ISSN: 2418-4209 (printed), 2418-4217 (online)

EUROPEAN REFORMS BULLETIN 2017 No4

Indexed & Shared by:

Academic Resource Index ResearchBib

AcademicKeys UNLOCKING ACADEMIC CAREERS

ISSN: 2418-4209 (printed), 2418-4217 (online)

European Reforms Bulletin

2017

scientific peer-reviewed journal No. 4

Founded and edited by Centre for European Reforms Studies, a.s.b.l. Grand Duchy of Luxembourg (Registre de commerce et des sociétés, Luxembourg, F 10.340, siège social: L-1541 Luxembourg, 36, boulevard de la Fraternité).

Tel.: +352661261668

e-mail: bulletin@email.lu

http://cers.eu.pn/bulletin.html

European Reforms Bulletin is an international, multilingual (English, Ukrainian, Russian), scholarly, peer-reviewed journal, which aims to publish the highest quality research material, both practical and theoretical, and appeal to a wide audience. It is an official bulletin of the Centre for European Reforms Studies and is published 4 times a year (quarterly). It includes articles related to legal and economic issues of reforms in European Union and Europe-oriented countries, including efficiency and experience of these reforms, comparative studies on all disciplines of law, cross-disciplinary legal and economic studies, and also educational issues. It welcomes manuscripts from all over the world, in particular from countries which made European choice recently. It accepts articles from professional academics, researchers, experts, practitioners and PhD students.

Responsibility for the accuracy of bibliographic citations, quotations, data, facts, private names, enterprises, organizations, institutions and government bodies titles, geographical locations etc. lies entirely with authors. All the articles are published in author's edition. Authors must accept full responsibility for the factual accuracy of the data presented and should obtain any authorization necessary for publication. The editorial board and the Centre for European Reforms Studies do not always share the views and thoughts expressed in the articles.

The editorial board reserves the right to refuse any material for publication and advises that authors should retain copies of submitted manuscripts and correspondence as material cannot be returned. Final decision about acceptance or rejection rests with the editor-in-chief and editorial board. By submitting an article for publication author declares that the submitted work is original and not being considered elsewhere for publication and has not been published before.

Recommended for publication by the Centre for European Reforms Studies (protocol of the general meeting No. 12 24.08.2017)

Table of contents

Educational and scientific establishment of the National police in ensuring cyber security strategy of Ukraine: the fundamental legal aspects

K.Yu. Ismaylov
Odessa State University of Internal Affairs, Ukraine
e-mail: 0997060070@ukr.net

Abstract: The article is devoted to determining the role of the scientific and educational institutions of the National police of Ukraine in implementation of national cybersecurity strategy and information security. Outlines the main directions of research and professional development protection of information space of the state and the information society.

Keywords: cybersecurity, information security, educational and scientific institutions of the police, information society.

Розвиток та безпека кіберпростору, запровадження електронного урядування, гарантування безпеки й сталого функціонування електронних комунікацій та державних електронних інформаційних ресурсів мають бути складовими державної політики у сфері розвитку інформаційного простору та становлення інформаційного суспільства в Україні.

Сьогодні стрімкий розвиток інформаційних технологій поступово трансформує світ. Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади і активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади, сприяє запобіганню корупції. Однак, переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб.

Поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення, персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет. Кіберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства і держави.

Актуальність питання кібербезпеки в теоретико-правовому плані обумовлена також тим, що агресія Російської Федерації, що триває, інші докорінні зміни у зовнішньому та внутрішньому безпековому середовищі України вимагають невідкладного створення національної системи кібербезпеки як складової системи забезпечення національної безпеки України. В свою чергу, перед науковим юридичним співтовариством постає завдання у відпрацюванні правових принципів, термінології та механізмів, що будуть сприяти втіленню в життя концептуальних положень кібербезпеки, що відпрацьовуються державно-владними інститутами.

Значну роль в цьому процесі мають відігравати і навчально-наукові установи в системі Національної поліції України, що зусиллями своїх співробітників, професорсько-викладацького складу мають сприяти створенню як фундаментально-правових, так і практично-юридичних основ для підготовки спеціалістів правоохоронної сфери, які залучаються до реалізації кібербезпеки України.

Метою даного дослідження є спроба виявлення найбільш суттєвих питань, що стосуються ролі навчально-наукових установ Національної поліції України в забезпеченні стратегії кібербезпеки держави.

Джерельною основою роботи є аналітично-науковий матеріал юридичного спрямування, нормативно-правові акти держави у сфері кібербезпеки та інформаційного обороту, енциклопедичні дані та науково-дослідні публікації вчених в інформаційно-правовій сфері.

