



USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

ПРОГРАМА РАДА



ЛАБОРАТОРІЯ
ЗАКОНОДАВЧИХ
ІНІЦІАТИВ
www.laboratory.org.ua



ІнфоЦентр

ЗАКОНОДАВСТВО ТА СТРАТЕГІЇ У СФЕРІ КІБЕРБЕЗПЕКИ КРАЇН ЄВРОПЕЙСЬКОГО СОЮЗУ США, КАНАДИ ТА ІНШИХ

Інформаційна довідка, підготовлена Європейським
інформаційно-дослідницьким центром на запит
народного депутата України

Кібербезпека

– сукупність організаційних, правових, технічних та освітніх заходів, спрямованих на забезпечення безперервного функціонування кіберпростору (*Політика захисту кіберпростору Республіки Польща*).

– бажаний стан безпеки інформаційних технологій, за якого ризики для кіберпростору скорочені до прийнятного мінімуму (*Стратегія кібербезпеки Німеччини*).

– заходи з попередження шкоди від збоїв в роботі ІКТ та в її усуненні (*Національна стратегія кібербезпеки Королівства Нідерланди*).

– бажаний стан інформаційної системи, за якого вона може протидіяти викликам кіберпростору, які можуть негативно вплинути на достовірність, цілісність та конфіденційність даних, що зберігаються або обробляються даною системою (*Стратегія безпеки та оборони інформаційних систем Франції*).

Серед основних загроз національним кіберпросторам стратегії більшості країн визначають:

- Кібершпигунство та військові дії, які здійснюються за підтримки або з відома держави. Усі технологічно розвинені держави та корпорації стають об'єктом кібершпигунства, яке має на меті заволодіння державними або промисловими таємницями, персональними даними або іншою цінною інформацією¹. Так, однією з найрезонансніших кібератак за останній час стали дії КНДР проти компанії "Sony Pictures Entertainment", внаслідок яких зловмисники заволоділи конфіденційними даними, в тому числі інформацією про комерційні операції компанії².
- Використання Інтернету у терористичних цілях. Терористичні угруповання використовують Інтернет з метою пропаганди, збору коштів і вербування прихильників³.
- Кіберзлочинність: викрадення персональних даних та відмивання коштів, отриманих незаконним шляхом. Зловмисники продають інформацію про номери банківських карток, паролі від комп'ютерних серверів та шкідливе ПЗ⁴.

Відповідно, національні законодавства країн, як правило, регулюють питання:

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

Для цілей даного дослідження були використані дані з "*Cyberwellness profiles*" Міжнародного телекомунікаційного союзу.

¹ Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada
<http://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/cbr-scrst-strtg/cbr-scrst-strtg-eng.pdf>

² The Department Of Defense Cyber Strategy http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

³ Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada
<http://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/cbr-scrst-strtg/cbr-scrst-strtg-eng.pdf>

⁴ Там само

США

Кримінальне законодавство у сфері кіберзлочинності

- Закон «Про боротьбу зі спамом» (Controlling the Assault of Non-solicited Pornography and Marketing, 2003)⁵;
- Закон «Про злочини, пов'язані з засобами доступу» (Fraud and related activity in connection with access devices)⁶;
- Закон «Про злочини, пов'язані з комп'ютерами» (Fraud and related activity in connection with computers)⁷;
- Закон «Про злочини, пов'язані з електронною поштою» (Fraud and related activity in connection with electronic mail)⁸;
- Закон «Про перехоплення електронних повідомлень та прослуховування переговорів» (Wire and Electronic Communications in Terception and Interception of Oral Communications)⁹;
- Закон «Про зберігання повідомлень та доступ до записів транзакцій» (Stored Wire and Electronic Communications and Transactional Record Access)¹⁰.

Закони, що регулюють питання, пов'язані з кібербезпекою

- Закон «Про національну безпеку» (Homeland Security Act)¹¹;
- Закон «Про дослідження та розвиток кібербезпеки» (Cyber Security Research and Development Act)¹²;
- Закон «Про інформаційну безпеку» (Federal Information Security Management Act)¹³;
- Закон «Про недоторканість особистого життя» (Privacy Act)¹⁴;

⁵15 U.S. Code Chapter 103 - Controlling the Assault of Non-Solicited Pornography and Marketing
<https://www.law.cornell.edu/uscode/text/15/chapter-103>

⁶18 U.S. Code § 1029 - Fraud and Related Activity in Connection with Access devices
<https://www.law.cornell.edu/uscode/text/18/1029>

⁷18 U.S. Code § 1030 - Fraud and related activity in connection with computers
<https://www.law.cornell.edu/uscode/text/18/1030>

⁸18 U.S. Code § 1037 - Fraud and related activity in connection with electronic mail
<https://www.law.cornell.edu/uscode/text/18/1037>

⁹18 U.S. Code Chapter 119 - Wire and electronic communications in terception and interception of oral communications
<https://www.law.cornell.edu/uscode/text/18/part-I/chapter-119>

¹⁰18 U.S. Code Chapter 121 - Stored wire and electronic communications and transactional records access
<https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121>

¹¹An Act to establish the Department of Homeland Security, and for other purposes
http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf

¹²Cyber Security Research and Development Act
https://www.law.cornell.edu/topn/cyber_security_research_and_development_act

¹³Information Security <http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>

- Закон «Про електронні транзакції» (Uniform Electronic Transactions Act)¹⁵;
- Закон «Про захист дітей у XXI ст.» (Protecting Children in the 21st Century Act)¹⁶;
- Закон «Про захист дітей» (Keeping the Internet Devoid of Sexual Predators Act, 2008)¹⁷;
- Закон «Про захист дітей в Інтернеті» (Children's Internet Protection Act)¹⁸;
- Закон «Про електронні підписи» (Electronic Signatures in Global and National Commerce Act)¹⁹.

