08/231-477/ПР
19.06.2026

КИЇВСЬКА МІСЬКА РАДА
V сесія IX скликання

Р І Ш Е Н Н Я

_____ Київ № _____

ПРОЄКТ

Про внесення змін до рішення Київської міської ради від 12 грудня 2024 року № 477/10285

Відповідно до Закону України «Про місцеве самоврядування в Україні», частин четвертої та п'ятої статті 5 Закону України «Про основні засади забезпечення кібербезпеки України», Закону України «Про захист інформації в інформаційно-комунікаційних системах», постанови Кабінету Міністрів України від 29 березня 2006 року № 373 «Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем», рішення Київської міської ради від 07 грудня 2023 року № 7516/7557 «Про затвердження Комплексної міської цільової програми «Цифровий Київ» на 2024 - 2027 роки», Київська міська рада

ВИРІШИЛА:

1. Унести до рішення Київської міської ради від 12 грудня 2024 року № 477/10285 «Про деякі питання забезпечення кібербезпеки в місті Києві» такі зміни:

1.1. Заголовок рішення викласти в такій редакції:

«Про деякі питання забезпечення кібербезпеки інформаційних (автоматизованих), електронних комунікаційних та інформаційно-комунікаційних систем, що належать до комунальної власності територіальної громади міста Києва».

1.2. У пункті 1 слова «в місті Києві» замінити словами «інформаційних (автоматизованих), електронних комунікаційних та інформаційно-комунікаційних систем, що належать до комунальної власності територіальної громади міста Києва».

1.3. У пункті 3 слова «Уповноважити Київського міського голову» замінити словами «Виконавчому органу Київської міської ради (Київській міській державній адміністрації)».

1.4. У пункті 4 слова «протягом одного року з дня прийняття цього рішення» замінити словами «до 31 грудня 2028 року».

2. Затвердити зміни до Положення про забезпечення кібербезпеки в місті Києві, затвердженого рішенням Київської міської ради від 12 грудня 2024 року № 477/10285, що додаються.

3. Оприлюднити це рішення в установленому порядку.

4. Це рішення набирає чинності з моменту його оприлюднення.

5. Контроль за виконанням цього рішення покласти на постійну комісію Київської міської ради з питань транспорту, зв'язку та реклами, постійну комісію Київської міської ради з питань цифрової трансформації та регулювання надання публічних послуг.

Київський міський голова Віталій КЛИЧКО

ПОДАННЯ:

Заступник голови КМДА — Валентин МОНДРИЇВСЬКИЙ

Директор Департаменту інформаційно-комунікаційних технологій — Вікторія ІЦКОВИЧ

Заступник директора департаменту – начальник управління правового забезпечення та організації, супроводження процесів цифровізації — Ганна ЛИСИК

ПОГОДЖЕНО:

Виконувач обов'язків першого заступника голови Київської міської державної адміністрації — Петро ПАНТЕЛЕЄВ

з зауваженнями юридичного управління 17.06.2026

Заступник голови КМДА — Вячеслав НЕПОП

Заступниця голови КМДА — Ганна СТАРОСТЕНКО

Заступниця голови КМДА з питань здійснення самоврядних повноважень — Марина ХОНДА

Заступниця голови КМДА з питань здійснення самоврядних повноважень — Олена ГОВОРОВА

Заступник голови КМДА з питань здійснення самоврядних повноважень — Костянтин УСОВ

Заступник голови КМДА з питань здійснення самоврядних повноважень — Владислав АНДРОНОВ

Заступник голови КМДА з питань здійснення самоврядних повноважень — Володимир ПРОКОПІВ

Заступник голови КМДА з питань здійснення самоврядних повноважень — Олег КУЯВСЬКИЙ

Керуючий справами — Євген СИТНІЧЕНКО

Виконувач обов'язків директора СКП «Київтелесервіс» — Олександр ВОЛОЩУК

Заступник керівника апарату – начальник юридичного управління — Леся ВЕРЕС

погоджує 16.06.26

Керівник апарату — Дмитро ЗАГУМЕННИЙ

Голова постійної комісії Київської міської ради з питань транспорту, зв'язку та реклами — Олексій ОКОПНИЙ

Голова постійної комісії Київської міської ради з питань цифрової трансформації та регулювання надання публічних послуг — Максим НЕФЬОДОВ

Начальник управління правового забезпечення діяльності Київської міської ради — Валентина ПОЛОЖИШНИК

ЗАТВЕРДЖЕНО
Рішення Київської міської ради
від_____

Зміни до Положення про забезпечення кібербезпеки в місті Києві, затвердженого рішенням Київської міської ради від 12 грудня 2024 року № 477/10285

1. Назву Положення викласти в такій редакції:

«Положення про забезпечення кібербезпеки інформаційних (автоматизованих), електронних комунікаційних та інформаційно-комунікаційних систем, що належать до комунальної власності територіальної громади міста Києва».

2. У тексті положення слова «реагування на кіберінциденти та кібератаки» замінити словами «реагування на кіберінциденти, кібератаки, кіберзагрози,».

3. У розділі I:

3.1.Пункт 1.1. викласти в такій редакції:

«1.1. Положення про забезпечення кібербезпеки інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, що належать до комунальної власності територіальної громади міста Києва (далі – Системи територіальної громади) (далі – Положення) розроблено з метою забезпечення кібербезпеки Систем територіальної громади шляхом вжиття заходів кіберзахисту, спрямованих на швидке виявлення, аналіз, мінімізацію шкоди від інцидентів кібербезпеки (далі - кіберінцидентів), кібератак, кіберзагроз, належне інформування про них, тощо.».

3.2. Пункт 1.2. викласти в такій редакції:

«1.2. Дія цього Положення поширюється на секретаріат Київської міської ради, структурні підрозділи виконавчого органу Київської міської ради (Київської міської державної адміністрації), районні в місті Києві державні адміністрації, підприємства, установи та організації, що належать до комунальної власності територіальної громади міста Києва.».

3.3. У пункті 1.3:

3.3.1. Після слів ««Про публічні електронні реєстри»,» доповнити словами «Про Державну службу спеціального зв'язку та захисту інформації України»,».

3.3.2. Слова «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» замінити словами «Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем».

4. У розділі II:

4.1. Пункт 2.2. викласти в такій редакції:

«2.2. У цьому Положенні терміни вживаються у такому значенні:

власник об'єкта кіберзахисту – територіальна громада міста Києва від імені та в інтересах якої права суб'єкта комунальної власності здійснює Київська міська рада, секретаріат Київської міської ради, структурні підрозділи виконавчого органу Київської міської ради (Київської міської державної адміністрації), районні в місті Києві державні адміністрації, підприємства, установи та організації, що належать до комунальної власності територіальної громади міста Києва, які визначають розпорядника та/або адміністратора відповідного об'єкта кіберзахисту;

розпорядник та/або адміністратор об'єкта кіберзахисту – секретаріат Київської міської ради, структурний підрозділ виконавчого органу Київської міської ради (Київської міської державної адміністрації), районна в місті Києві державна адміністрація або її структурний підрозділ, підприємство, установа та організація, що належать до комунальної власності територіальної громади міста Києва, або інша визначена власником об'єкта кіберзахисту юридична (фізична) особа, на яку покладено (відповідно до повноважень або за договором) обов'язок забезпечувати функціонування об'єкта кіберзахисту та/або яка безпосередньо здійснює його адміністрування;

об'єкти кіберзахисту – інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні, комунікаційні та технологічні системи, електронні комунікаційні мережі, що належать до комунальної власності територіальної громади міста Києва та/або які використовуються в інтересах органів місцевого самоврядування.».

4.2. Перший абзац пункту 2.3. викласти в такій редакції:

«2.3. Суб'єктами відносин, задіяними у межах своєї компетенції в забезпеченні кібербезпеки (далі - суб'єкти відносин), є:».

4.3.У пункті 2.4. слова «реагування на кіберінциденти та кібератаки, усунення їх наслідків тощо, сприяє:» замінити словами «реагування на кіберінциденти, кібератаки, кіберзагрози, усунення їх наслідків тощо, сприяє:».

4.4. Пункт 2.5. викласти в такій редакції:

«2.5. Власник об'єкта кіберзахисту здійснює організаційне, методологічне забезпечення функціонування об'єкта кіберзахисту, та забезпечує виконання вимог з кіберзахисту на підставі та в порядку, визначеному законодавством України.».

4.5. Пункт 2.6. виключити.

4.6. У пункті 2.7.:

4.6.1. Підпункт 4 викласти в такій редакції:

«4) в межах відповідної компетенції вжиття заходів з пошуку та/або виявлення потенційних вразливостей відповідного об'єкта кіберзахисту та усунення їх наслідків;».

4.6.2. У підпункті 6 слова «та кібератак» замінити словами «, кібератак, кіберзагроз;».

4.6.3. У підпункті 10 слово «аналізу» замінити словом «оцінювання».

4.6.4. У підпункті 13 слово «проведення» замінити словами «ідентифікацію та періодичну».

4.7. У пункті 2.8:

4.7.1. Підпункт 1 викласти в такій редакції:

«1) здійснення моніторингу та сканування об’єктів кіберзахисту з метою виявлення вразливостей, які можуть мати значний вплив;».

4.7.2. Підпункт 2 викласти в такій редакції:

«2) виявлення і реагування на кіберінциденти, кібератаки, кіберзагрози щодо об'єктів кіберзахисту, які в установленому порядку підключені до Системи;».

4.7.3. У підпункті 4 після слів «даних про кіберінциденти, кібератаки,» доповнити словом «кіберзагрози».

4.7.4. Підпункт 5 викласти в такій редакції:

«5) здійснення в установленому порядку інформування суб'єктів відносин та інших суб'єктів забезпечення кібербезпеки про кіберінциденти, кібератаки, кіберзагрози, виявлені або про потенційні вразливості відповідних об'єктів кіберзахисту;».

4.7.5. Підпункт 6 викласти в такій редакції:

«6) встановлення постійного зв'язку, обміну інформацією та налагодження взаємодії з суб'єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози, в обов'язковому порядку - з національною командою реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA (далі - національний CSIRT), правоохоронними, розвідувальними та контррозвідувальними органами, суб’єктами оперативно-розшукової діяльності в межах, необхідних для виконання ними повноважень, визначених законом та в порядку, встановленому законодавством України;».

4.7.6. У підпункті 9 слово «аналізу» замінити словом «оцінювання».

4.7.7. У підпункті 13 слово «законодавств» замінити словом «законодавства».

4.8. Пункт 2.10. викласти в такій редакції:

«2.10. Інформаційний обмін, координація та спільні дії суб'єктів відносин з іншими суб'єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози, під час реагування на кіберінциденти, кібератаки, кіберзагрози здійснюються в порядку, визначеному законодавством України.».

