Котух Євген Володимирович,
к.т.н., доцент кафедри кібербезпеки та інформаційних технологій,
Університет митної справи та фінансів,
м. Дніпро
ORCID 0000-0003-4997-620X

УДК 351.865 **doi: 10.34213/ap.19.02.03**

ПРОБЛЕМИ КІБЕРБЕЗПЕКИ В СУЧАСНОМУ СВІТІ

Розглянуто види кіберзагроз (політично вмотивовані, неполітичні; зовнішні, внутрішні) та специфіку реалізації заходів щодо кібезбезпеки в публічному секторі, які застосовуються у світовій практиці. Доведено, що в Україні необхідною є розробка типових механізмів публічного управління інформаційною безпекою в умовах кіберзагроз, а також фінансове забезпечення створення, досліджень та апробації захисту інформаційних систем в цій сфері. Враховуючи глобальний характер загрози, при розробці заходів з кібербезпеки нагальною є тісна співпраця країн у вирішенні цього питання.
Ключові слова: публічне управління, кіберзагроза, кібербезпека, інформаційно-комунікаційні технології, електронний уряд.

Постановка проблеми. Глобальна взаємопов'язаність невпинно зростає й поширюється, стає необхідною як для фізичних осіб, бізнесу, так і держави. На жаль, чим більше ми перебуваємо онлайн, тим більше стаємо уразливими для кіберзагроз. Тому актуальним напрямком наукових досліджень стає аналіз сучасних тенденцій розвитку кіберпростору, що дозволить підвищити рівень обізнаності та запропонувати комплекс пріоритетних заходів із забезпечення кібербезпеки в публічному секторі. У широкому сенсі це передбачає запровадження комплексу заходів зі зниження вразливості комп'ютерних систем, у тому числі й вебсайтів, та їх захисту від несанкціонованого доступу або нападу.

Аналіз останніх досліджень і публікацій. Питанням кібербезпеки та її ролі у забезпеченні національної безпеки присвячено наукові праці І. Діордіци, Є. Живила, З. Коваля, В. Куцаєва, В. Ліпкана, С. Срібного, В. Ткаченка, В. Шеломенцева та ін. Проте в сучасних умовах реформування публічного сектору виникають нові проблеми, що вимагають вдосконалення підходів для визначення особливостей забезпечення дотримання культури кібербезпеки в органах публічного управління. Водночас у вітчизняній науковій літературі бракує комплексного аналізу існуючих проблеми кібербезпеки в сучасному світі з урахуванням специфіки публічного управління.

Мета статті – обґрунтування проблем і напрямків забезпечення кібербезпеки в публічному секторі з урахуванням сучасних змін соціально-економічного стану країни.

Виклад основного матеріалу. Щоб зрозуміти кібербезпеку в публічному секторі, слід усвідомити конвергенцію трьох основних чинників – глобалізації, ступеня підключення до мережі та тенденції надання послуг публічного сектора в Інтернеті, що зазвичай називають електронним урядом (е-урядом).

Інтернет пропонує загальну платформу, за допомогою якої кожна людина може віртуально взяти участь у глобалізації. Доступ до вебсайту в усьому світі однаково простий і люди користуються такою можливостю. Враховуючи переваги інформаційно-комунікаційних технологій (ІКТ), країни наполегливо працюють над тим, щоб залучити решту своїх громадян до Інтернету.

Час перебування людей в Інтернеті також постійно збільшується. Наша довіра до Інтернету, ймовірно, зростатиме й далі. Розробка технології радіочастотної ідентифікації (RFID) в поєднанні з упровадженням шостої версії протоколу Інтернету зробила можливим, наприклад, створення "Інтернету речей", що технічно надає можливість підключити до Інтернету будь що, включаючи повсякденні об'єкти, зокрема, автомобілі. Чому б не мати можливість віддалено розблокувати автомобіль у разі надзвичайної ситуації, або не встановити у ньому бездротове обладнання для покращення можливостей комунікації? Минуло не так багато часу, і це вже реальна мжливість.

