Законодавство та стратегії у сфері кібербезпеки

(досвід країн Європейського Союзу та США)

Інформаційна довідка, підготовлена Європейським інформаційно-дослідницьким центром на запит Комітету Верховної Ради України

Європейський інформаційно-дослідницький центр створено з метою надання народним депутатам України інформації, яка може бути використана ними у законотворчій діяльності. Діяльність Європейського інформаційно-дослідницького центру здійснюється в рамках програми USAID "Рада: підзвітність, відповідальність, демократичне парламентське представництво", що виконується Фондом "Східна Європа". Більше про центр на сайті http://euinfocenter.rada.gov.ua/

Кібербезпека: поняття та основні підходи

Кібербезпека:

- це сукупність організаційних, правових, технічних та освітніх заходів, спрямованих на забезпечення безперервного функціонування кіберпростору *(Політика захисту кіберпростору Республіки Польща)*
- це бажаний стан безпеки інформаційних технологій, за якого ризики для кіберпростору скорочені до прийнятного мінімуму *(Стратегія кібербезпеки ФРН)*
- це бажаний стан інформаційної системи, за якого вона може протидіяти викликам кіберпростору, що можуть негативно вплинути на достовірність, цілісність та конфіденційність даних, які зберігаються або обробляються даною системою *(Стратегія безпеки та оборони інформаційних систем Франції)*
- це захист інформаційних систем, що входять до складу кіберпростору, від нападів, забезпечення конфіденційності, цілісності та доступності інформації, яка обробляється в цьому просторі; виявлення та протидія атакам і кіберінцидентам *(Національна кіберстратегія Туреччини)*

Оскільки проблема кібербезпеки має глобальний характер, важливою є позиція міжнародних організацій. Так, **Міжнародний телекомунікаційний союз** (*International Telecommunication Union, ITU)*[1] у своїй Рекомендації дає таке визначення: *кібербезпека* — це набір засобів, стратегії, принципи забезпечення безпеки, гарантії безпеки, підходи до управління ризиками, дії, професійна підготовка, практичний досвід, страхування та технології, які можуть бути використані для захисту кіберсередовища, ресурсів організації та користувача.

Більшість держав світу *(США, ЄС, Китай, Індія та ін.)* перебувають у процесі трансформації власних військових підрозділів з огляду на можливості використання мережі Інтернет. Формуються **спеціальні підрозділи**, що мають на меті: ведення розвідувальної роботи в мережах, захист власних мереж, блокування структур супротивника із використанням можливостей кіберпростору.

Згідно з офіційними заявами, такі підрозділи створено у США (***U.S. Cyber Command***[2]), Великобританії (урядовий ***Cyber Security Operations Centre***), Німеччині (***Internet Crime Unit ma Federal Office for Information Security***), Австралії (***The Cyber security operations centre***). Активну позицію щодо протидії кіберзагрозам посідає провідна міжнародна безпекова організація НАТО (***Cooperative Cyber Defence Centre of Excellence***)[3]. Таким чином, держави все більше уваги приділяють розвитку та захисту власних інформаційних ресурсів, а також можливості впливати на інформаційні ресурси інших країн.[4]

Крім того, держави світу активно беруть участь у навчаннях щодо протидії кібератакам. Досвід США (***Cyber Storm***)[5] та ЄС (**Cyber Europe**[6], навчання на

[1] International Telecommunication Union — http://www.itu.int/ru/Pages/default.aspx
[2] U.S. Cyber Command — http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/
[3] Cooperative Cyber Defence Centre of Excellence — https://ccdcoe.org/
[4] Кібербезпека: світові тенденції та виклики для України — http://www.niss.gov.ua/articles/510/
[5] Cyber Storm — https://www.dhs.gov/cyber-storm

спеціальному полігоні Northrop Grumman) доводить, що подібні навчання мають значний ефект для виявлення проблемних зон захисту інфраструктури, моделювання можливих інцидентів і вироблення типових схем реагування, поліпшення міжвідомчої взаємодії.[7] У Європейському Союзі у зв'язку з розумінням важливості проблеми кібербезпеки в 2004 році було створено **Європейське агентство з мережевої та інформаційної безпеки** *(European Union Agency for Network and Information Security).*[8]