5. У розділі III:

5.1. Пункт 3.1. викласти в такій редакції:

«3.1. Центр моніторингу та кібербезпеки для здійснення заходів, передбачених законодавством України у сфері кібербезпеки, та з метою забезпечення виконання завдань, визначених цим Положенням, використовує Систему, яка призначена для проведення цілодобового моніторингу, аналізу, реагування на кіберінциденти, кібератаки, кіберзагрози, які відбулися або відбуваються на об'єктах кіберзахисту, а також для виявлення та блокування іншої підозрілої поведінки та передачі відповідної інформації.».

5.2. У пункті 3.2.:

5.2.1. Підпункт 1 викласти в такій редакції:

«1) автоматизація та цифровізація процесів збору і збереження інформації про кіберінциденти, кібератаки, кіберзагрози, їх категоризації та пріоритезації (визначення першочерговості заходів реагування для ефективного розподілу

ресурсів, зменшення негативних наслідків кіберінциденту, кібератаки, кіберзагрози), інформування (звітності) та ідентифікації (атрибуції);».

5.2.2. У підпункті 2 слова «та кібератакою щодо об'єктів кіберзахисту» замінити словами «кібератакою, кіберзагрозою об'єктів кіберзахисту».

5.2.3. У підпункті 4 слова «та кібератак» замінити словами «, кібератак, кіберзагроз».

5.2.4. У підпунктах 5 та 6 слова «та кібератаки» замінити словами «, кібератаки, кіберзагрози».

5.2.5. Підпункт 7 викласти в такій редакції:

«7) проведення пошуку та/або виявлення потенційних вразливостей об'єктів кіберзахисту;».

5.3. Пункт 3.6. після абзацу четвертого доповнити новим абзацом п'ятим такого змісту:

«Перелік складових Системи не є вичерпним і може доповнюватися у разі здійснення модернізації (модифікації, розвитку) Системи.».

6. У розділі IV:

6.1. В абзаці першому пункту 4.4. слово «відповідності» замінити словом «можливості».

6.2. Пункт 4.6. викласти в такій редакції:

«4.6. У разі, якщо розпорядник та/або адміністратор об'єкта кіберзахисту за результатом опрацювання рекомендацій щодо необхідності налаштування об'єкта кіберзахисту для забезпечення технічної можливості подальшого підключення до Системи повідомляє про неможливість здійснення відповідних налаштувань, такий об'єкт кіберзахисту підключається Центром моніторингу та кібербезпеки після усунення розпорядником та/або адміністратором об'єкта кіберзахисту причин, які перешкоджали підключенню.

6.3. Пункт 4.8 викласти в такій редакції:

«4.8. Відключення об'єкта кіберзахисту від Системи здійснюється Центром моніторингу та кібербезпеки у разі подання розпорядником та/або адміністратором об'єкта кіберзахисту заяви про відключення об'єкта кіберзахисту від Системи у зв'язку з припиненням експлуатації такого об'єкта кіберзахисту.».

6.4. В абзаці третьому пункту 4.9 слова «та кібератак» замінити словами «, кібератак, кіберзагроз,».

6.5. В абзаці четвертому пункту 4.10 після слова «кіберінцидентів» доповнити словами «, кібератак, кіберзагроз».

7. Пункт 5.1. розділу V викласти в такій редакції:

«5.1. Паспорт об'єкта кіберзахисту:

задокументований у паперовій та/або електронній формі;

містить повну та актуальну інформацію щодо основних характеристик об'єкта кіберзахисту (у тому числі архітектурних рішень), розробляється та затверджується розпорядником та/або адміністратором об'єкта кіберзахисту за формою, затвердженою згідно з додатком до цього Положення.

Відомості, що містяться в паспорті об'єкта кіберзахисту та його складових можуть бути інформацією з обмеженим доступом, вимога щодо захисту якої встановлена законом.».

8. Додаток до Положення викласти в такій редакції:

«Додаток до Положення

ФОРМА ПАСПОРТА
об'єкта кіберзахисту
(далі - ОК)

Назва ОК:	
Індекс ОК:	
Короткий опис ОК:	
Основні користувачі ОК:	Перелік типів користувачів, організацій
Кількість користувачів ОК:	
Розпорядник ОК:	
Прізвище, власне ім'я, по батькові (за наявності) та номер телефону керівника розпорядника ОК:	
Адміністратор ОК:	
Прізвище, власне ім'я, по батькові (за наявності) та номер телефону керівника адміністратора ОК:	
Документ про створення, впровадження ОК:	
Документ про введення в експлуатацію ОК (дослідну, промислову):	
Архітектура ОК:	
Архітектура ОК:	Актуальна архітектура ОК (програмно-апаратні, технічні засоби, складові) у паперовій та електронній формах

Складові ОК:	Перелік складових, програмно-апаратні, технічні засоби, що входять до складу ОК у паперовій та електронній формах		
Резервне копіювання			
Схема резервного копіювання:	Документ зі схемою резервування інформації, порядком створення бекапу та інструкціями з відновлення, у паперовій та електронній формах		
Резервні копії:			
порядок створення			
порядок зберігання			
порядок відновлення			
порядок видалення			
наявність гарячого резервування			
наявність холодного резервування			
Зберігання резервних копій:			
хмарні ресурси			
центри обробки даних, розташовані за адресами			
ВІДНОВЛЕННЯ РОБОТИ:			
Сценарій: ПРОБЛЕМА	Часткова чи повна деградація (непрацездатність) ОК, що призводить до неможливості надання послуг внаслідок виходу з ладу одного зі складових ОК, при працездатності суміжних ОК, від яких залежить працездатність ОК		
Вірогідність виникнення (на рік):	Кількість випадків згідно з історичними даними чи експертною оцінкою		
Час відновлення, годин:			
План аварійного відновлення:	Документ з інструкціями щодо відновлення штатного режиму роботи ОК.		
Порядок інформування:	Вказати хто, кого та в який спосіб інформує		
Час	Хто	Кого	Метод
30 хв			
60 хв			

2 год			
4 год			
8 год			
Альтернативний сценарій дій на час відновлення роботи ОК:	Описати інструкцію щодо дій виконавців, які мають бути виконані під час відновлення працездатності для зменшення негативного ефекту від непрацездатності ОК		
Відповідальний за кіберзахист ОК			
Посада, Прізвище, власне ім'я, по батькові (за наявності), електронна пошта та номер телефону відповідального за кіберзахист ОК:	Особа або керівник організації чи підрозділу який визначений розпорядником, як відповідальний за кіберзахист ОК		
Відновлення, тестування, аудит планів аварійного відновлення робити ОК:			
Тип перевірки	«Стендові випробування» (імітаційний стенд) або офлайн-тестування (в умовах реального часу)		
Частота перевірки			

Додаток 1.1. **Архітектура ОК**

Додаток 1.2. **Складові ОК**

Додаток 1.3. **Схема резервного копіювання**

Додаток 1.4. **План безперервної діяльності ОК**

Додаток 1.5. **План аварійного відновлення штатного режиму роботи ОК».**

Київський міський голова Віталій КЛИЧКО

ПОЯСНЮВАЛЬНА ЗАПИСКА
до проєкту рішення Київської міської ради
«Про внесення змін до рішення Київської міської ради
від 12 грудня 2024 року № 477/10285»
(далі – проєкт рішення)

1. Опис проблем, для вирішення яких підготовлено проєкт рішення, обґрунтування відповідності та достатності передбачених у проєкті рішення механізмів і способів вирішення існуючих проблем, а також актуальності цих проблем для територіальної громади міста Києва.

Відповідно до статті 5 Закону України «Про основні засади забезпечення кібербезпеки України» (далі – Закон про кібербезпеку), суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки є, зокрема органи місцевого самоврядування, які у межах своєї компетенції, серед іншого:

здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту;

здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору.

Так, з урахуванням вимог частин четвертої та п'ятої статті 5 Закону України «Про основні засади забезпечення кібербезпеки України», Київською міською радою 12 грудня 2024 року прийнято рішення № 477/10285 «Про деякі питання забезпечення кібербезпеки в місті Києві» (далі – рішення), яким, зокрема затверджено Положення про забезпечення кібербезпеки в місті Києві (далі – Положення про кібербезпеку) та впроваджено інформаційно-комунікаційну систему моніторингу та кібербезпеки (далі – Система).

Відповідно до пункту 3.1 Положення про кібербезпеку, Центр моніторингу та кібербезпеки міських сервісів спеціалізованого комунального підприємства «Київтелесервіс» (далі – Центр моніторингу та кібербезпеки), як один із суб'єктів відносин, задіяних в забезпеченні кібербезпеки (пункт 2.3 Положення про кібербезпеку), для здійснення заходів, передбачених законодавством України у сфері кібербезпеки, та з метою забезпечення виконання завдань, визначених цим Положенням, використовує Систему, яка призначена для проведення цілодобового моніторингу, аналізу, реагування та передачі інформації про кіберінциденти та кібератаки, які відбулися або відбуваються на об'єктах кіберзахисту, а також для виявлення та блокування іншої підозрілої поведінки.

Слід зазначити, що підпорядковане Департаменту інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації) спеціалізоване комунальне підприємство «Київтелесервіс» (далі – СКП «Київтелесервіс»), як співвиконавець визначених заходів Переліку заходів з подальшого впровадження інформаційно-комунікаційних технологій у сфери життєдіяльності міста Києва на 2018 рік, затвердженому розпорядженням виконавчого органу Київської міської ради (Київської міської державної адміністрації) від 11 квітня 2018 року № 614 (зі змінами), Комплексної міської цільової програми «Електронна столиця» на 2019-2023 роки, затвердженої

рішенням Київської міської ради від 18 грудня 2018 року № 461/6512 (із змінами) та Комплексної міської цільової програми «Цифровий Київ» на 2024 – 2027 роки, затвердженої рішенням Київської міської ради від 07 грудня 2023 року № 7516/7557 (у редакції рішення Київської міської ради від 12 грудня 2024 року № 449/10257), забезпечив створення центру моніторингу та кібербезпеки міських сервісів та продовжує його впровадження, розвиток тощо для виконання превентивних заходів і забезпечення оперативного реагування на кіберінциденти, пов'язані з міськими електронними інформаційними ресурсами та міською мережевою інфраструктурою, зокрема з використанням Системи, яка призначена для проведення цілодобового моніторингу, аналізу, реагування та передачі інформації про кіберінциденти та кібератаки, які відбулися або відбуваються на об'єктах кіберзахисту, а також для виявлення та блокування іншої підозрілої поведінки (пункт 3.1 Положення про кібербезпеку).

Вищезгадані функціональні можливості Системи спрямовані на об’єкти кіберзахисту (далі – ОК), підключені до Системи у порядку, визначеному Положенням про кібербезпеку, та за умови налагодження інформаційного обміну (інтеграції) з Системою, що зобов’язані забезпечити розпорядник та/або адміністратор відповідного ОК (пункт 4 рішення, підпункт 7 пункту 2.7 Положення про кібербезпеку), потребує додаткового часу для реалізації.

