії військовим загрозам, охоплює також інші проблеми на кшталт зміни клімату, дефіциту енергетичних і водних ресурсів, міграції, тероризму, торгівлі наркотиками, кібератак тощо[17].

Стратегія кібербезпеки Фінляндії, затверджена 2013 р., наголошує на тому, що загрози, які виходять із кіберпростору, стають все більш серйозними, адже кібератаки можуть використовуватися як засіб політичного й економічного тиску, зокрема й поряд із традиційними засобами військової сили. Водночас кіберпростір є джерелом величезного потенціалу та ресурсів, адже він збільшує можливості розвитку бізнесу, працевлаштування та залучення іноземних інвесторів. Стратегія також визначає, що Фінляндія як невелика й відкрита до співробітництва країна, має «гарні шанси піднятися до авангарду кібербезпеки», тоді як бачення кібербезпеки полягає в такому: Фінляндія може забезпечити свої життєво важливі функції і протистояти кіберзагрозам у всіх ситуаціях; громадяни, органи влади й юридичні особи можуть ефективно використовувати безпечний кіберпростір, що виникає в результаті заходів кібербезпеки, здійснюваних на національному й міжнародному рівнях; до 2016 р. Фінляндія має стати провісником повної готовності до протидії кіберзагрозам і управління порушеннями, що викликані цими загрозами. Якщо розслідування кіберінцидентів здійснює поліція, то організація всеосяжного кіберзахисту покладається на Сили оборони Фінляндії під керівництвом Міністерства оборони. Можливості військового кіберзахисту передбачають розвідку, а також кібератаку та ведення кібервійн, однак основним елементом військової сили в кіберпросторі є інтелектуальне попередження загроз. Зауважимо, що 2015 р. Міністерство внутрішніх справ Фінляндії виступило з ініціативою оновлення закону про розвідувальну діяльність ss метою надання поліції і військовим права на розвідку в інформаційних мережах[18].

Програми становлення інформаційного суспільства Австрійської Республіки втілюють політичну стратегію об'єднання Європи на базі новітніх технологій, інформаційно-комунікаційної інфраструктури й інтелектуального потенціалу регіону. На інформаційну політику Австрії суттєво впливають міжнародні організації, резиденції яких розміщені у Відні, і складником програм діяльності яких є розвиток інформаційного суспільства.

---

[15] The national cybersecurity strategy of the republic. URL: http://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf/

[16] Хорватія повернула свої території за три дні, а інформаційна війна тривала ще 15 років. URL: http://milnavigator.com.ua/.

[17] Finland's Cyber Security Strategy (2013). URL: http://www.yhteiskunnanturvallisuus.fi/en/materials/doc_download/40-finlandas-cyber-security-strategy.

[18] Орпо: надо как можно скорее разрешить сетевую разведку. URL: http://yle.fi/novosti/novosti/article8459992.html.

Ірландію, де розташовані великі європейські офіси таких компаній, як "Google" і "Facebook", часто називають європейською Кремнієвою долиною, оскільки ця країна докладає багато зусиль для підготовки та працевлаштування IT-фахівців. 2013 р. компанія "Microsoft" інвестувала 170 мільйонів євро у створення та розвиток європейського дата-центру в Ірландії. Ця ініціатива була підтримана місцевою владою, адже Ірландія прагне стати європейським лідером у сфері оброблення big data, а її кліматичні умови підходять для підтримки необхідної температури роботи серверів. Також у Дубліні має з'явитися тренінговий центр, що в тісному співробітництві з урядом Ірландії та навчальними закладами проводитиме навчання в таких перспективних галузях, як захист критичної інфраструктури й кібербезпека транспорту.

Національна стратегія кібербезпеки Ірландії на 2015–2017 рр. передбачає, що уряд Ірландії всіляко сприятиме стійкій і безпечній експлуатації комп'ютерних мереж і відповідної інфраструктури ірландськими громадянами й підприємствами.

Висновки. Для України як держави, що зіткнулася із проблемами втягнення в гібридну війну та тимчасово окупованих територій, не зайвим буде досвід країн Центральної Європи щодо гарантування інформаційної безпеки, зокрема Хорватії, протидія сепаратизму в якій закінчилася успішною реінтеграцією самопроголошеної «республіки». Отже, наразі нам варто брати на озброєння передові методи протидії російській інформаційній агресії, треба постійно представляти якісний інформаційний продукт на тимчасово окупованих територіях. Доцільним буде також наслідувати досвід Німеччини в переході до принципу «активної оборони» щодо інформаційної безпеки, адже остання держави становить постійний процес діяльності компетентних органів, спрямований на попередження, протидію загрозам в інформаційній сфері, а також застосування активних заходів інформаційного впливу і сукупність умов такої діяльності, які реалізуються й здатні контролюватися тривалий час.

