Аналітична записка
з питань порівняльного законодавства Європейського Союзу, держав-членів ЄС та інших держав щодо забезпечення кібербезпеки*

Анотація. *Проведено порівняльний аналіз законодавства Європейського Союзу, окремих держав-членів ЄС та інших держав з питань кібербезпеки. На цій основі охарактеризовано спільні та відмінні підходи до визначення правового статусу суб'єктів забезпечення кібербезпеки у конкретних державах, проаналізовано процедури й засоби захисту державних електронних інформаційних ресурсів від сучасних кіберзагроз, розкрито окремі особливості забезпечення кібербезпеки найвразливіших сфер суспільного життя.*

Досліджено специфіку правового регулювання суспільних відносин у сфері кібербезпеки на рівні законодавства ЄС. У цьому контексті охарактеризовано механізм формування органів влади ЄС у сфері кібербезпеки та національних органів держав-членів ЄС, виявлено особливості формування та структуру національних стратегій забезпечення кібербезпеки. Поряд із цим проаналізовано з позицій законодавства ЄС механізм забезпечення кіберстійкості інформаційної інфраструктури на основі європейської системи сертифікації кіберризиків, стандартизації та технічної специфікації ІТ-продукції, послуг та процесів в інформаційній сфері.

За результатами проведеного дослідження сформульовано окремі рекомендації щодо удосконалення законодавства України про кібербезпеку з урахуванням євроінтеграційних зобов'язань та кращих практик у цій сфері правового регулювання. У висновках надано пропозиції для формування дорожньої карти для України щодо адаптації національного законодавства про кібербезпеку до законодавства ЄС, визначено шляхи подальшого оновлення національних стандартів України на основі стандартів ISO.

Вступ. В умовах активного розвитку сучасних інформаційно-комунікаційних технологій (далі – ІКТ), розгортання гібридних війн та масштабних кібератак забезпечення кібербезпеки стало одним з основних завдань національного законодавства більшості держав світу[1].

Нині значного прогресу у вирішенні вказаного завдання досяг Європейський Союз та більшість держав-членів ЄС, а також окремі держави, які є членами Ради Європи, проте не входять до Європейського Союзу. Йдеться, зокрема, про Велику Британію та Швейцарію, законодавство про кібербезпеку яких вже тривалий час є орієнтиром для парламентів багатьох держав.

Ще в минулому десятилітті ЄС зробив важливі кроки для забезпечення кібербезпеки та підвищення довіри до цифрових технологій.

У 2013 році прийнято Стратегію кібербезпеки Європейського Союзу, щоб керувати політикою відповіді Союзу на кіберзагрози та ризики. Із метою кращого

[1] Семенченко А. І., Плескач В. Л., Заярний О. А., Плескач М. В. Організаційно-правові механізми державного управління забезпеченням кібербезпеки та кіберзахисту України: сутність, стан та перспективи розвитку. *Проблеми програмування.* Спеціальний випуск. 2020. № 2–3. С. 279. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/180473/27-Semenchenko.pdf?sequence=1

захисту громадян в Інтернеті в 2016 році прийнято перший правовий акт ЄС у сфері кібербезпеки у формі Директиви (ЄС) 2016/1148 Європейського Парламенту та Ради. Відповідно до Директиви (ЄС) 2016/1148 встановлено вимоги щодо національних можливостей у сфері кібербезпеки; створено перші механізми для посилення стратегічної й оперативної співпраці між державами-членами; запроваджено зобов'язання щодо заходів безпеки та повідомлень про інциденти в усіх секторах, які є життєво важливими для економіки та суспільства – енергетика, транспорт, постачання та розподіл питної води, банківська справа, інфраструктура фінансового ринку, охорона здоров'я, цифрова інфраструктура, ключові постачальники цифрових послуг (пошукові системи, послуги хмарних обчислень та онлайн-ринки).

Метою цієї аналітичної записки є порівняльно-правовий аналіз законодавства ЄС, окремих держав-членів ЄС та інших держав у сфері кібербезпеки, виокремлення спільних і відмінних підходів до врегулювання окремих відносин у цій сфері правового регулювання.

Предмет дослідження не охоплює питання забезпечення кібербезпеки на внутрішньому (корпоративному) рівні, особливості захисту персональних даних, розробки політик конфіденційності, а також технічний захист інформації.

Основна частина.

Законодавство ЄС та держав-членів ЄС про кібербезпеку.

1. Правове регулювання кібербезпеки на наднаціональному рівні.

Аналогічно до інших сфер правового регулювання, в ЄС законодавство про кібербезпеку розвивається шляхом визначення на наднаціональному рівні низки питань, до врегулювання яких застосований універсальний підхід на рівні регламентів і директив ЄС та окремих аспектів забезпечення кібербезпеки, врегулювання яких віднесено до сфери відання національного законодавства держав-членів ЄС.

Важливе значення для формування законодавчих засад правового забезпечення кібербезпеки має Регламент 2019/881 Європейського Парламенту і Ради від 17 квітня 2019 року про Агентство Європейського Союзу з кібербезпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій, а також скасування Регламенту (ЄС) № 526/2013 (Акти про кібербезпеку), (далі – Регламент ЄС 881/2019)[2].

Зазначений акт набрав чинності з 27 червня 2019 року і є обов'язковим для всіх держав-членів ЄС. Відповідно до статті 1 Регламенту 2019/881 встановлено: цілі, завдання та організаційні питання, пов'язані з ENISA; рамки для створення європейських схем сертифікації кібербезпеки з метою забезпечення належного рівня кібербезпеки для продуктів ІКТ, послуг ІКТ та процесів ІКТ в СЄ, а також з метою уникнення фрагментації внутрішнього ринку щодо схеми сертифікації кібербезпеки в Союзі[3].

---

[2] Регламент 2019/881 Європейського Парламенту і Ради від 17 квітня 2019 року про Агентство Європейського Союзу з кібербезпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій, а також про скасування Регламенту (ЄС) № 526/2013 (Акти про кібербезпеку). URL: https://zakon.rada.gov.ua/laws/show/984_024-19#Text

[3] Регламент 2019/881 Європейського Парламенту і Ради від 17 квітня 2019 року про Агентство Європейського Союзу з кібербезпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних

Регламентом 2019/881 визначені повноваження, завдання та структура Агентства Європейського Союзу з кібербезпеки (далі – Агентство ЄС), встановлено обов'язки виконавчого директора, правління, експертної групи високого рівня, яка створена при ньому.

За своїм правовим статусом Агентство ЄС, відповідно до статей 38, 39 Регламенту 2019/881, є органом влади ЄС, має статус юридичної особи та відшкодовує у повному обсязі шкоду, заподіяну своїми рішеннями чи посадовими особами. Згідно з положеннями статей 3 – 12 Регламенту 2019/881 на Агентство ЄС, серед іншого, покладено виконання завдань з: розробки рекомендацій щодо сертифікації ІТ-продукції та послуг у частині кібербезпеки в межах території ЄС; проведення сертифікації національних комісарів з питань кібербезпеки; здійснення навчальних заходів з питань забезпечення кібербезпеки; підготовки щорічного висновку про стан забезпечення кібербезпеки в ЄС; затвердження Європейської рамки професійних компетентностей у відповідній сфері правового регулювання тощо.