Натомість, за інформацією СКП «Київтелесервіс», протягом дії рішення останнім вжито, зокрема таких заходів:

зібрано інформацію щодо наявних ОК в секретаріаті Київської міської ради, структурних підрозділах виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністраціях, підприємствах, установах, організаціях, що належать до комунальної власності територіальної громади міста Києва з визначенням категорії критичності, дати розробки Паспорту ОК та відповідальних за функціонування ОК;

сформовано реєстр ОК (на поточний момент більше 500 од);

проведено вебінар з представниками секретаріату Київської міської ради, структурних підрозділах виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ, організацій, що належать до комунальної власності територіальної громади міста Києва щодо оформлення Паспорту ОК та додатків до нього, а також роз'яснено механізм підключення до Системи;

забезпечено поетапне підключення ОК з високим рівнем критичності до Системи, з яких вже підключено, зокрема: інформаційно-комунікаційні системи «Реєстр територіальної громади міста Києва», «Платформа цифрових мобільних сервісів «Київ Цифровий», «Єдиний інформаційний простір територіальної громади міста Києва», «Єдиний веб-портал територіальної громади міста Києва», автоматизованої системи обліку оплати проїзду в міському пасажирському транспорті міста Києва незалежно від форм власності та інші.

З метою приведення у відповідність до Закону України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних

інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури», зокрема термінології, яка використовується в Положенні про кібербезпеку, зміні строків його виконання та спрощення деяких процедур, даним проєктом рішення передбачається внесення змін до рішення та Положення про кібербезпеку.

Враховуючи вищевикладене, є необхідність у прийнятті Київською міською радою даного рішення.

2. Правове обґрунтування необхідності прийняття рішення Київської міської ради (із посиланням на конкретні положення нормативно-правових актів, на підставі й на виконання яких підготовлено проєкт рішення).

Проєкт рішення розроблено відповідно до:

Закону України «Про місцеве самоврядування в Україні»;

Закону України «Про основні засади забезпечення кібербезпеки України»;

Закону України «Про захист інформації в інформаційно-комунікаційних системах»;

постанови Кабінету Міністрів України від 29 березня 2006 року № 373 «Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем»;

рішення Київської міської ради від 07 грудня 2023 року № 7516/7557 «Про затвердження Комплексної міської цільової програми «Цифровий Київ» на 2024 - 2027 роки».

3. Опис цілей і завдань, основних положень проєкту рішення Київської міської ради, а також очікуваних соціально-економічних, правових та інших наслідків для територіальної громади міста Києва від прийняття запропонованого проєкту рішення Київської міської ради.

Проєкт рішення підготовлений з метою приведення у відповідність до законодавства України, зокрема термінології, яка використовується в Положенні про кібербезпеку та рішенні.

Реалізація цього рішення не передбачає використання додаткових коштів з бюджету міста Києва.

4. Інформація про те, чи містить проєкт рішення інформацію з обмеженим доступом у розумінні статті 6 Закону України «Про доступ до публічної інформації».

Проєкт рішення не містить інформацію з обмеженим доступом у розумінні статті 6 Закону України «Про доступ до публічної інформації».

5. Інформація про те, чи містить проєкт рішення інформацію про фізичну особу (персональні дані) у розумінні статей 11 та 21 Закону України «Про інформацію» та статті 2 Закону України «Про захист персональних даних»

Проєкт рішення не містить інформацію про фізичну особу (персональні дані) у розумінні статей 11 та 21 Закону України «Про інформацію» та статті 2 Закону України «Про захист персональних даних».

5. Інформація про те, чи стосується проєкт рішення прав і соціальної захищеності осіб з інвалідністю та який вплив він матиме на життєдіяльність цієї категорії.

Проєкт рішення не стосується прав і соціальної захищеності осіб з інвалідністю та не матиме впливу на життєдіяльність цієї категорії.

6. Прізвище або назва суб'єкта подання, прізвище, посада, контактні дані доповідача проєкту рішення на пленарному засіданні та особа, відповідальна за супроводження проєкту рішення Київської міської ради.

Суб'єктом подання проєкту рішення Київської міської ради є виконавчий орган Київської міської ради (Київської міської державної адміністрації).

Особою, відповідальною за супроводження проєкту рішення Київради та доповідачем по проєкту рішення на пленарному засіданні Київської міської ради є директор Департаменту інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації) Вікторія ІЦКОВИЧ, 366-86-75, 366-86-72.

Заступник голови Київської міської
державної адміністрації Валентин МОНДРИЇВСЬКИЙ

Порівняльна таблиця
до проєкту рішення Київської міської ради
«Про внесення змін до рішення Київської міської ради від 12 грудня 2024 року № 477/10285»

Діюча редакція	Запропонована редакція
Рішення Київської міської ради від 12 грудня 2024 року № 477/10285 «Про деякі питання забезпечення кібербезпеки в місті Києві»	
Про деякі питання забезпечення кібербезпеки **в місті Києві**	Про деякі питання забезпечення кібербезпеки **інформаційних (автоматизованих), електронних комунікаційних та інформаційно-комунікаційних систем, що належать до комунальної власності територіальної громади міста Києва**
1. Затвердити Положення про забезпечення кібербезпеки **в місті Києві**, що додається.	1. Затвердити Положення про забезпечення кібербезпеки **інформаційних (автоматизованих), електронних комунікаційних та інформаційно-комунікаційних систем, що належать до комунальної власності територіальної громади міста Києва**, що додається.
2. Впровадити інформаційно-комунікаційну систему моніторингу та кібербезпеки.	2. Впровадити інформаційно-комунікаційну систему моніторингу та кібербезпеки.
3. ~~Уповноважити Київського міського голову~~ здійснити організаційно-правові заходи щодо введення інформаційно-комунікаційної системи моніторингу та кібербезпеки в експлуатацію.	3. **Виконавчому органу Київської міської ради (Київській міській державній адміністрації)** здійснити організаційно-правові заходи щодо введення інформаційно-комунікаційної системи моніторингу та кібербезпеки в експлуатацію.
4. Секретаріату Київської міської ради, структурним підрозділам виконавчого органу Київської міської ради (Київської міської державної адміністрації), районним в місті Києві державним адміністраціям, підприємствам, установам, організаціям, що належать до комунальної власності	4. Секретаріату Київської міської ради, структурним підрозділам виконавчого органу Київської міської ради (Київської міської державної адміністрації), районним в місті Києві державним адміністраціям, підприємствам, установам, організаціям, що належать до комунальної власності

територіальної громади міста Києва або координація діяльності яких здійснюється виконавчим органом Київської міської ради (Київською міською державною адміністрацією), ~~протягом одного року з дня прийняття цього рішення~~ забезпечити:	територіальної громади міста Києва або координація діяльності яких здійснюється виконавчим органом Київської міської ради (Київською міською державною адміністрацією), **до 31 грудня 2028 року** забезпечити:
4.1. Вжиття організаційно-правових заходів щодо підключення об'єктів кіберзахисту, визначених у Положенні, затвердженому згідно з пунктом 1 цього рішення, до інформаційно-комунікаційної системи моніторингу та кібербезпеки.	4.1. Вжиття організаційно-правових заходів щодо підключення об'єктів кіберзахисту, визначених у Положенні, затвердженому згідно з пунктом 1 цього рішення, до інформаційно-комунікаційної системи моніторингу та кібербезпеки.
4.2. Затвердження паспортів об'єктів кіберзахисту, визначених у Положенні, затвердженому згідно з пунктом 1 цього рішення.	4.2. Затвердження паспортів об'єктів кіберзахисту, визначених у Положенні, затвердженому згідно з пунктом 1 цього рішення.
5. Оприлюднити це рішення в установленому порядку.	5. Оприлюднити це рішення в установленому порядку.
6. Це рішення набирає чинності з моменту його оприлюднення.	6. Це рішення набирає чинності з моменту його оприлюднення.
7. Контроль за виконанням цього рішення покласти на постійну комісію Київської міської ради з питань транспорту, зв'язку та реклами та постійну комісію Київської міської ради з питань цифрової трансформації та регулювання надання публічних послуг.	7. Контроль за виконанням цього рішення покласти на постійну комісію Київської міської ради з питань транспорту, зв'язку та реклами та постійну комісію Київської міської ради з питань цифрової трансформації та регулювання надання публічних послуг.
Положення про забезпечення кібербезпеки в місті Києві, затвердженого рішенням Київської міської ради від 12 грудня 2024 року № 477/10285	
ПОЛОЖЕННЯ **про забезпечення кібербезпеки ~~в місті Києві~~**	**ПОЛОЖЕННЯ** **про забезпечення кібербезпеки інформаційних (автоматизованих), електронних комунікаційних та інформаційно-комунікаційних систем, що належать до**

	комунальної власності територіальної громади міста Києва
І. Загальні положення	**І. Загальні положення**
1.1. Положення про забезпечення кібербезпеки ~~**в місті Києві**~~ (далі – Положення) розроблено з метою забезпечення кібербезпеки ~~**в місті Києві**~~ шляхом вжиття заходів кіберзахисту, спрямованих на швидке виявлення та ~~захист~~ від інцидентів кібербезпеки (далі – кіберінцидентів) та кібератак, належне інформування про них, запобігання негативним наслідкам, їх мінімізації та усунення, ~~**виправлення**~~ вразливостей, ~~**а також відновлення сталості і надійності функціонування об'єктів кіберзахисту, визначених цим Положенням, що належать до комунальної власності територіальної громади міста Києва та/або використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних послуг, електронної комерції, електронного документообігу**~~ тощо.	1.1. Положення про забезпечення кібербезпеки **інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, що належать до комунальної власності територіальної громади міста Києва (далі – Системи територіальної громади)** (далі – Положення) розроблено з метою забезпечення кібербезпеки **Систем територіальної громади** шляхом вжиття заходів кіберзахисту, спрямованих на швидке виявлення, **аналіз, мінімізацію шкоди** від інцидентів кібербезпеки (далі - кіберінцидентів), кібератак, **кіберзагроз,** належне інформування про них, тощо.
1.2. Дія цього Положення поширюється на секретаріат Київської міської ради, структурні підрозділи виконавчого органу Київської міської ради (Київської міської державної адміністрації), районні в місті Києві державні адміністрації, підприємства, установи та організації, що належать до комунальної власності територіальної громади міста Києва ~~або координація діяльності яких здійснюється виконавчим органом Київської міської ради (Київською міською державною адміністрацією)~~.	1.2. Дія цього Положення поширюється на секретаріат Київської міської ради, структурні підрозділи виконавчого органу Київської міської ради (Київської міської державної адміністрації), районні в місті Києві державні адміністрації, підприємства, установи та організації, що належать до комунальної власності територіальної громади міста Києва.
1.3. У цьому Положенні терміни вживаються у значенні, наведеному в законах України «Про основні засади	1.3. У цьому Положенні терміни вживаються у значенні, наведеному в законах України «Про основні засади

