ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ

ІРПІНСЬКИЙ ЮРИДИЧНИЙ ЧАСОПИС

Науковий журнал

Випуск 3 (12)

Ірпінь ● ДПУ ● 2023

ISSN 2617-4154
УДК 34:33(477)(08)

Засновник: Університет державної фіскальної служби України
Заснований 2018 року
Продовжуване видання (виходить у міру накопичення матеріалу)
Мови видання: українська, англійська
Свідоцтво про Державну реєстрацію друкованого засобами масової інформації:
Серія КВ № 23215-13055ПР від 22.03.2018
Рекомендовано до друку та поширення через мережу «Інтернет» рішенням Вченої ради
Державного податкового університету (протокол № 12 від 25.05.2023)

Ірпінський юридичний часопис : науковий журнал / редкол. : В. В. Топчій (голов. ред.) та ін. – Ірпінь : Державний податковий університет, 2023. – Випуск 3 (12). – 372 с. – (Серія : право).

У виданні вміщені наукові статті, присвячені актуальним проблемам юридичної науки та практики.

Науковий журнал започатковано з метою опублікування результатів наукових досліджень проблем правової науки, теоретико-прикладних проблем правового забезпечення фіскальної політики держави, удосконалення законодавства та правозастосування.

Для науковців, викладачів, аспірантів, студентів та всіх, хто цікавиться проблемами теорії права та правозастосування.

Науковий журнал індексується в Google Scholar,

Національною бібліотекою України імені В. І. Вернадського.

Розміщений на відкритій інформаційній платформі OJS Державного податкового університету.

DOI (digital object identifier) – цифровий індикатор об’єкта привласнюється науковим статтям видання.

Редакція журналу веде систематичну роботу із включення наукового видання до міжнародних електронних бібліотек, каталогів та наукометричних баз даних з метою входження в світовий науковий інформаційний простір, підвищення рейтингу журналу та індексів цитування його авторів. Наразі редколегія провадить роботу щодо входження збірника у Scopus та Web of Science.

Адреса редакційної колегії:
Україна, 08201, Ірпінь, Київська обл., вул. Університетська, 31,
e-mail: irpin-yur-chas@ukr.net

STATE TAX UNIVERSITY

IRPIN LEGAL CHRONICLLES

The Scientific Journal

Issue 3 (12)

Irpin ● STU ● 2023

ISSN 2617-4154
UDC 34:33(477)(08)

Founder: University of the State Fiscal Service of Ukraine
The scientific journal «Irpin legal chronicIles» was founded in 2018

Continued edition (released with the accumulation of material)
Languages of edition: Ukrainian, English

The certificate of state registration of the printed mass media:
KV № 23215-13055PR, 22.03.2018

Recommended for printing and Internet distribution by the decision of the
Academic Council of the State Tax University (protocol № 12, 25.05.2023)

Irpin legal chronicIles : The Scientific Journal / Editorial Board : V. V. Topchiy (Editor-in-chief) and others. – Irpin : State Tax University, 2023. – Issue 3 (12). – 372 p. – (Series : Law).

The edition contains scientific articles devoted to the actual problems of legal science and practice.

The scientific journal was founded with the purpose of publishing the results of researches on problems of legal science, theoretical and applied problems of legal provision of the state fiscal policy, improvement of legislation and law enforcement.

The journal is intended for researchers, lecturers, postgraduates, students and anyone who is interested in law theory and law enforcement.


The Scientific Journal is indexed by Google Scholar,


V. I. Vernadsky National Library of Ukraine.

The scientific journal is located on the open information platform OJS of the State Tax University.


DOI digital object identifier is assigned to the scientific articles of the edition.

The editorial board carries out systematic work on integration of the scientific edition to the international electronic libraries, catalogs and scientometric databases with the purpose of entering the world scientific information space, increasing the rating of the journal and the citation indices of its authors. The editorial board is currently working on the inclusion of the scientific journal in Scopus and Web of Science.

