

## LAW AND INTERNATIONAL LAW

# Актуальні питання забезпечення кібербезпеки «Smart City»/«Cyber City» як напряму реформування територіальних громад в Україні

**Діордіца Ігор Володимирович<sup>1</sup>**

<sup>1</sup> доктор юридичних наук, професор, професор кафедри приватного та публічного права;  
Київський національний університет технологій та дизайну; Україна

Сучасні розумні міста збирають величезну кількість різноманітних даних. Сіетл, наприклад, збирає інформацію про все: від водійських прав до членства в профспілках. А з більшою кількістю даних і центрів їх обробки міста піддаються підвищеному ризику кібератак. У цьому новому цифровому ландшафті обов'язок захищати конфіденційні дані покладається на муніципальні органи влади. З метою забезпечення кібербезпеки штат Нью-Йорк інвестував понад 60 млн. доларів у створення спільного операційного центру кібербезпеки в Брукліні для обслуговування міст Нью-Йорк, Олбані, Сіракузи, Ваффало, Рочестер і Йонкерс. У Сіетлі бюджет міста на цифрову безпеку збільшився із з 5,3 млн. доларів у 2020 році до 8,4 млн. доларів у 2021 році, хоча на 2022 рік бюджет зменшився до 7,5 мільйона доларів (однак такі видатки також є суттєвими) [1].

Територіальні громади в Україні, нажаль, не вважають за необхідне належним чином фінансувати заходи із забезпечення кібербезпеки конфіденційної інформації, що перебуває у їх віданні.

Зокрема, у 2017 році (вже після масованих атак вірусу Petya) Київська міська рада спромоглася на прийняття Рішення «Про вжиття заходів кібербезпеки» від 22.06.2017 № 614/2776, яким виконавчому органу КМДА доручалося вжити протягом 2017 року заходів щодо впровадження вітчизняного програмного забезпечення для потреб місцевих органів виконавчої влади та органів місцевого самоврядування, підприємств, установ та організацій, що належать до комунальної власності

## LAW AND INTERNATIONAL LAW

територіальної громади міста Києва, без додаткових витрат з бюджету міста Києва [2].

У листопаді 2018 року в м. Дніпро було створено перший регіональний центр СБУ, основними завданнями якого є реагування на кібератаки, націлені на державні електронні інформресурси та об'єкти критичної інфраструктури Дніпропетровщини [3]. А наприкінці 2018 року Дніпровська міська рада уклала меморандум про співпрацю із СБУ. У рамках меморандуму фахівцям цієї міської ради було надано доступ до платформи MISP-UA (Malware Information Sharing Platform) – для ефективного реагування на кіберінциденти» [4].

За допомогою цієї платформи Дніпровська міська рада та Ситуаційний центр СБУ в режимі реального часу можуть обмінюватися технологічною інформацією про кіберзагрози, що забезпечить підвищення рівня безпеки та мінімізує час реакції на інциденти.

У лютому 2023 року на позачерговій сесії Мукачівської міської ради депутати розглянули проект Меморандуму про організацію взаємодії у сфері кібербезпеки та кіберзахисту між Державним центром кіберзахисту Державної служби спеціального зв'язку та захисту інформації України та Мукачівською міською радою. З метою організації співпраці та координації дій Сторін у сфері кібербезпеки та кіберзахисту, оперативного реагування на кіберінциденти (SOC) в межах функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, затвердили текст меморандуму та уповноважили Мукачівського міського голову на його підписання [5].

Зауважимо, що зазначені вище заходи щодо забезпечення кібербезпеки з боку територіальних громад не є системними. Так, залучаються до співпраці спеціальні державні органи (СБУ, ДССЗІУ і т. ін.), до повноважень яких належить реалізація державної політики щодо кіберзахисту державних підприємств, установ та організацій і об'єктів критичної інфраструктури. Проте безпосередніх повноважень щодо кіберзахисту інформаційних ресурсів, які перебувають у віданні підприємств, установ та організацій територіальних громад, дані органи не мають.

Звертаємо увагу, що у розрізі паралельного реформування місцевого самоврядування та інформаційної безпекової сфери, зокрема прийняття Стратегії кібербезпеки України (2021 р.), Доктрини інформаційної безпеки України (2017 р.), Стратегії інформаційної безпеки України (2021 р.), будь-які згадки про кібербезпеку інформаційних ресурсів, що створюються

## LAW AND INTERNATIONAL LAW

територіальними громадами та перебувають у їх віданні, у даних нормативно-правових актах взагалі відсутні.