забезпечення кібербезпеки України», «Про електронні комунікації», «Про захист інформації в інформаційно-комунікаційних системах», «Про публічні електронні реєстри», постановах Кабінету Міністрів України від 29 березня 2006 року № 373 «~~Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах~~», від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури», від 16 травня 2023 року № 497 «Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж», Методичних рекомендаціях щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесам, затверджених наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 29 травня 2023 року № 463, Методичних рекомендаціях щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затверджених наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 03 липня 2023 року № 570, національних стандартах України з питань інформаційної безпеки та інших нормативно-правових актах.	забезпечення кібербезпеки України», «Про електронні комунікації», «Про захист інформації в інформаційно-комунікаційних системах», «Про публічні електронні реєстри», **«Про Державну службу спеціального зв'язку та захисту інформації України»,** постановах Кабінету Міністрів України від 29 березня 2006 року № 373 «**Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем**», від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури», від 16 травня 2023 року № 497 «Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж», Методичних рекомендаціях щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесам, затверджених наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 29 травня 2023 року № 463, Методичних рекомендаціях щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затверджених наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 03 липня 2023 року № 570, національних стандартах України з питань інформаційної безпеки та інших нормативно-правових актах.
II. Основні засади забезпечення кібербезпеки	

2.1. Діяльність із забезпечення кібербезпеки спрямована на зниження ризиків кібербезпеки, носить безперервний циклічний характер та формує цикл управління кібербезпекою, який складається з п'яти функцій кібербезпеки: ідентифікація ризиків; кіберзахист; виявлення кіберінцидентів; реагування; відновлення поточного стану кібербезпеки.	2.1. Діяльність із забезпечення кібербезпеки спрямована на зниження ризиків кібербезпеки, носить безперервний циклічний характер та формує цикл управління кібербезпекою, який складається з п'яти функцій кібербезпеки: ідентифікація ризиків; кіберзахист; виявлення кіберінцидентів; реагування; відновлення поточного стану кібербезпеки.
2.2. У розумінні цього Положення **Пункт 2.5.** ~~**2.5.**~~ **В**ласник~~**ом**~~ об'єкта кіберзахисту ~~**є:**~~ територіальна громада міста Києва від імені та в інтересах якої права суб'єкта комунальної власності здійснює Київська міська рада, секретаріат Київської міської ради, структурні підрозділи виконавчого органу Київської міської ради (Київської міської державної адміністрації), районні в місті Києві державні адміністрації, підприємства, установи та організації, що належать до комунальної власності територіальної громади міста Києва, які визначають розпорядника та/або адміністратора відповідного об'єкта кіберзахисту. **Пункт 2.6.** ~~2.6.~~ Розпорядник та/або адміністратор об'єкта кіберзахисту - визначені власником об'єкта кіберзахисту юридичні особи, що належать до комунальної власності територіальної громади міста Києва, які здійснюють	2.2. У **цьому Положенні терміни вживаються у такому значенні:** **в**ласник об'єкта кіберзахисту – територіальна громада міста Києва від імені та в інтересах якої права суб'єкта комунальної власності здійснює Київська міська рада, секретаріат Київської міської ради, структурні підрозділи виконавчого органу Київської міської ради (Київської міської державної адміністрації), районні в місті Києві державні адміністрації, підприємства, установи та організації, що належать до комунальної власності територіальної громади міста Києва, які визначають розпорядника та/або адміністратора відповідного об'єкта кіберзахисту; **р**озпорядник та/або адміністратор об'єкта кіберзахисту – **секретаріат Київської міської ради, структурний підрозділ виконавчого органу Київської міської ради (Київської міської державної адміністрації), районна в місті Києві**

комплекс організаційних, технічних та інших заходів, спрямованих на забезпечення функціонування відповідного об'єкта кіберзахисту, його доступності для користувачів, та/або іншого управління програмними та/або апаратними засобами чи ресурсами об'єкта кіберзахисту, що належить секретаріату Київської міської ради, структурним підрозділам виконавчого органу Київської міської ради (Київської міської державної адміністрації), районним в місті Києві державним адміністраціям, підприємствам, установам та організаціям, що належать до комунальної власності територіальної громади міста Києва або координація діяльності яких здійснюється виконавчим органом Київської міської ради (Київською міською державною адміністрацію об'єктами кіберзахисту є: інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні, комунікаційні та технологічні системи, електронні комунікаційні мережі, що належать до комунальної власності територіальної громади міста Києва та/або використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних послуг, електронної комерції, електронного документообігу; інші об'єкти кіберзахисту відповідно до актів органів місцевого самоврядування в місті Києві.	**державна адміністрація або її структурний підрозділ, підприємства, установи та організації, що належать до комунальної власності територіальної громади міста Києва, або інша визначена власником об'єкта кіберзахисту юридична (фізична) особа, на яку покладено (відповідно до повноважень або за договором) обов'язок забезпечувати функціонування об'єкта кіберзахисту та/або яка безпосередньо здійснює його адміністрування;** об'єкти кіберзахисту – інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні, комунікаційні та технологічні системи, електронні комунікаційні мережі, що належать до комунальної власності територіальної громади міста Києва **та/або які використовуються в інтересах органів місцевого самоврядування.**
2.3. Суб'єктами відносин, задіяними в забезпеченні кібербезпеки (далі - суб'єкти відносин), є:	2.3. Суб'єктами відносин, задіяними **у межах своєї компетенції** в забезпеченні кібербезпеки (далі - суб'єкти відносин), є:

Департамент інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації); власник об'єкта кіберзахисту; розпорядник та/або адміністратор об'єкта кіберзахисту; Центр моніторингу та кібербезпеки міських сервісів спеціалізованого комунального підприємства «Київтелесервіс» (далі - Центр моніторингу та кібербезпеки).	Департамент інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації); власник об'єкта кіберзахисту; розпорядник та/або адміністратор об'єкта кіберзахисту; Центр моніторингу та кібербезпеки міських сервісів спеціалізованого комунального підприємства «Київтелесервіс» (далі - Центр моніторингу та кібербезпеки).
2.4. Департамент інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації) з метою впровадження комплексу заходів щодо виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків тощо, сприяє: 1) створенню та функціонуванню Центру моніторингу та кібербезпеки; 2) розробленню спільно з Центром моніторингу та кібербезпеки концептуальних засад щодо підвищення ефективності заходів стосовно виявлення та усунення чинників, які формують потенційні і реальні загрози у сфері кібербезпеки, підготовки проєктів відповідних документів щодо їх попередження і нейтралізації; 3) узагальненню міжнародного досвіду у сфері забезпечення кібербезпеки об'єктів кіберзахисту.	2.4. Департамент інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації) з метою впровадження комплексу заходів щодо виявлення і реагування на кіберінциденти, **кібератаки, кіберзагрози,** усунення їх наслідків тощо, сприяє: 1) створенню та функціонуванню Центру моніторингу та кібербезпеки; 2) розробленню спільно з Центром моніторингу та кібербезпеки концептуальних засад щодо підвищення ефективності заходів стосовно виявлення та усунення чинників, які формують потенційні і реальні загрози у сфері кібербезпеки, підготовки проєктів відповідних документів щодо їх попередження і нейтралізації; 3) узагальненню міжнародного досвіду у сфері забезпечення кібербезпеки об'єктів кіберзахисту.
2.5. ~~Власником об'єкта кіберзахисту є: територіальна громада міста Києва від імені та в інтересах якої права суб'єкта комунальної власності здійснює Київська міська~~	**2.5. Власник об'єкта кіберзахисту здійснює організаційне, методологічне забезпечення функціонування об'єкта кіберзахисту, та забезпечує виконання вимог з**

~~рада, секретаріат Київської міської ради, структурні підрозділи виконавчого органу Київської міської ради (Київської міської державної адміністрації), районні в місті Києві державні адміністрації, підприємства, установи та організації, що належать до комунальної власності територіальної громади міста Києва, які визначають розпорядника та/або адміністратора відповідного об'єкта кіберзахисту.~~	**кіберзахисту на підставі та в порядку, визначеному законодавством України.**
~~2.6.~~ Розпорядник та/або адміністратор об'єкта кіберзахисту - визначені власником об'єкта кіберзахисту юридичні особи, що належать до комунальної власності територіальної громади міста Києва, які здійснюють комплекс організаційних, технічних та інших заходів, спрямованих на забезпечення функціонування відповідного об'єкта кіберзахисту, його доступності для користувачів, та/або іншого управління програмними та/або апаратними засобами чи ресурсами об'єкта кіберзахисту, що належить секретаріату Київської міської ради, структурним підрозділам виконавчого органу Київської міської ради (Київської міської державної адміністрації), районним в місті Києві державним адміністраціям, підприємствам, установам та організаціям, що належать до комунальної власності територіальної громади міста Києва або координація діяльності яких здійснюється виконавчим органом Київської міської ради (Київською міською державною адміністрацію).	**Виключити (перенесено у пункт 2.2.)**
2.7. Завданнями розпорядника та/або адміністратора об'єкта кіберзахисту є забезпечення: 1) визначення структурного підрозділу, який виконуватиме функції із забезпечення взаємодії з Центром	2.7. Завданнями розпорядника та/або адміністратора об'єкта кіберзахисту є забезпечення: 1) визначення структурного підрозділу, який виконуватиме функції із забезпечення взаємодії з Центром моніторингу та

моніторингу та кібербезпеки з питань кіберзахисту об'єкта або посадової (службової) особи з цих питань;	кібербезпеки з питань кіберзахисту об'єкта або посадової (службової) особи з цих питань;
2) розроблення, затвердження, підтримки в актуальному стані документів, необхідних для забезпечення кібербезпеки відповідного об'єкта кіберзахисту, у тому числі, але не виключно, паспорта об'єкта кіберзахисту;	2) розроблення, затвердження, підтримки в актуальному стані документів, необхідних для забезпечення кібербезпеки відповідного об'єкта кіберзахисту, у тому числі, але не виключно, паспорта об'єкта кіберзахисту;
3) функціональності, безперервності роботи, відновлюваності, цілісності та стійкості відповідного об'єкта кіберзахисту;	3) функціональності, безперервності роботи, відновлюваності, цілісності та стійкості відповідного об'єкта кіберзахисту;
4) ~~систематичного проведення аналізу вразливостей, ідентифікованих Центром моніторингу та кібербезпеки, впровадження оновлень програмного забезпечення, спрямованих на усунення вразливостей відповідного об'єкта кіберзахисту;~~	4) **в межах відповідної компетенції вжиття заходів з пошуку та/або виявлення потенційних вразливостей відповідного об'єкта кіберзахисту та усунення їх наслідків;**
5) контролю доступу до об'єкта кіберзахисту та використання облікових записів користувачів відповідного об'єкта кіберзахисту;	5) контролю доступу до об'єкта кіберзахисту та використання облікових записів користувачів відповідного об'єкта кіберзахисту;
6) реєстрації кожним компонентом об'єкта кіберзахисту подій для виявлення кіберінцидентів ~~та~~ кібератак;	6) реєстрації кожним компонентом об'єкта кіберзахисту подій для виявлення кіберінцидентів, кібератак, **кіберзагроз**;
7) підключення відповідного об'єкта кіберзахисту до інформаційно-комунікаційної системи моніторингу та кібербезпеки (далі - Система), у порядку, визначеному цим Положенням, створення облікових записів із відповідними повноваженнями для працівників Центру моніторингу та кібербезпеки та налагодження інформаційного обміну (інтеграції) з Системою тощо;	7) підключення відповідного об'єкта кіберзахисту до інформаційно-комунікаційної системи моніторингу та кібербезпеки (далі - Система), у порядку, визначеному цим Положенням, створення облікових записів із відповідними повноваженнями для працівників Центру моніторингу та кібербезпеки та налагодження інформаційного обміну (інтеграції) з Системою тощо;
8) виконання рекомендацій Центру моніторингу та кібербезпеки щодо необхідності вжиття додаткових заходів	8) виконання рекомендацій Центру моніторингу та кібербезпеки щодо необхідності вжиття додаткових заходів