Address of the editorial board:
31, Universitetskaya str., Irpin, Kyiv region, Ukraine, 08201
e-mail: irpin-yur-chas@ukr.net

ЗМІСТ

Господарське право і процес

Кримінальне право та кримінологія; кримінально-виконавче право

Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність

Трибуна молодого науковця

CONTENTS

Commercial law and process

Criminal law and criminology; Penal law

Criminal procedure and criminalistics; forensic examination; operational-search activity

Tribune of the young scientist

УДК 343.9:004.49
DOI 10.33244/2617-4154.3(12).2023.219-227

О. А. Павлюх,
канд. юрид. наук, доцент,
Державний податковий університет
e-mail: pavlyuh@gmail.com
ORCID ID 0000-0002-7850-8977;
Г. Ф. Санжарова,
старший викладач кафедри романської філології та порівняльно-типологічного мовознавства,
Київський університет імені Бориса Грінченка
e-mail: h.sanzharova@kubg.edu.ua
ORCID ID 0000-0002-0557-9192;
В. А. Санжаров,
канд. істор. наук,
Державний податковий університет
e-mail: 6253693@gmail.com
ORCID ID 0000-0003-4075-8572

ВИКЛИКИ СУЧАСНОЇ КІБЕРБЕЗПЕКИ: ІНСТИТУЦІЙНІ І ПРАВОВІ ВІДПОВІДІ НІМЕЧЧИНИ

Стаття присвячена дослідженню німецької концепції кібербезпеки та її інституційного і законодавчого наповнення. Новітні «розумні» системи та технології, що лежать в основі повсякденного життя, такі як електромережі, системи управління повітряним рухом, супутники, медичні технології, промислові підприємства та світлофори, підключені до інтернету, потенційно наражаються на небезпеку несанкціонованого віддаленого втручання. Способи протидії інформаційним загрозам і ризикам різних країн формуються по-різному.

У статті проаналізовано законодавчі кіберініціативи німецького уряду впродовж останніх десятиліть. Німецьке законодавство намагається враховувати зміни кібернетичного, геополітичного та технологічного ландшафту (поява аналітики великих даних, автономних систем, надійних промислових систем управління, кіберфізичних систем та «інтернету речей», технологій «інтелектуального міста», автоматизованої верифікації систем) та створити дієву систему кібербезпеки, за якої створення продуктів, систем та послуг є «безпечними за умовчанням». Констатовано, що унікальною рисою німецького законодавства є визначення такою, що потребує захисту поруч з об'єктами критичної інфраструктури, категорії «важливих» об'єктів.

Зазначено, що кібербезпекова стратегія Німеччини використовує невійськовий підхід, не пропонує включення кіберструктур Бундесверу до Національного центру реагування чи Національної ради з кібербезпеки, не розглядає можливості проведення упереджувальних наступальних кібероперацій. Можна вважати доведеним, що подальше розширення інструментів, які є в розпорядженні німецького уряду та військових, для роботи в кіберсфері залишається обмеженим жорсткими правовими нормами.

Автори вважають безперечним, що Німеччина завдяки своїм різноманітним зусиллям у юридичній, технологічній та виробничій сферах, постійному вдосконаленню політики, правил і законодавства наразі готова долати виклики та загрози, властиві кіберсфері. Зроблено висновок, що далекоглядний характер законодавчих зусиль робить Німеччину одним з лідерів в ЄС і на світовій арені в питаннях кібербезпеки.

Ключові слова: *кіберпростір, кібербезпека, кіберзлочин, Федеральне відомство з інформаційної безпеки, Кібербезпековий акт Євросоюзу*.

Постановка завдання. Метою нашого дослідження є аналіз німецької концепції кібербезпеки та її інституційного і законодавчого наповнення.