На відміну від актів законодавства ЄС про кібербезпеку, які приймалися Європейським Парламентом до 2018 року, Регламент 2019/881 запровадив механізм забезпечення кібербезпеки за правилом стримання загроз за проєктуванням інформаційних систем, а не за захистом і протидії загрозам. Із цією метою відповідно до Регламенту 2019/881 створено Європейські рамки сертифікації кібербезпеки. Як зазначено у статті 46 Регламенту 2019/881, Європейські рамки сертифікації кібербезпеки створюються з метою покращення умов для функціонування внутрішнього ринку шляхом підвищення рівня кібербезпеки на території Союзу та забезпечення узгодженого підходу на рівні Союзу до європейських схем сертифікації кібербезпеки з метою створення єдиного цифрового ринку для продуктів ІКТ, послуг ІКТ та процесів ІКТ.

Європейські рамки сертифікації кібербезпеки встановлюють механізм для створення європейських схем сертифікації кібербезпеки та підтвердження того, що продукти ІКТ, послуги ІКТ та процеси ІКТ, які були оцінені відповідно до таких схем, відповідають визначеним вимогам безпеки з метою захисту доступності, автентичності, цілісності, конфіденційності збережених, переданих або оброблених даних, функцій, послуг, які пропонуються або доступні через ці продукти, послуги та процеси протягом їх життєвого циклу.

Основні пріоритети Європейських рамок сертифікації кібербезпеки визначаються окремою робочою програмою. Відповідно до статті 46 Регламенту 2019/881 Європейська Комісія публікує поточну робочу програму ЄС для європейської сертифікації кібербезпеки. Включення конкретних ІКТ-продуктів, ІКТ-послуг і ІКТ-процесів або їх категорій до зазначеної програми ЄС повинно бути виправдано на основі однієї або кількох із таких підстав: наявність та розробка національних схем сертифікації кібербезпеки, що охоплюють конкретну категорію продуктів ІКТ, послуг ІКТ або процесів ІКТ і, зокрема, щодо ризику фрагментації; відповідне законодавство чи політика ЄС чи держави-члена

технологій, а також про скасування Регламенту (ЄС) № 526/2013 (Акти про кібербезпеку). URL: https://zakon.rada.gov.ua/laws/show/984_024-19#Text

ЄС; ринковий попит; розвиток ландшафту кіберзагроз; запит на підготовку конкретної кандидатської схеми ECCG. Із метою ознайомлення з вимогами вказаного документа, кращими практиками у сфері кібербезпеки, опрацювання національних умов сертифікації Агентство ЄС створило окремий сайт, функціонування якого є обов'язковим згідно з Регламентом 2019/881.

Запроваджені Європейські рамки сертифікації кібербезпеки можуть визначати один або кілька таких рівнів надійності для ІКТ-продуктів, ІКТ-послуг і ІКТ-процесів: базовий, істотний, високий. Рівень достовірності повинен бути пропорційним рівню ризику, пов'язаного з передбачуваним використанням продукту ІКТ, послуги ІКТ або процесу ІКТ, з точки зору ймовірності та впливу інциденту.

Вимоги безпеки, що відповідають кожному рівню гарантії, повинні бути надані у Європейських рамках сертифікації кібербезпеки, включаючи відповідні функціональні можливості безпеки та відповідну суворість і глибину оцінки, яку має пройти продукт ІКТ, послуга ІКТ або процес ІКТ.

Сертифікат або заява ЄС про відповідність мають посилатися на технічні специфікації, стандарти та процедури, пов'язані з ними, включно з технічними засобами контролю, метою яких є зменшення ризику або запобігання інцидентам кібербезпеки.

Європейський сертифікат кібербезпеки або заява ЄС про відповідність, яка відноситься до базового рівня гарантії, повинна забезпечувати впевненість у тому, що ІКТ-продукти, ІКТ-послуги та ІКТ-процеси, для яких виданий цей сертифікат або заява ЄС про відповідність, відповідають відповідним вимогам безпеки, включаючи функції безпеки, і що вони були оцінені на рівні, призначеному для мінімізації відомих основних ризиків інцидентів і кібератак. Діяльність з оцінки, яку необхідно провести, повинна включати принаймні огляд технічної документації. Якщо такий перегляд є недоцільним, повинні бути проведені замінні оцінювальні заходи з еквівалентним ефектом.

Європейський сертифікат кібербезпеки, який відноситься до рівня надійності «високий», забезпечує гарантію того, що ІКТ-продукти, ІКТ-послуги та ІКТ-процеси, для яких видано цей сертифікат, відповідають відповідним вимогам безпеки, включаючи функції безпеки, і що вони були оцінені на рівень, призначений для мінімізації ризику найсучасніших кібератак, здійснених «акторами» зі значними навичками та ресурсами. Діяльність з оцінки, яка має бути здійснена, повинна принаймні включати: огляд для демонстрації відсутності загальновідомих вразливостей; тестування, яке демонструє, що продукти ІКТ, послуги ІКТ або процеси ІКТ правильно реалізують необхідні функціональні можливості безпеки на найсучаснішому рівні техніки; оцінку їх стійкості до кваліфікованих зловмисників за допомогою тестування на проникнення.

Таким чином, будучи первинним актом ЄС, Регламент 2019/881 закріпив для всіх держав-членів ЄС оновлений підхід щодо забезпечення кібербезпеки, який виходить із необхідності проєктування електронних інформаційних ресурсів за принципом стримання кіберзагроз, відповідності міжнародним стандартам та європейським сертифікатам безпечності ІТ-продукції.

Розвиваючи закладений Регламентом підхід до забезпечення кібербезпеки, 14 грудня 2022 року Рада ЄС затвердила Директиву (ЄС) 2022/2555 про заходи для високого загального рівня кібербезпеки в Союзі, внесення змін до Регламенту (ЄС) № 910/2014 і Директиви (ЄС) 2018/1972, а також про скасування Директиви (ЄС) 2016/1148 (NIS 2 Directive)[4], (далі – Директива 2022/2555).

Директива 2022/2555 запроваджує заходи, спрямовані на досягнення високого загального рівня кібербезпеки в Союзі з метою покращення функціонування внутрішнього ринку. Для досягнення цієї мети відповідно до Директиви: встановлено зобов'язання, які вимагають від держав-членів прийняття національних стратегій кібербезпеки та призначення або створення компетентних органів, органів управління кіберкризами, єдиних контактних пунктів з питань кібербезпеки (єдиних контактних пунктів) і груп реагування на інциденти комп'ютерної безпеки (CSIRT); запроваджено заходи з управління ризиками кібербезпеки та встановлено зобов'язання щодо звітності для суб'єктів господарювання, чия діяльність не пов'язана з управлінням критичною інфраструктурою, а також для суб'єктів, визначених як критично важливі за Директивою (ЄС) 2022/2557; встановлено правила та визначено зобов'язання щодо обміну інформацією про кібербезпеку; визначено наглядові та примусові зобов'язання держав-членів ЄС (стаття 1).

Директива ЄС 2022/2555 встановлює базову лінію для заходів з управління ризиками кібербезпеки та зобов'язань щодо звітності в усіх секторах, які входять до сфери її дії. Положення згаданої Директиви не обмежують повноваження Європейського Парламенту та національних органів законодавчої влади держав-членів ЄС щодо прийняття галузевих законодавчих актів із питань кібербезпеки, управління кіберизиками в окремих сферах суспільного життя.

