деструктивного змісту та агітаційних ресурсів спрямованих на виправдання дій росії;

– проведення загальної та індивідуальної профілактично-роз'яснювальної роботи серед незахищених та схильних

– для впливу верств населення з метою недопущення подібних випадків; цілеспрямована робота з батьками, учителями та викладачами для роз'яснення способів виявлення дітей підданих деструктивному впливу та методам проведення профілактичної роботи серед молоді.

_____

1. «Флешмоб» від ПВК «Редан» так і не розгорнувся за рф-сценарієм. URL: https://www.ukrinform.ua/rubric-ato/3676617-pvk-redan-ranise-molodnak-bivsa-na-tancah-a-teper-v-trc.html.
2. «ПВК Редан» в Україні: чергова поразка російських провокаторів. URL: https://informator.ua/uk/pvk-redan-v-ukrajini-chergova-porazka-rosiyskih-provokatoriv.
3. «Редан»: чому російська субкультура поширюється в Україні. URL: https://www.radiosvoboda.org/a/pavuky-redan-subkultura-biyky/32292295.html.
4. ПВК «Редан»: чому підлітки влаштовують масові бійки, як їх зупинити і до чого тут Росія. URL: https://24tv.ua/pvk-redan-ukrayini-chomu-pidlitki-vlashtovuyut-biyki-yak-tse_n2264503.

УДК 342.95+004
DOI: 10.31733/17-03-2023-521-524

Володимир ПЯДИШЕВ
професор кафедри кібербезпеки
та інформаційного забезпеченння
Одеського державного
університету внутрішніх справ,
доктор юридичних наук, професор

Олександр ПРОЦЕНКО
магістрант
Одеського державного
університету внутрішніх справ

ЄВРОПЕЙСЬКИЙ ПІДХІД ДО ПИТАНЬ БОРОТЬБИ З КІБЕРЗАГРОЗАМИ

Сьогодні саме українські фахівці набувають безпрецедентний досвід боротьби з кіберзагрозами. Проте у цій справі не можна нехтувати досвідом відповідних служб інших держав, зокрема, зі складу Євросоюзу.

Правовою основою боротьби з кіберзагрозами в країнах Євросоюзу є «Регламент (ЄС) 2021/887 Європейського Парламенту та Ради від 20 травня 2021 року про заснування Європейського промислового, технологічного та дослідницького центру компетенції з кібербезпеки та мережі національних координаційних центрів» [1]. Проте кожна окрема держава через власні причини більшу увагу звертає на розвиток тих або інших напрямів.

Австрія. У документі «Стратегія кібербезпеки Австрії» [2] окремий інтерес становлять відповідні принципи:

– Всеосяжна політика кібербезпеки;

– Комплексна політика кібербезпеки має наголошувати на поділі завдань між державою, економікою, академічними колами та громадянським суспільством;

– Проактивна політика кібербезпеки означає роботу щодо запобігання загрозам кіберпростору та людям у кіберпросторі;

– Верховенство права: управління кібербезпекою має гарантувати дотримання прав людини, зокрема конфіденційність;

– Субсидіарність: кібербезпека є законним активом. Тому держава не може брати на себе виняткову відповідальність за захист кіберпростору.

З ним її ділять власники та оператори інформаційних та комунікаційних технологій:

– Саморегулювання: слід прагнути підвищення рівня захисту з допомогою власних ініціатив учасників. Проте завдання держави залишається створення нормативно-правової

бази захисту ІКТ;

– Пропорційність: Заходи щодо підвищення рівня захисту та відповідні витрати повинні бути пропорційні відповідному ризику та можливостям обмеження цих загроз.

Бельгія. У документі «Національна оцінка ризиків Бельгії» [3] зазначено, що у 2018 році Національний кризовий центр (NCCN) координував великомасштабну оцінку ризиків для Бельгії на період 2018-2023 років. Було залучено 100 експертів від 40 різних громадських організацій. Опускаючи деякі елементи складного процесу здійснення оцінки, а також результати (цікаві насамперед самим бельгійцям) зосередимося на прийнятих до уваги аспектах впливу на націю: 1) вплив на людину: кількість загиблих, кількість поранених; 2) соціальні наслідки: збої в роботі життєво важливих служб; 3) вплив на навколишнє середовище: площа поразки (км²), шкода екосистемі, можливий ступінь відновлення; фінансові втрати, зростання безробіття, скорочення кількості активних компаній.

Естонія. На державному рівні захист мереж державного та приватного секторів та інформаційних систем, необхідних для функціонування естонської держави, організує Управління інформаційних систем (RIA) [4].

Послуги, необхідні для суспільства, визначено у розділі 3 Закону про кібербезпеку (Cybersecurity Act). Тут, зокрема, визначено мету та діяльність із захисту критичної інформаційної інфраструктури.