технічного та організаційного характеру для забезпечення підключення відповідного об'єкта кіберзахисту до Системи; 9) участі в інформаційному обміні та сприяння Центру моніторингу та кібербезпеки у реагуванні на кіберінциденти ~~та~~ кібератаки, забезпечення встановлення причин та умов їх виникнення та/або наслідків реалізації; 10) вжиття заходів, рекомендованих Центром моніторингу та кібербезпеки за результатами проведеного ним ~~аналізу~~ стану кіберзахисту відповідного об'єкта кіберзахисту; 11) надання інформації на запити Центру моніторингу та кібербезпеки, необхідної для здійснення реагування на кіберінциденти ~~та~~ кібератаки в термін та в обсязі, що зазначені в таких запитах; 12) організації проведення аудиту інформаційної безпеки об'єкта кіберзахисту; 13) ~~проведення~~ оцінки ризиків кібербезпеки об'єкта кіберзахисту відповідно до стандартів, обов'язковість застосування яких установлена нормативно-правовими актами; 14) створення та зберігання резервних копій інформації відповідного об'єкта кіберзахисту в установленому порядку та своєчасної заміни відповідних компонентів об'єкта кіберзахисту в разі виходу їх із ладу; 15) організації навчань та підвищення кваліфікації працівників з питань кіберзахисту; 16) здійснення інших заходів із забезпечення кібербезпеки об'єкта кіберзахисту.	технічного та організаційного характеру для забезпечення підключення відповідного об'єкта кіберзахисту до Системи; 9) участі в інформаційному обміні та сприяння Центру моніторингу та кібербезпеки у реагування на кіберінциденти, кібератаки, **кіберзагрози,** забезпечення встановлення причин та умов їх виникнення та/або наслідків реалізації; 10) вжиття заходів, рекомендованих Центром моніторингу та кібербезпеки за результатами проведеного ним **оцінювання** стану кіберзахисту відповідного об'єкта кіберзахисту; 11) надання інформації на запити Центру моніторингу та кібербезпеки, необхідної для здійснення реагування на кіберінциденти, кібератаки, **кіберзагрози,** в термін та в обсязі, що зазначені в таких запитах; 12) організації проведення аудиту інформаційної безпеки об'єкта кіберзахисту; 13) **ідентифікацію та періодичну** оцінку ризиків кібербезпеки об'єкта кіберзахисту відповідно до стандартів, обов'язковість застосування яких установлена нормативно-правовими актами; 14) створення та зберігання резервних копій інформації відповідного об'єкта кіберзахисту в установленому порядку та своєчасної заміни відповідних компонентів об'єкта кіберзахисту в разі виходу їх із ладу; 15) організації навчань та підвищення кваліфікації працівників з питань кіберзахисту; 16) здійснення інших заходів із забезпечення кібербезпеки об'єкта кіберзахисту.

2.8. Завданнями Центру моніторингу та кібербезпеки є забезпечення: 1) збору та аналізу інформації про вразливості об'єктів кіберзахисту; 2) виявлення і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту, усунення їх наслідків, у тому числі, але не виключно, за допомогою Системи; 3) підключення об'єктів кіберзахисту до Системи в порядку, визначеному цим Положенням; 4) накопичення та проведення аналізу даних про кіберінциденти та кібератаки щодо об'єктів кіберзахисту; 5) здійснення інформування суб'єктів відносин та інших суб'єктів забезпечення кібербезпеки про кіберінциденти та кібератаки щодо об'єктів кіберзахисту в установленому порядку; 6) встановлення постійного зв'язку, обміну інформацією та налагодження взаємодії з ~~іншими~~ суб'єктами ~~забезпечення кібербезпеки~~, в обов'язковому порядку - з ~~фахівцями урядової команди реагування на комп'ютерні надзвичайні події України~~ CERT-UA ~~та~~ правоохоронними органами;	2.8. Завданнями Центру моніторингу та кібербезпеки є забезпечення: 1) **здійснення моніторингу та сканування об'єктів кіберзахисту з метою виявлення вразливостей, які можуть мати значний вплив;** 2) виявлення і реагування на кіберінциденти, кібератаки, **кіберзагрози** щодо об'єктів кіберзахисту, **які в установленому порядку підключені до Системи;** 3) підключення об'єктів кіберзахисту до Системи в порядку, визначеному цим Положенням; 4) накопичення та проведення аналізу даних про кіберінциденти, кібератаки, **кіберзагрози** щодо об'єктів кіберзахисту; 5) **здійснення в установленому порядку інформування суб'єктів відносин та інших суб'єктів забезпечення кібербезпеки про кіберінциденти, кібератаки, кіберзагрози, виявлені або про потенційні вразливості відповідних об'єктів кіберзахисту**; 6) встановлення постійного зв'язку, обміну інформацією та налагодження взаємодії з суб'єктами **національної системи реагування на кіберінциденти, кібератаки, кіберзагрози**, в обов'язковому порядку - з **національною командою реагування на кіберінциденти, кібератаки, кіберзагрози** CERT-UA **(далі - національний CSIRT)**, правоохоронними, **розвідувальними та контррозвідувальними** органами, **суб'єктами оперативно-розшукової діяльності в межах, необхідних для виконання ними повноважень, визначених законом та в порядку, встановленому законодавством України**;

7) реалізації в установленому порядку інформаційного обміну щодо реалізованих та потенційних кіберзагроз; 8) розробки та впровадження методичних документів (рекомендацій, інструкцій тощо) щодо покращення рівня кібербезпеки об'єктів кіберзахисту для реалізації запобіжних, технічних, організаційних, освітніх та інших заходів у сфері кібербезпеки та кіберзахисту; 9) надання розпорядникам та/або адміністраторам об'єктів кіберзахисту рекомендацій за результатами проведеного ~~аналізу~~ стану кіберзахисту відповідного об'єкта кіберзахисту; 10) запровадження постійного перегляду й оновлення ролей працівників Центру моніторингу та кібербезпеки, зон їх відповідальності та повноважень кожного працівника; 11) визначення потреб у технічній підготовці працівників Центру моніторингу та кібербезпеки, відповідальних за реагування на кіберінциденти ~~та~~ кібератаки; 12) удосконалення інструментів, необхідних для виконання заходів із захисту, виявлення, аналізу та/або реагування на кіберінциденти та кібератаки; 13) зберігання та обробки інформації з обмеженим доступом відповідно до законодавств; 14) здійснення інших заходів із забезпечення розвитку та безпеки кіберпростору.	7) реалізації в установленому порядку інформаційного обміну щодо реалізованих та потенційних кіберзагроз; 8) розробки та впровадження методичних документів (рекомендацій, інструкцій тощо) щодо покращення рівня кібербезпеки об'єктів кіберзахисту для реалізації запобіжних, технічних, організаційних, освітніх та інших заходів у сфері кібербезпеки та кіберзахисту; 9) надання розпорядникам та/або адміністраторам об'єктів кіберзахисту рекомендацій за результатами проведеного **оцінювання** стану кіберзахисту відповідного об'єкта кіберзахисту; 10) запровадження постійного перегляду й оновлення ролей працівників Центру моніторингу та кібербезпеки, зон їх відповідальності та повноважень кожного працівника; 11) визначення потреб у технічній підготовці працівників Центру моніторингу та кібербезпеки, відповідальних за реагування на кіберінциденти, кібератаки, **кіберзагрози**; 12) удосконалення інструментів, необхідних для виконання заходів із захисту, виявлення, аналізу та/або реагування на кіберінциденти, кібератаки, **кіберзагрози**; 13) зберігання та обробки інформації з обмеженим доступом відповідно до законодавств**а**; 14) здійснення інших заходів із забезпечення розвитку та безпеки кіберпростору.
2.9. Організаційне, інформаційне та матеріально-технічне забезпечення виконання Центром моніторингу та кібербезпеки завдань, визначених цим Положенням,	2.9. Організаційне, інформаційне та матеріально-технічне забезпечення виконання Центром моніторингу та кібербезпеки завдань, визначених цим Положенням, здійснюється

здійснюється спеціалізованим комунальним підприємством «Київтелесервіс».	спеціалізованим комунальним підприємством «Київтелесервіс».
2.10. Інформаційний обмін, координація та спільні дії суб'єктів відносин з іншими суб'єктами ~~забезпечення кібербезпеки~~ під час реагування на кіберінциденти та кібератаки здійснюються в порядку, визначеному законодавством України.	2.10. Інформаційний обмін, координація та спільні дії суб'єктів відносин з іншими суб'єктами **національної системи реагування на кіберінциденти, кібератаки, кіберзагрози**, під час реагування на кіберінциденти, кібератаки, **кіберзагрози** здійснюються в порядку, визначеному законодавством України.
III. Інформаційно-комунікаційна система моніторингу та кібербезпеки	
3.1. Центр моніторингу та кібербезпеки для здійснення заходів, передбачених законодавством України у сфері кібербезпеки, та з метою забезпечення виконання завдань, визначених цим Положенням, використовує Систему, яка призначена для проведення цілодобового моніторингу, аналізу, реагування та ~~передачі інформації про кіберінциденти та кібератаки~~, які відбулися або відбуваються на об'єктах кіберзахисту, а також для виявлення та блокування іншої підозрілої поведінки.	3.1. Центр моніторингу та кібербезпеки для здійснення заходів, передбачених законодавством України у сфері кібербезпеки, та з метою забезпечення виконання завдань, визначених цим Положенням, використовує Систему, яка призначена для проведення цілодобового моніторингу, аналізу, реагування на кіберінциденти, кібератаки, **кіберзагрози,** які відбулися або відбуваються на об'єктах кіберзахисту, а також для виявлення та блокування іншої підозрілої поведінки **та передачі відповідної інформації.**
3.2. Відповідно до завдань Центру моніторингу та кібербезпеки Система має такі функціональні можливості: 1) автоматизація та цифровізація процесів збору і збереження інформації про кіберінциденти, категоризації ~~кіберінцидентів та кібератак,~~ їх пріоритезації (визначення першочерговості заходів реагування для ефективного розподілу ресурсів, зменшення негативних наслідків кіберінциденту та кібератаки), інформування (звітності) та ідентифікації (атрибуції);	3.2. Відповідно до завдань Центру моніторингу та кібербезпеки Система має такі функціональні можливості: 1) автоматизація та цифровізація процесів збору і збереження інформації про кіберінциденти, **кібератаки, кіберзагрози, їх** категоризації та пріоритезації (визначення першочерговості заходів реагування для ефективного розподілу ресурсів, зменшення негативних наслідків кіберінциденту, кібератаки, **кіберзагрози**), інформування (звітності) та ідентифікації (атрибуції);