Дія норм Директиви 2022/2555 не поширюється на суб'єктів, чия діяльність переважно здійснюється у сферах національної безпеки, громадської безпеки, оборони, або діяльність органів кримінальної юрисдикції (включаючи запобігання, розслідування, виявлення та переслідування кримінальних правопорушень). Проте якщо діяльність суб'єктів владних повноважень не підпадає під вказані критерії, до них застосовуються положення Директиви 2022/25 за загальним правилом.

Важливим компонентом регулювання, відповідно до Директиви 2022/2555, є діяльність суб'єктів владних повноважень у сфері кібербезпеки. Так, положеннями статей 8 – 10 щодо держав-членів ЄС визначені зобов'язання про: необхідність утворення у кожній з цих держав органів влади (відповідальних за забезпечення кібербезпеки, управління кіберінцидентами); призначення уповноважених представників держав із питань кібербезпеки. На вказаних суб'єктів владних повноважень покладаються обов'язки з моніторингу стану забезпечення кібербезпеки, розробки національних стратегій у цій сфері правового регулювання, формування політик кібербезпеки у різних сферах суспільного життя, взаємодії з Агентством Європейського Союзу з кібербезпеки,

[4] Директива (ЄС) 2022/2555 про заходи для високого загального рівня кібербезпеки в Союзі, внесення змін до Регламенту (ЄС) № 910/2014 і Директиви (ЄС) 2018/1972, а також про скасування Директиви (ЄС) 2016/1148. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555

створення національних рамок управління кіберризиками тощо. За вказаними суб'єктами владних повноважень закріплюються обов'язки зі сприяння розробці галузевих технічних специфікацій ІТ-продукції, участі в розробці національних стандартів у сфері кібербезпеки, організації проєктів публічно-приватного партнерства у вказаних напрямах суспільної діяльності, а також розробки правил забезпечення кібербезпеки у транскордонних інформаційних обмінах.

Директивою також визначені зобов'язання для держав-членів ЄС щодо розробки національних стратегій кібербезпеки. Ці нормативно-правові акти повинні надаватися для опрацювання Агентству ЄС не пізніше трьох місяців із дати їх схвалення державами-членами та переглядатися кожних п'ять років з урахуванням рівня прояву системних кіберзагроз.

Відповідно до статті 7 Директиви 2022/2555 національна стратегія кібербезпеки, серед іншого, має включати положення щодо: основних напрямів та засобів забезпечення кібербезпеки; заходів з управління ризиками, стандартизації і сертифікації продуктів та рішень, які впливають на кібербезпеку; правового статусу уповноважених органів; умов реалізації проєктів публічно-приватного партнерства у відповідній сфері; механізмів інформування уповноважених органів та Агентства ЄС про істотні кіберінциденти тощо.

Невід'ємною складовою національних стратегій є політики забезпечення кібербезпеки в окремих сферах суспільних відносин. Саме цими нормативно-правовими актами закладаються правові засади управління кіберризиками на галузевому рівні, визначаються спеціальні засоби протидії кіберзагрозам та завдання діяльності суб'єктів владних повноважень по забезпеченню кібербезпеки з урахуванням галузевих особливостей.

Відповідно до частини четвертої статті 9 Директиви 2022/2555 кожна держава-член ЄС повинна прийняти національний план реагування на масштабні інциденти та кризи у сфері кібербезпеки, де викладено цілі та заходи щодо управління масштабними інцидентами та кризами у сфері кібербезпеки. Цей план повинен визначати, зокрема: цілі національних заходів та діяльності щодо готовності; завдання та відповідальність органів управління кіберкризою; процедури управління кіберкризою, включаючи їх інтеграцію в загальну національну структуру управління кризою та канали обміну інформацією; національні заходи готовності, включаючи навчання та навчальну діяльність; відповідні державні та приватні зацікавлені сторони та залучену інфраструктуру; національні процедури та домовленості між відповідними національними органами та органами для забезпечення ефективної участі держави-члена, підтримки скоординованого управління великомасштабними інцидентами та кризами кібербезпеки на рівні ЄС[5].

Директивою 2022/2555 для держав-членів ЄС встановлюються зобов'язання щодо гарантування запровадження суб'єктами господарювання зі

[5] Директива (ЄС) 2022/2555 про заходи для високого загального рівня кібербезпеки в Союзі, внесення змін до Регламенту (ЄС) № 910/2014 і Директиви (ЄС) 2018/1972, а також про скасування Директиви (ЄС) 2016/1148. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555

значним та великим ризиком діяльності системи управління кіберінцидентами (статті 20, 21).

Управління кіберризиками та інцидентами, серед іншого, повинно включати: політики щодо аналізу ризиків та безпеки інформаційної системи; огляд інцидентів; безперервність бізнесу, наприклад керування резервним копіюванням і аварійне відновлення, а також управління кризовими ситуаціями; безпеку ланцюга постачання, включаючи пов'язані з безпекою аспекти, що стосуються відносин між кожним суб'єктом господарювання та його прямими постачальниками або постачальниками послуг; безпеку в придбанні, розробці та обслуговуванні мережевих й інформаційних систем, включаючи обробку вразливостей та розкриття інформації; політики та процедури для оцінки ефективності заходів з управління ризиками кібербезпеки; базові практики кібергігієни та навчання з кібербезпеки; політики та процедури щодо використання криптографії та, де це доречно, шифрування; безпеку людських ресурсів, політики контролю доступу та управління активами; використання рішень багатофакторної автентифікації або безперервної автентифікації, захищеного голосового, відео- та текстового зв'язку та захищених систем екстреного зв'язку в межах організації, де це доцільно.

Розвиваючи підходи до законодавчого забезпечення кібербезпеки, закладені у Регламенті ЄС 2019/881, Директива 2022/2555 легалізувала правило переходу від захисту об'єктів інформаційної інфраструктури до кіберстійкості. У зв'язку з цим зазначеною Директивою визначено окрему групу положень, що стосуються стандартизації ІТ-продукції, ІТ-послуг і процесів у частині відповідності сучасним вимогам кібербезпеки. Для досягнення цієї мети удосконалено європейський механізм сертифікації продукції, товарів, послуг на предмет відповідності вимогам кібербезпеки. Поряд із цим для держав-членів ЄС встановлено зобов'язання щодо подальшої імплементації міжнародних стандартів ISO, які стосуються кібербезпеки. Також Агентству ЄС доручено активізувати роботу з розробки саме європейських стандартів кібербезпеки, підготовки технічних специфікацій ІТ-продукції, послуг та процесів, спрямованих на забезпечення їхньої кіберстійкості.

Слід підкреслити, що Директивою 2022/2555 започатковано створення Єдиної бази кіберінцидентів, які мали прояв на території ЄС. Така база вважається офіційним джерелом інформації. Розпорядником бази визнано Агентство Європейського Союзу з кібербезпеки, а доступ до відомостей з бази надається національним органам забезпечення кібербезпеки, національним групам реагування на кіберінциденти, іншим уповноваженим органам і посадовим особам ЄС.