Постановка проблеми. Інформатизація, інтернет, цифрові технології у державному управлінні створили новітнє явище «е-держава», «е-уряд» тощо. Це вимагає відповідних змін правових механізмів державно-правових інститутів. Невирішеність низки правових проблем, пов’язаних з інформаційно-комунікаційною сферою, унеможливлює протистояння сучасним кіберзагрозам за допомогою чинного законодавства. Ландшафт кіберпростору швидко еволюціонує і залежно від розвитку технологій постійно з’являються нові проблеми: виникла організована кіберзлочинність, кібератаки стають більш масовими, витонченими та мають руйнівні наслідки у разі успішного здійснення. Економіка, управління державою та надання основних послуг залежать від цілісності кіберпростору, а також інфраструктури, систем та даних, що лежать у його основі. Новітні «розумні» системи та технології, що лежать в основі повсякденного життя, такі як електромережі, системи управління повітряним рухом, супутники, медичні технології, промислові підприємства та світлофори, підключені до інтернету, потенційно наражаються на небезпеку несанкціонованого віддаленого втручання. Способи протидії інформаційним загрозам і ризикам різних країн формуються по-різному. Концепція кібербезпеки Німеччини пройшла шлях від базового розуміння безпеки приватної особи до питань безпеки на державному рівні, які зобов’язують уряд до створення посилених оборонних і наступальних кібер- та інформаційних інституцій і технологій, до організації співпраці урядових установ з приватними корпораціями та транснаціональними організаціями, до поширення кібербезпекових заходів з підприємств критичної інфраструктури на життєво-важливі для економіки і суспільства [1]. Законодавчі ініціативи Німеччини як на національному, так і на міжнародному рівнях є важливим джерелом для вивчення.

Аналіз останніх досліджень і публікацій. Вітчизняна наукова література з проблем кіберзлочинності, інструментів і засобів її запобігання, створення дієвої

системи кібербезпеки постійно зростає насамперед через актуальність і серйозність загрози. Аналіз останніх публікацій показав, що в центрі уваги дослідників є питання визначення поняття кіберзлочину [2, с. 188–189; 3, с. 409]; сутності і типології кримінальних правопорушень у сфері інформаційних технологій у національних законодавствах і міжнародному праві [2; 4; 5]; розроблення єдиної кримінальної стратегії, пов'язаної з протидією кіберзлочинності [2, с. 192]; технологічних, інституційних, законодавчих складників системи кібербезпеки [6; 7]. Міжнародний досвід найбільш економічно- і технологічно-розвинених країн у цій царині [1, с. 71–73; 8, с. 80–82; 9, с. 151–160] повинен вивчатися і активно використовуватися у процесі вдосконалення існуючого національного законодавства.

Виклад основного матеріалу. Німеччина з населенням трохи більше 80 млн осіб має 66,4 млн інтернет-користувачів (близько 84 % німців); у країні зафіксовано майже 137 мільйонів підключень до мобільних мереж; німці охоче беруть участь у різноманітних сферах електронної комерції. Використання інтернету німцями вище середнього по ЄС.

Водночас Німеччина посідає 24 місце з 27 країн-членів Європейського Союзу за послугами електронного урядування. Німецький федералізм є викликом для впровадження дієвої системи електронного урядування. Крім федерального уряду, у Німеччині є 16 земель і понад 10 000 громад, які надають адміністративні послуги. Поділ між федеральною та земельною юрисдикцією є одним із стовпів Конституції Німеччини. Електронний уряд визначено як найбільшу проблему для країни у сфері цифровізації. Уряд Німеччини зробив основним пріоритетом покращення та розширення існуючої інфраструктури та досягнення амбітної мети забезпечити достатню інтернет-інфраструктуру до 2025 року [10, с. 6].

Зусилля та бажання Німеччини боротися з кіберзагрозами в державному та приватному секторах виникли з їх появою і продовжують розвиватися в міру розвитку цих загроз [11, с. 74–76]. 1991 року уряд Німеччини створив Федеральне відомство з інформаційної безпеки (Bundesamt für Sicherheit in der Informationstechnik, BSI) [12]. «Стратегія кібербезпеки Німеччини», опублікована 2011 року, стала базовим документом і основою для стратегії кібербезпеки Федеративної Республіки Німеччина [1, с. 72].

Бундестаг з раннього етапу законодавчих кіберініціатив зрозумів, що зусилля із захисту ІТ-інфраструктури, як основи кібербезпеки, – це співпраця між усіма акторами кіберпростору: приватними корпораціями, урядовими установами та транснаціональними організаціями. Зусилля уряду та представників ділового світу в Німеччині корегує Альянс з кібербезпеки (Allianz für Cyber-Sicherheit, AfCS), який був спільно ініційований BSI та цифровою асоціацією Німеччини (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien, BITKOM). Членство в Альянсі надає доступ до певної інформації щодо кібербезпеки та дозволяє використовувати логотип «AfCS», що демонструє активну підтримку компанією кібербезпеки. Наразі близько 4 000 компаній роблять внески в AfCS (більше 2 500 2018 року) [10, с. 14].

