УДК 342.9
DOI https://doi.org/10.32782/39221437

Діордіца І. В.,
доктор юридичних наук, професор,
завідувач кафедри кримінального права, процесу та криміналістики
Академії праці, соціальних відносин і туризму

Журавель Я. В.,
доктор юридичних наук, професор, декан юридичного факультету
Академії праці, соціальних відносин і туризму

ІННОВАЦІЙНІСТЬ КОНЦЕПТУ "SMART CITY" ТА ЮРИДИЧНІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ЙОГО КІБЕРБЕЗПЕКИ В УМОВАХ РЕФОРМУВАННЯ ТЕРИТОРІАЛЬНИХ ГРОМАД В УКРАЇНІ

INNOVATION OF THE "SMART CITY" CONCEPT AND LEGAL MECHANISMS FOR ENSURING ITS CYBERSECURITY IN THE CONTEXT OF REFORMING TERRITORIAL COMMUNITIES IN UKRAINE

У статті автори здійснили дослідження евристичних можливостей інтеграції інноваційних процесів у сучасний концепт «Smart City» у їх теоретичному і практичному сенсі та юридичні механізми забезпечення його кібербезпеки в умовах реформування територіальних громад в Україні. Актуальність дослідження обумовлена значним збільшенням інтересу до даного питання з боку держави та територіальних громад, що чітко відображено у Державній стратегії регіонального розвитку на 2021–2027 роки. З'ясовано, що основною передумовою невироблення чітких критеріїв концепції «Smart City» при формуванні стратегій розвитку регіонів чи територіальних громад є некоректне усвідомлення її сутності. Окреслено чотири блоки проблем, які ускладнюють впровадження концепції «Smart City» в українських містах, а саме: 1) у зв'язку з некоректним розумінням сутності концепту «Smart City» відсутнє стратегічне бачення щодо вибудування архітектоніки та практичного впровадження програм «Smart City» для конкретного міста чи територіальної громади; 2) джерела фінансування конкретної програми «Smart City»; 3) недостатні кваліметричні спроможності працівників територіальних громад, які б могли розробляти та супроводжувати реалізацію програми «Smart City» на належному рівні; 4) відсутність централізованого органу, на який би нормативно покладалися повноваження щодо централізованого урядування питань, пов'язаних із концептом «Smart City». Доведено, що територіальні громади в Україні не вважають за необхідне належним чином фінансувати заходи із забезпечення кібербезпеки конфіденційної інформації, що перебуває у їх віданні. Висновується, що у Законі України «Про місцеве самоврядування в Україні» (1997 р.) про повноваження органу місцевого самоврядування як суб'єкта забезпечення кібербезпеки не згадується жодним чином і, як наслідок, у бюджетах територіальних громад не закладаються видатки на забезпечення кібербезпеки інформаційних ресурсів, які перебувають у їх віданні. Запропоновано доповнити Закон України «Про місцеве самоврядування в Україні» (1997 р.) положеннями, які усунуть зазначену вище проблематику.

Ключові слова: *Smart City, територіальна громада, місцеве самоврядування, інформаційна безпека, кібербезпека, кіберзахист.*

In the article, the authors study the heuristic possibilities of integrating innovative processes into the modern concept of «Smart City» in their theoretical and practical sense and the legal mechanisms for ensuring its cybersecurity in the context of reforming territorial communities in Ukraine. The relevance of the study is due to a significant increase in interest in this issue on the part of the State and territorial communities, which is clearly reflected in the State Strategy for Regional Development for 2021–2027. It is found that the main prerequisite for the failure to develop clear criteria for the «Smart City» concept in the formation of strategies for the development of regions or territorial communities is an incorrect understanding of its essence. Four sets of problems that complicate the implementation of the «Smart City» concept in Ukrainian cities are outlined, namely: 1) due to an incorrect understanding of the essence of the «Smart City» concept, there is no strategic vision for building the architectonics and practical implementation of «Smart City» programmes for a particular city or territorial community; 2) sources of funding for a particular «Smart City» programme; 3) insufficient qualification and metric capabilities of employees of territorial communities who could develop and

support the implementation of the «Smart City» programme at the proper level; 4) lack of a centralised body that would be legally responsible for centralised government. It is proved that territorial communities in Ukraine do not consider it necessary to properly finance measures to ensure cybersecurity of confidential information under their jurisdiction. It is concluded that the Law of Ukraine «On Local Self-Government in Ukraine» (1997) does not mention the powers of a local self-government body as a subject of cybersecurity and, as a result, the budgets of territorial communities do not include expenditures for ensuring cybersecurity of information resources under their jurisdiction. It is proposed to supplement the Law of Ukraine «On Local Self-Government in Ukraine» (1997) with provisions that will eliminate the above-mentioned problems.