Таким чином, Директива 2022/2555 конкретизувала вимоги до правового забезпечення кібербезпеки у секторах, не пов'язаних із національною безпекою, громадським порядком та правоохоронною діяльністю. Водночас вказаним законодавчим актом конкретизовано низку положень Регламенту ЄС 2019/881, які стосуються стандартизації і сертифікації ІТ-продукції та послуг на предмет кіберстійкості, юрисдикційні аспекти протидії кіберзагрозам, а також вимоги до національних стратегій забезпечення кібербезпеки у державах-членах ЄС.

Важливе значення для правового забезпечення кібербезпеки в ЄС має Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних)[6]. Незважаючи на те, що предметом регулювання вказаного законодавчого акта є суспільні відносини у сфері обробки персональних даних, його нормами охоплюється значна група питань, пов'язаних із безпекою обробки персональних даних.

Основні засоби забезпечення безпеки обробки персональних даних передбачені у статті 32 Загального регламенту про захист даних. Не вдаючись до детального аналізу положень зазначеного Регламенту, оскільки це виходить за межі предмета дослідження цієї аналітичної записки, слід підкреслити, що забезпечення безпеки даних розділено фактично на дві складові – за проєктуванням інформаційних систем, призначених для обробки персональних даних, та за замовчуванням, тобто у процесі самої обробки. Такий висновок випливає із системного тлумачення положень статей 25, 32, 43 Загального регламенту про захист даних.

У значенні засобів забезпечення безпеки обробки персональних даних згаданий Регламент, серед іншого, називає: сертифікацію ІКТ, призначених для роботи з персональними даними; політики конфіденційності, інформування суб'єктів персональних даних про дії з персональними даними; стандартизацію; відповідальність контролерів, операторів та оброблювачів персональних даних тощо. Загалом Загальний регламент про захист даних приділяє значну увагу забезпеченню безпеки персональних даних на стадії розробки ІКТ, тобто за проєктуванням інформаційних продуктів. Для цього для контролерів запроваджуються обов'язки щодо можливості використання суб'єктами персональних даних псевдонімів, паролів, спеціальних ідентифікаторів, інших засобів забезпечення конфіденційності даних.

Необхідно підкреслити, що за правилами статті 3 Загального регламенту про захист даних, якщо обробка персональних даних здійснюється контролером із місцем походження в ЄС (реєстрації), або така обробка здійснюється на території ЄС, або дії контрагентів з інших держав, які не в ходять до складу ЄС щодо обробки даних громадян Союзу, на них поширюється дія зазначеного Регламенту, включно із вимогами до забезпечення безпеки персональних даних.

Отже, нині акти Європейського Парламенту охоплюють своїм змістом не лише загальні аспекти кібербезпеки, але і встановлюють загальні вимоги до безпеки обробки окремих видів інформації.

1.1. Національне законодавство про кібербезпеку окремих держав-членів ЄС.

Польща. Основними законодавчими актами, що регулюють питання кібербезпеки та захисту критичної інфраструктури в Польщі, є:

[6] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text

– Закон від 5 липня 2018 року «Про національну систему кібербезпеки»[7]. Закон визначає основні принципи та положення, пов'язані з національною системою кібербезпеки, включаючи обов'язкові вимоги для операторів критичної інфраструктури щодо захисту їхніх інформаційних систем та звітності про інциденти;

– постанова Міністерства цифрової трансформації Республіки Польща від 8 квітня 2021 року «Щодо критичної інфраструктури інформаційних технологій». Постанова визначає види інформаційних технологій, які вважаються критичною інфраструктурою, і встановлює вимоги щодо забезпечення їх кібербезпеки;

– Закон від 16 листопада 2007 року «Про компетентні органи уряду в галузі кібернетичної безпеки»[8]. Закон визначає компетенції та повноваження уряду й інших органів влади щодо кібербезпеки, включаючи планування заходів у випадку кібератак та забезпечення координації;

– Закон від 30 червня 2017 року «Про Національну агенцію забезпечення кібербезпеки»[9]. Закон встановлює положення щодо створення та функціонування Національної агенції забезпечення кібербезпеки, яка відповідає за координацію та здійснення заходів у галузі кібербезпеки.

У Польщі виконання функцій кібербезпеки покладено на кілька державних органів та структур. До ключових державних органів, відповідальних за кібербезпеку, належать:

– Національне центральне бюро розслідувань (CBŚP). CBŚP відіграє важливу роль у виявленні та розслідуванні кіберзлочинів, кібератак та інших кіберзагроз;

– Національна агентура зв'язку (UKE). UKE відповідає за регулювання телекомунікаційного ринку, а також забезпечує кібербезпеку та захист інфраструктури зв'язку;

– Міністерство цифрової трансформації та Телекомунікацій (MAC). Зазначене відомство займається розробкою та впровадженням політики в галузі цифрових технологій, у тому числі щодо кібербезпеки;

– Міністерство національної оборони (MON). MON забезпечує кібербезпеку національної інфраструктури та військових систем;

– Центр кібербезпеки (CSIRT.PL). Це основний національний центр інцидентного реагування на кіберзагрози, який співпрацює з державними органами, приватним сектором та іншими зацікавленими сторонами;

– Національна рада кібербезпеки. Рада є консультативним органом з питань кібербезпеки, до складу якого входять представники різних державних органів та експерти у цій галузі;

– Поліція також займається розслідуванням кіберзлочинів, проводить заходи для протидії кіберзагрозам;

---

[7] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. URL: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/U/D20181560Lj.pdf

[8] Ustawa z dnia 16 listopada 2007 r. o uprawnieniach Rady Ministrów w zakresie cyberbezpieczeństwa URL: https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/krajowy-system-cyberbezpieczenstwa-18746756.

[9] Ustawa z dnia 30 czerwca 2017 r. o Krajowej Agencji Bezpieczeństwa Cyberprzestrzeni. URL: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560

– Міністерство внутрішніх справ (MSW). Міністерство забезпечує кібербезпеку національної інфраструктури та здійснює координацію заходів у цій сфері.

У Польщі, як і в багатьох інших державах, громадські організації можуть відігравати важливу роль у забезпеченні кібербезпеки та сприянні виконанню функцій у цій сфері. Громадські організації сприяють підвищенню свідомості серед громадян щодо кібербезпеки шляхом організації та проведення семінарів, тренінгів, воркшопів та інших події, на яких надаються поради та рекомендації щодо безпечної поведінки в Інтернеті, захисту персональних даних тощо. Громадські організації також сприяють розробці й удосконаленню законодавства в галузі кібербезпеки, взаємодіють з урядовими органами та парламентом, висловлюють свої погляди щодо необхідних заходів для підвищення кібербезпеки нації. Задля спільної розробки та реалізації проектів, спрямованих на підвищення рівня кібербезпеки, громадські організації можуть об'єднувати зусилля з приватними компаніями, які спеціалізуються на кібербезпеці, займатися дослідженням у сфері кібербезпеки, аналізувати поточні тренди та загрози, інформувати громадськість про них та сприяти розробці нових підходів до захисту від кібератак. Громадські організації також проводять інформаційні кампанії, спрямовані на популяризацію засобів захисту від кіберзагроз і запобігання поширеним кібератакам (наприклад, фішингу) та співпрацюють із міжнародними організаціями, міжнародними партнерами для обміну досвідом, найкращими практиками та спільного вирішення глобальних кіберзагроз.