Методологічну основу роботи складає сукупність прийомів і методів філософської і матеріалістичної діалектики, логіко-структурний підхід та прийоми хронологічного виявлення походження категорій і понять в сфері інформаційної безпеки та кіберзахисту.

15 березня 2016 року Указом Президента України № 96/2016 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» означена Стратегія була затверджена, а відповідне рішення РНБО введене в дію.

Відповідно до положень означеної Стратегії забезпечення кібербезпеки України як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів, має базуватися на принципах:

– верховенства права і поваги до прав та свобод людини і громадянина;

– забезпечення національних інтересів України;

– відкритості, доступності, стабільності та захищеності кіберпростору;

– державно-приватного партнерства, широкої співпраці з громадянським суспільством у сфері забезпечення кібербезпеки та кіберзахисту;

– пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам;

– пріоритетності запобіжних заходів;

– невідворотності покарання за вчинення кіберзлочинів;

– пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу;

– міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в протиправних та воєнних цілях;

– забезпечення демократичного цивільного контролю над утвореними відповідно до законів України військовими формуваннями та правоохоронними органами держави, що діють у сфері кібербезпеки [1].

Тут важливо виходити з базового розуміння категорії кібербезпеки. Кібербезпека (комп'ютерна безпека) – це сукупність проблем у галузі телекомунікацій та інформатики, пов'язаних з оцінкою і контролюванням ризиків, що виникають при користуванні комп'ютерами та комп'ютерними мережами і розглядуваних з точки зору конфіденційності, цілісності і доступності. Створення безпечних комп'ютерних систем і додатків є метою діяльності мережевих інженерів і програмістів, а також предметом теоретичного дослідження як у галузі телекомунікацій та інформатики, так і економіки, правознавства, психології та політології. У зв'язку із складністю і трудомісткістю більшості процесів і методів захисту цифрового обладнання, інформації та комп'ютерних систем від ненавмисного чи несанкціонованого доступу вразливості комп'ютерних систем становлять значну проблему для їхніх користувачів [2].

Згідно із загальноприйнятим визначенням, безпечна комп'ютерна інформаційна система — це ідеальна система, яка коректно і у повному обсязі реалізує ті і лише ті цілі, що відповідають намірам її власника [3]. На практиці побудувати складну систему, що задовольняє цьому принципові, неможливо, і не лише з огляду на ймовірність виникнення несправностей і помилок, але й через складність визначення і формулювання часто-густо суперечливих очікувань проектувальника системи, програміста, законного власника системи, власника даних, що обробляються, та кінцевого користувача. Навіть після їхнього визначення у багатьох випадках важко або й неможливо з'ясувати, чи функціонує програма у відповідності із сформульованими вимогами. У зв'язку з цим забезпечення безпеки зводиться найчастіше до управління ризиком: визначення потенційних загроз, оцінка ймовірності їхнього настання та оцінка потенційної шкоди, із наступним ужиттям запобіжних заходів в обсязі, що враховує технічні можливості й економічні обставини.

Під час російсько-української війни, що розпочалась з анексії Криму в 2014 році, інформаційно-обчислювальні системи України ставали об'єктами атак з боку Росії. Так, наприклад, 23 грудня 2015 року російським зловмисникам вдалось успішно атакувати комп'ютерні системи управління в диспетчерській «Прикарпаттяобленерго» та вимкнули близько 30 підстанцій, залишивши близько 230 тисяч мешканців без світла протягом однієї-шести годин. Ця атака стала першою у світі підтвердженою атакою, спрямованою на виведення з ладу енергосистеми [4].

16 березня 2016 Президент України Петро Порошенко підписав указ, яким увів в дію рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». У концепції зазначається: «Економічна, науково-технічна, інформаційна сфера, сфера державного управління, оборонно-промисловий і транспортний комплекси, інфраструктура електронних комунікацій, сектор безпеки і оборони України стають все більш уразливими для розвідувально-підривної діяльності іноземних спецслужб у кіберпросторі. Цьому сприяє широка, подекуди домінуюча, присутність в інформаційній інфраструктурі України організацій, груп, осіб, які прямо чи опосередковано пов'язані з Російською Федерацією» [5].

Державна служба спеціального зв’язку та захисту інформації України повідомила, що хакери здійснили 179 спроб втрутитися у роботу сайтів органів державної влади та державних підприємств впродовж 2014-2015 років.