Програмні документи

На державному рівні прийняті:

- [Міжнародна стратегія для кіберпростору «Процвітання, безпека, відкритість у мережевому світі» \(2011\)](#)²⁰.
- [Кіберстратегія Міністерства оборони від квітня 2015 року](#)²¹.
- [Міжвідомчий план дій з кібербезпеки систем управління](#) (Cross-Sector Roadmap for Cybersecurity of Control Systems)²²
- [План дій з посилення кібербезпеки найважливіших об'єктів інфраструктури](#) (Roadmap for Improving Critical Infrastructure Cybersecurity, 2014)²³
- [План дій з забезпечення кібербезпеки систем енергопостачання](#) (Roadmap to Achieve Energy Delivery Systems Cybersecurity)²⁴

Відповідальні органи

Координатор органів виконавчої влади з питань кібербезпеки, який виступає в якості помічника Президента. Функції з контролю та координації імплементації національної стратегії кібербезпеки, політики та згаданих планів дій органами

¹⁴5 U.S. Code § 552a – Records maintained on individuals <https://www.law.cornell.edu/uscode/text/5/552a>

¹⁵Uniform Electronic Transactions Act (1999)

http://www.uniformlaws.org/shared/docs/electronic%20transactions/ueta_final_99.pdf

¹⁶Protecting Children in the 21st Century Act

https://www.law.cornell.edu/topn/protecting_children_in_the_21st_century_act

¹⁷KIDS Act of 2008 https://www.law.cornell.edu/topn/kids_act_of_2008

¹⁸Children's Internet Protection <http://ifea.net/cipa.pdf>

¹⁹Electronic Signatures in Global and National Commerce <https://www.law.cornell.edu/uscode/text/15/chapter-96>

²⁰International Strategy for Cyberspace https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/international_strategy_for_cyberspace_US.pdf

²¹The Department Of Defense Cyber Strategy http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

²²Cross-Sector Roadmap for Cybersecurity of Control Systems https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/Cross-Sector_Roadmap_9-30.pdf

²³Roadmap for Improving Critical Infrastructure Cybersecurity, 2014

<http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf>

²⁴Roadmap to Achieve Energy Delivery Systems Cybersecurity

http://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf

виконавчої влади виконують Міністерство національної безпеки та Міністерство Оборони.

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 кіберпростору²⁵;
- Спільний План дій з кібербезпеки Міністерства національної безпеки США та Міністерства державної безпеки Канади²⁶;
- Партнерство у сфері кібербезпеки та свободи інтернету між США та Естонією;
- Комп'ютерна група реагування на надзвичайні ситуації ([US-CERT](#));
- [FIRST](#)²⁷.

Міжвідомче співробітництво

Програми та плани з розподілу повноважень між органами державної влади та приватним сектором.

- Національний план із захисту інфраструктури (National Infrastructure Protection Plan, 2013)²⁸;
- Меморандум між Міністерством національної безпеки та Міністерством оборони (2010) про захист важливих цивільних та військових комп'ютерних систем та мереж;
- Пілотна ініціатива Міністерства національної безпеки, Міністерства оборони та Центру розповсюдження та аналізу інформації про фінансові послуги ([FS-ISAC](#)) із захисту основних мереж та об'єктів інфраструктури у сфері фінансових послуг шляхом обміну чутливою інформацією, що дає підстави для судового переслідування²⁹.

²⁵EU-US cooperation on cyber security and cyberspace

http://www.eeas.europa.eu/statements/docs/2014/140326_01_en.pdf

²⁶Cybersecurity Action Plan Between Public Safety Canada and the Department of Homeland Security

<http://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/cybrscrt-ctn-plan/cybrscrt-ctn-plan-eng.pdf>

²⁷Cyberwellness Profile United States [http://www.itu.int/en/ITU-](http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/United_States.pdf)

[D/Cybersecurity/Documents/Country_Profiles/United_States.pdf](http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/United_States.pdf)

²⁸NIPP 2013: Partnering for Critical Infrastructure Security and Resilience

http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf

²⁹Cyberwellness Profile United States [http://www.itu.int/en/ITU-](http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/United_States.pdf)

[D/Cybersecurity/Documents/Country_Profiles/United_States.pdf](http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/United_States.pdf)

Канада

Кримінальне законодавство у сфері кіберзлочинності

Положення Кримінального кодексу (1985)³⁰.

Закони, що регулюють питання, пов'язані з кібербезпекою

- Закон «Про боротьбу зі спамом» (Anti-Spam Act)³¹;
- Постанова «Про безпеку електронних підписів» (Secure Electronic Signature Regulations)³²;
- Постанова «Про захист електронної комерції» (Electronic Commerce Protection Regulations)³³;
- Закон «Про електронні документи та захист персональних даних» (Personal Information Protection and Electronic Documents Act)³⁴.

Програмні документи

- [Стратегія кібербезпеки Канади](#) (2010)³⁵;
- [План дій стратегії кібербезпеки на 2010-2015 рр](#)³⁶.

Відповідальні органи

- Королівська канадська кінна поліція;
- Центр реагування на надзвичайні ситуації у кіберпросторі (Canadian Cyber Incident Response Centre);
- Офіс омбудсмена з питань персональних даних (Office of the Privacy Commissioner of Canada);

³⁰Criminal Code (R.S.C., 1985, c. C-46) <http://laws-lois.justice.gc.ca/eng/acts/C-46/>

³¹ An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act (S.C. 2010, c. 23) <http://laws-lois.justice.gc.ca/eng/acts/E-1.6/FullText.html>

³² Secure Electronic Signature Regulations (SOR/2005-30) <http://laws-lois.justice.gc.ca/eng/regulations/SOR-2005-30/page-1.html>

³³ Electronic Commerce Protection Regulations (CRTC) (SOR/2012-36) <http://laws-lois.justice.gc.ca/eng/regulations/SOR-2012-36/page-1.html>

³⁴ Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5) <http://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-1.html>

³⁵Canada's Cyber Security Strategy <http://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/cbr-scrt-strtg/cbr-scrt-strtg-eng.pdf>

³⁶Action Plan 2010-2015 for Canada's Cyber Security Strategy <http://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf>

- Управління захисту важливих об'єктів інфраструктури та готовності до надзвичайних ситуацій Міністерства державної безпеки (Office of Critical Infrastructure Protection and Emergency Preparedness)³⁷.

Міжнародне співробітництво

- Співробітництво з США в рамках спільного Плану дій з кібербезпеки Міністерства національної безпеки США та Міністерства державної безпеки Канади;
- Співробітництво канадського Центру реагування на надзвичайні ситуації у кіберпросторі ([CCIRC](#)) з відповідними органами у США ([US-CERT](#)), Великобританії ([Gov Cert UK](#)), Австралії ([CERT Australia](#)), Новій Зеландії ([NewZealand CCIP](#));
- Співробітництво у сфері кібербезпеки в рамках FIRST, ОАД, ОБСЄ³⁸.