Німецьке регулювання кібербезпеки передує загальноєвропейському завдяки «Закону про підвищення безпеки систем інформаційних технологій» (ITSiG) від 17 липня 2015 року [13], 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 року [14]. До списку критичної інфраструктури було віднесено сектори фінансів та страхування, транспорту та дорожнього руху, а також охорони здоров'я. 2016 року 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 2016 року призвело лише до незначних змін Регламенту від 21 червня 2017 року та ухвалення «Закону про введення в дію NIS» від 23 червня 2017 року [11, 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 і федеральною розвідувальною службою.

Важливість кіберпростору як нового й унікального поля бою, крім традиційних наземних, морських і повітряних сфер ведення бойових дій призвела до створення німецького військового кіберландшафту. Однією із найпомітніших подій у новітній німецькій військовій історії стала поява 2017 нового військового підрозділу під назвою Служба кібер- та інформаційної сфери (Cyber- und Informationsraum, CIR) з батальйонами та спеціалізованими центрами по всій Німеччині (особовий склад 11 600 осіб) [10, с. 16–18]. Нове кіберкомандування зі штаб-квартирою в Бонні очолив інспектор кібернетичного та інформаційного простору – генерал-лейтенант Людвіг Лейнхос (з 25.09.2020 цю посаду обіймає віцеадмірал Томас Даум). Міністерство оборони повідомило, що ІТ-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 [11, с. 82]. Командуванню у кібернетичному та інформаційному просторі 2021 були підпорядковані понад 13 500 співробітників і інноваційний центр, який з'єднує військових із технологічними стартапами. Водночас подальше розширення інструментів, які є в розпорядженні німецького уряду та військових для роботи в кіберсфері, залишається обмежен жорсткими правовими нормами. Кіберзагрози виходять за рамки класичного розмежування між внутрішньою та зовнішньою безпекою і юрисдикційного поділу між поліцією та військовими, тому було створено Кіберагентство (Agentur für Innovation in der Cybersicherheit, Cyberagentur), яким спільно керують Міністерство внутрішніх справ і Міністерство оборони з бюджетом близько 352,5 мільйона євро [10, с. 18].

Хоча зусилля в боротьбі з кіберзагрозами німецьких збройних сил визнані, кібербезпекова стратегія Німеччини використовує невійськовий підхід, не пропонує

включення кіберструктур Бундесверу до Національного центру реагування чи Національної ради з кібербезпеки, не розглядає можливості проведення упереджувальних наступальних кібероперацій.

18 травня 2021 року Бундестаг ФРН ухвалив «Закон про підвищення безпеки систем інформаційних технологій 2.0.» [15]. Закон (ITSiG 2.0.) реагує на проблеми IT-безпеки у 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 являють собою особливий суспільний інтерес; розширюють та посилюють повноваження Федерального відомства (BSI). 1 січня 2022 року 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. Водночас 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», що регулюють важливі сектори, які не підпадають під дію «Закону про Федеральне управління з інформаційної безпеки» [16, 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, тобто вони відрізняються від категорії секторів критичної інфраструктури, але законодавці вважають, що вони також потребують і заслуговують на захист. Отже, 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.

Німецьке законодавство намагається враховувати зміни кібернетичного, геополітичного та технологічного ландшафту (поява аналітики великих даних, автономних систем, надійних промислових систем управління, кіберфізичних систем та «інтернету речей», технологій «інтелектуального міста», автоматизованої верифікації систем) у створити дієву систему кібербезпеки, за якої створення продуктів, систем та послуг є «безпечними за умовчанням», міркування безпеки враховуються вже на етапі

проєктування, а для деактивації функцій безпеки потрібне усвідомлене рішення користувача.

Висновки. Національна правова база Німеччини в галузі кібербезпеки відповідає суті змін, передбачених «Директивою про безпеку мережевих та інформаційних систем 2.0.» (NIS2) для імплементації в національне законодавство країн-членів ЄС [16, 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 рішення Федеральне управління з інформаційної безпезпеки створило платформу обміну інформацією про шкідливі програми.