2) моніторинг, виявлення та сповіщення про підозрілу поведінку, що може бути пов'язана з кіберінцидентом ~~та кібератакою щодо об'єктів кіберзахисту~~;	2) моніторинг, виявлення та сповіщення про підозрілу поведінку, що може бути пов'язана з кіберінцидентом, **кібератакою, кіберзагрозою об'єктів кіберзахисту**;
3) автоматизація заходів із запобігання, виявлення та реагування на кіберінциденти ~~та кібератаки~~, усунення їх наслідків;	3) автоматизація заходів із запобігання, виявлення та **реагування на кіберінциденти, кібератаки, кіберзагрози,** усунення їх наслідків;
4) здійснення аналізу та моделювання поведінки зловмисника відповідно до життєвого циклу відомих (типових) вивчених кіберінцидентів ~~та кібератак~~;	4) здійснення аналізу та моделювання поведінки зловмисника відповідно до життєвого циклу відомих (типових) вивчених кіберінцидентів, кібератак, **кіберзагроз**;
5) систематизація, узагальнення інформації та перетворення її у формат, придатний для проведення подальшого аналізу ефективності заходів із реагування на кіберінциденти ~~та кібератаки~~, а також виконання процесів автоматизованого формування статистичних даних, узагальнюючих та аналітичних показників, звітності тощо;	5) систематизація, узагальнення інформації та перетворення її у формат, придатний для проведення подальшого аналізу ефективності заходів із реагування на кіберінциденти, **кібератаки, кіберзагрози,** а також виконання процесів автоматизованого формування статистичних даних, узагальнюючих та аналітичних показників, звітності тощо;
6) забезпечення формування необхідної звітності, побудови та візуалізації інформаційних панелей (дашбордів) з інформацією про кіберінциденти ~~та кібератаки~~ та вжиті заходи щодо реагування на них;	6) забезпечення формування необхідної звітності, побудови та візуалізації інформаційних панелей (дашбордів) з інформацією про кіберінциденти, **кібератаки, кіберзагрози** та вжиті заходи щодо реагування на них;
7) проведення пошуку та виявлення вразливостей об'єктів кіберзахисту;	7) проведення пошуку та/**або** виявлення **потенційних** вразливостей об'єктів кіберзахисту;
8) захист кінцевих точок від шкідливого програмного забезпечення;	8) захист кінцевих точок від шкідливого програмного забезпечення;
9) забезпечення електронної взаємодії з об'єктами кіберзахисту;	9) забезпечення електронної взаємодії з об'єктами кіберзахисту;
10) захист інформації від несанкціонованого доступу, модифікації (зміни) шляхом здійснення відповідних організаційних і технічних заходів, упровадження засобів та методів захисту інформації;	10) захист інформації від несанкціонованого доступу, модифікації (зміни) шляхом здійснення відповідних організаційних і технічних заходів, упровадження засобів та методів захисту інформації;

11) забезпечення кібербезпеки вебпорталів та вебдодатків; 12) виконання інших завдань, необхідних для забезпечення виконання Центром моніторингу та кібербезпеки завдань, визначених цим Положенням.	11) забезпечення кібербезпеки вебпорталів та вебдодатків; 12) виконання інших завдань, необхідних для забезпечення виконання Центром моніторингу та кібербезпеки завдань, визначених цим Положенням.
3.3. Власником Системи є територіальна громада міста Києва в особі Київської міської ради.	3.3. Власником Системи є територіальна громада міста Києва в особі Київської міської ради.
3.4. Розпорядником Системи є виконавчий орган Київської міської ради (Київська міська державна адміністрація) в особі Департаменту інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації), який забезпечує: 1) вирішення організаційних питань щодо забезпечення функціонування Системи; 2) організацію електронної взаємодії Системи з іншими інформаційними, електронними комунікаційними та інформаційно-комунікаційними системами в установленому порядку; 3) погодження створення, модернізації Системи за поданням адміністратора Системи; 4) здійснення інших завдань, необхідних для функціонування Системи.	3.4. Розпорядником Системи є виконавчий орган Київської міської ради (Київська міська державна адміністрація) в особі Департаменту інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації), який забезпечує: 1) вирішення організаційних питань щодо забезпечення функціонування Системи; 2) організацію електронної взаємодії Системи з іншими інформаційними, електронними комунікаційними та інформаційно-комунікаційними системами в установленому порядку; 3) погодження створення, модернізації Системи за поданням адміністратора Системи; 4) здійснення інших завдань, необхідних для функціонування Системи.
3.5. Адміністратором Системи є Центр моніторингу та кібербезпеки, який забезпечує: 1) створення, адміністрування, безперебійне функціонування та підтримку працездатності Системи;	3.5. Адміністратором Системи є Центр моніторингу та кібербезпеки, який забезпечує: 1) створення, адміністрування, безперебійне функціонування та підтримку працездатності Системи;

2) модернізацію Системи за попереднім погодженням із розпорядником Системи; 3) технічну можливість електронної взаємодії Системи з іншими інформаційними, електронними комунікаційними та інформаційно-комунікаційними системами в установленому порядку; 4) розроблення та впровадження методичних документів для забезпечення належного функціонування Системи; 5) актуальність, достовірність, повноту та захист інформації, яка обробляється або зберігається в Системі, у тому числі, але не виключно, захист інформації від несанкціонованого доступу, знищення, модифікації та блокування доступу до неї шляхом проведення організаційних заходів, впровадження засобів та методів технічного та криптографічного захисту інформації; 6) конфіденційність, цілісність та доступність електронних інформаційних ресурсів Системи; 7) проведення технічних і технологічних заходів для забезпечення функціонування Системи та її компонентів; 8) забезпечення проведення технічних та організаційних заходів з підключення об'єктів кіберзахисту до Системи в порядку, визначеному цим Положенням; 9) впровадження нових компонентів Системи; 10) розроблення та здійснення заходів щодо підвищення відмовостійкості Системи; 11) ведення обліку об'єктів кіберзахисту, підключених до Системи в порядку, визначеному цим Положенням;	2) модернізацію Системи за попереднім погодженням із розпорядником Системи; 3) технічну можливість електронної взаємодії Системи з іншими інформаційними, електронними комунікаційними та інформаційно-комунікаційними системами в установленому порядку; 4) розроблення та впровадження методичних документів для забезпечення належного функціонування Системи; 5) актуальність, достовірність, повноту та захист інформації, яка обробляється або зберігається в Системі, у тому числі, але не виключно, захист інформації від несанкціонованого доступу, знищення, модифікації та блокування доступу до неї шляхом проведення організаційних заходів, впровадження засобів та методів технічного та криптографічного захисту інформації; 6) конфіденційність, цілісність та доступність електронних інформаційних ресурсів Системи; 7) проведення технічних і технологічних заходів для забезпечення функціонування Системи та її компонентів; 8) забезпечення проведення технічних та організаційних заходів з підключення об'єктів кіберзахисту до Системи в порядку, визначеному цим Положенням; 9) впровадження нових компонентів Системи; 10) розроблення та здійснення заходів щодо підвищення відмовостійкості Системи; 11) ведення обліку об'єктів кіберзахисту, підключених до Системи в порядку, визначеному цим Положенням; 12) виконання інших завдань, необхідних для забезпечення функціонування Системи.

12) виконання інших завдань, необхідних для забезпечення функціонування Системи.	
3.6. Складовими Системи є: центральна підсистема; підсистеми; модулі. **Відсутній**	3.6. Складовими Системи є: центральна підсистема; підсистеми; модулі. **Перелік складових Системи не є вичерпним і може доповнюватися у разі здійснення модернізації (модифікації, розвитку) Системи.**
IV. Порядок підключення об'єктів кіберзахисту до Системи	
4.1. Для підключення об'єкта кіберзахисту до Системи розпорядник та/або адміністратор об'єкта кіберзахисту надає Центру моніторингу та кібербезпеки заяву в довільній формі про підключення до Системи, до якої додається паспорт на відповідний об'єкт кіберзахисту, що відповідає вимогам, визначеним у цьому Положенні, та формі, згідно з додатком до цього Положення. У разі потреби Центр моніторингу та кібербезпеки може витребувати від розпорядника та/або адміністратора об'єкта кіберзахисту додаткову інформацію або документи про відповідний об'єкт кіберзахисту. Перед підключенням об'єкта кіберзахисту до Системи їх електронна взаємодія може перевірятися Центром моніторингу та кібербезпеки в тестовому середовищі Системи.	4.1. Для підключення об'єкта кіберзахисту до Системи розпорядник та/або адміністратор об'єкта кіберзахисту надає Центру моніторингу та кібербезпеки заяву в довільній формі про підключення до Системи, до якої додається паспорт на відповідний об'єкт кіберзахисту, що відповідає вимогам, визначеним у цьому Положенні, та формі, згідно з додатком до цього Положення. У разі потреби Центр моніторингу та кібербезпеки може витребувати від розпорядника та/або адміністратора об'єкта кіберзахисту додаткову інформацію або документи про відповідний об'єкт кіберзахисту. Перед підключенням об'єкта кіберзахисту до Системи їх електронна взаємодія може перевірятися Центром моніторингу та кібербезпеки в тестовому середовищі Системи.