Співробітництво між відомствами

Управління захисту важливих об'єктів інфраструктури та готовності до надзвичайних ситуацій Міністерства державної безпеки разом з Shared Services Canada (SSC) сприяють комунікації між організаціями та бізнесом. Центр реагування на надзвичайні ситуації у кіберпросторі співпрацює з провайдерами інтернет-послуг з метою сприяння у визначенні загроз у кіберпросторі та розробки ефективних заходів з їх протидії³⁹.

³⁷Cyberwellness Profile Canada http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Canada.pdf

³⁸Там само.

³⁹Там само.

Австралія

Кримінальне законодавство у сфері кіберзлочинності

- Закон «Про внесення змін у законодавство про кіберзлочинність» (Cybercrime Legislation Amendment Act, 2012)⁴⁰;

Закони, що регулюють питання, пов'язані з кібербезпекою

- Закон «Про боротьбу зі спамом» (SPAM ACT 2003)⁴¹.

Програмні документи

- Стратегія кібербезпеки Австралії (2009)⁴²;
- Національний план по боротьбі з кіберзлочинністю⁴³;
- План дій з діяльності у інформаційному середовищі – 2020⁴⁴.

Відповідальні органи

- Відділ кіберполіції та кіберрозвідки;
- Міністерство Генерального прокурора;
- Управління радіотехнічної оборони⁴⁵.

Міжнародне співробітництво

- Співробітництво у сфері кібербезпеки та реагування на надзвичайні ситуації між Міністерством національної безпеки США та Міністерством Генерального прокурора Австралії;
- Співробітництво в рамках дво- та багатосторонніх угод між національним центром швидкого реагування на надзвичайні ситуації у кіберпросторі ([CERT Australia](#)) та державними і приватними центрами реагування по всьому світу⁴⁶.

⁴⁰ Cybercrime Legislation Amendment Act 2012 <https://www.comlaw.gov.au/Details/C2012A00120>

⁴¹ Spam Act, 2003 http://www.austlii.edu.au/au/legis/cth/consol_act/sa200366/

⁴² <https://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf>

⁴³ National Plan to Combat Cybercrime

<https://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Documents/National%20Plan%20to%20Combat%20Cybercrime.pdf>

⁴⁴ National Security Information Environment Roadmap:2020 Vision

http://web.archive.org/web/20110311232850/http://www.dpmc.gov.au/national_security/docs/national_security_information_environment_roadmap.pdf

⁴⁵ Cyberwellness Profile Australia http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Australia.pdf

⁴⁶ Там само.

Співробітництво між відомствами

Через платформи [Govdex](#) та [Govshare](#) держава заохочує державні органи та приватний сектор обмінюватись знаннями та ресурсами з метою пошуку ефективних, дієвих та інноваційних рішень для кібербезпеки⁴⁷.

В рамках мережі обміну інформацією [TISN](#) відбувається обмін ресурсами між державним та приватним сектором⁴⁸.

⁴⁷Cyberwellness Profile Australia http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Australia.pdf

⁴⁸Там само.

Ізраїль

Кримінальне законодавство у сфері кіберзлочинності

- Закон «Про комп'ютери» (1995)⁴⁹.

Закони, що регулюють питання, пов'язані з кібербезпекою

- Закон «Про електронні підписи»⁵⁰;
- Законопроект «Про електронну комерцію»⁵¹;
- Закон «Про безпеку державних органів» (1998);
- Резолюція В/84 «Про обов'язок захищати комп'ютеризовані системи Ізраїлю»⁵².

Програмні документи

Наріжними каменями політики Ізраїлю у сфері кібербезпеки є Національна кібер-ініціатива 2010 та [Резолюція уряду №3611](#) від 7 серпня 2011 року, яка є планом дій Національної кібер-ініціативи⁵³.

Відповідальні органи

- [Національне кібербюро Ізраїлю](#);
- Національний департамент інформаційної безпеки⁵⁴.

Міжнародне співробітництво

- Членство в ініціативі Міжнародного телекомунікаційного союзу [ITU-IMPACT](#);
- Співробітництво Національного кібербюро з відповідними органами закордоном.

Співробітництво між відомствами

Національне кібербюро співпрацює з іншими державними органами, приватним сектором, науковцями, промисловими компаніями та іншими органами, пов'язаними з кібербезпекою⁵⁵.

⁴⁹http://law.co.il/media/computer-law/computers_law_nevo.pdf

⁵⁰Electronic Signature Law, 5761 – 2001 <http://www.justice.gov.il/NR/rdonlyres/7554DECF-BA18-465E-8565-D8F090F56018/0/3.pdf>

⁵¹Electronic Commerce Bill, 5768 – 2008 <http://law.huji.ac.il/upload/ecommerce.pdf>

⁵²Cyberwellness Profile Israel http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Israel.pdf

⁵³Там само.

⁵⁴Там само.

Естонія

Кримінальне законодавство у сфері кіберзлочинності

- Кримінальний кодекс⁵⁶

Закони, що регулюють питання, пов'язані з кібербезпекою

- Закон «Про електронні підписи»⁵⁷;
- Закон «Про захист персональних даних»⁵⁸;
- Закон «Про електронні повідомлення»⁵⁹;
- Закон «Про електронні платіжні системи»⁶⁰;
- Закон «Про публічну інформацію»⁶¹;
- Закон «Про послуги інформаційного суспільства»⁶².

Програмні документи

Основою політики Естонії у сфері кібербезпеки є [Стратегія кібербезпеки](#) 2014 року.

Щорічно Управління інформаційних систем публікує доповіді про кібербезпеку⁶³.

Відповідальні органи

- Управління інформаційних систем ([RIA](#));
- [CERT Estonia](#);

⁵⁵Cyberwellness Profile Israel http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Israel.pdf

⁵⁶Penal Code

<http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30068K10&keel=en&pg=1&ptyyp=RT&tyyp=X&query=karistusseadustik>

⁵⁷Digital Signatures Act

<http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30081K6&keel=en&pg=1&ptyyp=RT&tyyp=X&query=digitaalalkirja>

⁵⁸Personal Data Protection Act

<http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=XXX041K1&keel=en&pg=1&ptyyp=RT&tyyp=X&query=isikuandmete+kaitse+seadus>

⁵⁹Electronic Communications Act

<http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X90001K7&keel=en&pg=1&ptyyp=RT&tyyp=X&query=elektroonilise+side+seadus>

⁶⁰Payment Institutions and E-money Institutions Act

<http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=2012X09&keel=en&pg=1&ptyyp=RT&tyyp=X&query=makseasutuste>

⁶¹Public Information Act

<http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X40095K5&keel=en&pg=1&ptyyp=RT&tyyp=X&query=avaliku+teabe>

⁶²Information Society Services Act

<http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X80043k1&keel=en&pg=1&ptyyp=RT&tyyp=X&query=info%FChiskonna>

⁶³2014 Annual Report Cyber Security Branch of the Estonian Information System Authority

https://www.ria.ee/public/Kuberturvalisus/RIA-Kyberturbe-aruanne-2014_ENG.pdf

- Департамент захисту важливих об'єктів інфраструктури ([CIIP](#)).