Отже, Німеччина є активним учасником зусиль з роз'яснення принципів застосування і практичного дотримання міжнародного права в кіберпросторі. Німеччина завдяки своїм різноманітним зусиллям у 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.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Санжарова Г. Ф., Мацелик М. О., Санжаров В. А. Еволюція стратегії кібербезпеки Німеччини протягом останніх трьох десятиліть: інституційний та правничий виміри. *Наукові тренди постіндустріального суспільства :* матеріали IV Міжнародної наукової конференції, м. Суми, 31 березня 2023 р. Вінниця : Європейська наукова платформа, 2023. С. 71–73.

2. Топчій В. В., Бодунова О. М. Система кримінальних правопорушень у сфері інформаційних технологій: міжнародно-правовий вимір. *Ірпінський юридичний часопис. Серія: право*. 2023. Вип. 1 (10). С. 187–194. DOI: https://doi.org/10.33244/2617-4154.1(10).2023.187-194.

3. Юртаєва К. В. Кримінальна відповідальність за кіберзлочини, вчинені під час збройного конфлікту: міжнародні тенденції та українські реалії. *Юридичний науковий електронний журнал*. Запоріжжя, 2022. № 12. С. 409–414. DOI: https://doi.org/10.32782/2524-0374/2022-12/96.

4. Лисько Т. Д., Меланіч В. В., Славіта Ю. В. Протидія кіберзлочинності: сучасний стан вітчизняного законодавства та досвід зарубіжних країн. *Актуальні проблеми держави і права*. 2022. № 96. С. 44–49. DOI: https:// doi.org/10.32782/apdp.v96.2022.4.

5. Лугіна Н. А., Лучук А. М. Порівняльний аналіз вітчизняного та європейського законодавства з питань запобігання кіберзлочинності. *Ірпінський юридичний часопис. Серія: право*. 2023. Вип. 1 (10). С. 180–186. DOI: https://doi.org/10.33244/2617-4154.1(10).2023.180-186.

6. Лактіонов І., Кміт А., Опірский І., Гарасимчук О. Дослідження інструментів захисту інтернет-ресурсів від DDOS-атак під час кібервійни. *Кібербезпека: освіта, наука, техніка*. 2022. Вип. 1(17). С. 91–111. DOI: https://doi.org/10.28925/2663-4023.2022.17.91111.

7. Барченко Н., Лубчак В., Лаврик Т. Модель індикаторів оцінки національного рівня цифровізації та кібербезпеки держав світу. *Кібербезпека : освіта, наука, техніка*. 2022. Вип. 2(18). С. 73–85. DOI: https://doi.org/10.28925/2663-4023.2022.18.7385

8. Шевченко А. Є., Павлюх О. А., Санжаров В. А. Питання кібербезпеки в сучасному італійському законодавстві: національний безпековий периметр. *Наукові тренди постіндустріального суспільства :* матеріали IV Міжнародної наукової конференції, м. Суми, 31 березня 2023 р. Вінниця : Європейська наукова платформа, 2023. С. 80–82.

9. Колосов О. О. Особливості протидії кіберзлочинам у Сполучених Штатах Америки. *Ірпінський юридичний часопис. Серія: право*. 2023. Вип. 1 (10). С. 151–160. DOI 10.33244/2617-4154.1(10).2023.151-160.

10. Cymutta S. National Cybersecurity Organisation: Germany. Tallinn, 2020. 21 p. URL : https://ccdcoe.org/uploads/2020/12/Country_Report_DEU.pdf

11. 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.

12. Historie des BSI. URL : https://www.bsi.bund.de/DE/Das-BSI/BSI-Historie/bsi-historie_node.html

13. 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.

14. 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.

15. 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.

16. 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.

REFERENCES

1. Sanzharova G., Macelyk M., Sanzharov V. The Evolution of Germany's Cyber Security Strategy over the Past Three Decades: Institutional and Legal Dimensions. *Scientific Trends of the Post-Industrial Society :* materials of the IV International Scientific Conference. Vinnytsia : European Scientific Platform, 2023. P. 71–73.