Стратегія кібербезпеки на 2019-2022 роки була присвячена стійкості та зосереджена в основному на таких цілях: створення стійкого цифрового суспільства, підтримка індустрії кібербезпеки, досліджень та розробок, участь як провідний міжнародний учасник та підвищення обізнаності суспільства про кіберграмотність. Основними принципами стратегії є:

– захист та заохочення прав та свобод у кіберпросторі;

– кібербезпека розглядається як фактор та підсилювач швидкого цифрового розвитку Естонії;

– для Естонії визнається виняткова важливість забезпечення безпеки криптографічних рішень;

– стверджується, що прозорість та суспільна довіра мають основне значення для цифрового суспільства.

Іспанія. У матеріалах Національного центру захисту інфраструктури та кібербезпеки [5] можна виділити такі моменти.

Національний центр захисту інфраструктури та кібербезпеки (CNPIC) є органом, відповідальним за просування, координацію та нагляд за всією діяльністю із захисту критичних інфраструктур та кібербезпеки, під контролем Міністерства внутрішніх справ Іспанії.

CNPIC підзвітний Державному секретарю з безпеки,Іспанське законодавство щодо захисту від критичної інфраструктури покладає відповідальність за безпечне забезпечення належного надання основних послуг на CNPIC.

Німеччина. У питаннях безпеки критично важливих інформаційних інфраструктур велику увагу приділяється взаємодії з KPMG [6]. Це одна з найбільших у світі мереж, що надають професійні послуги, та одна з аудиторських компаній. Міжнародна штаб-квартира розташована у Амстелвені (Нідерланди). Співпраця з KPMG забезпечує переваги: 1) виявлення вимог на технічному, технологічному та організаційному рівнях; 2) ефективне зниження ризику; 3) надійне юридичне становище у разі інциденту з безпекою; 4) запобігання втратам; 5) придбання нових груп клієнтів; 6) конкурентна перевага перед менш захищеними господарюючими суб'єктами; 7) належний аудит відповідно до Закону про Федеральне управління інформаційною безпекою.

Португалія. У документі «Португалія: кібербезпека» [7] привертає увагу секція «3.1. Заходи безпеки». Закон про безпеку кіберпростору на відповідні організації покладає такі обов'язки: 1) дотримуватись встановлених законом вимог безпеки; 2) повідомляти CNCS про всі інциденти, що серйозно впливають на безпеку мереж, інформаційних систем або надання послуг.

Тут же вказується, що при гарантуванні безпеки мереж та інформаційних систем повинні враховуватися такі фактори: (a) безпека систем та установок; (b) обробка інцидентів; (c) управління безперервністю бізнесу; (d) моніторинг, аудит та тестування; (e) відповідність міжнародним стандартам.

Румунія. У документі «Кібербезпека та захист критичних інфраструктур» [8] інтерес викликає розділ «Проекти щодо досліджень, розробок та інновацій»:

– Інституційні можливості та послуги з дослідження, моніторингу та прогнозування ризиків у космічному просторі – SAFESPACE;
– Кібернетичний полігон для промислових систем керування;
– Проект «Єдиний принцип» – TOOP;
– Центри компетенцій HPC (Високопродуктивні обчислення);
– Дослідження щодо визначення індикаторів та обґрунтування порогових значень щодо наслідків інцидентів кібербезпеки, необхідних для перенесення Директиви ЄС 1148/2016 у Румунії;
– Дослідження передових рішень щодо захисту критично важливих інфраструктур від кібератак – дослідження топологій «SCADA»;
– Вивчення безпеки передачі даних в інтелектуальних середовищах з упором на цілісність і справжність даних, що передаються;
– Дослідження щодо встановлення показників для вимірювання кібербезпеки на національному рівні;
– Розробка на національному рівні сценаріїв управління значними кіберинцидентами;
– Вивчення адаптивних систем раннього розпізнавання кібератак державних ресурсів.

Угорщина. У документі «Закони Угорщини про захист даних та кібербезпеку» [9] перелічено 16 законів, а також зазначено орган, уповноважений за обробку даних – Національне управління захисту даних та свободи інформації. Інтерес представляє розділ «3 Очікувані зміни в місцевому законодавстві» з коротким викладом очікуваних змін по наступним секторам:
– Повідомлення про захист даних про співробітників (про обмеження особистих прав, про інформацію, яку запитували у співробітників, про біометричну інформацію);
– Зміни щодо відеоспостереження та систем доступу;
– Зміни щодо охорони здоров'я;
– Зміни щодо фінансового сектора.

Фінляндія. У той час, як у США кібербезпека традиційно розглядалася як військова проблема, наразі вона сприймається як загроза для всіх підприємств. Країна має унікальну історію співпраці між державним та приватним секторами у сфері захисту критичної інфраструктури [10]. Деякі новаторські винаходи родом із Фінляндії, наприклад, шифрування SSH для веб-браузерів, мережі 5G, які тепер дозволяють використовувати Інтернет речей, і перша в Європі попереджувальна національна стратегія кібербезпеки. Фіни знають, що з високими технологіями пов'язаний великий ризик.