Серед основних засобів забезпечення кібербезпеки у Польщі необхідно виокремити такі:

– здійснення координації та належного реагування на кіберінциденти в державі. Поради та інформацію з питань кібербезпеки різним організаціям надає Національний центр кібербезпеки (NC Cyber), який є державною організацією;

– сертифікація та стандартизація. Польща працює над встановленням стандартів та сертифікаційних схем для забезпечення кібербезпеки в різних секторах, зокрема на важливих інфраструктурних об'єктах;

– співпраця з міжнародними організаціями, а також освіта та навчання в інформаційній сфері. Польща активно співпрацює з іншими державами, ЄС та міжнародними партнерами у сфері кібербезпеки. Зокрема, у державі запроваджено навчальні програми та тренінги з кібербезпеки для спеціалістів та громадян із метою підвищення обізнаності щодо кіберзагроз;

– партнерство з громадянами Польщі. Збільшення усвідомленості громадян щодо кіберзагроз та їхня взаємодія із засобами кібербезпеки, що є також важливим аспектом державної політики.

Зазвичай вимоги до кібербезпеки об'єктів критичної інфраструктури можуть включати такі аспекти:

– ідентифікацію та аналіз загроз. Організації повинні провести оцінку загроз та ризиків для їхньої інфраструктури. Це включає аналіз потенційних кіберзагроз, які можуть вплинути на функціонування критичних систем;

– заходи забезпечення доступу. Забезпечення контролю над фізичним та логічним доступом до критичних систем. Це може включати встановлення

міцних аутентифікаційних методів, контроль над обмеженнями доступу та моніторинг активності користувачів;

– шифрування. Захист інформації шляхом шифрування даних під час передачі та зберігання. Шифрування може застосовуватися для захисту конфіденційної інформації, яка передається по мережі;

– мережева безпека. Захист мережевої інфраструктури від DDoS-атак та інших злочинних дій. Це може включати встановлення брандмауерів, систем виявлення вторгнень тощо;

- оновлення та патчі. Регулярне оновлення програмного забезпечення та встановлення патчів для виправлення відомих вразливостей;

– системи виявлення і реагування на інциденти. Розробка та впровадження систем для виявлення й реагування на кіберінциденти, що допомагають швидко реагувати на атаки та мінімізувати їх наслідки;

– навчання та освіта. Навчання персоналу стосовно кібербезпеки, включаючи ідентифікацію підозрілих активностей та правильні дії у випадку кіберінциденту;

– взаємодія з регуляторами. Дотримання законодавства та регулювання у галузі кібербезпеки, зокрема щодо об'єктів критичної інфраструктури.

Німеччина. У Німеччині регулювання питань кібербезпеки здійснюється відповідно до законодавчих актів. Це, зокрема:

– Закон про кібербезпеку[10]. Закон визначає функції та повноваження Федерального управління з безпеки в інформаційних технологіях (BSI) щодо забезпечення кібербезпеки в Німеччині. Законодавчий акт містить положення щодо заходів з кіберзахисту, інцидентів у галузі кібербезпеки та співпраці з іншими суб'єктами;

– Закон про критичну інфраструктуру[11]. Закон стосується забезпечення кібербезпеки в критичних секторах (енергетика, водопостачання, телекомунікації тощо). Відповідно до вимог закону оператори критичної інфраструктури здійснюють заходи з кіберзахисту, включаючи подання звітності про кіберінциденти та заходи проти їх відновлення;

– Закон про кіберінциденти[12]. Відповідно до закону розширено права споживачів у випадках кіберінцидентів та порушень даних. Споживачам надається право вимагати компенсацію у разі порушення заходів кібербезпеки;

– Закон про телекомунікації[13]. Окремі статті закону стосуються забезпечення безпеки та кібербезпеки в галузі телекомунікацій.

---

[10] Закон про кібербезпеку / Gesetz über das Bundesamt für Sicherheit in der Informationstechnik – BSIG. URL: https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html

[11] Закон про критичну інфраструктуру / Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme - IT-Sicherheitsgesetz. URL: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s1122.pdf%27%5D__1692044144132

[12] Закон про кіберінциденти / Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts. URL: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl116s0233.pdf%27%5D__1692044243290

[13] Закон про телекомунікації / Telekommunikationsgesetz – TKG. URL: https://dejure.org/gesetze/TKG

У Німеччині виконання функцій кібербезпеки покладено на кілька державних інституцій:

– Федеральний офіс інформаційної безпеки (BSI) – центральний орган у сфері кібербезпеки в Німеччині. BSI відповідає за захист інформаційної інфраструктури держави, розробляє стандарти та рекомендації щодо кібербезпеки, проводить дослідження й аналіз загроз;

– Федеральний центр захисту інформації (BSZ) – відповідає за захист інформації у федеральних органах і структурах влади, надає підтримку та консультації у сфері кібербезпеки уряду;

– Федеральне міністерство внутрішніх справ (BMI) – має повноваження щодо визначення політики кібербезпеки та координації заходів у цій сфері;

– Федеральний комітет з розслідування інтернет-злочинів (BCDI) – відповідає за розслідування кіберзлочинів і злочинів, пов'язаних із використанням Інтернету;

– Федеральний офіс конституційного захисту (BfV) – спеціалізується на захисті конституційного ладу й контррозвідці та виявленні загроз у сфері кібербезпеки, які можуть вплинути на національну безпеку.

Зазначені органи координують свою діяльність і співпрацюють з іншими суб'єктами, у тому числі з галузевими організаціями, приватним сектором, академічною спільнотою задля забезпечення комплексного підходу до кібербезпеки в державі.

Основні характеристики засобів забезпечення кібербезпеки в Німеччині включають:

– вдосконалення, розробку стандартів безпеки, проведення досліджень і здійснення аналізу загроз кібербезпеці, надання порад та підтримки урядовим органам, приватним компаніям (забезпечує BSI);

– впровадження урядом Німеччини стратегії кібербезпеки, спрямованої на захист критично важливих інфраструктур, забезпечення безпеки в інформаційному просторі та співпрацю з іншими державами;

– законодавче регулювання, спрямоване на забезпечення кібербезпеки. Наприклад, Закон про кібербезпеку (IT-Sicherheitsgesetz), відповідно до якого встановлено обов'язкові вимоги щодо кібербезпеки для критично важливих інфраструктур і компаній;

– співпрацю влади Німеччини з приватним сектором, у тому числі з IT-компаніями та провайдерами послуг, задля спільного реагування на кіберзагрози, обміну інформацією про нові загрози;

– навчання та освіту. Німеччина також приділяє увагу освіті у галузі кібербезпеки. Університети та навчальні заклади надають програми з кібербезпеки для підготовки фахівців у цій сфері;

– моніторинг загроз, аналіз і відповідь на інциденти в кіберпросторі, що здійснюють центри інформаційної безпеки, які підтримуються урядом і приватними компаніями;

– міжнародну співпрацю Німеччини з іншими державами, міжнародними організаціями та об'єднаннями для обміну інформацією, дослідженнями та спільної боротьби з кіберзагрозами.

Німеччина має високі стандарти щодо забезпечення кібербезпеки об'єктів критичної інфраструктури. Принципово важливі інфраструктурні об'єкти – енергетичні мережі, транспортні системи, телекомунікаційні мережі тощо – є предметом особливої уваги у зв'язку з потенційними кіберзагрозами.

