СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ПРАВА

РЕФОРМУВАННЯ ПРАВОВОЇ СИСТЕМИ В КОНТЕКСТІ ЄВРОІНТЕГРАЦІЙНИХ ПРОЦЕСІВ

МАТЕРІАЛИ
VI Міжнародної науково-практичної конференції
(Суми, 19–20 травня 2022 року)

Суми
Сумський державний університет
2022

2. Денисюк Д. С. Принципи діяльності національної поліції України: теорія та практика реалізації. Митна справа. 2015. № 5. С. 63-68.
3. Звіт Національної поліції України про результати роботи у 2021 році URL: https://www.npu.gov.ua/assets/userfiles/files/zvity/Zvit_NPU_2021_.pdf.

ПРАВООХОРОННІ ОРГАНИ ЯК СУБ'ЄКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Ільченко О. В.
к.ю.н., доцент, доцент кафедри КПДС ННІ права
Сумського державного університету
Корощенко К.Р.
студентка IV курсу ННІ права
Сумського державного університету

Інформаційна безпека в Україні є важливою галуззю з забезпечення простору від внутрішніх та зовнішніх загроз. Варто зауважити, що інформація безпека держави – широке поле для аналізу як вченими, так і для законодавчого врегулювання. Адже не припиняються намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації. Положення України в інформаційному полі є відображенням здатності держави захистити себе на всіх можливих рівнях. Дуже важливою частиною інформаційної безпеки є кібербезпека держави, ця галузь є значно вужчою для регулювання. В останні роки в Україні почали діяти реформи та модернізаційні процеси щодо цієї галузі. Неодмінно необхідно наголосити на тому, що всі процеси тісно пов'язі з євроінтеграційними заходами, це може підтвердити значна фінансова та інформаційна допомога партнерів.

Сьогодні поняття "інформаційна безпека" розглядається в аспекті "кіберпезпека". Закон України "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 № 2163-VIII визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Загрози кібербезпеці і безпеці інформаційних ресурсів визначаються в уразливості об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак, а

також у фізичній і моральній застарілості системи охорони державної таємниці та інших видів інформації з обмеженим доступом [1].

На думку Б. Кормич забезпечення функціонування інформаційної безпеки у широкому сенсі, та кібербезпеки, можливе через систему органів розглядає державно-правовий механізм інформаційної безпеки систему органів державної влади загальної і спеціальної компетенції, задіяних у процесі формування та реалізації політики інформаційної безпеки, внутрішні й зовнішні ролі та відносини якої регулюються системою правових норм і принципів в [2].

Основними суб'єктами національної системи кібербезпеки є: Державна служба спеціального зв'язку та захисту інформації України; Національна поліція України; Служба безпеки України; Міністерство оборони України; Генеральний штаб Збройних Сил України; розвідувальні органи; Національний банк України.

Державна служба спеціального зв'язку та захисту інформації України (далі-ДСС). У сфері забезпечення кібербезпеки ДСС України займається формуванням і реалізацією політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах; координує діяльність інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту; забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту; інформує про кіберзагрози та відповідні методи захисту від них; забезпечує впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури тощо [3].

У своїй діяльності Національна Поліція підпорядковується Кабінету Міністрів України і спрямовується та координується через Міністерство внутрішніх справ України, на яке покладається реалізація повноважень щодо: створення і забезпечення функціонування підрозділів із протидії кіберзлочинності; розробки та реалізації комплексу організаційних і практичних заходів, спрямованих на боротьбу з кіберзлочинами; створення і забезпечення функціонування цілодобової контактної мережі для надання невідкладної допомоги у розслідуванні кіберзлочинів тощо [4].

Служба безпеки України здійснює запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам

держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки [5].

Якщо говорити про повноваження Міністерство оборони України (далі-МО) та Генерального штабу Збройних Сил України у сфері забезпечення кібербезпеки, то слід зазначити, що відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» вони є майже ідентичними: зазначені державні органи здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснюють військову співпрацю з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз; впроваджують заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану Розвідувальні органи (Служба зовнішньої розвідки України, розвідувальні органи МО, розвідувальні органи спеціально уповноваженого центрального органу виконавчої влади у справах охорони державного кордону здійснюють у сфері забезпечення кібербезпеки розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки [3].

Національний банк України визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки у банківській системі України та для суб'єктів переказу коштів, здійснює контроль за їх виконанням; створює центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту у банківській системі України; забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки на об'єктах критичної інфраструктури у банківській системі України [5].

Як зазначає В. Бурячок, досвід іноземних країн та особливості українських реалій свідчать, що розв'язання основних завдань кібербезпеки неможливе без створення: міжвідомчого структурного органу, який на постійній основі забезпечував би координацію діяльності певних відомств, правоохоронних і силових структур України з питань забезпечення кібернетичної безпеки; центральних органів у структурі певних відомств, правоохоронних і силових структур України з функціями виявлення й оцінювання рівня (визначення ступеня) критичності стороннього кібервпливу, розроблення концептуальних засад і надання рекомендацій щодо протидії його проявам, а також активної протидії кібератакам протиборчих сторін і впливу на їх інформаційно-телекомунікаційні системи; органів власної інформаційної та кібербезпеки – державних

установ (відомств) і комерційних структур, які повинні тісно взаємодіяти із зазначеними центральними органами з питань вироблення єдиної політики щодо захисту як власного, так і спільного національного інформаційного і кіберпросторів [6].

Висновки. Інформаційна безпека в Україні – це важлива частина національної безпеки, яка полягає у досягненні стану захищеності держави від внутрішніх і зовнішніх загроз, що забезпечує умови існування людини, держави і суспільства, які гарантовані Конституцією. Ми вважаємо, що кібербезпека є складовою інформаційної безпеки і покликана захищати життєво важливі інтереси людини і громадянина, суспільства та держави під час використання кіберпростору, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. Важливим державним механізмом для забезпечення кібербезпеки в інформаційному просторі є правоохоронні органи, які у межах своїх повноважень здійснюють всі заходи для досягнення цілей та завдань. Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України, Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України – це ті правоохоронні органи, які здійснюють різнохарактерні заходи та виконують завдання щодо захисту кіберпростору, розслідування злочинів, співпраці з міжнародними органами і реалізують ще дуже багато функцій. Актуальним залишається питання координації всіх органів для досягнення більшої ефективності.

ЛІТЕРАТУРА:

1. Шемчук В.В. Конституційно-правове забезпечення інформаційної безпеки сучасних держави: порівняльно-правовий аналіз. дис. … канд. юрид. наук: 12.00.02. Ужгород, 2020. 411 с.

2. Кормич Б.А. Інформаційне право : підруч. Харків : БУРУН і К., 2011. 334 с.

3. Про Державну службу спеціального зв'язку та захисту інформації України від 23.02.2006.№30/ *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення: 02.04.2022).

4. Тарасюк А.В. Система суб'єктів забезпечення кібербезпеки в Україні. *Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки.* 2020. № 2 (25). С. 119-125.

5. Про основні засади забезпечення кібербезпеки України від 05.10.2017. №45/ *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 02.04.2022).