У грудні минулого 2015 року хакери атакували сайти видавничої групи «Картель» «Депо» (depo.ua) та «Деловая столица» (dsnews.ua). Зловмисники вимагали від редакцій гроші, аби припинити DDoS-атаки. У січні 2016 року спеціалізований структурний підрозділ Державного центру кібернетичного захисту та запобігання кібернетичним загрозам Державної служби спеціального

зв'язку та захисту України попередив про ймовірність нових хакерських атак. 28 січня 2016 року через потужну хакерську атаку на деякий час припинило свою роботу івано-франківське інтернет-видання «Курс». Видання також отримало погрози. Замість вмісту сайту відображався напис англійською мовою: «Ми не пробачимо, ми не забудемо, чекайте на нас. Аноніми» [6].

Кіберпростір поступово перетворюється на окрему, поряд із традиційними «Земля», «Повітря», «Море» та «Космос», сферу ведення бойових дій, у якій все більш активно діють відповідні підрозділи збройних сил провідних держав світу. З урахуванням широкого застосування сучасних інформаційних технологій у секторі безпеки і оборони, створення єдиної автоматизованої системи управління Збройних Сил України оборона нашої держави стає більш уразливою до кіберзагроз.

Відповідно до Стратегії кібербезпеки України основу національної системи кібербезпеки становитимуть Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи. Зокрема на Національну поліцію України покладені в установленому порядку такі основні завдання:

- забезпечення захисту прав і свобод людини та громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; запобігання, виявлення, припинення та розкриття кіберзлочинів; підвищення поінформованості громадян про безпеку в кіберпросторі.

Водночас, державна влада бере на себе обов’язок по створенню умов для залучення підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інфраструктури, до забезпечення кібербезпеки України. Зокрема, мають бути врегульовані питання щодо обов'язковості вжиття ними заходів із забезпечення захисту інформації та кіберзахисту відповідно до вимог законодавства, а також щодо сприяння ними державним органам у виконанні завдань із забезпечення кібербезпеки та кіберзахисту.

Держава зобов’язується сприяти залученню наукових установ, навчальних закладів, організацій, громадських об'єднань і громадян до розробки та реалізації заходів із кібербезпеки і кіберзахисту. Вищеозначене передбачає, що, зокрема для системи наукових і навчальних структур Національної поліції України пріоритетними напрямами забезпечення кібербезпеки постають в якості інструментів розвитку безпечного, стабільного і надійного кіберпростору насамперед:

– створення вітчизняної нормативно-правової та термінологічної бази у цій сфері, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної та кібербезпеки відповідно до міжнародних стандартів і стандартів ЄС та НАТО;

– залучення експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки проектів концептуальних документів у сфері кібербезпеки;

– підвищення цифрової грамотності громадян та культури безпечного поводження в кіберпросторі, комплексних знань, навичок і здібностей, необхідних для підтримки цілей кібербезпеки, впровадженні державних і громадських проектів підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту [1, п. 4, 4.1].

В свою чергу, такий обсяг завдань передбачає створення розвинутої системи навчальних програм і проведення учбових занять інформаційно-правового спрямування в всіх закладах науково-навчального спрямування структури Національної поліції України. Проведення відповідних наукових досліджень, розробки за їх результатами пропозицій удосконалення інформаційного законодавства та створення наукових лабораторій і груп, що будуть узагальнювати судову, правоохоронну та адміністративну практики, задля впровадження досвіду в освітянський процес. А така робота передбачає значне збільшення обсягу відповідних навчальних годин у програмах і, як наслідок – збільшення штатного персоналу. Крім цього, значимість оптимально організованого інформаційно--аналітичного забезпечення полягає в тому, що воно сприяє прийняттю найбільш доцільних управлінських рішень на всіх рівнях, що є однією з головних умов підвищення ефективності діяльності оперативних підрозділів [7, с. 3-9]. Однак, в сучасних умовах ми спостерігаємо недостатність практичних кроків у цьому напряму.

Науково-дослідні інститути під відомства Міністерства внутрішніх справ, а також відповідні університети з підготовки кадрів для Національної поліції створюють основу для кіберзахисту державних електронних інформаційних ресурсів та інформаційної інфраструктури, призначеної для обробки інформації. Для цього мають бути розроблені нові методи запобігання кібератакам, кіберінцидентам та поширенню інформації про них.

На проектно-нормативному рівні вченими цих установ повинні бути розробленні вимоги (правила, настанови) щодо безпечного використання мережі Інтернет та надання електронних послуг державними органами.

Відповідно до концептуальних положень Стратегії кібербезпеки України мають на систематичному рівні проводитися відповідні заходи з підвищення обізнаності працівників державних органів у сфері інформаційної безпеки та кібербезпеки, проведенні відповідних тренінгів, навчань [1, п. 4.2].