Основні підходи до забезпечення кібербезпеки об'єктів критичної інфраструктури в Німеччині включають такі компоненти:

– наявність відповідного законодавства. У Німеччині діє Закон про кіберзахист критичної інфраструктури (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, або IT-Sicherheitsgesetz), відповідно до якого встановлено вимоги до забезпечення кібербезпеки для операторів критичної інфраструктури, обов'язкові стандарти безпеки та звітності для цих об'єктів;

– ідентифікація та класифікація критичної інфраструктури. Оператори критичної інфраструктури повинні ідентифікувати свої об'єкти та визначити їх рівень критичності, що допомагає зосередитися на найважливіших аспектах кібербезпеки;

– мінімальні стандарти безпеки. Законодавство зобов’язує операторів критичної інфраструктури встановити мінімальні стандарти безпеки для своїх інформаційних систем;

– заходи захисту. Оператори повинні вживати заходів захисту для запобігання кібератакам та виявлення вразливостей. Це може забезпечуватися шляхом застосування вогневих стін, антивірусних програм, мережевого моніторингу тощо;

– звітність і співпраця. Оператори зобов'язані повідомляти про кіберінциденти та взаємодіяти з відповідними органами управління кризовими ситуаціями;

– стратегія кібербезпеки. Оператори повинні розробити стратегії кібербезпеки, включаючи плани відновлення після інцидентів, тестування на вразливості та проводити навчання персоналу;

– співпраця з іншими державними органами. Органи кібербезпеки Німеччини співпрацюють з операторами критичної інфраструктури для обміну інформацією про загрози та заходи захисту.

Естонія. Основними законодавчими актами, що регулюють питання кібербезпеки в Естонії, є:

– Закон про кібербезпеку[14]. Закон прийнятий в 2018 році та має на меті забезпечення кібербезпеки в електронному просторі Естонії. Відповідно до Закону визначено обов'язки та встановлена відповідальність організацій і урядових структур щодо захисту інформації, інфраструктури та інших аспектів кібербезпеки;

– Закон про критичну інфраструктуру[15] прийнятий для забезпечення захисту та безпеки критичної інфраструктури, яка є важливою для функціонування суспільства й економіки. Закон визначає категорії критичної

[14] Закон про кібербезпеку / Estonian CyberSecurity Act. URL: https://www.riigiteataja.ee/en/eli/523052018003/consolide

[15] Закон про критичну інфраструктуру / Estonian Critical Infrastructure Act

інфраструктури та встановлює вимоги щодо їх захисту від можливих кібератак та інших загроз;

– Закон про інформаційну безпеку[16] врегульовує питання інформаційної безпеки в державному та приватному секторі, встановлює вимоги до захисту інформації і даних, обмеження доступу до них, а також визначає процедури реагування на інциденти в інформаційному просторі;

– Закон про персональні дані[17] встановлює правила для обробки та захисту персональних даних, має значний регулятивний вплив на аспекти кібербезпеки, оскільки забезпечення конфіденційності та безпеки персональних даних є важливою частиною заходів кіберзахисту;

– Закон про телекомунікації[18] врегульовує правовідносини у телекомунікаційному секторі і містить положення щодо кібербезпеки та захисту мережевої інфраструктури.

В Естонії кібербезпека є важливим аспектом національної безпеки, виконання функцій у цій сфері покладено на декілька державних органів та агентств:

– Міністерство економіки та комунікацій відповідає за розробку та координацію національної політики з питань інформаційних технологій та комунікацій, включаючи кібербезпеку;

– Естонський центр кібербезпеки (Estonian Cyber Security Centre, CERT-EE) – державне агентство, яке відповідає за дослідження та відстеження кіберзагроз, реагування на інциденти кібербезпеки й надає консультації з цих питань;

– поліція та прикордонна служба розслідують кіберзлочини та протидіють кіберзагрозам;

– Кіберресурсний центр Збройних сил відповідає за кібероборону та забезпечення кібербезпеки оборонних структур держави;

– Національне бюро розслідувань веде розслідування важливих кіберзлочинів та кібератак, які можуть впливати на національну безпеку;

– Естонська інформаційно-системна агентура (RIA) – організація, яка відповідає за розвиток та захист інформаційних систем, включаючи кібербезпеку, у державних і недержавних секторах.

Естонія відома своїм високим рівнем кібербезпеки та інноваційними підходами до цього питання. Держава впроваджує широкий спектр заходів задля забезпечення кібербезпеки на різних рівнях: урядовому, корпоративному та індивідуальному.

Електронна ідентифікація та електронний підпис. Естонія впровадила систему електронної ідентифікації для громадян та резидентів, використовуючи національні ID-карти, мобільні ID та ідентифікаційні картки e-resident. Це сприяє

[16] Закон про інформаційну безпеку / Estonian Information Security Act. URL: https://www.riigiteataja.ee/akt/412102013007

[17] Закон про персональні дані / Estonian Personal Data Protection Act. URL: https://www.riigiteataja.ee/en/eli/523012019001/consolide

[18] Закон про телекомунікації / Estonian Electronic Communications Act. URL: https://www.riigiteataja.ee/en/eli/518032022002/consolide

захисту особистих даних та забезпечує безпеку електронних транзакцій. В Естонії достатньо захищена електронна інфраструктура. Уряд Естонії інвестує в розвиток кіберінфраструктури та захищені мережі, що забезпечує оптимальну захищеність від кібератак. Навчання та підвищення кваліфікації для громадян і підприємств з питань кібербезпеки здійснюється відповідно до спеціальних навчальних програм, що сприяє свідомому використанню технологій та запобіганню кібератакам.

Важливо наголосити, що в Естонії функціонує Національний центр кіберінцидентів (CERT-EE), який відповідає за виявлення, відповідь та реагування на кібератаки. Центр координує співпрацю між різними секторами для ефективної боротьби з кіберзагрозами. Законодавство Естонії регулює питання кібербезпеки, кіберзлочинності та захисту персональних даних і встановлює кримінальну відповідальність за кіберзлочини, забезпечує захист персональних даних і встановлює відповідальність за порушення кібербезпеки.

Уряд співпрацює з приватною сферою для спільної реалізації проектів щодо підвищення кібербезпеки. Таке партнерство дозволяє обмінюватися інформацією та кращими практиками. Естонія бере активну участь у міжнародних ініціативах з кібербезпеки, співпрацюючи з іншими державами, організаціями та експертами для обміну досвідом та спільної боротьби з кіберзагрозами. Важливою складовою підвищення кібербезпеки є сприяння розвитку кібербезпекових стартапів та інноваційних проектів, яким уряд Естонії надає можливість тестувати свої рішення та продукти на національному рівні.