Серед **основних загроз** національним кіберпросторам більшість країн визначають:

- ***Кібершпигунство*** та ***військові дії***, які здійснюються за підтримки або з відома держави. Усі технологічно розвинені держави та корпорації стають об'єктом кібершпигнуства, яке має на меті заволодіння державними або промисловими таємницями, персональними даними або іншою цінною інформацією.
- Використання Інтернету у ***терористичних цілях***. Терористичні угрупування використовують Інтернет з метою пропаганди, вербування прихильників.
- ***Кіберзлочинність***: викрадення персональних даних та відмивання коштів, отриманих незаконним шляхом. Зловмисники продають інформацію про номери банківських карток, паролі та шкідливе ПЗ.[9]

Національне законодавство розглянутих країн, як правило, регулюють питання:

- Захисту персональних даних *(Канада, Нідерланди, Естонія, Швеція, Фінляндія)*
- Захисту електронної комерції, безпеки електронних транзакцій та платіжних інструментів *(США, Канада, Польща, Естонія, Італія)*
- Захисту важливих об'єктів інфраструктури та інформаційних систем *(Франція)*

Отже, більшість держав активно модернізує власні сектори безпеки у відповідності до викликів сучасності, і особливо — зважаючи на потенціал використання мережі Інтернет. Цей процес відбувається із: активним реформуванням систем управління відповідним сектором безпеки; впорядкуванням нормативного поля, що має забезпечити цілісність державної політики в даній сфері; активною роз'яснювальною роботою серед населення щодо небезпек кіберзагроз; збільшенням чисельності підрозділів, зайнятих у системі кіберзахисту; розробкою кіберозброєнь та проведення пробних військово-розвідувальних акцій у кіберпросторі; посилення контролю за національним інформаційним простором.[10]

Сполучені Штати Америки

Закони, що регулюють питання, пов'язані з кібербезпекою:

1. Закон «Про національну безпеку» *(Homeland Security Act)*[11]

---

[6] Cyber Europe — https://ec.europa.eu/jrc/en
[7] Кібербезпека: світові тенденції та виклики для України — http://www.niss.gov.ua/articles/510/
[8] European Union Agency for Network and Information Security — https://www.enisa.europa.eu/
[9] Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada — http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf
[10] Кібербезпека: світові тенденції та виклики для України — http://www.niss.gov.ua/articles/510/
[11] Homeland Security Act — http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf

2. Закон «Про дослідження та розвиток кібербезпеки» *(Cyber Security Research and Development Act)*[12]
3. Закон «Про інформаційну безпеку» *(Federal Information Security Management Act)*[13]
4. Закон «Про недоторканість особистого життя» *(Privacy Act)*
5. Закон «Про електронні транзакції» *(Uniform Electronic Transactions Act)*[14]
6. Закон «Про захист дітей в Інтернеті» *(Children's Internet Protection Act)*[15]
7. Закон «Про електронні підписи» *(Electronic Signatures in Global and National Commerce Act)*[16]
8. Закон «Про злочини, пов'язані з комп'ютерами» *(Fraud and related activity in connection with computers)*[17]
9. Закон «Про боротьбу зі спамом» *(Controlling the Assault of Non-solicited Pornography and Marketing)*[18]
10. Закон «Про перехоплення електронних повідомлень та прослуховування переговорів» *(Wire and Electronic Communications in Terception and Interception of Oral Communications)*[19]

Досить активною політикою в сфері кібербезпеки була за Адміністрації Б.Обами:

- у 2009 р. оприлюднено «Огляд кібербезпеки» (*Cyber Security Review*) — комплексний документ, що визначав основні пріоритети нової команди у сфері кібербезпеки
- створено U.S. Cyber Command; приблизна чисельність структури — 30 тис. військових
- оприлюднено нову «Стратегію національної безпеки» (2010), в якій кіберзагрозам вперше відведено окреме місце у структурі загроз США
- оголошено про додаткові заходи із посилення внутрішньої кібербезпеки; із жовтня 2009 року оголошено про набір додатково 1000 співробітників до спеціального кібербезпекового департаменту Управління національної безпеки (*Department of Homeland Security*), які займаються виключно безпекою високотехнологічних систем США
- збільшено держзамовлення на розроблення нових засобів ведення війни, зокрема кіберозброєнь та нових, більш захищених, військових мереж[20]