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 ([NATO CCDCOE](#));
- Співробітництво з [TERENA](#), [TF-CSIRT](#);
- Дочірній статус CERT Estonia у [FIRST](#)⁶⁴.

Співробітництво між відомствами

[X-Road](#) є національною платформою для співробітництва з державним та приватним сектором у сфері кібербезпеки.

⁶⁴Cyberwellness Profile Republic Of Estonia http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Estonia.pdf

Німеччина

Кримінальне законодавство у сфері кіберзлочинності

- Кримінальний кодекс (1998)⁶⁵.

Закони, що регулюють питання, пов'язані з кібербезпекою

- Закон «Про електронні підписи» (2001)⁶⁶;
- Закон «Про захист федеральних даних» (2009)⁶⁷;
- Закон «Про Федеральну службу інформаційної безпеки» (2009)⁶⁸;
- Закон «Про свободу інформації» (2013)⁶⁹;
- Закон «Про посилення безпеки федеральних інформаційних технологій» (2009)⁷⁰.

Програмні документи

Основою політики Німеччини у сфері кібербезпеки є [Стратегія кібербезпеки](#) 2011 року та [Національний план із захисту інформаційної інфраструктури](#).

Відповідальні органи

- Федеральне управління інформаційної безпеки ([BSI](#)).

Міжнародне співробітництво

- Співробітництво із США в рамках двосторонніх зустрічей, присвячених питанням кібербезпеки;
- Співробітництво з [TERENA](#), [FIRST](#), [ENISA](#), [APCERT](#), [EGC](#)⁷¹.

⁶⁵German Criminal Code http://www.gesetze-im-internet.de/englisch_stgb/index.html

⁶⁶Gesetzüber Rahmenbedingungen für elektronische Signaturen http://www.gesetze-im-internet.de/sigg_2001/BJNR087610001.html

⁶⁷Bundes daten schutz gesetz http://www.gesetze-im-internet.de/bdsg_1990/

⁶⁸Gesetzüber das Bundes amt für Sicherheit in der Informations technik http://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html

⁶⁹Gesetz zur Regelung des Zugangs zu Informationen des Bundes <http://www.gesetze-im-internet.de/ifg/index.html>

⁷⁰ 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

⁷¹Cyberwellness Profile Germany http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Germany.pdf

Співробітництво між відомствами

- Спільна ініціатива Федерального управління захисту громадян та допомоги в надзвичайних ситуаціях (BBK) та Федерального управління інформаційної безпеки (BSI) зі створення Інтернет-платформи із захисту важливих об'єктів інфраструктури;
- Програма «Союз заради кібербезпеки» Федерального управління інформаційної безпеки, Федеральної Асоціації інформаційних технологій, телекомунікації та нових ЗМІ, метою якої є інформування про надзвичайні ситуації у кіберпросторі⁷².

⁷²Cyberwellness Profile Germany http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Germany.pdf

Швеція

Кримінальне законодавство у сфері кіберзлочинності

- §10 (а) розділу 16 Кримінального кодексу⁷³.

Закони, що регулюють питання, пов'язані з кібербезпекою

- Закон «Про електронні підписи»⁷⁴;
- Закон «Про захист персональних даних»⁷⁵;
- Закон «Про електронні повідомлення»⁷⁶;
- Закон «Про доступ до публічної інформації»⁷⁷;
- Закон «Про електронні оголошення»⁷⁸;

Програмні документи

Основою політики Швеції у сфері кібербезпеки є [Стратегія з покращення інтернет-безпеки](#) 2006 року та [План дій з інформаційної безпеки](#) 2012 року.

Відповідальні органи

- Збройні сили Швеції;
- Служба безпеки Швеції;
- Управління інформаційного забезпечення та кібербезпеки;
- Національне бюро розслідувань⁷⁹.

Міжнародне співробітництво

- Співробітництво [CERT-SE](#) з іноземними партнерами в рамках [FIRST](#), [ENISA](#), [IGE](#), ОБСЄ, Групи урядових експертів ООН, Північно-Балтійської Вісімки (NB8)⁸⁰.

Співробітництво між відомствами

CERT-SE є національною платформою для співробітництва з державними органами у сфері кібербезпеки.

⁷³Brottsbalk <http://www.notisum.se/rnp/sls/lag/19620700.htm>

⁷⁴ Qualified Electronic Signatures Act (SFS 2000:832)

<http://www.pts.se/upload/Documents/SE/engelsk%20oversattning%20av%20lag%20elektroniska%20signaturer.pdf>

⁷⁵Person upp giftslag (1998:204) <http://www.notisum.se/rnp/sls/lag/19980204.htm>

⁷⁶ Lag (2003:389) om elektronisk kommunikation http://www.wipo.int/wipolex/en/text.jsp?file_id=242555

⁷⁷Offentlighets-ochsekretesslag (2009:400) http://www.wipo.int/wipolex/en/text.jsp?file_id=242336

⁷⁸ Lag (1998:112) omansvar för elektronisk aan slagstavlor <http://www.notisum.se/rnp/sls/lag/19980112.HTM>

⁷⁹Cyberwellness Profile Sweden http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Sweden.pdf

⁸⁰Там само.

Фінляндія

Кримінальне законодавство у сфері кіберзлочинності

- Кримінальний кодекс⁸¹.

Закони, що регулюють питання, пов'язані з кібербезпекою

- Закон «Про конфіденційність електронних повідомлень»⁸².

Програмні документи

Основою політики Фінляндії у сфері кібербезпеки є [Стратегія кібербезпеки](#) 2013 року, яка визначає основні цілі та способи реагування на загрози, спрямовані проти кібербезпеки Фінляндії. Планом дій у даній сфері є [Програма інформаційного суспільства Фінляндії](#).