З огляду на переваги Інтернету публічний сектор теж його використовує. Найчастіше згадуваний приклад підвищення ефективності – податки. Так, у 2011 р. шведський податковий орган очікував, що 65 % громадян країни подаватимуть інформацію про податки он-лайн, що заощаджує час, зусилля та кошти уряду й водночас полегшує життя виборців. Як зазначено у ст. 128 Звіту ООН щодо світового громадського сектору 2003 р., "Уряди усе більше усвідомлюють важливість використання електронного уряду для покращення надання громадянам послуг публічного сектору" [2, с. 39]. Але Інтернет-середовище також виходить за рамки надання простих сервісів і надає урядам на всіх рівнях змогу покращити можливості обліку, розвиток, ефективність і прозорість.

Різноманітні міжнародні огляди показників електронних урядів за останні 10 років демонструють великий прогрес і переконання в тому, що більшість країн світу вже "електронно-готові". Отже, у випадку ООН, вимірювання показників перейшло від "готовності" до фактичного "розвитку". Щоб підкреслити цю тенденцію Консалтингове агентство досліджень та аналізу Групи Economist (The Economist Intelligence Unit, EIU) навіть змінило назву свого щорічного рейтингу, якому вже понад 10 років. Від рейтингу "електронної готовності" агентство перейшло до скалання рейтингу "цифрової економіки".

Хоча попит на електронне урядування (його використання) відстає від пропозиції (його доступності), уряди переконують своїх виборців користуватися їх послугами та перевагами онлайн-інформації. Наразі у 27 країнах ЄС 42 % громадян віком від 16 до 74 років використовують Інтернет для взаємодії з органами публічної влади. Ключова мета Цифрової програми Стратегії ЄС з використання цифрових інструментів для розвитку економіки – збільшити цю кількість до 2015 р. до 50 % (що й було зроблено) і надалі зберігати відповідні темпи. Включення в Інтернет також є одним із семи центральних стовпів Цифрової програми й має на меті підвищення цифрової грамотності, навичок та підключення.

Зусилля з переведення активності уряду в режим он-лайн усе частіше зустрічаються на всіх рівнях урядів у всьому світі. В одних випадках це відбувається задля зовнішніх цілей, щоб задовольнити попит користувачів на персоналізовані пропозиції за допомогою різних каналів, таких як мобільний уряд (м-уряд) та інструменти Web 2.0. В інших – із внутрішніх причин ефективності, щоб працювати з секретною інформацією або підключити електростанції до Інтернету. Хоча, безумовно, рушійною силою є ефективність, але й публічний сектор піддається все зростаючому тиску використовувати Інтернет задля прозорості.

Глобалізація та Інтернет зумовили зростання можливостей публічного сектору для підвищення внутрішньої ефективності й кращого обслуговування виборців у формі електронного уряду. Але зі збільшенням кількості користу-

вачів та зростанням ролі Інтернету в житті кожної людини, цифрові інструменти також піддають публічний сектор великим ризикам, що обумовлює важливість кібербезпеки. Як наголошувало свого часу керівництво Сітібанку (Citibank), у взаємопов'язаному світі інформаційні мережі вразливі для нападу будь-кого та у будь-який час [3].

Кіберзагрози можна класифікувати декількома способами, один з яких – порівняння політично вмотивованих загроз (кібервійна, кібертероризм, шпигунство та хактивізм – хакерство в політичних цілях) із неполітичними (зазвичай фінансово мотивованими – кіберзлочин, крадіжка інтелектуальної власності та шахрайство, злам для розваги чи відплати, наприклад, від незадоволеного працівника). Цікавим у цій класифікації є усвідомлення того, що міжнародна співпраця є складною щодо політично мотивованих загроз, оскільки хтось, ймовірно, може захищати злочинців. Водночас існує тенденція до широкого порозуміння у боротьбі з кіберзлочинністю, оскільки більшість урядів зацікавлені в цьому.