Key words: *Smart City, territorial community, local self-government, information security, cybersecurity, cyber defence.*

Постановка проблеми. Нині концепція «Smart City» є найпоширенішим підходом до створення розуміння можливих перспективних і життєздатних напрямів розвитку міст у всьому світі. Відповідно до цієї концепції, розвиток міського середовища переважно залежить від впровадження та збільшення використання сучасних цифрових технологій. Багатовекторне використання можливостей передачі даних через Інтернет, який вважається невід'ємною частиною «Smart City», забезпечує постійний моніторинг та оптимізацію багатьох сфер, таких як транспорт, паркування, освітлення, водопостачання, безпека та навіть процеси утилізації відходів, а також моніторинг може використовуватися для ініціювання реакції на різні події. Використання цифрових технологій є поширеним підходом до створення нових рішень, які відповідають викликам глобалізації, щоб покращити якість життя та зробити міста конкурентоспроможними та стійкими.

Центральні органи виконавчої влади України здійснюють поступові кроки щодо впровадження даної концепції в реальну практику територіальних громад. Зокрема, одним із завдань Державної стратегії регіонального розвитку на 2021–2027 роки є «сприяння запровадженню інноваційних технологій у системи управління розвитком міст на засадах концепції розумного міста («Smart City»). Водночас Міністерством розвитку громад та територій України розроблена Стратегія цифрової трансформації соціальної сфери з трьома основними напрямами: 1) розвиток електронної інфраструктури та цифровізація процесів міністерства; 2) запуск загальнонаціональних проєктів цифрової трансформації; 3) створення програми цифрового розвитку регіонів [1, с. 92; 2; 3].

Аналіз останніх досліджень і публікацій. В Україні чимало вчених займалися дослідженням окремих аспектів організаційного забезпечення смарт-інфраструктури як сталого розвитку громад. Так на рівні наукових робіт можемо відмітити праці С.А. Чукут та В.І. Дмитренка [4], О.Л. Єршової та Л.І. Бажан [5], А.А. Дискіної, О.М. Федорчук, О.І. Протосвіцька [6], Д.С. Луніна [7], В.А. Ліпкана [8] та ін. Однак, враховуючи безперервну динаміку розвитку даного явища, вважаємо за необхідне окреслити новели концепту «Smart City» та визначити юридичні механізми забезпечення його кібербезпеки в умовах реформування територіальних громад в Україні.

Формулювання цілей. Мета статті – розглянути евристичні можливості інтеграції інноваційних процесів у сучасний концепт «Smart City» у їх теоретичному та практичному сенсі. З огляду на порушену в науковій роботі проблематику, нами були поставлені наступні завдання: 1) окреслити новели концепту «Smart City»; 2) визначити юридичні механізми забезпечення його кібербезпеки в умовах реформування територіальних громад в Україні.

Виклад основного матеріалу. На наше переконання основною передумовою невироблення чітких критеріїв концепції «Smart City» при формуванні стратегій розвитку регіонів чи територіальних громад є некоректне усвідомлення її сутності.

Так, в останні роки міста почали використовувати більше технологій і стають розумнішими. Нові технології разом із швидким і простим зв'язком дозволяють містам краще використовувати свої джерела, економити гроші та надавати своїм громадянам найсучасніші послуги. Конкуренція між містами за залучення капіталу, нових жителів і туристів призвела до збільшення уваги до забезпечення високої якості життя та динамічної економічної ситуації. Уряди дійшли висновку, що хоча обмежені

бюджети, дефіцитні ресурси та застарілі системи часто ставлять під сумнів їхні цілі, інноваційні технології можуть перетворити ці виклики на можливості [9].