Відповідальні органи

- Комітет з питань безпеки (на стадії створення);
- Національне агентство допомоги в надзвичайних ситуаціях⁸³.

Міжнародне співробітництво

- Співробітництво з іншими державами в рамках [FIRST](#), Міжнародного телекомунікаційного союзу, Групи центрів комп'ютерного реагування на надзвичайні ситуації європейських держав ([EGC group](#))⁸⁴.

⁸¹ The Criminal Code of Finland <http://finlex.fi/en/laki/kaannokset/1889/en18890039.pdf>

⁸² Act on the Protection of Privacy in Electronic Communications
<http://www.finlex.fi/en/laki/kaannokset/2004/en20040516.pdf>

⁸³ Cyberwellness Profile Finland http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Finland.pdf

⁸⁴ Там само.

Великобританія

Кримінальне законодавство у сфері кіберзлочинності

- Закон «Про боротьбу з комп'ютерними злочинами» (1990)⁸⁵;
- Закон «Про захист даних» (1998)⁸⁶;
- Закон «Про шахрайство» (2006)⁸⁷.

Закони, що регулюють питання, пов'язані з кібербезпекою

- Постанова «Про Уповноваженого з питань інформації».

Програмні документи

Основою державної політики у сфері кібербезпеки є [Національна стратегія кібербезпеки](#) 2011 року.

Відповідальні органи

- Управління кібербезпеки та інформаційного забезпечення;
- Центр захисту національної інфраструктури.

Міжнародне співробітництво

Співробітництво в рамках [FIRST](#), Міжнародного телекомунікаційного союзу, Групи центрів комп'ютерного реагування на надзвичайні ситуації європейських держав ([EGC group](#)), [TF-CSIRT](#), НАТО, ОБСЄ, ООН⁸⁸.

Співробітництво між відомствами

Управління кібербезпеки та інформаційного забезпечення координує партнерство з приватним сектором. Центр захисту національної інфраструктури здійснює обміни інформацією з приватними компаніями, які відповідають за важливі об'єкти інформаційної інфраструктури⁸⁹.

⁸⁵Computer Misuse Act 1990 <http://www.legislation.gov.uk/ukpga/1990/18>

⁸⁶Data Protection Act 1998 <http://www.legislation.gov.uk/ukpga/1998/29>

⁸⁷Fraud Act 2006 <http://www.legislation.gov.uk/ukpga/2006/35>

⁸⁸Cyberwellness Profile United Kingdom http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/United_Kingdom.pdf

⁸⁹Там само.

Франція

Кримінальне законодавство у сфері кіберзлочинності

- Закон «Про електронну економіку» №2004-575 від 21 червня 2004 року⁹⁰;
- Конвенція Ради Європи про кіберзлочинність.

Закони, що регулюють питання, пов'язані з кібербезпекою

- Закон «Про комп'ютери, файли та свободи»⁹¹;
- Закон «Про електронні докази та електронні підписи»⁹²;
- Указ від 2011 року та міжвідомча заява №1300 «Про захист конфіденційної інформації, пов'язаної з обороною держави»⁹³;
- Декрет №2009-834 «Про створення Служби безпеки національної інформаційної системи»⁹⁴;
- Рекомендація №901 від березня 1994 «Про захист інформаційних систем»⁹⁵.

Програмні документи

В основі діяльності Франції в кіберпросторі лежить [Стратегія безпеки та оборони інформаційних систем](#) 2011 року.

Відповідальний орган

Національна служба безпеки інформаційних технологій ([ANSSI](#)).

Міжнародне співробітництво

- Співробітництво з Федеральним управлінням інформаційної безпеки Німеччини ([BSI](#));

⁹⁰Loi №2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique
http://www.wipo.int/wipolex/en/text.jsp?file_id=276258

⁹¹Loi № 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
http://www.legifrance.gouv.fr/affichTexte.do?jsessionid=2A2EF6C91837B853539CEB3201AA05F5.tpdjo14v_1?cidTexte=JORFTEXT000000886460&dateTexte=20121203

⁹² Code civil <http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070721&dateTexte=20121115>

⁹³Arrêté du 30 novembre 2011 portant approbation de l'instruction générale interministérielle №1300 sur la protection du secret de la défense nationale

<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000024892134&categorieLien=id>

⁹⁴Décret № 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé «Agence nationale de la sécurité des systèmes d'information»

<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020828212>

⁹⁵ Recommandation pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense http://circulaire.legifrance.gouv.fr/pdf/2009/04/cir_2007.pdf

- Співробітництво з британською Групою із забезпечення прихованої роботи засобів зв'язку і електронного устаткування ([CESG](#))
 - Співробітництво з Агентством національної безпеки та Міністерством національної безпеки США;
 - Угода між Францією та Великобританією про співробітництво у сфері безпеки і оборони;
 - Угода між Францією та Естонією про співробітництво у сфері кібероборони⁹⁶;
 - Співробітництво в рамках НАТО, ОБСЄ, ЄС, [FIRST](#)⁹⁷.
-

⁹⁶Cyberwellness Profile France http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/France.pdf

⁹⁷Там само.

Австрія

Кримінальне законодавство у сфері кіберзлочинності

Кримінальний кодекс⁹⁸.

Закони, що регулюють питання, пов'язані з кібербезпекою

- Закон «Про електронну комерцію»⁹⁹;
- Федеральний закон «Про електронні підписи»¹⁰⁰;
- Закон «Про електронний уряд»¹⁰¹;
- Федеральний закон «Про захист персональних даних»¹⁰².

Програмні документи

Засади політики Австрії у сфері кібербезпеки визначають [Національна стратегія безпеки інформаційно-комунікаційних технологій](#) 2012 року та [Стратегія кібербезпеки](#) 2013 року.

Відповідальні органи

- Керівна група з кібербезпеки;
- Експертний центр з питань кіберзлочинності¹⁰³.

Міжнародне співробітництво

- Участь у навчаннях НАТО [CWIX](#);
- Співробітництво з Чехією в рамках Платформи кібербезпеки, створеної у 2013¹⁰⁴;
- Участь в [FIRST](#), [ENISA](#), НАТО (участь у кіберкоаліції НАТО), ОБСЄ, ЄС, ООН.