Міжнародне співробітництво

З метою сприяння посиленню кібербезпеки у всьому світі США офіційно визнали партнерство з такими країнами та організаціями:

- Співробітництво між США та ЄС у сфері кібербезпеки та кіберпростору

[12] Cyber Security Research and Development Act — https://www.law.cornell.edu/topn/cyber_security_research_and_development_act
[13] Federal Information Security — http://csrc.nist.gov/drivers/documents/FISMA-final.pdf
[14] Uniform Electronic Transactions Act — http://www.uniformlaws.org/shared/docs/electronic%20transactions/ueta_final_99.pdf
[15] Children's Internet Protection — http://ifea.net/cipa.pdf
[16] Electronic Signatures in Global and National Commerce — https://www.law.cornell.edu/uscode/text/15/chapter-96
[17] Fraud and related activity in connection with computers — https://www.law.cornell.edu/uscode/text/18/1030
[18] https://www.law.cornell.edu/uscode/text/15/chapter-103
[19] Wire and electronic communications in terception and interception of oral communications — https://www.law.cornell.edu/uscode/text/18/part-I/chapter-119
[20] Кібербезпека: світові тенденції та виклики для України — http://www.niss.gov.ua/articles/510/

- Спільний План дій з кібербезпеки Міністерства національної безпеки США та Міністерства державної безпеки Канади
- Комп'ютерна група реагування на надзвичайні ситуації (US-CERT) та ні.[21]

Естонія

Основою політики Естонії у сфері кібербезпеки є **Стратегія кібербезпеки 2014-2017 рр**.[22] Щорічно **Управління інформаційних систем**[23] *(Riigi Infosüsteemi Amet)* публікує доповіді про кібербезпеку. Ще одним відповідальним органом за реалізацію кіберстратегії є *Департамент захисту важливих об'єктів інфраструктури*. **X-Road**[24] є національною платформою для співробітництва з державним та приватним сектором у сфері кібербезпеки.

Закони, що регулюють питання, пов'язані з кібербезпекою:

1. Закон «Про захист персональних даних»
2. Закон «Про електронні повідомлення»
3. Закон «Про електронні платіжні системи»
4. Закон «Про послуги інформаційного суспільства»

Міжнародне співробітництво

- Співробітництво із США. Ініціатива зі співробітництва була ініційована на зустрічі глав держав Естонії, Литви та Латвії та Президента США Барака Обами у серпні 2013 року. Метою зустрічі став обмін досвідом в контексті активізації безпекового діалогу між країнами Балтійського регіону та США
- Участь у Об'єднаному центрі передових технологій з кібероборони НАТО
- Співробітництво з *TERENA*[25], *TF-CSIRT*.

Латвія

Основоположними документами, що визначають політику Латвії у сфері кібербезпеки, є **Концепція національної безпеки** та **Стратегія кібербезпеки Латвії 2014-18**[26]. Відповідальним органом за реалізацію кіберстратегії є **Національна рада безпеки інформаційних технологій.**

Закони, що регулюють питання, пов'язані з кібербезпекою:

1. Закон «Про національну інформаційну систему»[27]
2. Закон «Про електронні повідомлення»[28]

[21] Законодавство та стратегії у сфері кібербезпеки — http://euinfocenter.rada.gov.ua/uploads/documents/28982.pdf
[22] Cyber Security Strategy — https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf
[23] Riigi Infosüsteemi Amet — https://www.ria.ee/ee/index.html
[24] X-Road — https://e-estonia.com/component/x-road/
[25] TERENA — https://www.terena.org/
[26] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/
[27] Valsts informācijas sistēmu likums — http://likumi.lv/doc.php?id=62324
[28] 116Elektronis kosakaru likums — http://likumi.lv/doc.php?id=96611