Отже, «Smart City» – це місто, яке надає переваги системі автоматизації та модифікації муніципальних обов'язків і покращує життя його мешканців. Розумне місто складається з різних типів датчиків Інтернету речей (IoT). Ці датчики включають розумні датчики паркування, структуровану інформацію про здоров'я, миттєве картографування міського шуму, контроль дорожнього руху, оптимізацію смуг руху та розумне освітлення і т. ін. [10]. IoT – це активна технологія, яка використовується для згаданих компонентів розумного міста. Однак хмара є активною платформою для зберігання та інтерпретації централізованих даних розумного міста.

Архітектоніка розумного міста може включати такі елементи:

1. Розумне/електронне урядування: «розумна рада громади» створює цінність для сталого суспільного продукту, використовуючи інтеграцію ІКТ для планування, управління та операцій на одному рівні або між ними. Іншими словами, в розумному урядуванні саме впровадження бізнес-процесів на основі інформаційно-комунікаційних технологій активізує безперервність інформації між радою громади і наданням високоякісних послуг. Розумне урядування є наступним кроком для електронного урядування. Розумне урядування використовує миттєву інформацію, щоб зменшити кількість злочинів, підвищивши рівень обізнаності про ситуацію, забезпечуючи ефективне та дієве реагування на аварії, розслідуючи надзвичайні ситуації та покращуючи муніципальні послуги.

2. Розумна охорона здоров'я: розумна охорона здоров'я – це служба охорони здоров'я, яка використовує такі технології, як Інтернет речей (переносні сучасні медичні засоби) і мобільний Інтернет, для динамічного доступу до інформації, з'єднуючи людей, медичні заклади та установи. Також вона активно керує потребами екосистеми та реагує на них розумно. Розумна охорона здоров'я складається з кількох основних компонентів: лікарів, пацієнтів, лікарень та медичних науково-дослідних установ. Інтелектуальна охорона здоров'я має різні виміри, включаючи профілактику захворювань, моніторинг пацієнтів, діагностику та лікування, управління лікарнями, прийняття рішень щодо охорони здоров'я та медичні дослідження. Віддаленого моніторингу можна досягти шляхом бездротового підключення інтелектуальних пристроїв до медичних центрів і систем аналізу даних [11].

3. Розумна енергетика: традиційна інфраструктура енергетичної мережі не відповідає зростаючим потребам громад. Попит на надійність, масштабованість, керованість, екологічно чисте виробництво енергії та економічну ефективність викликав необхідність у створенні розумної та сучасної енергетичної мережі. Розумна енергетична мережа, оснащена технологіями ІС, може підтримувати двосторонній зв'язок і електричні струми між різними об'єктами в мережі. Розумна мережа забезпечує миттєвий моніторинг, забезпечуючи оптимальні потоки електроенергії між енергосистемою та клієнтами. Це також дозволяє виробляти екологічно чисту енергію шляхом інтеграції відновлюваних джерел енергії в мережу (як для енергетичної компанії, так і для споживачів) [12].

4. Розумний транспорт: у сучасних системах управління дорожнім рухом оптимальне використання наявних об'єктів і сучасних технологій є метою планувальників. У зв'язку з цим однією з кінцевих цілей систем управління дорожнім рухом є підвищення ефективності мережі, а також підвищення безпеки транспортних засобів і людей та скорочення часу в дорозі. Для досягнення зазначеної вище мети транспортна мережа потребує ефективних систем для обслуговування транспортного сектору та, з іншого боку, належного управління цими системами. Найважливішими перевагами використання розумних транспортних систем є зменшення заторів, підвищення рівня безпеки, економія часу, зменшення споживання палива та покращення рівня обслуговування. Серед визначальних пристроїв цієї системи – системи моніторингу та фіксації порушень, система інформації про метеорологічний стан, система попередження водія та система інформації про транспортні засоби, а також полегшення швидкого та своєчасного виконання законних повноважень поліцією та підвищення безпеки громадян.