Метою політично мотивованих атак є порушення роботи різних служб, а також завдання фізичної шкоди. Поширений підхід полягає у використанні так званого бот-нету (мережі ботів), коли застосовується якась кількість інфікованих комп'ютерів (агентів), якими хтось може керувати віддалено, щоб запускати так звані атаки DDoS (розподілені атаки на обладнання з метою перевантажити обладнання та спричинити його відмову працювати). Мета таких атак – зірвати роботу обраного сайту, переповнюючи його трафіком. Широко відомий приклад такої атаки на Естонію під час її дипломатичного протистояння з Росією у квітні 2007 р., коли низка урядових вебсайтів були недоступними протягом трьох тижнів. Проблема бот-нету, ймовірно, посилиться, оскільки мережі ботів дедалі більше націлюються на "завжди увімкнені" широкосмугові пристрої, кількість яких зростає.

Напади з фізичними наслідками трапляються порівняно рідко з огляду на необхідну досвідченість. Втім, такі напади викликають занепокоєння та, ймовірно, поширюватимуться й надалі, оскільки дедалі більше об'єктів стають підключеними до Інтернету. Наприклад, у 2010 р. комп'ютерний хробак Stuxnet став першим шкідливим програмним забезпеченням. Він був спеціально розроблений для нападу на критичну інфраструктуру – ядерні енергетичні реактори Ірану, того разу атаку вдалося зірвати. Критична інфраструктура, наприклад, електростанції, часто є важливою для діяльності урядів, але у багатьох випадках належить приватному сектору або керується ним. Отже, з урахуванням необхідності захисту таких систем, все частіше лунають заклики до публічно-приватного партнерства (ППП).

Політично мотивовані напади також можуть прагнути розголосу, маючі на меті підірвати сприйняття, довіру громадськості. Коли напади на вебсайти публічного сектору вдаються, досягають своєї мети, вони можуть вплинути на довіру до електронного уряду настільки, що сприйняття громадськості стає все більш негативним. У таких випадках люди можуть бути проти виконання певних транзакцій в Інтернеті, не бажати ділитися даними, або не вірити наданій інформації. І це вже проблема. Згідно з даними вебсайту "Цифрового порядку денного для Європи", лише 12 % європейських користувачів відчувають себе цілком безпечно під час здійснення онлайн-транзакцій [2, с. 234].

Поширені підроблені банківські електронні листи та вебсайти, які виглядають схожими на їх справжні аналоги. Мабуть, лише питання часу, коли ми побачимо такі підробки в публічному секторі, які будуть запитувати в нас

конфіденційні дані або надавати нам оманливу інформацію. Певною мірою це вже відбувається. Інтернет широко використовувався в повстаннях 2010, 2011 рр. на Середньому Сході й урядові вебсайти часто повідомляли інформацію, яка відрізнялась від тієї, що повідомляли блогери. Траплялося, що деякі уряди, наприклад, Єгипту, намагалися вимкнути Інтернет, щоб зупинити лавину інформації.

Політично мотивовані загрози також зачіпають безпеку контенту та даних, наприклад, у випадках шпигунства, що далі поширюються внаслідок того, що все більше інформації потрапляє в Інтернет.

Мотивація неполітичних атак зазвичай фінансова і більшість нападів вважатимуться кіберзлочинами. Вони тяжіють до крадіжки даних, як то інформація про кредитну карту, й їх чисельність зберігається на низькому рівні. Поширений підхід полягає у використанні зловмисного програмного забезпечення, яке або розробляється з нуля, або переналаштовується існуюче, чи то купляється на чорному ринку. Зловмисне програмне забезпечення може поширюватися різними шляхами, зокрема електронною поштою або через вебсайти, і може виконувати різноманітні дії, як то встановлення додатків, які можуть відстежувати ключові характеристики індивідуальних пристроїв. Воно також може зламати комп'ютери та зробити їх частиною бот-нету, які можна взяти в оренду на чорному ринку для проведення DDoS-атак, або використовувати як платформу для розповсюдження спам-листів.

