DOI https://doi.org/10.30525/978-9934-26-313-2-9

GERMANY'S NATIONAL LEGAL FRAMEWORK IN THE FIELD OF CYBER SECURITY

НАЦІОНАЛЬНА ПРАВОВА БАЗА ГЕРМАНІЇ В ГАЛУЗІ КІБЕРБЕЗПЕКИ

Shevchenko A. E.
Doctor of Law, Professor
Honored lawyer of Ukraine
Head of Department of Theoretical and Legal Disciplines
State Tax University
Irpin, Ukraine

Шевченко А. Є.
доктор юридичних наук, професор,
Заслужений юрист України,
завідувач кафедри теоретико-правових дисциплін
Державний податковий університет
м. Ірпінь, Україна

Pavliukh O. A.
Candidate of Legal Sciences,
Associate Professor,
Associate Professor of the Department of Criminal Justice
State Tax University
Irpin, Ukraine

Павлюх О. А.
кандидат юридичних наук,
доцент кафедри кримінальної юстиції
Державний податковий університет
м. Ірпінь, Україна

Sanzharova G. F.
Senior Lecturer Chair of Romance Philology and Comparative-typological Linguistics
Borys Grinchenko Kyiv University
Kyiv, Ukraine

Санжарова Г. Ф.
старший викладач кафедри романської філології та порівняльно-типологічного мовознавства
Київський університет імені Бориса Грінченка
м. Київ, Україна

Зусилля та бажання Німеччини боротися з кіберзагрозами в державному та приватному секторах виникли з їх появою і продовжують розвиватися в міру розвитку цих загроз [1, с. 74–76]. Бундестаг із самого раннього етапу законодавчіх кібер-ініціатив зрозумів, що зусилля із захисту ІТ-інфраструктури, як основи кібербезпеки, – це співпраця між усіма акторами кіберпростору: приватними корпораціями, урядовими установами та транснаціональними організаціями.

Німецьке регулювання кібербезпеки передує загальноєвропейському завдяки «Закону про підвищення безпеки систем інформаційних технологій» (ITSiG) від 17 липня 2015 р. [2], а також «Положенню (регламенту) про визначення критичної інфраструктури» відповідно до Закону про Федеральне управління з інформаційної безпеки (Bundesamt für Sicherheit in der Informationstechnik) від 22 квітня 2016 р. [3]. До списку критичної інфраструктури було віднесено сектори фінансів та страхування, транспорту та дорожнього руху, а також охорони здоров'я. У 2016 році ЄС прийняв «перше всеосяжне загальноєвропейське законодавство» щодо кібербезпеки, «Директиву про безпеку мережевих та інформаційних систем» (NIS). Щоб повністю відповідати стандарту ЕС знадобились лише незначні поправки та роз'яснення щодо визначення критичних інфраструктур у галузі енергетики, води, продуктів харчування та інформаційно-комунікаційних технологій.

Набуття чинності відповідного законодавства ЄС у 2016 році призвело лише до незначних змін «Регламенту» від 21 червня 2017 року та прийняття «Закону про введення в дію NIS» від 23 червня 2017 р. [1, с. 76–77]. Поправки включали правила про провайдерів цифрових послуг, розділ про відновлення захищеності функціональних можливостей систем інформаційних технологій у нез'ясованих випадках, а також положення про обмін інформацією та взаємодію з органами військової контррозвідки та федеральною розвідувальною службою. У 2017 р. Бундесвер створив нове кіберкомандування зі штаб-квартирою в Бонні на чолі з інспектором кібернетичного та інформаційного простору – генерал-лейтенантом Людвігом Лейнхосом (з 25.09.2020 р. цю посаду обіймає віце-адмірал Томас Даум). Міністерство оборони повідомило, що IT-системи Бундесверу зазнали близько 280 000 атак за перші дев'ять тижнів 2017 року, причому російські хакери, спонсоровані державою, підозрюються у сприянні значній частині цих атак [1, с. 82]. Командуванню в кібернетичному та інформаційному просторі в 2021 році були підпорядковані понад 13500 співробітників і інноваційний центр, який з'єднує військових із технологічними стартапами. Разом з тим подальше розширення інструментів, які є в розпорядженні німецького уряду та військових для роботи в кіберсфері залишаються обмеженими жорсткими правовими нормами.