Розуміючи нагальну потребу в цих заходах, втім не можна не звернути увагу про доцільність збільшення академічних годин у навчальних установах органів внутрішніх справ з інформаційно-правового навчання.

Постають перед науково-дослідними і навчальними закладами завдання і у питанні кіберзахисту критичної інфраструктури, насамперед, у:

– комплексному вдосконаленні правової основи кіберзахисту об'єктів критичної інфраструктури, визначенні критеріїв віднесення інформаційних (автоматизованих), телекомунікаційних, інформаційно-телекомунікаційних систем до критичної інформаційної інфраструктури;

– установленні кваліфікаційних вимог для окремих категорій працівників об'єктів критичної інфраструктури з урахуванням сучасних тенденцій кібербезпеки та актуальних кіберзагроз, упровадження для таких працівників обов'язкової періодичної атестації на предмет відповідності зазначеним вимогам [1, п. 4.3]. Така робота частково проводиться, але не охоплює весь спектр працівників правоохоронної сфери, а є здебільш вибірковою та несистематичною. В якості науково-консультативних фахівців мають залучатися представники науково-дослідного і навчального секторів Національної поліції до розвитку потенціалу сектору безпеки і оборони у сфері забезпечення кібербезпеки, що передбачатиме здійснення в установленому порядку, зокрема, таких заходів:

– реалізація державного стратегічного планування та програмно-цільового забезпечення у сфері розвитку електронних комунікацій, інформаційних технологій, захисту інформації та кіберзахисту;

– розвиток підрозділів кібербезпеки та кіберзахисту Національної поліції України, досягнення сумісності із відповідними підрозділами кібербезпеки та кіберзахисту держав - членів НАТО;

– розмежування кримінальної відповідальності за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, вчинені щодо державних та інших інформаційних ресурсів, щодо об'єктів критичної інформаційної інфраструктури та інших об'єктів, а також відповідне розмежування підслідності;

– розвиток системи підготовки кадрів для потреб органів сектору безпеки і оборони України та розвиток науково-виробничого потенціалу такої системи [1, п. 4.4].

Означені положення Стратегії кібербезпеки України передбачають певну спеціалізаційну фахову підготовку кадрів у системі Національної поліції. Зокрема, йдеться про підготовку фахівців на кшталт юристів-програмістів, що 10 років тому здійснювалась у Харківському національному університеті внутрішніх справ, на інформатико-правовому факультеті. Випускники цього факультету, доречі, пізніше сформували основу професорсько-викладацького складу не тільки самого ХНУВС, але й зайняли значне місце у складі інших закладів юридичної школи Харкова, керуючи кафедрами, лабораторіями, юридичними клініками. Втім, МОН України і МВС України з часом наполягли на закритті вищеозначеного факультету і така підготовка з бюрократичних міркувань була згорнута.

Боротьба з кіберзлочинністю передбачатиме також участі навчально-наукових установ і їх професорсько-викладацького потенціалу у здійсненні таких заходів:

– удосконалення процесуальних механізмів щодо збирання доказів в електронній формі, що стосуються злочину, удосконалення класифікації, методів, засобів і технологій ідентифікації та фіксації кіберзлочинів, проведення експертних досліджень;

– підготовка слідчих для роботи з доказами, що стосуються злочину, отриманими в електронній формі, з урахуванням особливостей кіберзлочинів [1, п. 4.5].

Важко зрозуміти як потреба в підготовці означеного кола фахівців корелюється з проголошенням на рівні Міністерства освіти і науки України на протязі останніх 10 років концепту про те, що в державі існує перевиробництво фахівців з напрямку «правознавство», а відтак не має потреби у відповідному держзамовленні. Це, в свою чергу, призвело до масових скорочень правничих програм, досліджень, звільнень і скорочень штату, нівелюванні правознавчої сфери науки і як наслідок – розширенню правового нігілізму на державно-владному рівні. Піднесення зневажливого ставлення до права і закону до рангу державної політики.

Підсумовуючи наведене, можна зробити декілька висновків теоретико-правового спрямування:

1. Навчально-науковим установам Національної поліції України відводиться значний спектр завдань учбового, дослідного і практичного змісту в концепції Стратегії кібербезпеки України.

2. Проголошення Стратегією кібербезпеки України цілої низки завдань для відповідних державницьких структур, на жаль, перенасичене здебільш неконкретизованими, а подекуди просто схоластичними положеннями на кшталт «поглибити», «розширити», «організувати» і таке інше, що в свою чергу, хоча і традиційно притаманне актам стратегічно-концептуального змісту, але не сприяє практичній і терміновій реалізації.