3. Закон «Про безпеку інформаційних технологій»[29]

Міжнародне співробітництво

- Співробітництво з ЄС, НАТО, скандинавськими та балтійськими країнами, США
- Партнерство *CERT.LV*[30] з європейськими партнерами

Німеччина

Основою політики Німеччини у сфері кібербезпеки є **Стратегія кібербезпеки**[31] та **Національний план із захисту інформаційної інфраструктури**. Відповідальним органом за реалізацію кіберстратегії є **Федеральне управління інформаційної безпеки** *(Bundesamt für Sicherheit in der Informationstechnik).*[32]

Закони, що регулюють питання, пов'язані з кібербезпекою:

1. Закон «Про електронні підписи» (2001)[33]
2. Закон «Про захист федеральних даних» (2009)[34]
3. Закон «Про Федеральну службу інформаційної безпеки» (2009)[35]
4. Закон «Про посилення безпеки федеральних інформаційних технологій» (2009)[36]

Міжнародне співробітництво

- Співробітництво із США в рамках зустрічей, присвячених питанням кібербезпеки
- Співробітництво з TERENA, FIRST, ENISA, APCERT, EGC[37]

Польща

Засади державної політики у сфері кібербезпеки визначають **Національна стратегія безпеки 2007 року** та **Політика захисту кіберпростору**[38] Республіки Польща 2013 року.

Закони, що регулюють питання, пов'язані з кібербезпекою:

[29] Informācijas tehnoloģi judrošības likums — http://likumi.lv/doc.php?id=220962
[30] CERT.LV — https://cert.lv/lv
[31] Cyber Security Strategy for Germany — https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile
[32] Bundesamt für Sicherheit in der Informationstechnik — https://www.bsi.bund.de/DE/Home/home_node.html
[33] Gesetzüber Rahmenbeding ungen für elektronische Signaturen — http://www.gesetze-iminternet.de/sigg_2001/BJNR087610001.html
[34] Bundes daten schutz gesetz — http://www.gesetze-im-internet.de/bdsg_1990/
[35] Gesetzüber das Bundes amt für Sicherheit in der Informations technik — http://www.gesetze-iminternet.de/bsig_2009/BJNR282110009.html
[36] Act to Strengthen the Security of Federal Information Technology — https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/BSI_Act_BSIG.pdf;jsessionid=5A1E1C722E66B37569F491E7A5D25A31.2_cid359?__blob=publicationFile
[37] Cyberwellness Profile Germany — http://www.itu.int/en/ITUD/ Cybersecurity/Documents/Country_Profiles/Germany.pdf
[38] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf

1. Закон «Про електронні підписи»[39]
2. Закон «Про захист персональних даних»[40]
3. Закон «Про комп'ютеризацію операцій підприємств, що виконують державні завдання»[41]
4. Закон «Про електронні платіжні інструменти»[42]
5. Закон «Про надання послуг через електронні засоби»[43]

Органи, відповідальні за реалізацію кіберстратегії: *Адміністрація впровадження цифрових технологій*, *Міністерство національної оборони*, *Служба внутрішньої безпеки*.[44]

Франція

В основі діяльності Франції в кіберпросторі лежить **Стратегія безпеки та оборони інформаційних систем**.[45] Орган, відповідальний за реалізацію кіберстратегії, — **Національна служба безпеки інформаційних технологій** *(Agence nationale de la sécurité des systèmes d'information).*[46]

Закони, що регулюють питання, пов'язані з кібербезпекою:

1. Закон «Про комп'ютери, файли та свободи»[47]
2. Закон «Про електронні докази та електронні підписи»[48]
3. Указ від 2011 року та міжвідомча заява №1300 «Про захист конфіденційної інформації, пов'язаної з обороною держави»
4. Декрет №2009-834 «Про створення Служби безпеки інформаційної системи»
5. Рекомендація №901 від березня 1994 «Про захист інформаційних систем»