Анотація

Стаття присвячена дослідженню питань гарантування інформаційної безпеки в країнах Європи. Під час дослідження визначаються пріоритети та проблеми гарантування інформаційної безпеки в зазначених країнах. Також оцінюється значущість досвіду країн Європи у сфері гарантування інформаційної безпеки для України.

Summary

The article is devoted to the research of the information security subject in the countries of Europe. The study identifies priorities and problems of ensuring information security in these countries. The importance of the experience of European countries in the field of information security for Ukraine is also assessed.

Використана література:

1. Information Tecnhology Security Evaluation Criteria. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITS icherheitskriterien/itsec-en_pdf.pdf.
2. Common Criteria for Information Technology Security Evaluation. URL: https://www.commoncriteriaportal.org/files/ccfiles/CCPART 2V3.1R4.pdf.
3. Нестеряк Ю. Міжнародні критерії інформаційної безпеки держави: теоретико-методологічний аналіз. URL: http://visnyk.academy.gov.ua/wp-content/uploads/2014/02/2013-3-8.pdf.
4. Communication from the European Commission: Network and Information Security: Proposal for a European Policy Approach. COM (2001) 298. URL: http://ec.europa.eu/information_society/eeurope/2002/ news_library/pdf_files/netsec_en.pdf.
5. Safer Internet Programme. URL: http://ec.europa.eu/ information_society/activities/sip/policy/programme/current_prog/index_en.htm.

6. Communication from the Commission: Towards a general policy on the fight against cybercrime. COM (2007). URL: http://eurlex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf.
7. Communication from the Commission on Critical Information Infrastructure Protection: Protecting Europe from large scale cyberattacks and disruptions: enhancing preparedness, security and resilience. COM (2009) 149. URL: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ ciip/index_en.htm.
8. Костенко О. Європейські стандарти правового регулювання обігу інформації з обмеженим доступом у роботі органів прокуратури. Науковий вісник Ужгородського національного університету. Серія «Право». Випуск 34. Том 3. 2015. С. 109–114.
9. Про доступ до інформації, яка знаходиться в розпорядженні державних органів: рекомендації Ради Європи № R (81)19. URL: http://medialaw.org.ua/library/rekomendatsiya-r-81-19-pro-dostup-do-informatsiyi-shho-znahodytsya-u-rozporyadzhenni-derzhavnyh-organiv.
10. The right to privacy in the digitalage: General Assembly Resolution A/RES/68/167. URL: http://www.ohchr.org/EN/Issues/ DigitalAge/Pages/DigitalAgeIndex.aspx.
11. Размєтаєва Ю. Приватність в інформаційному суспільстві: проблеми правового розуміння та реегулювання. Науковий вісник Ужгородського національного університету. Серія «Право». Випуск 37. Том 1. 2016. С. 43–46.
12. Gesetzüber die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen (Sicherheitsüberprüfungsgesetz – SÜG. URL: http://www. gesetze -im-internet.de/s_g/BJNR086700994.html.
13. Chappell Laura, Palgrave Macmillan. Germany, Poland and the Common Security and Defence Policy: Converging Security and Defence Perspectives in an Enlarged EU. 29 august 2012. 232 p.
14. Затинайко О., Павленко В., Бочарніков В., Свєшніков С. Політика безпеки і воєнно-політичні відносини Угорщини. Наука і оборона. 2014. № 1. С. 9–18.
15. The national cybersecurity strategy of the republic. URL: http://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf.
16. Хорватія повернула свої території за три дні, а інформаційна війна тривала ще 15 років. URL: http://milnavigator.com.ua/.
17. Communication from the Commission: Towards a general policy on the fight against cyber crime. COM (2007). URL: http://eurlex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf.
18. Орпо: надо как можно скорее разрешить сетевую разведку. URL: http://yle.fi/novosti/novosti/article8459992.html.

Taras Tkachuk,
Ph. D., Associate Professor
of Institute of Information security