⁹⁸Bundes recht konsolidiert: Gesamte Recht svorschrift für Strafgesetzbuch, Fassung vom 14.07.2015 www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296

⁹⁹ Federal Act governing certain legal aspects of electronic commercial and legal transaction http://www.ris.bka.gv.at/Dokumente/ErV/ERV_2001_1_152/ERV_2001_1_152.pdf

¹⁰⁰ Federal Electronic Signature Law http://www.ris.bka.gv.at/Dokumente/ErV/ERV_1999_1_190/ERV_1999_1_190.pdf

¹⁰¹ The Austrian E-Government Act http://www.a-sit.at/pdfs/e-govg_engl.pdf

¹⁰² Federal Act concerning the Protection of Personal Data http://www.ris.bka.gv.at/Dokumente/ErV/ERV_1999_1_165/ERV_1999_1_165.pdf

¹⁰³Cyberwellness Profile Austria http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Austria.pdf

¹⁰⁴Там само.

Співробітництво між відомствами

- Програма державно-приватного партнерства у сфері захисту важливих об'єктів інфраструктури, метою якої є розробка всеохоплюючої стратегії та конкретних заходів із об'єднання державних та приватних операторів інфраструктури «під одним дахом»¹⁰⁵.

¹⁰⁵Cyberwellness Profile Austria http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Austria.pdf

Чехія

Кримінальне законодавство у сфері кіберзлочинності

Кримінальне законодавство Чехії не містить положень, які регулюють питання, пов'язані з кіберзлочинністю та кібербезпекою.

Закони, що регулюють питання, пов'язані з кібербезпекою

Закон «Про кібербезпеку та внесення змін до пов'язаних законів»¹⁰⁶.

Програмні документи

В основі політики Чехії щодо кібербезпеки лежить [Національна стратегія кібербезпеки 2015-2020](#).

Відповідальні органи

- Управління національної безпеки (Národní bezpečnostní úřad);
- Національний центр кібербезпеки¹⁰⁷.

Міжнародне співробітництво

- Участь у [FIRST](#), [TRUSTED INTRODUCER](#), [EUROPOL](#), [TERENA](#), [ENISA](#);
- Участь у Об'єднаному центрі передових технологій з кібероборони НАТО ([NATO CCDCOE](#));
- Співробітництво з Австрією в рамках Платформи кібербезпеки, створеної у 2013¹⁰⁸.

¹⁰⁶Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) <http://www.nbu.cz/cs/pravni-predpisy/zakon-o-kyberneticke-bezpecnosti-a-o-zmene-souvisejicich-zakonu-zakon-o-kyberneticke-bezpecnosti/>

¹⁰⁷Cyberwellness Profile Czech Republic http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Czech_Republic.pdf

¹⁰⁸Там само.

Італія

Кримінальне законодавство у сфері кіберзлочинності

Кримінальний кодекс¹⁰⁹.

Закони, що регулюють питання, пов'язані з кібербезпекою

- Закон «Про електронну комерцію»¹¹⁰;
- Закон «Про електронні повідомлення»¹¹¹;
- Закон «Про електронні підписи»¹¹².

Програмні документи

Національна кіберстратегія Італії ґрунтується на [Основах національної стратегії щодо безпеки кіберпростору](#) 2013 року та [Національному плані із захисту кіберпростору та безпеки інформаційно-комунікаційних технологій](#) 2013 року.

Відповідальний орган

Голова Ради міністрів (глава уряду) несе відповідальність за імплементацію національної стратегії кібербезпеки та плану дій.

Міжнародне співробітництво

- Участь в ініціативі Міжнародного телекомунікаційного союзу «Міжнародне багатостороннє партнерство проти кіберзагроз» ([ITU-IMPACT](#));
- Участь у Європейській платформі мережевої та інформаційної безпеки ([NIS](#))¹¹³.

¹⁰⁹Codice Penale <http://www.studiocataldi.it/codicepenale/>

¹¹⁰Attuazione del la direttiva 2000/31/CE relativa a tal unia spetti giuri dici dei servizi del la società del l'informazionen elmercato interno, con particolare riferimento al commercio elettronico <http://www.parlamento.it/parlam/leggi/deleghe/03070dl.htm>

¹¹¹Codice del le comunicazioni elettroniche <http://www.parlamento.it/parlam/leggi/deleghe/03259dl.htm>

¹¹²Attuazione del la direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche <http://www.camera.it/parlam/leggi/deleghe/testi/02010dl.htm>

¹¹³Cyberwellness Profile Italy http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Italy.pdf

Латвія

Кримінальне законодавство у сфері кіберзлочинності

Кримінальний кодекс¹¹⁴.

Закони, що регулюють питання, пов'язані з кібербезпекою

- Закон «Про національну інформаційну систему»¹¹⁵;
- Закон «Про електронні повідомлення»¹¹⁶;
- Закон «Про безпеку інформаційних технологій»¹¹⁷.

Програмні документи

Основоположними документами, що визначають політику Латвії у сфері кібербезпеки, є [Концепція національної безпеки](#) 2011 року та [Стратегія кібербезпеки Латвії 2014-2018](#).

Відповідальний орган

- Національна рада безпеки інформаційних технологій;
- Міністерство оборони.

Міжнародне співробітництво

- Партнерство [CERT.LV](#) з європейськими партнерами;
- Співробітництво з ЄС, НАТО, скандинавськими та балтійськими країнами, США¹¹⁸.

¹¹⁴Krimināl likums <http://m.likumi.lv/doc.php?id=88966>

¹¹⁵Valsts informācijas sistēmu likums <http://likumi.lv/doc.php?id=62324>

¹¹⁶Elektronis kosakaru likums <http://likumi.lv/doc.php?id=96611>

¹¹⁷Informācijas tehnoloģi jdrošības likums <http://likumi.lv/doc.php?id=220962>

¹¹⁸Cyberwellness Profile Republic of Latvia http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Latvia.pdf

Нідерланди

Кримінальне законодавство у сфері кіберзлочинності

Кримінальний кодекс¹¹⁹.

Закони, що регулюють питання, пов'язані з кібербезпекою

- Закон «Про електронні підписи»;
- Закон «Про захист даних»¹²⁰.

Програмні документи

В основі кіберстратегії Королівства Нідерландів лежать [Національна стратегія кібербезпеки](#) та [Оборонна кіберстратегія](#). В якості плану дій прийнята [Програма дій 2014-2016](#).

Відповідальні органи:

- Національне управління з питань безпеки та контртероризму;
- Національний центр кібербезпеки¹²¹.