Однак у п. 1 ч. 2 ст. 4 Закону України «Про основні засади забезпечення кібербезпеки України» (2017 р.) зазначено, що об'єктами кіберзахисту є комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону. Ч. 4 ст. 5 цього Закону визначено, що з-поміж інших, суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є органи місцевого самоврядування.

У статті 13 цього ж Закону, яка має назву «Фінансове забезпечення заходів кібербезпеки», зазначено, що джерелами фінансування робіт і заходів із забезпечення кібербезпеки, крім іншого, є кошти і місцевих бюджетів.

Однак, у ЗУ «Про місцеве самоврядування в Україні» (1997р.) про повноваження органу місцевого самоврядування як суб'єкта забезпечення кібербезпеки не згадується жодним чином. Як наслідок, у бюджетах територіальних громад не закладаються видатки на забезпечення кібербезпеки інформаційних ресурсів, які перебувають у їх віданні. Тобто такі видатки територіальні громади не вважають обов'язковими [6; 7].

Отже, з метою вирішення даної проблематики, пропоную доповнити Закон України «Про місцеве самоврядування в Україні» (1997 р.) такими положеннями: 1) ч. 1, ст. 26 Закону пунктом 59, розширивши повноваження сільських, селищних, міських рад, а саме: «Затвердження обов'язкових вимог із кібербезпеки об'єктів, що перебувають у власності територіальних громад»; 2) ч. 1, ст. 38 Закону пунктом 11, уповноваживши виконавчі органи сільських, селищних, міських рад на наступне: «Здійснення заходів щодо підготовки обов'язкових вимог із кібербезпеки об'єктів, що перебувають у власності територіальних громад».

### References:

- [1] Jordan McDonald. The smarter the city, the scarier the cyber risk. *Emerging Tech Brew*. 2022. URL: <https://www.emergingtechbrew.com/stories/2022/09/06/the-smarter-the-city-the-scarier-the-cyber-risk>
- [2] Рішення Київської міської ради «Про вжиття заходів кібербезпеки» від 22.06.2017 № 614/2776. URL: [https://kyivcity.gov.ua/npa/pro\\_vzhittya\\_zakhodiv\\_z\\_kiberbezpeki/e](https://kyivcity.gov.ua/npa/pro_vzhittya_zakhodiv_z_kiberbezpeki/e)

## LAW AND INTERNATIONAL LAW

iloxqlprq\_614-2776.pdf

- [3] У Дніпрі створили перший регіональний центр кібербезпеки СБУ (2018).  
*Укрінформ*. URL: <https://www.ukrinform.ua/rubric-regions/2585234-u-dnipri-stvorili-persij-regionalnij-centr-kiberbezpeki-sbu.html>
- [4] Дніпровська міська рада підписала меморандум про співпрацю з СБУ у сфері кібернетичної безпеки. URL: <https://dniprorada.gov.ua/uk/articles/item/28689/dniprovska-miska-rada-pidpisala-memorandum-pro-spivpracyu-z-sbu-u-sferi-kibernetichnoi-bezpeki>
- [5] У Мукачеві погодили меморандум у сфері кібербезпеки та кіберзахисту. URL: <https://cybersec.net.ua/novyny/496-u-mukachevi-pohodyly-memorandum-u-sferi-kiberbezpeky-ta-kiberzakhystu.html>
- [6] Рішення Київської міської ради «Про бюджет міста Києва на 2023 рік» від 08.12.2022 № 5828/5869. URL: [https://kyivcity.gov.ua/publiczna\\_informatsiia\\_Tag\\_166122/rishennya\\_pro\\_byudzheth\\_mista\\_kiyeva\\_na\\_2023\\_rik/](https://kyivcity.gov.ua/publiczna_informatsiia_Tag_166122/rishennya_pro_byudzheth_mista_kiyeva_na_2023_rik/)
- [7] Рішення Дніпровської міської ради від 08.12.2021 № 2/13 «Про бюджет Мукачівської міської територіальної громади на 2022 рік» URL: <https://dniprorada.gov.ua/uk/articles/item/48395/rishennya-miskoi-radi-vid-08-12-2021-213-pro-byudzheth-dniprovskoi-miskoi-teritorialnoi-gromadi-na-2022-rik>