Одна з поширених спам-технік – фішинг, шахрайська спроба вимагати від користувачів конфіденційну інформацію, як то логіни, паролі за допомогою небажаного електронного листа, який посилається на зловмисний вебсайт. Й хоча людей постійно попереджують про те, щоб вони не надавали таку інформацію, це залишається проблемою з огляду на витонченість цих електронних листів. Щоб підвищити рівень обізнаності про фішинг у публічному секторі, Тайванська національна команда реагування на надзвичайні ситуації надіслала 186 564 імітованих фішингових електронних листів 31 094 працівникам публічного сектору в 62 публічних установах. Загалом 15 484 (8,3 %) цих електронних листів було відкрито й натиснуто 7 836 (4,2 %) посилань, які в них містилися. Потенційно це піддавало ризику тисячі довірливих працівників публічного сектору та їхнього роботодавця – уряд.

Ще один спосіб класифікації кібератак за ознакою загрози – зовнішня і внутрішня. У більшості наведених вище випадків це загроза зовнішня. Джерелом внутрішніх загроз можуть, наприклад, бути нинішні чи колишні незадоволені працівники. Відомі числені випадки, коли зовнішній носій пам'яті може бути використаний для того, щоб встановити на комп'ютер програму чи програмне забезпечення, як от встановлення "таємних дверей" (backdoor), для інших, шкідливих, цілей, таких як моніторинг натискань клавіш або прихований віддалений доступ до нього. Наводять приклад, коли USB-накопичувачі використали для встановлення високо-розвинутого хробака Conficker на комп'ютери Манчестерського муніципалітету. Цей інцидент спричинив збитки на суму приблизно в 1,5 млн фунтів стерлінгів. З того часу муніципалітет заборонив використовувати такі носії пам'яті, а також відключила всі USB-порти. Як врівноважити продуктивність щодо моніторингу користувачів та призначення їм відповідних рівнів доступу – це питання, що хвилює організації публічного сектора в усьому світі.

Важливо розуміти, що кожен підключений до Інтернету пристрій є потенційною загрозою, оскільки хтось інший може його перепідпорядкувати та використовувати в якості агенту, наприклад, як частину мережі ботів.

Оскільки глобалізація, Інтернет та електронний уряд постійно еволюціонують, публічний сектор повинен знайти шлях подолання виклику кібербезпеки в усе більш взаємопов'язаному світі. Кожного дня все більше людей долучаються до Інтернету, публічний сектор все більше використовує інформаційно-комунікаційні технології, зростають і наслідки кібератак.

Слід зазначити, що кібербезпека – це організаційна проблема, але водночас і глобальне явище. А отже, це має вирішуватися на всіх рівнях – від міжнародного до регіонального, національного та місцевого рівнів. Загрози можуть бути однаковими, але реакція може бути різною.

Врешті-решт, кібербезпека – це глобальний виклик. Як показує аналіз основних положень у дослідженнях із забезпечення кібербезпеки, пропонується ставитися до безпеки та захисту даних як до нагальної технічної проблеми, водночас вирішувати це питання слід поступово та пропорційно, беручі до уваги необхідність досягнення компромісу між підвищеною безпекою та використанням. Найчастіше оптимальний підхід полягає в побудові безпеки та захисту даних з самого початку будь-якої ініціативи електронного уряду.

Слід погодитись з думкою В. Ліпкана та І. Діордіці, що Україна має створити ключові механізми публічного управління інформаційною безпекою в умовах кіберзагроз у вигляді спеціалізованих центрів та інститутів, а також експериментувати з операціями щодо ведення інформаційної війни, фінансувати експертні дослідження у сфері інформаційних операцій і створювати структури для наукових досліджень та розробок в цій сфері [1, с. 178].