Міжнародне співробітництво

- Партнерство з Групою центрів комп'ютерного реагування на надзвичайні ситуації європейських держав ([EGC group](#)), [CSIRT](#);
- Співробітництво Національного центру кібербезпеки з [FIRST](#), [TERENA](#), [ENISA](#)¹²².

Співробітництво між відомствами

Національна програма передбачає співробітництво з державним і приватним секторами у сфері кібербезпеки через Національний центр кібербезпеки¹²³.

¹¹⁹Wetboek van Strafrecht http://wetten.overheid.nl/BWBR0001854/volledig/geldigheidsdatum_23-11-2012#Opschrift

¹²⁰ Personal Data Protection Act

http://www.coe.int/t/dghl/standardsetting/dataprotection/national%20laws/NL_DP_LAW.pdf

¹²¹Cyberwellness Profile the Netherlands http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Netherlands.pdf

¹²²Cyberwellness Profile the Netherlands http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Netherlands.pdf

¹²³Там само.

Іспанія

Кримінальне законодавство у сфері кіберзлочинності

Кримінальний кодекс¹²⁴.

Закони, що регулюють питання, пов'язані з кібербезпекою

- Закон «Про електронні підписи»;
- Закон «Про захист персональних даних»¹²⁵.

Програмні документи

Засади державної політики у сфері кібербезпеки визначає [Національна стратегія кібербезпеки](#) 2013 року.

Відповідальні органи

- Національний центр криптології;
- Національний центр розвідки;
- Національна служба безпеки¹²⁶.

Міжнародне співробітництво

- Участь в ініціативі Міжнародного телекомунікаційного союзу «Міжнародне багатостороннє партнерство проти кіберзагроз» ([ITU-IMPACT](#));
- Співробітництво з [FIRST](#), [TERENA](#), [ENISA](#), [Trusted Introducer](#), [APWG](#);
- Співробітництво Комп'ютерної групи реагування на надзвичайні ситуації Іспанії ([CCN-CERT](#)) з іноземними партнерами¹²⁷.

¹²⁴Código Penal (Ley Orgánica Nº 10/1995, de 23 de noviembre de 1995)
http://www.wipo.int/wipolex/en/text.jsp?file_id=181459

¹²⁵ Organic Law 15/1999 of 13 December on the Protection of Personal Data

<http://www.google.ch/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCAQFjAA&url=http%3A%2F%2Fwww.legislationline.org%2Fdocuments%2Fid%2F9044&ei=HbjIVPzXCMOdPbmBgZAG&usg=AFQjCNGd5kvCv7F99hymukX4cQhg3fSJA&sig2=c16AdS8RIplyHZWCwlmUTA&bvm=bv.84607526.d.ZWU>

¹²⁶Cyberwellness Profile Spain http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Spain.pdf

¹²⁷Там само.

Польща

Кримінальне законодавство у сфері кіберзлочинності

Кримінальний кодекс¹²⁸.

Закони, що регулюють питання, пов'язані з кібербезпекою

- Закон «Про електронні підписи»¹²⁹;
- Закон «Про захист персональних даних»¹³⁰;
- Закон «Про комп'ютеризацію операцій підприємств, що виконують державні завдання»¹³¹;
- Закон «Про електронні платіжні інструменти»¹³²;
- Закон «Про надання послуг через електронні засоби»¹³³.

Програмні документи

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

Відповідальні органи

- Міністерство адміністрації та впровадження цифрових технологій;
- Міністерство національної оборони;
- Служба внутрішньої безпеки¹³⁴.

¹²⁸The Penal Code https://www.imolin.org/doc/amlid/Poland_Penal_Code1.pdf

¹²⁹The 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

¹³⁰ Act of August 29, 1997 on the Protection of Personal Data

http://www.google.ch/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CCcQFjAB&url=http%3A%2F%2Fwww.gio.do.gov.pl%2Fdata%2Ffilemanager_en%2F61.doc&ei=rAjKVMXuFYfbPZ_XglAH&usg=AFQjCNEZllyrzOw0g7YIXb8XvHlwUXCOswHA&sig2=teUft7Bha_G7AwmiV3SU1g&bvm=bv.84607526.d.ZWU

¹³¹ Act of 17 February 2005 on the Computerization of Activities of Entities Performing Public Tasks

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=IwfkVOi1EonaOPntgZgE&usg=AFQjCNEZllyrzOw0g7YIXb8XvHlwUXVq-w&sig2=9h4ynjVluoZq4TzVQqmd-w&bvm=bv.84607526.d.ZWU

¹³² Act of 12 September 2002 on Electronic Payment Instruments https://www.nbp.pl/en/system_platniczy/mf.pdf

¹³³ Act of 18 July, 2002 on Providing Services by Electronic Means

https://www.itu.int/osg/spu/spam/legislation/Ustawa%20SUDE-eng_ver.pdf

¹³⁴Cyberwellness Profile Republic of Poland http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Poland.pdf

Міжнародне співробітництво

- Участь в ініціативі Міжнародного телекомунікаційного союзу «Міжнародне багатостороннє партнерство проти кіберзагроз» ([ITU-IMPACT](#));
- Співробітництво Комп'ютерних груп реагування на надзвичайні ситуації Польщі ([CERT.GOV.PL](#) і [CERT Polska](#)) з [FIRST](#), [ENISA](#), [Trusted Introducer](#), НАТО¹³⁵.

¹³⁵ Cyberwellness Profile Republic of Poland http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Poland.pdf

Стратегія кібербезпеки ЄС

[Стратегія кібербезпеки ЄС](#) 2013 року стала першим всеохоплюючим документом ЄС у даній сфері. Документ охоплює усі аспекти кіберпростору: внутрішній ринок, правосуддя, внутрішню та зовнішню політику.

Разом із Стратегією була розроблена та прийнята [законодавча пропозиція про посилення безпеки інформаційних систем ЄС](#).

Пріоритетами міжнародної політики ЄС у кіберпросторі, як їх визначає Стратегія, є:

- Свобода та відкритість: стратегія визначає принципи користування основоположними правами людини та громадянина у кіберпросторі;
- Застосування законодавства ЄС у кіберпросторі у тій самій мірі, як і у фізичному світі. Відповідальність за безпеку кіберпростору лежить на усьому глобальному суспільстві: від пересічних громадян до держав;
- Розвиток потенціалу кібербезпеки через співробітництво з міжнародними партнерами та організаціями, приватним сектором та громадянським суспільством¹³⁶.

