: https://er.dduvs.in.ua/bitstream/123456789/7274/1/2.pdf.

6. Халапсіс О. В. Міжнародні виміри правових міфів. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2021. Спеціальний випуск № 2. С. 354–360. URL : https://doi.org/10.31733/2078-3566-2021-6-354-360.

Людмила РИБАЛЬЧЕНКО
завідувач кафедри інформаційних технологій Дніпропетровського державного університету внутрішніх справ,
кандидат економічних наук, доцент

Марина ЛИСЯК
студентка ННІ права та інноваційної освіти Дніпропетровського державного університету внутрішніх справ

СИСТЕМА ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Система забезпечення кібербезпеки становить органічне поєднання спільною метою державних і недержавних інституцій, а також інших суб'єктів, що беруть участь у здійсненні заходів, спрямованих на забезпечення кібербезпеки. Спектр суб'єктів забезпечення кібербезпеки не може обмежуватися виключно державними органами та їхніми посадовими особами. У складі суб'єктів забезпечення кібербезпеки виділяють загальних і спеціальних суб'єктів. До останніх належать державні органи, котрі, крім загальних функцій, уповноважені на здійснення боротьби з кіберзлочинністю та кібертероризмом, а також на забезпечення кібернетичного захисту об'єктів національної критичної інфраструктури.

Метою даного дослідження є проаналізувати стан забезпечення кібербезпеки в Україні та визначити перспективи його подальшого розвитку.

Питання забезпечення кібернетичної безпеки, у тому числі в контексті проблематики забезпечення інформаційної та національної безпеки, досліджувались у працях О. Баранова, В. Бутузова, О. Довганя, Б. Кормича, Р. Лукянчука, А. Марущака, М. Ожевана, В. Пилипчука, М. Погорецького, Т. Качука, О. Тронько, І. Сопілки, В. Шеломенцева та інших науковців.

Закон України «Про основні засади забезпечення кібербезпеки України», прийнятий 5 жовтня 2017 р., заклав загальні основи для побудови національної системи кібербезпеки, а також визначив основні завдання та компетенцію інституцій кібербезпеки, до яких належать Національний координаційний центр з кібербезпеки, Міністерство оборони, Генеральний штаб Збройних Сил України, Державна служба спеціального зв'язку та

захисту інформації, Служба безпеки України, Національна поліція, Національний банк, Секретна служба України та ін. У цьому Законі передбачено створення умов для протидії кібершахрайству та захисту національної системи кібербезпеки, підприємств, установ і організацій, незалежно від форм власності, що провадять діяльність у сфері електронного зв'язку, захисту інформації та/або є власниками (керівниками), об'єкти критичної інфраструктури, наукові установи, навчальні заклади, організації, громадські об'єднання тощо.

Кібербезпека – це захист підключених до Інтернету систем, таких як обладнання, програмне забезпечення та дані, від кіберзагроз. Ця практика використовується окремими особами та підприємствами для захисту від несанкціонованого доступу до центрів обробки даних та інших комп'ютеризованих систем.

Систему безпеки визначають і як механізм розробки, трансформації та реалізації концепцій, стратегій та тактики у сфері безпеки за допомогою скоординованої діяльності уряду та неурядових структур, сукупність організаційно об'єднаних органів управління, сил і засобів, призначених для вирішення відповідних завдань забезпечення національної безпеки [1, с. ___].

Система національної безпеки функціонує як організаційна система державних і недержавних інститутів, інших органів, що призначені для вирішення завдань забезпечення національної безпеки в порядку, встановленому законом [2]. Надійна стратегія кібербезпеки може забезпечити надійний захист від зловмисних атак, призначених для доступу, зміни, видалення, знищення або виманювання систем і конфіденційних даних організації чи користувача. Кібербезпека відіграє важливу роль у запобіганні атакам, що мають на меті вимкнення або порушення роботи системи чи пристрою.

Зі збільшенням кількості користувачів, пристроїв і програм на сучасному підприємстві в поєднанні зі збільшенням потоку даних, значна частина яких є конфіденційними, важливість кібербезпеки продовжує зростати. Зростаюча кількість і складність кіберзловмисників і методів атак ще більше обтяжують проблему.

Кібербезпека належить до сфери адміністративних правовідносин, оскільки відносини між учасниками ґрунтуються на владності та підпорядкованості. Вона передбачає також створення механізму кіберзахисту, користуючись діючим чинним законодавством. Отже, забезпечення кібербезпеки є стратегічним завданням держави.

Кібербезпеці постійно загрожують хакери, втрата даних, порушення конфіденційності, управління ризиками та зміна стратегій кібербезпеки. Скорочення кількості кібератак найближчим часом зростає. Крім того, збільшення точок входу для атак, наприклад, із появою Інтернету речей, і зростаюча площа атак збільшують потребу у захисті мереж і пристроїв.

Кіберзлочинність постійно вдосконалюється і зростає з розвитком

інформаційних технологій. Це ускладнює виявлення та протидію зазначеним протиправним діям, і проблема кібербезпеки стає проблемою не лише загальнодержавного рівня, а кожного окремо взятого підприємства, організації.

Таким чином, у сфері кібербезпеки існує низка проблем, що не можуть бути повністю вирішені звичайними засобами і потребують уваги суспільства та відповідних державних органів. Масштабна кіберзлочинність, що зачіпає всі сфери життя суспільства, спирається на новітні методи проведення кібератак та управління громадською обізнаністю, вимагає системного підходу до створення комплексної національної системи кібербезпеки, здатної протистояти цим загрозам. Важливими елементами цієї системи є реалізація регулятивної та охоронної функції права, запровадження правових механізмів забезпечення кібербезпеки як складової національної безпеки України.

Список використаних джерел

1. Ліпкан В. А., Ліпкан О. С. Національна і міжнародна безпека у визначеннях та поняттях. Київ : Текст, 2008. 400 с.

2. Тімкін І. Ф., Новікова Н. Є. Структурно-функціональна характеристика системи забезпечення національної безпеки України. *Науковий вісник Міжнародного гуманітарного університету. Серія : Історія. Філософія. Політологія.* 2016. № 11. С. 64–68. URL : http://vestnik-humanities.mgu.od.ua/archive/2016/11/11-2016.pdf#page=64.

3. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text.

4. Рибальченко Л. В. Кіберзлочинність в глобальному просторі. *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* 2022. Спеціальний випуск № 2(121). С. 524–530.

5. Rybalchenko L., Kosychenko O., Klinytskyi I. Ensuring economic security of enterprises taking into account the peculiarities of information security. *Philosophy, Economics and Law Review.* 2022. Vol. 1(3). P. 71–81.

6. Дисковський А. О., Косиченко О. О., Рибальченко Л. В. Основи організації захисту об’єктів та інформації від злочинних посягань : навч. посібник для слухачів магістратури. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2020. 104 с.

7. Рибальченко Л. В., Махницький О. В. Кібербезпека під час воєнного стану. *Шкідливі програми як загроза об’єктам критичної інфраструктури в умовах кібервійни : зб. матеріалів міжвідомчого круглого столу* (м. Київ, 21 лют. 2023 р.). Київ : ІСТЕ СБУ, 2023. С. 120–124.