4.2. За результатами розгляду заяви про підключення до Системи, паспорта об'єкта кіберзахисту та проведеного тестування (у разі потреби), Центром моніторингу та кібербезпеки готується висновок про підключення об'єкта кіберзахисту до Системи або рекомендації щодо необхідності налаштування відповідного об'єкта кіберзахисту для забезпечення технічної можливості подальшого підключення до Системи.	4.2. За результатами розгляду заяви про підключення до Системи, паспорта об'єкта кіберзахисту та проведеного тестування (у разі потреби), Центром моніторингу та кібербезпеки готується висновок про підключення об'єкта кіберзахисту до Системи або рекомендації щодо необхідності налаштування відповідного об'єкта кіберзахисту для забезпечення технічної можливості подальшого підключення до Системи.
4.3. Висновок про підключення до Системи або рекомендації щодо необхідності налаштування відповідного об'єкта кіберзахисту для забезпечення технічної можливості подальшого підключення до Системи надсилаються Центром моніторингу та кібербезпеки розпоряднику та/або адміністратору об'єкта кіберзахисту протягом десяти робочих днів з дня завершення проведення перевірки її поточного стану та кіберзахищеності, але не пізніше тридцяти календарних днів з дня подання розпорядником та/або адміністратором об'єкта кіберзахисту заяви про підключення. Листування та обмін інформацією чи документами, передбаченими цим Положенням, здійснюється за допомогою засобів інформаційно-комунікаційної системи "Єдиний інформаційний простір територіальної громади міста Києва", створеної на базі програмного забезпечення електронного документообігу АСКОД з дотриманням вимог законодавства України.	4.3. Висновок про підключення до Системи або рекомендації щодо необхідності налаштування відповідного об'єкта кіберзахисту для забезпечення технічної можливості подальшого підключення до Системи надсилаються Центром моніторингу та кібербезпеки розпоряднику та/або адміністратору об'єкта кіберзахисту протягом десяти робочих днів з дня завершення проведення перевірки її поточного стану та кіберзахищеності, але не пізніше тридцяти календарних днів з дня подання розпорядником та/або адміністратором об'єкта кіберзахисту заяви про підключення. Листування та обмін інформацією чи документами, передбаченими цим Положенням, здійснюється за допомогою засобів інформаційно-комунікаційної системи "Єдиний інформаційний простір територіальної громади міста Києва", створеної на базі програмного забезпечення електронного документообігу АСКОД з дотриманням вимог законодавства України.
4.4. У разі підтвердження технічної ~~відповідності~~, за результатами проведеного тестування (у разі потреби),	4.4. У разі підтвердження технічної **можливості**, за результатами проведеного тестування (у разі потреби),

підключення відповідного об'єкта кіберзахисту до Системи здійснюється протягом одного місяця з дати отримання розпорядником та/або адміністратором об'єкта кіберзахисту відповідного висновку про підключення до Системи. Узгодження необхідних параметрів моніторингу, захисту та інших показників, що мають індивідуальний характер здійснюється Центром моніторингу та кібербезпеки спільно з розпорядником та/або адміністратором об'єкта кіберзахисту окремо для кожного об'єкта кіберзахисту.	підключення відповідного об'єкта кіберзахисту до Системи здійснюється протягом одного місяця з дати отримання розпорядником та/або адміністратором об'єкта кіберзахисту відповідного висновку про підключення до Системи. Узгодження необхідних параметрів моніторингу, захисту та інших показників, що мають індивідуальний характер здійснюється Центром моніторингу та кібербезпеки спільно з розпорядником та/або адміністратором об'єкта кіберзахисту окремо для кожного об'єкта кіберзахисту.
4.5. У разі отримання розпорядником та/або адміністратором об'єкта кіберзахисту рекомендацій щодо необхідності налаштування об'єкта кіберзахисту для забезпечення технічної можливості подальшого підключення до Системи такий розпорядник та/або адміністратор об'єкта кіберзахисту протягом п'ятнадцяти робочих днів з дати отримання таких рекомендацій надсилає Центру моніторингу та кібербезпеки інформацію про їх опрацювання.	4.5. У разі отримання розпорядником та/або адміністратором об'єкта кіберзахисту рекомендацій щодо необхідності налаштування об'єкта кіберзахисту для забезпечення технічної можливості подальшого підключення до Системи такий розпорядник та/або адміністратор об'єкта кіберзахисту протягом п'ятнадцяти робочих днів з дати отримання таких рекомендацій надсилає Центру моніторингу та кібербезпеки інформацію про їх опрацювання.
4.6. У разі, якщо розпорядник та/або адміністратор об'єкта кіберзахисту за результатом опрацювання рекомендацій щодо необхідності налаштування об'єкта кіберзахисту для забезпечення технічної можливості подальшого підключення до Системи повідомляє про неможливість відповідних налаштувань, Центр моніторингу та кібербезпеки не несе відповідальності за забезпечення кібербезпеки такого об'єкта кіберзахисту.	4.6. У разі, якщо розпорядник та/або адміністратор об'єкта кіберзахисту за результатом опрацювання рекомендацій щодо необхідності налаштування об'єкта кіберзахисту для забезпечення технічної можливості подальшого підключення до Системи повідомляє про неможливість **здійснення** відповідних налаштувань, **такий об'єкт кіберзахисту підключається** Центр**ом** моніторингу та кібербезпеки **після усунення розпорядником та/або адміністратором об'єкта кіберзахисту причин, які перешкоджали підключенню.**

4.7. Підключення Центром моніторингу та кібербезпеки об'єктів кіберзахисту до Системи відбувається в такому порядку: встановлення програмного забезпечення; налаштування конфігурації програмного або апаратного забезпечення; створення користувацьких, технічних або сервісних облікових записів та надання необхідних повноважень на рівні об'єкта кіберзахисту; налаштування механізмів експорту подій моніторингу та кібербезпеки; налаштування необхідної інтеграції між об'єктом кіберзахисту та Системою.	4.7. Підключення Центром моніторингу та кібербезпеки об'єктів кіберзахисту до Системи відбувається в такому порядку: встановлення програмного забезпечення; налаштування конфігурації програмного або апаратного забезпечення; створення користувацьких, технічних або сервісних облікових записів та надання необхідних повноважень на рівні об'єкта кіберзахисту; налаштування механізмів експорту подій моніторингу та кібербезпеки; налаштування необхідної інтеграції між об'єктом кіберзахисту та Системою.
4.8. Відключення об'єкта кіберзахисту від Системи здійснюється Центром моніторингу та кібербезпеки у разі ~~вчинення розпорядником та/або адміністратором об'єкта кіберзахисту таких дій:~~ подання розпорядником та/або адміністратором об'єкта кіберзахисту заяви про відключення об'єкта кіберзахисту від Системи; ~~внесення змін розпорядником та/або адміністратором об'єкта кіберзахисту до функціональних можливостей об'єкта кіберзахисту, які впливають на роботу програмного або апаратного забезпечення Системи;~~ ~~порушення розпорядником та/або адміністратором об'єкта кіберзахисту вимог щодо забезпечення захисту інформації;~~	4.8. **Відключення об'єкта кіберзахисту від Системи здійснюється Центром моніторингу та кібербезпеки у разі подання розпорядником та/або адміністратором об'єкта кіберзахисту заяви про відключення об'єкта кіберзахисту від Системи у зв'язку з припиненням експлуатації такого об'єкта кіберзахисту.**

~~видалення розпорядником та/або адміністратором об'єкта кіберзахисту раніше створених облікових записів для працівників Центру моніторингу та кібербезпеки об'єктів кіберзахисту, які необхідні для роботи програмного або апаратного забезпечення Системи;~~ ~~анулювання розпорядником та/або адміністратором об'єкта кіберзахисту раніше наданих повноважень облікових записів працівників Центру моніторингу та кібербезпеки об'єктів кіберзахисту, які необхідні для роботи програмного або апаратного забезпечення Системи;~~ ~~розгортання розпорядником та/або адміністратором об'єкта кіберзахисту програмних або апаратних комплексів, які негативно впливають або зовсім блокують роботу програмного або апаратного забезпечення Системи.~~	
4.9. Під час здійснення кіберзахисту та моніторингу об'єктів кіберзахисту засобами Системи Центр моніторингу та кібербезпеки має право: обробляти та зберігати всю інформацію (телеметрію, журнали подій, індикатори компрометації тощо), отриману шляхом здійснення моніторингу; у разі фіксування кіберінцидентів ~~та кібератак~~ ізолювати постраждалі об'єкти кіберзахисту або їх окремі компоненти на час, необхідний для вжиття заходів з реагування та усунення наслідків, про що невідкладно інформувати розпорядника та/або адміністратора відповідного об'єкта кіберзахисту в установленому порядку; здійснювати інші необхідні дії для забезпечення захисту та цілісності Системи.	4.9. Під час здійснення кіберзахисту та моніторингу об'єктів кіберзахисту засобами Системи Центр моніторингу та кібербезпеки має право: обробляти та зберігати всю інформацію (телеметрію, журнали подій, індикатори компрометації тощо), отриману шляхом здійснення моніторингу; у разі фіксування кіберінцидентів, **кібератак, кіберзагроз,** ізолювати постраждалі об'єкти кіберзахисту або їх окремі компоненти на час, необхідний для вжиття заходів з реагування та усунення наслідків, про що невідкладно інформувати розпорядника та/або адміністратора відповідного об'єкта кіберзахисту в установленому порядку; здійснювати інші необхідні дії для забезпечення захисту та цілісності Системи.

4.10. У разі наявності в розпорядників та/або адміністраторів об'єктів кіберзахисту власних інформаційних, електронних комунікаційних або інформаційно-комунікаційних систем кібербезпеки, що експлуатуються, такі розпорядники та/або адміністратори об'єктів кіберзахисту зобов'язані: повідомити Центр моніторингу та кібербезпеки про наявність таких інформаційних, електронних комунікаційних або інформаційно-комунікаційних систем; налаштувати інтеграцію інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем кібербезпеки з Системою; забезпечити шляхом інтеграції передачу в режимі реального часу інформації щодо ідентифікованих кіберінцидентів.	4.10. У разі наявності в розпорядників та/або адміністраторів об'єктів кіберзахисту власних інформаційних, електронних комунікаційних або інформаційно-комунікаційних систем кібербезпеки, що експлуатуються, такі розпорядники та/або адміністратори об'єктів кіберзахисту зобов'язані: повідомити Центр моніторингу та кібербезпеки про наявність таких інформаційних, електронних комунікаційних або інформаційно-комунікаційних систем; налаштувати інтеграцію інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем кібербезпеки з Системою; забезпечити шляхом інтеграції передачу в режимі реального часу інформації щодо ідентифікованих кіберінцидентів, **кібератак, кіберзагроз**.
V. Вимоги до паспорта об'єкта кіберзахисту	
5.1. Паспорт об'єкта кіберзахисту: задокументований у паперовій та електронній формах; містить повну та актуальну інформацію щодо основних характеристик об'єкта кіберзахисту (у тому числі архітектурних рішень), ~~можливих сценаріїв загроз, схем резервного копіювання та моніторингу, планів безперервної діяльності та аварійного відновлення, каналів комунікації тощо,~~ розробляється розпорядником та/або адміністратором об'єкта кіберзахисту за формою, затвердженою згідно з додатком до цього Положення;	5.1. **Паспорт об'єкта кіберзахисту:** **задокументований у паперовій та/або електронній формі;** **містить повну та актуальну інформацію щодо основних характеристик об'єкта кіберзахисту (у тому числі архітектурних рішень), розробляється та затверджується розпорядником та/або адміністратором об'єкта кіберзахисту за формою, затвердженою згідно з додатком до цього Положення.**