3. Необхідно збільшити загальний обсяг навчально-аудиторних годин за всіма напрямами фахової правової підготовки в навчальних і наукових закладах системи Національної поліції України взагалі та інформаційно-правової підготовки зокрема.

References:

1. *Pro rishennya Rady natsionalnoyi bezpeky i oborony Ukrayiny vid 27 sichnya 2016 roku «Pro Stratehiyu kiberbezpeki Ukrayiny»: Ukaz Prezidenta Ukrainy vid 15 berez. 2016, No. 96/2016* [About the decision of the National Security and Defense Council of Ukraine, 27 january 2016 "About Cybersecurity Strategy of Ukraine ": Decree of the President of Ukraine, 15 March, 2016, No. 96/2016]. Available at: http:// http://zakon3.rada.gov.ua/laws/show/96/2016. (accessed 02.05.2016). (In Ukrainian).

2. *Kiberbezpeka. Komp'yuterna bezpeka* [Cybersecurity. Computer security]. Available at: https://uk.wikipedia.org/wiki/Комп%27ютерна_безпека. (accessed 02.05.2016). (In Ukrainian).

3. Pfitzmann B, Waidner M (1994): A General Framework for Formal Notions of "Secure" System; Hildesheimer Informatik-Berichte 11/94, Institut für Informatik, Universität Hildesheim, April 1994.

4. Kim Zetter (2016) *Khakerska ataka Rossyy na ukrayinsku enerhosistemu: yak tse bulo* [Russian hacker attack of the Ukrainian power system: how it was]. Available at: http://texty.org.ua/pg/article/newsmaker/read/66125/Hakerska_ataka_Rosiji_na_ukrajinsku_jenergosystemu_jak. (accessed 03.05.2016). (In Ukrainian).

5. *Poroshenko zatverdyvshy stratehiyu kiberbezpeki Ukrayiny. Hazeta «Den»* [Poroshenko approved Cybersecurity Strategy of Ukraine. «The Day» newspaper]. Available at: http://www.day.kiev.ua/uk/news/160316-poroshenko-zatverdyv-strategiyu-kiberbezpeky-ukrayiny. (accessed 03.05.2016). (In Ukrainian).

6. *Za dva ostannikh roky derzhsayti Ukrayiny ziznalasya 179 khakerskix atak - Derzhspetszv'yazku* [Over the last two years state sites of Ukraine suffered from 179 hacker attacks - State Special]. Available at: http://osvita.mediasapiens.ua/web/cybersecurity/za_dva_ostannikh_roki_derzhsayti_ukraini_zaznali_179_khakersskikh_atak_derzhspetszvyazku/. (accessed 03.05.2016). (In Ukrainian).

7. Albul, S.V. (2009) *Informatsiyno-analitychne zabezpechennya vyyavlennya oznaka hospodarskykh zlochiniv: problemy y shlyakhy vyrishennyu* [Informational and analytical support of detecting signs of economic crimes: challenges and solutions]. Pivdennoukrayinskyy pravnychyy chasopys. [Southern law journal]. – 2009. – No. 1. – P. 3-9. (In Ukrainian).

Учебно-научные учреждения Национальной полиции в обеспечении стратегии кибербезопасности Украины: фундаментально-правовые аспекты

Исмайлов Карен Юрьевич, e-mail: 0997060070@ukr.ne,
Одесский государственный университет внутренних дел, Украина.

Аннотация: статья посвящается вопросам определения роли научных и учебных учреждений Национальной полиции Украины в обеспечении реализации государственной стратегии кибербезопасности и информационной безопасности. Очерчиваются основные направления исследовательского и профессионального усовершенствования защиты информационного пространства государства и информационного общества

Ключевые слова: кибербезопасность, информационная безопасность, учебно-научные учреждения полиции, информационное общество.

Centre for European Reforms Studies a.s.b.l.
(Grand Duchy of Luxembourg)

European Reforms Bulletin

scientific peer-reviewed journal

2017
No. 4

Passed for printing 24.08.2017. Appearance 17.09.2017.
Typeface Times New Roman. Circulation 100 copies.

Design, computer page positioning, layout: **Centre for European Reforms Studies, a.s.b.l. Grand Duchy of Luxembourg**
All the articles are published in author's edition. Publishing institution: **Centre for European Reforms Studies, a.s.b.l. Grand Duchy of Luxembourg** (Registre de commerce et des sociétés, Luxembourg, F 10.340, siège social: L-1541 Luxembourg, 36, boulevard de la Fraternité), +352661261668, e-mail: bulletin@email.lu, http://cers.eu.pn/bulletin.html