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямку. Як засвідчує світова й вітчизняна практики, вжиття заходів з кібербезпеки все складніше реалізовувати, особливо самотужки. Це повязано з посиленням рівня самих кібератак, винахідливістю їх проведення та ускладненням інформаціних відносин у глобальній економіці. Рушійною силою впровадження е-уряду стають прагнення ефективності та вимоги щодо прозорості. Для України актуальним є розроблення типових механізмів публічного управління інформаційною безпекою в умовах кіберзагроз, а також фінансове забезпечення створення, досліджень та апробації захисту інформаційних систем в цій сфері. Світ має довгу історію боротьби зі злочинністю та війною. Враховуючи глобальний характер загрози, це не така проблема, яку може вирішити одна окрема країна самотужки. Тому, для досягнення цієї мети має створюватись Глобальна програма кібербезпеки, елементи якої стануть предметом подальших досліджень.

Список використаних джерел

1. Ліпкан В., Діордіца І. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України. *Підприємництво, господарство і право*. 2017. № 5. С. 174–180.

2. Andreasson K. Cybersecurity: Public Sector Threats and Responses. *CRC Press. Taylor & Francis Group*. 2012. 392 p.

3. White House. June 2009. Cyberspace Policy Review: Assuring a Trusted and Resiliant Information and Communications Infrastructure. URL: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (дата звернення: 18.09.2019).

References

1. Lipkan, V., Diorditsa, I. (2017). Natsionalna systema kiberbezpeky yak skladova chastyna systemy zabezpechennia natsionalnoi bezpeky Ukrainy [National system of ciberbezpeci how component part of the system of providing of national safety of Ukraine]. *Pidpryemnytstvo, hospodarstvo i pravo, 5, 174–180* [in Ukrainian].

2. Andreasson, K. (2012). Cybersecurity: Public Sector Threats and Responses. *CRC Press. Taylor & Francis Group*.

3. White House. June 2009. Cyberspace Policy Review: Assuring a Trusted and Resiliant Information and Communications Infrastructure. URL: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

Kotukh Ye. V., *PhD in Technical Sciences, Associate Professor of Cyber Security and Information Technologies Department, University of Customs Service and Finances, Dnipro*
ORCID 0000-0003-4997-620X

CYBER SECURITY PROBLEMS IN MODERN WORLD

A pending issue in the present-day research domain is an analysis of the modern trends of cyberspace development, raising awareness as well as elaboration of a complex of priority measures for providing the cyber security in the field of public administration.

Globalization and the Internet have stipulated the growth of new opportunities for the public sector to enhance its internal efficiency and better servicing of voters in the e-government format. However, with an increased number of users and a growing role of the Internet in people's everyday life, digital tools also put the public sector at great risks, thus contributing to the importance of cyber security. Although the demand for e-government (its application) is lagging behind the supply (its availability), governments worldwide persuade voters to use their services, taking advantage of the on-line information benefits. Striving for efficiency and transparency requirements are becoming the driving forces of these processes.

To determine the specific features of cyber security in the public sector, it is important to realize the convergence of the following three factors: globalization, the degree of logging on to the Internet, and the trends of providing the public sector services in the Internet, which is normally called 'e-government'.

It is expedient to discern two kinds of cyber threats, namely: 1) politically motivated (for example, cyberwar, cyberterrorism, hacktivism, spying) and non-political threats (for instance, cybercrime, intellectual property theft, fraud, hacking for fun or revenge); 2) those based on potential threats (external or internal).

For Ukraine, it is essential to develop typical mechanisms for public administration of information security under the conditions of cyber threats, as well as financial provision of creation, research and trial of information protection systems in the said sphere. The world has had a long history of counteracting cybercrime. Considering the global nature of the threat, it is important to closely cooperate with other countries while developing cyber security measures.

Key words: public administration, cyber threat, cyber security, information and communication technologies, e-government.

Надійшла до редколегії 27.09.2019 р.