2. Topchii V., Bodunova O. The system of criminal offenses in the field of information technologies: the international legal dimension. *Irpin Legal Chroniclles: The Scientific Journal*. 2023. Issue 1 (10). P. 187–194.

3. Yurtaieva K. V. Criminal Liability for Cybercrimes Committed at the Time of the Armed Conflict: International Tendencies and Ukrainian Realities. *Juridical scientific and electronic journal.* 2022. Issue 12. P. 409–414.

4. Lysko T. D., Melanich V. V., Slavita Y. V. Combating cybercrime: the current state of domestic legislation and the experience of foreign countries. *Current Problems of State and Law*. 2022. Vol. 96. P. 44–49.

5. Luhina N., Luchuk A. Comparative analysis of Domestic and European legislation on cybercrime prevention. *Irpin Legal Chroniclles: The Scientific Journal*. 2023. Issue 1 (10). P. 180–186.

6. Laktionov I., Kmit A., Opirskyy I., Harasymchuk O. Research Tools for Protecting Internet Resources from Ddos-attack during Cyberwar. *Cybersecurity: Education, Science, Technique*. 2022. Issue 1(17). P. 91–111.

7. Barchenko N., Lubchak V., Lavryk T. Model of Indicators for the Assessment of the National Level of Digitalization and Cyber Security of the Countries of the World. *Cybersecurity: Education, Science, Technique*. 2022. Issue 2(18). P. 73–85.

8. Shevchenko A., Pavliukh O., Sanzharov V. Cybersecurity Issues in Contemporary Italian Law: the National Security Perimeter. *Scientific Trends of the Post-Industrial Society :* materials of the IV International Scientific Conference. Vinnytsia : European Scientific Platform, 2023. P. 80–82.

9. Kolosov O. Features of combating cybercrimes in the United States of America. *Irpin Legal Chroniclles: The Scientific Journal*. 2023. Issue 1 (10). P. 151–160.

10. Cymutta S. National Cybersecurity Organisation: Germany. Tallinn, 2020. 21 p. URL : https://ccdcoe.org/uploads/2020/12/Country_Report_DEU.pdf

11. 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.

12. Historie des BSI. URL : https://www.bsi.bund.de/DE/Das-BSI/BSI-Historie/bsi-historie_node.html

13. 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.

14. 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.

15. 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.

16. 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.

O. Pavliukh, G. Sanzharova, V. Sanzharov. Challenges of Modern Cyber Security: Germany's Institutional and Legal Responses

The article is devoted to the study of the German concept of cyber security and its institutional and legislative content. The latest "smart" systems and technologies that underpin everyday life, such as power grids, air traffic control systems, satellites, medical

technology, industrial plants and traffic lights, are connected to the Internet and thus potentially vulnerable to unauthorized remote interference. Ways of countering information threats and risks in different countries are formed in different ways.

The article analyzes the legislative cyber initiatives of the German government during the last decades. German legislation tries to take into account changes in the cyber, geopolitical and technological landscape (the emergence of big data analytics, autonomous systems, reliable industrial control systems, cyber-physical systems and the "Internet of Things", "intelligent city" technologies, automated system verification) and create an effective cyber security system, whose creation of products, systems and services are "secure by default". It was established that a unique feature of the German legislation is the definition of the category of "important" objects that require protection next to critical infrastructure objects.

It was noted that Germany's cyber security strategy uses a non-military approach, does not propose the inclusion of cyber structures of the Bundeswehr in the National Response Center or the National Cyber Security Council, does not consider the possibility of conducting preemptive offensive cyber operations. It can be considered proven that the further expansion of the tools at the disposal of the German government and the military to work in the cyber sphere remain limited by strict legal regulations.

The authors believe that it is indisputable that Germany, thanks to its various efforts in the legal, technological and industrial spheres, and the continuous improvement of policies, regulations and legislation, is currently ready to overcome the challenges and threats inherent in the cyber sphere. It was concluded that the far-sighted nature of legislative efforts makes Germany one of the leaders in the EU and on the world stage in matters of cyber security.

***Keywords**: Cyberspace, Cybersecurity, Cybercrime, Federal Office for Security in Information Technology, EU Cybersecurity Act.*

Стаття надійшла до редколегії 26 квітня 2023 року