Основні підходи до забезпечення кібербезпеки об'єктів критичної інфраструктури в Естонії включають такі компоненти:

– стандарти безпеки зазвичай включають дотримання міжнародних та національних стандартів безпеки ISO 27001, NIST Cybersecurity Framework тощо;

– системи виявлення та реагування на інциденти. Об'єкти критичної інфраструктури повинні бути обладнані системами виявлення та реагування на кіберінциденти, що дозволяє вчасно виявляти та ліквідовувати загрози;

– контроль доступу. Забезпечення обмеженого та контрольованого доступу до систем і даних, що включає аутентифікацію, авторизацію та аудит дій користувачів;

– захист мережі та трафіку означає встановлення захисних механізмів на рівні мережі (файрволи, інтра- та екстранети, системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS));

– захист від шкідливого програмного забезпечення передбачає оновлення антивірусного та антишпіонського програмного забезпечення для запобігання враженню шкідливими програмами;

– фізична безпека – це захист фізичних активів (серверні зали та обладнання) від несанкціонованого доступу;

– організація навчання та тренувань персоналу з питань кібербезпеки, а також проведення регулярних симуляцій кібератак для перевірки готовності реагування на інциденти;

– резервне копіювання та відновлення даних задля забезпечення регулярного резервного копіювання даних і розробка планів відновлення в разі кіберінцидентів;

– моніторинг та аналіз подій для виявлення незвичайних активностей та потенційних загроз;

– співпраця з урядовими органами, іншими об'єктами критичної інфраструктури та кібербезпековими компаніями для обміну інформацією та спільного реагування на загрози.

2. Національне законодавство про кібербезпеку окремих держав членів Ради Європи, які не є державами-членами ЄС.

Швейцарська Конфедерація. На відміну від більшості держав-членів ЄС, законодавство Швейцарії про кібербезпеку виходить не з комплексного підходу до врегулювання суспільних відносин у цій сфері, а застосовує галузевий підхід з урахуванням особливостей кіберризиків у конкретній сфері суспільного життя.

Поряд із цим федеральне законодавство про кібербезпеку Швейцарії закріплює лише базові критерії визначення кіберінцидентів та вимоги щодо засобів їх запобігання. Відповідно до Стратегії забезпечення кібербезпеки Швейцарії на 2018 – 2022 роки[19] закладено правило про необхідність підвищення значення міжнародних стандартів, зокрема стандартів ISO у протидії кіберзагрозам, встановлення технічних вимог до захисту національних і корпоративних електронних інформаційних ресурсів.

Серед загальних законів, що застосовуються на території Швейцарії у сфері кібербезпеки, необхідно виділити такі: Будапештська конвенція Ради Європи про кіберзлочинність від 23 листопада 2001 року[20]; Переглянута Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108+)[21]; Закон про електронні медичні записи[22]; Постанова про експорт та посередництво товарів для спостереження за Інтернетом та мобільним зв'язком[23]; Постанова про захист від кіберризиків у Федеральній адміністрації[24]; Федеральний закон про інформаційну безпеку[25].

У Швейцарії не існує загальноприйнятих обов'язкових вимог щодо кібербезпеки для критичної або важливої інфраструктури та послуг. Регулювання кібербезпеки для такої інфраструктури та послуг є щодо технічного захисту інформації. Велике значення у врегулюванні окресленої проблеми уряд

---

[19] Стратегія забезпечення кібербезпеки Швейцарії на 2018 – 2022 роки. URL: http://connections-qj.org/article/cybersecurity-switzerland-challenges-and-way-forward-swiss-armed-forces

[20] Будапештська конвенція Ради Європи про кіберзлочинність від 23 листопада 2001 року. URL: https://zakon.rada.gov.ua/go/994_575

[21] Модернізована Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних.

[22] Закон Швейцарської Конфедерації «Про електронні медичні засоби». URL: https://www.swissinfo.ch/eng/business/swiss-federal-council-pushes-for-universal-electronic-patient-records/48626606

[23] Verordnung der Schweizerischen Eidgenossenschaft "Über die Ausfuhr und Vermittlung von Waren zur Internet- und Mobilfunküberwachung». 13.05.2015. URL: https://www.admin.ch/opc/de/classified-compilation/20150564/index.html

[24] Verordnung der Schweizerischen Eidgenossenschaft «Über den Schutz vor Cyberrisiken in der Bundesverwaltung». URL: https://www.fedlex.admin.ch/eli/cc/2020/416/de

[25] Bundesgesetz der Schweizerischen Eidgenossenschaft "Über die Informationssicherheit. URL: https://www.fedlex.admin.ch/eli/fga/2023/85/de

Швейцарії та галузеві ІТ-асоціації відводять технічним стандартам Міжнародної організації зі стандартизації (ISO), зокрема групі 27100. Проте прийнята 18 квітня 2018 року Стратегія захисту критичної інфраструктури Швейцарії на 2018 – 2022 роки та Стратегія забезпечення кібербезпеки на 2023 – 2026 роки вказують на необхідність реалізації комплексу заходів, спрямованих на визначення ознак кіберризиків, забезпечення комплексного підходу до стандартизації і регулювання вимог до засобів забезпечення кібербезпеки національних електронних інформаційних ресурсів.

Нині законодавство Швейцарії не встановлює імперативний обов'язок для суб'єктів господарювання щодо повідомлення Федеральному центру кібербезпеки про всі кіберінциденти, за винятком випадків, коли їх прояв спрямований проти об'єктів критичної інформаційної інфраструктури. Згідно із Законом Швейцарії «Про інформаційну безпеку» та Стратегією забезпечення кібербезпеки в останньому випадку інформування про кіберінциденти є безпосереднім зобов'язанням будь-якого суб'єкта підприємницької діяльності та посадових осіб суб'єктів владних повноважень Швейцарії. Водночас відповідно до Закону Швейцарії «Про інформаційну безпеку» галузеві об'єднання підприємців та професійні об'єднання можуть стимулювати своїх учасників задля повідомлення про кіберінциденти у централізованому порядку.

Щодо контролю за дотриманням законодавства про кібербезпеку, включно з повідомленням про кіберінциденти, то законодавство Швейцарії застосовує предметний критерій для їх розподілу між різними суб'єктами владних повноважень. Так, зокрема, контроль за дотриманням законодавства про кібербезпеку об'єктів критичної інфраструктури здійснює Федеральний центр кібербезпеки, у сфері телекомунікацій – Національна комісія, яка здійснює регулювання ринку телекомунікацій та зв'язку. Щодо безпеки персональних даних, то дотримання законодавства у цій сфері правового регулювання є прерогативою Комісарів із захисту даних у межах конкретних кантонів Швейцарської Конфедерації.

Закон Швейцарії «Про договори страхування» дозволяє організаціям страхувати кіберризики поряд з іншими страховими випадками. Рішення для кіберстрахування дуже індивідуальні і можуть включати майже всі кіберризики, включаючи атаки на відмову в обслуговуванні та програми-вимагачі, витрати на внутрішні розслідування та кризове управління, відновлення вкрадених, знищених або пошкоджених даних, репутаційні збитки тощо.

Велика Британія. Законодавство Великої Британії про кібербезпеку також складається з Національної стратегії забезпечення кібербезпеки та галузевих актів законодавства, які визначають спеціальні вимоги до механізму забезпечення кібербезпеки в окремих сферах суспільного життя.