18 травня 2021 року Бундестаг ФРН прийняв «Закон про підвищення безпеки систем інформаційних технологій 2.0.» [4]. Закон (ITSiG 2.0.) реагує на проблеми IT-безпеки в галузі критично важливих інфраструктур і за їх межами, адаптуючи і вдосконалюючи заходи і стратегії кіберзахисту. Закон

насамперед передбачає зміни та поправки до центрального закону Німеччини про кібербезпеку «Закону про Федеральне управління з інформаційної безпеки» (BSI): вони стосуються правил використання так званих «критичних компонентів»; додають нову категорію компаній, що представляють особливий суспільний інтерес; розширюють та посилюють повноваження Федерального відомства (BSI). 1 січня 2022 р. набрало чинності нове «Положенням про критично важливі інфраструктури» в якому було внесено поправки і доповнення до кількох секторів визначених «Законом» (ITSiG 2.0.) шляхом запровадження нових типів критичної інфраструктури. Разом з цим порогові значення для існуючих інфраструктур були знижені, тобто зросла кількість інфраструктур, що вважаються критично важливими. Нарешті, «Закон» також ініціював зміни та доповнення до цілої низки законів – «Закону про телекомунікації», «Закону про економію енергії», «Постанови про зовнішню торгівлю та платежі», «Соціальний кодекс X» та безліч «lex specialis», які регулюють важливі сектори, які не підпадають під дію «Закону про Федеральне управління з інформаційної безпеки» [5, с. 303–307].

«Закон про підвищення безпеки систем інформаційних технологій» від 2021 року розширює сферу застосування центрального «Закону про Федеральне управління з інформаційної безпеки» на нові сектори: побутові відходи з життєво важливими послугами з їхнього видалення (збирання, утилізація, переробка); організації, які виробляють або розробляють товари «з особливим суспільним інтересом» (оборона, озброєння, федеральні інформаційні технології) та підприємства, які використовують небезпечні матеріали в межах своєї діяльності (наприклад, хімікати). Важливість цих секторів не перевищує порога критичності, тобото вони відрізняються від категорії секторів критичної інфраструктури, але законодавці вважають, що вони також потребують і заслуговують на захист. Таким чином, німецький законодавець проводить різницю між «критичними» (тобто суттєвими) об'єктами і «важливими» об'єктами. Визначення об'єктів, які вважаються «важливими» є унікальною рисою німецького законодавства. Основним суб'єктом нових правил залишаються оператори критичних інфраструктур. Вони зобов'язані зареєструвати критичну інфраструктуру у Федеральному управлінні з інформаційної безпеки.

Варто зазначити, що національна правова база Німеччини в галузі кібербезпеки відповідає суті пропонованих змін, передбачених «Директивою про безпеку мережевих та інформаційних систем 2.0.» (NIS2) для імплементації в національне законодавство країн-членів ЄС [5, с. 291–295]. «Закон про підвищення безпеки систем інформаційних

технологій» (ITSiG 2.0.) ввів зобов'язання використовувати сучасні системи виявлення кібератак з 1 травня 2023 року. Для підтримки цього Федеральне управління з інформаційної безпезпеки надає платформу обміну інформацією про шкідливі програми.

Німеччина є активним учасником зусиль із роз'яснення принципів застосування і практичного дотримання міжнародного права в кіберпросторі. Німеччина завдяки своїм різноманітним зусиллям в юридичній, технологічній та виробничій сферах, постійному вдосконаленню політики, правил і законодавства наразі готова долати виклики та загрози, властиві кіберсфері. Далекоглядний характер законодавчих зусиль робить країну одним з лідерів в ЄС і на світовій арені в питаннях кібербезпеки.

Література:

1. Romaniuk S. N., Claus M. Germany's cybersecurity strategy: confronting future challenges. *Routledge Companion to Global Cyber-Security Strategy* / ed. S. N. Romaniuk, M. Manjikian. London-New York: Routledge, 2021. P. 73–88.

2. Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015. *Bundesgesetzblatt Jahrgang*. Teil I. Nr. 31 vom 24.07.2015. S. 1324–1331.

3. Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV) vom 22. April 2016. *Bundesgesetzblatt Jahrgang*. Teil I. Nr. 20 am 2. Mai 2016. S. 958–969.

4. Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 18. Mai 2021. *Bundesgesetzblatt Jahrgang*. Teil I, Nr. 25 am 27.05.2021. S. 1122–1138.

5. Schmitz-Berndt S., Chiara P.G. One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive. *International Cybersecurity Law Review*. 2022. Vol. 3. P. 289–311. DOI: https://doi.org/ 10.1365/s43439-022-00058-7.