¹³⁶EU International Cyberspace Policy http://www.eeas.europa.eu/policies/eu-cyber-security/index_en.htm

Рекомендовані до ознайомлення документи

1. Ghernaouti-Hélie S. Cybersecurity Guide for Developing Countries [Електронний ресурс] / Solange Ghernaouti-Hélie // 2009 – Режим доступу до ресурсу: <http://www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf>.
2. Levin A. Securing Cyberspace: A Comparative Review of Strategies Worldwide [Електронний ресурс] / A. Levin, P. Goodrick, D. Ilkina. – 2012. – Режим доступу до ресурсу: http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_cyber_crime_final_report.pdf.
3. Wamala F. The ITU National Cybersecurity Strategy Guide [Електронний ресурс] / Frederick Wamala. – 2011. – Режим доступу до ресурсу: <http://www.itu.int/ITU-D/cyb/cybersecurity/docs//ITUNationalCybersecurityStrategyGuide.pdf>.
4. Герке М. Понимание киберпреступности: Явление, задачи и законодательный ответ [Електронний ресурс] / Марко Герке. – 2014. – Режим доступу до ресурсу: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_R.pdf.

	Інтернет-користувачі, % населення	Кіберстратегія	План дій	Відповідальні органи	Центр реагування на надзвичайні ситуації (CIRT)	Програми співробітництва з приватним сектором
Австралія	83.00%	Стратегія кібербезпеки Австралії (2009)	Національний план боротьби з кіберзлочинністю (2013) План дій з діяльності у інформаційному середовищі – 2020	Відділ кіберполіції та кіберрозвідки Міністерство Генерального прокурора Управління радіотехнічної оборони	CERT Australia	+
Австрія	80.62%	Національна стратегія безпеки інформаційно-комунікаційних технологій (2012) Стратегія кібербезпеки (2013)	–	Керівна група з кібербезпеки Експертний центр з питань кіберзлочинності	GovCERT.AT MilCERT (військовий центр реагування на надзвичайні ситуації)	+
Великобританія	89.84%	Національна стратегія	Національна стратегія	Управління кібербезпеки та	GovCertUK	

		кібербезпеки (2011)	кібербезпеки (2011)	інформаційного забезпечення Центр захисту національної інфраструктури	CPNI (центр захисту важливих об'єктів інфраструктури) MODCERT (військова мережа)	+
Естонія	80.00%	Стратегія кібербезпеки (2014)	Стратегія кібербезпеки (2014)	Управління інформаційних систем (RIA) CERT Estonia; Департамент захисту важливих об'єктів інфраструктури (CIIP)	CERT-EE	+
Ізраїль	70.80%	Національна кібер- ініціатива (2010)	Резолюція уряду №3611 від 7 серпня 2011 року	Національне кібербюро Ізраїлю Національний департамент інформаційної безпеки	CERT GOVIL IUCC-CERT	+

Іспанія	71.57%	Національна стратегія кібербезпеки (2013)	Розділ IV Національної стратегії кібербезпеки (2013)	Національний центр криптології Національний центр розвідки Національна служба безпеки	CNN-CERT	–
Італія	58.46%	Основи національної стратегії щодо безпеки кіберпростору (2013)	Національний план із захисту кіберпростору та безпеки інформаційно-комунікаційних технологій (2013)	Голова Ради міністрів	CERT-SPC	+
Канада	85.80%	Стратегія кібербезпеки Канади (2010)	План дій стратегії кібербезпеки на 2010-2015 рр.	Королівська канадська кінна поліція Центр реагування на надзвичайні ситуації у кіберпросторі Офіс омбудсмена з питань персональних даних Управління захисту важливих об'єктів	CCIRC СТЕС (Центр оцінювання кіберзагроз)	+

				інфраструктури та готовності до надзвичайних ситуацій Міністерства державної безпеки		
Латвія	75.23%	Концепція національної безпеки (2011) Стратегія кібербезпеки Латвії 2014-2018.	Політика кібербезпеки Латвії. Координування, стратегія, пріоритети.	Національна рада безпеки інформаційних технологій Міністерство оборони	CERT-LV	+
Нідерланди	93.95%	Національна стратегія кібербезпеки Оборонна кіберстратегія	Програма дій 2014-2016	Національне управління з питань безпеки та контртероризму Національний центр кібербезпеки	Національний центр кібербезпеки (NCSC)	+
Німеччина	83.96%	Стратегія кібербезпеки (2011)	Національний план із захисту інформаційної інфраструктури	Федеральне управління інформаційної безпеки	CERT Bund	+
Польща	62.85%	Національна стратегія безпеки (2007)	Політика захисту кіберпростору Республіки Польща	Міністерство адміністрації та впровадження цифрових технологій	CERT.GOV.PL	—

		Політика захисту кіберпростору Республіки Польща (2013)		Міністерство національної оборони Служба внутрішньої безпеки		
США	84.20%	Міжнародна стратегія для кіберпростору «Процвітання, безпека, відкритість у мережевому світі» (2011) Кіберстратегія Міністерства оборони від квітня 2015 року	Міжвідомчий план дій з кібербезпеки систем управління План дій з посилення кібербезпеки найважливіших об'єктів інфраструктури (2014) План дій з забезпечення кібербезпеки систем енергопостачання	Координатор органів виконавчої влади з питань кібербезпеки Міністерство національної безпеки Міністерство Оборони	US CERT ICS-CERT	+
Фінляндія	91.51%	Стратегія кібербезпеки (2013)	Програма інформаційного суспільства Фінляндії	Комітет з питань безпеки (на стадії створення) Національне	CERT-FI	–

				агентство допомоги в надзвичайних ситуаціях		
Франція	81.92%	Стратегія безпеки та оборони інформаційних систем (2011)	–	Національна служба безпеки інформаційних технологій	CERT-FR	+
Чехія	74.11%	Національна стратегія кібербезпеки 2015-2020	–	Управління національної безпеки Національний центр кібербезпеки	GovCert.CZ CSIRT.CZ	–
Швеція	94.78%	Стратегія з покращення інтернет-безпеки (2006)	План дій з інформаційної безпеки (2012)	Збройні сили Швеції Служба безпеки Швеції Управління інформаційного забезпечення та кібербезпеки Національне бюро розслідувань	CERT-SE	–

Інформацію підготувала Катерина Пенькова,
аналітик ЄІДЦ