Серед основних законодавчих актів Великої Британії, які складають основу забезпечення механізму кібербезпеки, можна виокремити Акт про захист персональних даних 2018 року[26]. Акт застосовується поряд із Законом про захист

[26] Data Protection Act 2018. URL: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

комп'ютерних мереж 1990 року[27] (зі змінами та доповненнями). Цей закон охоплює різні кіберзлочини та загалом спрямований на захист комп'ютерних матеріалів від несанкціонованого доступу або модифікації. У сфері кібербезпеки також діють:

Правила мережевих та інформаційних систем 2018 року («Правила NIS»)[28]. Правила NIS, які уряд наразі прагне оновити задля запровадження правових заходів для підвищення рівня безпеки (як з кіберперспективи, так і з точки зору фізичної стійкості), мережевих та інформаційних систем для надання основних послуг (наприклад, водопостачання, транспорт, енергетика, охорона здоров'я та цифрова інфраструктура) і цифрових послуг (пошукові системи, онлайн-ринок або послуги хмарних обчислень);

Закон про телекомунікації 2021 року[29]. Дія цього закону спрямована на посилення існуючих зобов'язань щодо безпеки відповідно до Закону про зв'язок 2003 року, а також встановлює різноманітні нові повноваження та штрафні санкції щодо правопорушень у сфері інформаційної безпеки;

Закон про регулювання слідчих повноважень 2000 року (RIPA 2000 у редакції 2016 року)[30]. Норми вказаного закону охоплюють протидію загрозам щодо перехоплення комунікацій, втручання в обладнання, а також отримання та збереження даних зв'язку, масових наборів персональних даних та іншої інформації правоохоронними органами.

Згідно із законом «Про телекомунікації» та Стратегією захисту критичної інформаційної інфраструктури запроваджується комплекс заходів щодо захисту цифрових і фізичних компонентів національної електронної інформаційної інфраструктури від можливих або потенційних кіберзагроз.

Стратегія забезпечення кібербезпеки Великої Британії покладає на операторів та провайдерів цифрових послуг обов'язки щодо інформування про кіберінциденти та заходи, які вживаються для протидії їхньому прояву.

Органом державної влади, до якого надсилаються такі повідомлення, є Національний центр кібербезпеки Великої Британії. Зазначений орган виконавчої влади не наділений регуляторними повноваженнями, а тому до його компетенції віднесено переважно завдання з моніторингу та контролю за станом забезпечення кібербезпеки. Також вказаний суб'єкт здійснює юрисдикційні провадження у справах про порушення законодавства про кібербезпеку, має право надавати власникам ІТ-систем вказівки, обов'язкові до виконання.

Разом із тим за законодавством Великої Британії забезпечення дотримання галузевих вимог щодо кібербезпеки, технічного захисту інформації є прерогативою органів галузевого управління та професійних об'єднань суб'єктів господарювання на конкретному ринку товарів, робіт, послуг.

Загалом законодавство Швейцарії та Великої Британії про кібербезпеку застосовує близькі до права ЄС підходи до врегулювання більшості суспільних

[27] Computer Misuse Act. URL: https://www.cps.gov.uk/legal-guidance/computer-misuse-act

[28] The NIS Regulations 2018. URL: https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018

[29] Telecommunications (Security) Act 2021. URL: https://www.lexology.com/library/detail.aspx?g=20beef3e-c535-47d1-855c-59fef1d06d5c

[30] Regulation of Investigatory Powers Act 2000. URL: https://www.legislation.gov.uk/ukpga/2000/23/contents

відносин у цій сфері. Основні відмінності переважно виявляються у формуванні національних органів влади, відповідальних за забезпечення кібербезпеки, відсутності комплексного законодавчого підходу до врегулювання суспільних відносин у цій сфері. Поряд із цим у Великій Британії та Швейцарії національне законодавство більш детально, порівняно із законодавством держав-членів ЄС, врегульовує юрисдикційні питання транскордонного забезпечення кібербезпеки, процедури та програми страхування від кіберризиків, спеціальні (галузеві) засоби протидії кіберзагрозам.

Висновки. Проведений порівняльний аналіз законодавства ЄС, окремих держав-членів, Великої Британії та Швейцарії про кібербезпеку дозволяє зробити такі висновки.

1. Нині законодавство ЄС та держав-членів ЄС розвивається переважно шляхом врегулювання ключових складових механізму забезпечення кібербезпеки на рівні загальних актів Європейського Парламенту, зокрема Регламенту 2019/881 та Директиви 2022/2555. На загальний рівень регулювання винесені, серед іншого, питання щодо: структури національних стратегій забезпечення кібербезпеки; планів реагування на кіберінциденти; загальних вимог до суб'єктів забезпечення кібербезпеки; основних підстав та видів юридичних стягнень за порушення у цій сфері правового регулювання; юрисдикційних аспектів забезпечення кібербезпеки на транскордонному рівні. На рівні національного законодавства держав-членів ЄС переважно врегульовані питання, пов'язані з: процедурами формування національних органів забезпечення кібербезпеки, протидією кіберделіктам, взаємодією галузевих асоціацій із відповідними суб'єктами владних повноважень із питань протидії кіберзагрозам, механізмами імплементації національних стандартів.

2. Законодавство ЄС, держав-членів ЄС, Великої Британії та Швейцарії про кібербезпеку у протидії кіберзагрозам робить основний акцент на забезпечення стійкості компонентів інформаційної інфраструктури від можливих кіберризиків. Це означає посилення юридичного значення міжнародних стандартів кібербезпеки, сертифікатів технічної відповідності ІТ-продукції, послуг та процесів вимогам кібербезпеки.

3. Значна увага в нормах законодавства ЄС, держав-членів ЄС, Великої Британії та Швейцарії приділяється запровадженню механізму залучення приватних компаній до забезпечення кібербезпеки. Це стосується не лише питань розробки програмного забезпечення в межах проєктів публічно-приватного партнерства, але й інформування про кіберінциденти, створення професійних асоціацій управління кіберризиками. Поряд із цим законодавство Великої Британії та Швейцарії приділяє увагу юрисдикційним аспектам забезпечення кібербезпеки, зокрема визначенню застосованого права до відповідних правовідносин, встановленню держави походження кіберризиків, визначенню відповідальних осіб за правопорушення у сфері кібербезпеки.

4. Сьогодні з офіційних джерел інформації невідомо про наявність затвердженої компетентними державними органами України дорожньої карти адаптації законодавства України про кібербезпеку до законодавства ЄС. Разом із

тим затвердження такого документа могло б сприяти виконанню міжнародних зобов'язань за Угодою про асоціацію України з ЄС.

5. Серед основних напрямів адаптації законодавства України про кібербезпеку до законодавства ЄС слід виділити такі: уточнення правового статусу органів, відповідальних за забезпечення кібербезпеки; формування механізму технічної специфікації та сертифікації ІТ-продукції, товарів, послуг та процесів на основі міжнародних стандартів; посилення юридичного значення національних та міжнародних стандартів в системі засобів забезпечення кібербезпеки; закріплення спеціальних процедур публічних закупівель товарів, робіт та послуг, які впливають безпосередньо на стан кібербезпеки; запровадження в національне законодавство спеціальних норм, спрямованих на врегулювання проєктів публічно-приватного партнерства у сфері кібербезпеки; уточнення правового статусу об'єднань суб'єктів господарювання в частині виконання заходів із протидії кіберзагрозам, інформування про кіберінциденти; конкретизація юрисдикційних аспектів забезпечення кібербезпеки на транскордонному рівні.

6. В умовах активної війни російської федерації проти України актуальною вбачається подальша імплементація Європейської рамки професійних компетентностей у сфері кібербезпеки.

Дослідницька служба
Верховної Ради України