5. Розумна будівля: розумні будівлі використовують датчики та мережеві технології для обміну даними між обладнанням будівель, повідомляють інтелектуальний лічильник про зареєстроване споживання енергії в розумну мережу та дозволяють передавати дані від розумної мережі до будівлі. Очікується, що ці будівлі динамічно регулюватимуть свої енергетичні профілі на основі можливостей інтелектуальної мережі, а також дозволять власникам будівель віддалено контролювати обладнання будівлі. Очевидно, що взаємодія розумної будівлі з розумною мережею призводить до досягнення деяких основних цілей розумної мережі. Деякі з найважливіших переваг цієї взаємодії: реагування на попит, ефективний зворотний зв'язок, зменшення пікових навантажень та обмін енергією.

6. Розумне водопостачання: за даними Всесвітньої організації охорони здоров'я, до 2025 року половина населення світу проживатиме в районах, що зазнають нестачі води, а до 2050 року глобальна урбанізація призведе до зростання споживання ресурсу на 55%. Тому в містах США, Канади, Німеччини, Японії вже сьогодні ухвалюють рішення щодо розумного використання водних ресурсів. Зокрема, у будинках встановлюють розумні лічильники, які збирають дані про використання води в режимі реального часу, що дозволяє запобігти витоку, а також раціонально використовувати водний ресурс.

«Smart City» по-українськи лише подекуди має зазначені вище ознаки. Так, у столиці України, місті Києві, натепер запроваджено цифровий квиток на транспорт, на низці вулиць та метро працює розумна система відеоспостереження, функціонують е-петиції, електронний документообіг, є можливість записатися на прийом до лікаря і т. ін. Однак, якщо порівнювати розумні можливості міст Києва та, наприклад, Сінгапуру, значну перевагу матиме останнє.

Висновуючи зазначене вище, вважаємо за необхідне сконцентрувати увагу на блоках проблем, які ускладнюють впровадження концепції «Smart City» в українських містах, а саме:

1. У зв'язку з некоректним розумінням сутності концепту «Smart City» відсутнє стратегічне бачення щодо вибудування архітектоніки та практичного впровадження програм «Smart City» для конкретного міста чи територіальної громади.

2. Джерела фінансування конкретної програми «Smart City». Такі програми мають реалізовуватись переважно за бюджетування інвесторів, меценатів, грантових проєктів та територіальної громади, оскільки коштів, які інколи виділяються з державного бюджету, завжди буде недостатньо.

3. Недостатні кваліметричні спроможності працівників територіальних громад, які б могли розробляти та супроводжувати реалізацію програми «Smart City» на належному рівні.

4. В Україні відсутній централізований орган, на який би покладалися повноваження щодо централізованого урядування питань, пов'язаних із концептом «Smart City». З поміж таких можемо назвати Міністерство розвитку громад та територій України, Міністерство цифрової трансформації України, громадські організації метою діяльності яких є забезпечення нормального функціонування територіальних громад і т. ін.

Наступним питанням, яке має систематично та ефективно вирішуватися розумним містом, є його кібербезпека.

Так, 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 мільйонів доларів у створення спільного операційного центру кібербезпеки в Брукліні для обслуговування міст Нью-Йорк, Олбані, Сіракузи, Баффало, Рочестер і Йонкерс. У Сіетлі бюджет міста на цифрову безпеку збільшився із з 5,3 мільйона доларів у 2020 році до 8,4 мільйона доларів у 2021 році, хоча на 2022 рік бюджет зменшився до 7,5 мільйона доларів (однак такі видатки також є суттєвими) [13].

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 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 територіальної громади міста Києва, *без додаткових витрат з бюджету міста Києва* [14].

У листопаді 2018 року в Дніпрі було створено перший регіональний центр СБУ, основними завданнями якого є реагування на кібератаки, націлені на державні електронні інформресурси та об'єкти критичної інфраструктури Дніпропетровщини [15].

Наприкінці 2018 року Дніпровська міська рада уклала меморандум про співпрацю із Службою безпеки України. Його мета – розширення взаємодії у сфері кібернетичної безпеки та підвищення рівня захищеності інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем міської ради. На думку виконувачки обов'язків заступника Дніпровського міського голови, Яніки Мерило, «органи місцевого самоврядування дедалі частіше стають об'єктами кібератак і поодиноких «аматорів», і добре організованих груп кіберзлочинців. У рамках меморандуму фахівцям Дніпровської міської ради було надано доступ до платформи MISP-UA (Malware Information Sharing Platform) – для ефективного реагування на кіберінциденти» [16].