Завдяки співпраці держави з приватним сектором Фінляндія посіла своє місце в авангарді виявлення достовірних загроз, з'ясування того, що з ними робити, та здобула перемогу у битві з чорними хакерами. Сьогодні фінські експерти розбираються: які уроки в галузі кібербезпеки піднесли їм останні десятиліття і як цей досвід пристосувати до ринку США та до місцевих проблем у галузі кібербезпеки, а також які конкретно вразливості слід враховувати.

Франція. У документі «Захист критичної інфраструктури у Франції» [11] у розділі «Цілі та проблеми» перелічені та розкриті такі секції:
– Що таке критична діяльність у Франції?
– Як призначаються критичні оператори?
– Що таке критична інфраструктура?
– Якою є політика захисту критичної інфраструктури?

Цікава деталізація останньої секції: розроблена та координована Генеральним секретаріатом оборони та національної безпеки (SGDSN) політика захисту критично важливої інфраструктури (CIP) забезпечує основу, в якій державні або приватні критично важливі оператори можуть допомогти у реалізації стратегії національної безпеки з точки зору захисту від зловмисних дій (тероризм, диверсії) і природних, техногенних та медичних ризиків. Як стрижень цієї системи, критично важливі оператори повинні аналізувати ризики, яким вони наражаються, і застосовувати заходи захисту в межах своєї компетенції, зокрема, відповідно до плану VIGIPIRATE. У Білій книзі з оборони та національної безпеки 2013 року цю політику визначено як засіб підвищення стійкості (незламності) нації.

У досвіді та планах подальшого розвитку питань боротьби з кіберзагрозами у розглянутих десяти держав є невід'ємні напрями, але й багато власних, властивих саме ним.

Для забезпечення комплексного підходу до подальшого кіберзахисту України всі вони підягають ретельному вивченню.

1. Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. Site. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0887.
2. Austrian Cyber Security Strategy. Enisa.Europa.EU. Site. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf.
3. Belgian National Risk Assessment. National Crisis Center. Site. URL: https://crisiscenter.be/en/what-does-national-crisis-center-do/risk-assessment-and-protection-critical-infra structures/belgian.
4. Cyber defence of critical infrastructure. Republic of Estonia Information System Authority. URL: https://www.ria.ee/en/cyber-security/cyber-defence-critical-infrastructure/cyber-defence-critical-infrastructure.
5. National Center for Infrastructure Protection and Cybersecurity (CNPIC) – Spain. Cyber Security Intelligence. URL: https://www.cybersecurityintelligence.com/national-center-for-infra structure-protection-and-cybersecurity-cnpic-spain-7799.html.
6. Critical Infrastructure and the IT Security Act. URL: https://kpmg.com/de/en/home /services/advisory/consulting/services/cyber-security/critical-infrastructure-and-it-security-law.html.
7. Portugal: Cybersecurity. One Trust DataCuidance. URL: https://www.dataguidance.com/opinion/portugal-cybersecurity.
8. Cyber Security Protection of Critical Infrastructures. ICI Bucureşti. URL: https://www.ici.ro/en/ research-structures/cybersecurity-and-critical-infrastructure/
9. Data protection and cybersecurity laws in Hungary. CMS Law Tax Future. URL: https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/hungary.
10. Cybersecurity – Securing Critical Infrastructure. Business Finland 27.4.2022. URL: https://www.businessfinland.fi/en/whats-new/events/2022/cybersecurity--securing-critical-infrastructure.
11. The Critical Infrastructure Protection in France. SGDSN.Gouv.Fr. URL: http://www.sgdsn.gouv.fr/uploads/2017/03/plaquette-saiv-anglais.pdf

УДК 342.95+351
DOI: 10.31733/17-03-2023-524-526

Алла ГІРМАН
доцент кафедри міжнародних економічних
відносин та регіональних студій
Університету митної справи та фінансів,
кандидат політичних наук

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ У СУЧАСНИХ УМОВАХ

XXI століття з усією впевненістю можна назвати століттям постінформаційних технологій. Життя в суспільстві нерозривно пов'язане з отриманням, обробкою, зберіганням
та передачею інформації. Наразі важко уявити собі сферу людської діяльності, яка не застосовує інформаційне наповнення за допомогою дії інформаційних технологій. Окремою складовою цього процесу, очевидно, є інформаційно-телекомунікаційна мережа «Інтернет». Життя без мережі «Інтернет» для будь-якого обивателя вже неможливе.

Відносини у сфері інформаційного простору та його вплив на суб'єкти правозастосування вимагають свого ефективного регламентування і це
вже не просто визнання важливості інформації як інструменту впливу на особистість, групу людей та їх поведінку, а констатація факту необхідності адекватного регулювання її отримання, обробки, зберігання та поширення.

Розвиток інформаційних технологій, масове поширення інструментів отримання та обробки інформації (гаджети, комп'ютери, мобільні станції, поява соцмереж, відеохостингів та ін.) з одного боку суттєво полегшило доступ до отримання будь-якої інформації, включаючи особисту, але, з іншого – створило передумови для ефекту масового зловживання нею, у тому числі, вторгненням у сферу особистих прав та свобод людини.

Відсутність ефективного механізму регулювання правовідносин у мережі «Інтернет»,