Міжнародне співробітництво

- Співробітництво з Федеральним управлінням інформаційної безпеки Німеччини
- Співробітництво з британською Групою із забезпечення прихованої роботи засобів зв'язку та електронного устаткування
- Співробітництво з Агентством національної безпеки та Міністерством національної безпеки США

[39] The Act of 18 September, 2001 on Electronic Signature — http://www.mg.gov.pl/NR/rdonlyres/9C534966-8336-49C9-8087-0F4A64F14D66/18224/act_on_eSignature.pdf
[40] http://www.google.ch/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CCcQFjAB&url=http%3A%2F%2Fwww.giodo.gov.pl%2Fdata%2Ffilemanager_en%2F61.doc&ei=rAjKVMXuFYfbPZ_XgJAH&usg=AFQjCNFmBLcFn_CAcIv3BpyUuNzACOswHA&sig2=teUft7Bha_G7AwmjV3SU1g&bvm=bv.84607526,d.ZWU
[41] http://www.google.ch/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CB4QFjAA&url=http%3A%2F%2Fprawo.vagla.pl%2Ffiles%2FAct_on_Computerisation.doc&ei=lwfKVOi1EonaOPntgZgE&usg=AFQjCNEZJIyrzOw0g7YIXb8XvHlwUXVq-w&sig2=9h4ynjVluoZq4TzVQqmd-w&bvm=bv.84607526,d.ZWU
[42] Act of 12 September 2002 on Electronic Payment Instruments — https://www.nbp.pl/en/system_platniczy/mf.pdf
43 https://www.itu.int/osg/spu/spam/legislation/Ustawa%20SUDE-eng_ver.pdf
44 Cyberwellness Profile Republic of Poland — http://www.itu.int/en/ITUD/Cybersecurity/Documents/Country_Profiles/Poland.pdf
[45] Стратегія безпеки та оборони інформаційних систем — https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf
[46] Agence nationale de la sécurité des systèmes d'information — https://www.ssi.gouv.fr/
[47] http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=2A2EF6C91837B853539CEB3201AA05F5.tpdjo14v_1?cidTexte=JORFTEXT000000886460&dateTexte=20121203
[48] Code civil — http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070721&dateTexte=20121115

Додаток

Країна	Кіберстратегія	Відповідальні органи
Австрія	Національна стратегія безпеки інформаційно-комунікаційних технологій *(2012)* Стратегія кібербезпеки *(2013)*	▪ Керівна група з кібербезпеки ▪ Експертний центр з питань кіберзлочинності
Великобританія	Національна стратегія кібербезпеки *(2011)*	▪ Управління кібербезпеки та інформаційного забезпечення ▪ Центр захисту національної інфраструктури
Естонія	Стратегія кібербезпеки *(2014)*	▪ Управління інформаційних систем ▪ Департамент захисту важливих об'єктів інфраструктури
Іспанія	Національна стратегія кібербезпеки *(2013)*	▪ Національний центр криптології ▪ Національний центр розвідки ▪ Національна служба безпеки
Італія	Основи національної стратегії щодо безпеки кіберпростору *(2013)*	▪ Голова Ради міністрів
Канада	Стратегія кібербезпеки Канади *(2010)*	▪ Центр реагування на надзвичайні ситуації у кіберпросторі ▪ Офіс омбудсмена з питань персональних даних ▪ Управління захисту важливих об'єктів інфраструктури
Латвія	Концепція національної безпеки *(2011)* Стратегія кібербезпеки Латвії	▪ Національна рада безпеки інформаційних технологій ▪ Міністерство оборони
Німеччина	Стратегія кібербезпеки *(2011)*	▪ Федеральне управління інформаційної безпеки
Польща	Національна стратегія безпеки *(2007)*	▪ Міністерство національної оборони ▪ Служба внутрішньої безпеки
Франція	Стратегія безпеки та оборони інформаційних систем *(2011)*	▪ Національна служба безпеки інформаційних технологій
Чехія	Національна стратегія кібербезпеки *2015-2020*	▪ Управління національної безпеки ▪ Національний центр кібербезпеки

Інформацію підготувала Анастасія Паршикова,
аналітик Європейського інформаційно-дослідницького центру
http://euinfocenter.rada.gov.ua/