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 проєкт 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 [17].

Зауважимо, що зазначені вище заходи щодо забезпечення кібербезпеки з боку територіальних громад не є системними. Так, залучаються до співпраці спеціальні державні органи (СБУ, ДССЗЗІУ 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 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» (1997 р.) *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 [18; 19; 20].

Висновок. Отже, з метою вирішення даної проблематики, пропонуємо наступне.

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».

ЛІТЕРАТУРА:

1. Ткач С.М. Управління розвитком міст на засадах концепції Smart City у Західному регіоні України. *Регіональна економіка*. 2021, № 2. С. 91–99.

2. Про затвердження Державної стратегії регіонального розвитку на 2021-2027 роки: постанова Кабінету Міністрів України від 05.08.2020 р. № 695. *Законодавство України*. URL: https://zakon.rada.gov.ua/laws/show/695-2020-%D0%BF#Text

3. Про схвалення Стратегії цифрової трансформації соціальної сфери: розпорядження Кабінету Міністрів України від 28.10.2020 р. № 1353-р. *Урядовий портал.* URL: https://zakon.rada.gov.ua/laws/show/1353-2020-%D1%80#Text

4. Чукут С.А., Дмитренко В.І. Смарт-сіті чи електронне місто: сучасні підходи до розуміння впровадження е-урядування на місцевому рівні. *Інвестиції: практика та досвід*. – 2016. – №13 – С. 89–93.

5. Єршова О.Л., Бажан Л.І. Розумне місто: концепція, моделі, технології, стандартизація. *Статистика України*. 2020. № 2–3. С. 68–77.

6. Дискіна, А.А., Федорчук О.М., Протосвіцька О.І. Використання інформаційно-комунікаційних технологій в контексті побудови конкурентоспроможної інфраструктури розумного міста. *Наук. вісн. Херсон. держ. ун-ту. Серія Економ. науки*. – 2019. – Вип. 33. – С. 93–96.

7. Лунін Д.С. Адміністративно-правові положення електронного урядування в Україні в контексті використання загальнодержавних е-сервісів. *Науковий вісник публічного та приватного права.* 2020. № 3-2. С. 132–138.

8. Ліпкан В.А. Понятійно-категорійний апарат стратегії державної інфраструктурної політики України. *Регіональні студії.* – Ужгород, Видавничий дім «Гельветика». Вип. 27. – 2021. – С. 55–62.

9. Secinaro, S., et al. Towards a hybrid model for the management of smart city initiatives. *Cities*. Vol. 116, September 2021. URL: https://doi.org/10.1016/j.cities.2021.103278

10. Nakano, S., Washizu, A. Will smart cities enhance the social capital of residents? The importance of smart neighborhood management. *Cities*. Vol. 115, August 2021. URL: https://doi.org/10.1016/j.cities.2021.103244

11. Singh, A., Chatterjee, K. Securing smart healthcare system with edge computing. *Computers & Security*. Vol. 108, September 2021. URL: https://doi.org/10.1016/j.cose.2021.102353

12. Behzad, r., Mehrpooya, M., Marefati, M. Parametric design and performance evaluation of a novel solar assisted thermionic generator and thermoelectric device hybrid system. *Renewable Energy*. Vol. 164, 2021. pp. 194–210.

13. 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

14. 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/eiloxqlprq_614-2776.pdf

15. 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

16. 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

17. 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

18. Рішення Київської міської ради «Про бюджет міста Києва на 2023 рік» від 08.12.2022 №5828/5869. URL: https://kyivcity.gov.ua/publichna_informatsiia_Tag_166122/rishennya_pro_byudzhet_mista_kiyeva_na_2023_rik/

19. 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-byudzhet-dniprovskoi-miskoi-teritorialnoi-gromadi-na-2022-rik

20. Рішення Мукачівської міської ради «Про бюджет міста Києва на 2023 рік» від 22.12.2022. URL: https://kyivcity.gov.ua/publichna_informatsiia_Tag_166122/rishennya_pro_byudzhet_mista_kiyeva_na_2023_rik/