~~затверджується розпорядником та/або адміністратором об'єкта кіберзахисту, та передбачає обов'язкове попереднє погодження задіяних відповідальних працівників розпорядника та/або адміністратора відповідного об'єкта кіберзахисту за такими напрямами: експлуатація, технічна підтримка, інформаційна безпека.~~ ~~Відомості, що містяться в паспорті об'єкта кіберзахисту та його складових, є інформацією з обмеженим доступом, вимога щодо захисту якої встановлена законом.~~	**Відомості, що містяться в паспорті об'єкта кіберзахисту та його складових можуть бути інформацією з обмеженим доступом, вимога щодо захисту якої встановлена законом.**
5.2. Один паперовий примірник паспорта об'єкта кіберзахисту, затверджений відповідно до пункту 5.1 цього Положення, передається розпорядником та/або адміністратором об'єкта кіберзахисту до Центру моніторингу та кібербезпеки для проведення моніторингу та організації кіберзахисту засобами Системи.	5.2. Один паперовий примірник паспорта об'єкта кіберзахисту, затверджений відповідно до пункту 5.1 цього Положення, передається розпорядником та/або адміністратором об'єкта кіберзахисту до Центру моніторингу та кібербезпеки для проведення моніторингу та організації кіберзахисту засобами Системи.
VI. Фінансування забезпечення створення, функціонування, адміністрування та модернізації Системи	
6.1. Фінансування забезпечення створення, функціонування, адміністрування та модернізації Системи здійснюється за рахунок коштів бюджету міста Києва на відповідні роки та інших незаборонених джерел фінансування.	6.1. Фінансування забезпечення створення, функціонування, адміністрування та модернізації Системи здійснюється за рахунок коштів бюджету міста Києва на відповідні роки та інших незаборонених джерел фінансування.
Додаток до Положення	Додаток до Положення

ФОРМА ПАСПОРТА
об'єкта кіберзахисту
(далі - ОК)

Назва ОК:	
Індекс ОК:	
Короткий опис ОК:	
Основні користувачі ОК:	Перелік типів користувачів, організацій
Кількість користувачів ОК:	
Балансоутримувач ОК:	
Прізвище, власне ім'я, по батькові (за наявності) та номер телефону керівника балансоутримувача ОК:	
Розпорядник ОК:	
Прізвище, власне ім'я, по батькові (за наявності) та номер телефону керівника розпорядника ОК:	
Адміністратор ОК:	
Прізвище, власне ім'я, по батькові (за наявності) та номер	

ФОРМА ПАСПОРТА
об'єкта кіберзахисту
(далі - ОК)

Назва ОК:	
Індекс ОК:	
Короткий опис ОК:	
Основні користувачі ОК:	Перелік типів користувачів, організацій
Кількість користувачів ОК:	
Розпорядник ОК:	
Прізвище, власне ім'я, по батькові (за наявності) та номер телефону керівника розпорядника ОК:	
Адміністратор ОК:	
Прізвище, власне ім'я, по батькові (за наявності) та номер телефону керівника	

телефону керівника адміністратора ОК:	
Документ про створення, впровадження КС:	
Документ про введення в експлуатацію ОК (дослідну, промислову):	
Архітектура ОК:	
Архітектура ОК:	Актуальна архітектура ОК (програмно-апаратні, технічні засоби, складові) у паперовій та електронній формі
Складові ОК:	Перелік складових, програмно-апаратні, технічні засоби, що входять до складу ОК у паперовій та електронній формі
Оцінка зрілості архітектури ОК:	**Низька** – ОК побудовано на застарілих рішеннях, без врахування сучасних вимог щодо відмовостійкості, масштабування, моніторингу та кіберзахисту. **Середня** – ОК побудовано на сучасних рішеннях, але не всі аспекти супроводу, кіберзахисту та відновлення враховано. Потрібне доопрацювання для досягнення

адміністратора ОК:	
Документ про створення, впровадження ОК:	
Документ про введення в експлуатацію ОК (дослідну, промислову):	
Архітектура ОК:	
Архітектура ОК:	Актуальна архітектура ОК (програмно-апаратні, технічні засоби, складові) у паперовій та електронній формах
Складові ОК:	Перелік складових, програмно-апаратні, технічні засоби, що входять до складу ОК у паперовій та електронній формах
Резервне копіювання	
Схема резервного копіювання:	Документ зі схемою резервування інформації, порядком створення бекапу та інструкціями з відновлення, у паперовій та електронній формах
Резервні копії:	
порядок створення	

	мети – підвищення зрілості архітектури. **Висока** – архітектура побудована з урахуванням сучасних вимог до надійності, кіберзахисту та відновлення					
Оцінка зрілості архітектури ОК:	Низька	Середня	Висока			
	+					
Характеристики ОК:						
БАЛ критичності: (розраховується у залежності від критичності забезпечення надання ОК життєво важливих послуг та функцій)	Використовується бальний принцип по сумі показників, таких як:					
	Фактори впливу /1 – відсутній, 5 – значний/					
	Кількість користувачів	+	+	+	+	+
	Репутаційні втрати	+				
	Фінансові втрати	+				
	Безпека громадян	+				
	Транспорт	+				
	Енергетика	+				
	Довкілля	+				

порядок зберігання	
порядок відновлення	
порядок видалення	
наявність гарячого резервування	
наявність холодного резервування	
Зберігання резервних копій:	
хмарні ресурси	
центри обробки даних, розташовані за адресами	
ВІДНОВЛЕННЯ РОБОТИ:	
Сценарій: ПРОБЛЕМА	Часткова чи повна деградація (непрацездатність) ОК, що призводить до неможливості надання послуг внаслідок виходу з ладу одного зі складових ОК, при працездатності суміжних ОК, від яких залежить працездатність ОК

	Житлово-комунальна сфера	+				
	Втрата керованості (управління) містом	+				
	Загальний бал:	**(середній бал всіх оцінок)**				
Режим роботи ОК:	Вказати режим, при якому не допускається деградація ОК нижче максимального рівня					
Рівень допустимої деградації ОК, %: (розраховується у порівнянні з штатним режимом роботи ОК та в залежності від критичності виконання ОК життєво важливих послуг та функцій)	20% для некритичних сервісів; 10% для середнього рівня; 5% для критичних сервісів.					
Допустимий простій під час штатного режиму роботи ОК, хв						
Допустимий простій під час режиму мінімального навантаження ОК, хв						

Вірогідність виникнення (на рік):	Кількість випадків згідно з історичними даними чи експертною оцінкою		
Час відновлення, годин:			
План аварійного відновлення:	Документ з інструкціями щодо відновлення штатного режиму роботи ОК.		
Порядок інформування:	Вказати хто, кого та в який спосіб інформує		
Час	Хто	Кого	Метод
30 хв			
60 хв			
2 год			
4 год			
8 год			
Альтернативний сценарій дій на час відновлення роботи ОК:	Описати інструкцію щодо дій виконавців, які мають бути виконані під час відновлення працездатності для зменшення негативного ефекту від непрацездатності ОК		
Відповідальний за кіберзахист ОК			
Посада, Прізвище, власне ім'я, по батькові (за наявності), електронна	Особа або керівник організації чи підрозділу який визначений розпорядником, як відповідальний за кіберзахист ОК		

Річний SLA, %	
Резервне копіювання	
Схема резервного копіювання:	Документ зі схемою резервування інформації, порядком створення бекапу та інструкціями з відновлення, у паперовій та електронній формі
Резервні копії:	
порядок створення	
порядок зберігання	
порядок відновлення	
порядок видалення	
наявність гарячого резервування	
наявність холодного резервування	
Зберігання резервних копій:	
хмарні ресурси	
Центри обробки даних, розташовані за адресами	
Архівна інформація:	
порядок створення	
порядок зберігання	
порядок відновлення	
порядок видалення	

пошта та номер телефону відповідального за кіберзахист ОК:	
Відновлення, тестування, аудит планів аварійного відновлення робити ОК:	
Тип перевірки	«Стендові випробування» (імітаційний стенд) або офлайн-тестування (в умовах реального часу)
Частота перевірки	

Додаток 1.1. **Архітектура ОК**

Додаток 1.2. **Складові ОК**

Додаток 1.3. **Схема резервного копіювання**

Додаток 1.4. **План безперервної діяльності ОК**

Додаток 1.5. **План аварійного відновлення штатного режиму роботи ОК**

ВІДНОВЛЕННЯ РОБОТИ:			
Сценарій 1: ПРОБЛЕМА	Часткова чи повна деградація (непрацездатність) ОК, що призводить до неможливості надання послуг внаслідок виходу з ладу одного зі складових ОК, при працездатності суміжних ОК, від яких залежить працездатність ОК		
Вірогідність виникнення (на рік):	Кількість випадків, згідно історичних даних чи експертної оцінки		
Час відновлення, годин:			
План аварійного відновлення:	Документ з інструкціями щодо відновлення штатного режиму роботи ОК.		
Порядок інформування:	Вказати хто, кого та в який спосіб інформує		
Час	Хто	Кого	Метод
30хв			
60хв			
2 год			
4 год			
8 год			
Альтернативний сценарій дій на час відновлення роботи ОК:	Описати інструкцію щодо дій виконавців, які мають бути виконані під час відновлення працездатності для зменшення		

	негативного ефекту від непрацездатності ОК		
Сценарій 2: АВАРІЯ	Масова проблема: Часткова чи повна деградація (непрацездатність) ОК, що призводить до неможливості надання послуг, внаслідок виходу з ладу одного зі складових ОК, при цьому значна частина (до 50%) пов'язаних критичних ОК (сервісів) також непрацездатні		
Критичні ОК, від роботи яких залежить робота ОК:	Вказати індекси критичних сервісів		
Час відновлення, годин:			
Порядок відновлення:	Вказати послідовність індексів ОК/сервісів, що мають бути відновлені або додати схему відновлення, у паперовій та електронній формі		
План аварійного відновлення:	Вказати, чи по всім вказаним вище ОК/сервісам є плани аварійного відновлення		
Порядок інформування:	Вказати хто, кого та в який спосіб інформує		
Час	Хто	Кого	Метод
30хв			

60хв			
2 год			
4 год			
8 год			
Альтернативний сценарій дій на час відновлення роботи ОК:	Описати інструкцію щодо дій виконавців, які мають бути виконані під час відновлення штатного режиму роботи для зменшення негативного ефекту від непрацездатності ОК		
Сценарій 3: НАДЗВИЧАЙНА СИТУАЦІЯ	Масова проблема: Часткова чи повна деградація (непрацездатність) ОК, що призводить до неможливості надання послуг внаслідок виходу з ладу одного зі складових ОК, при цьому значна частина (до 50%) пов'язаних критичних ОК/сервісів також непрацездатні та є факти часткової чи повної втрати працездатності ЦОД, на яких експлуатується ОК		
Критичні сервіси/ОК, від роботи яких залежить робота ОК:	Вказати індекси критичних сервісів		
Перелік ЦОД, від яких залежить роботи ОК:	Перелік ЦОД (індекси)		

Порядок відновлення:	Вказати послідовність індексів ОК/сервісів, що мають бути відновлені або додати схему відновлення, у паперовій та електронній формі		
План аварійного відновлення:	Вказати, чи по всім вказаним вище ОК/сервісам є плани аварійного відновлення		
Час відновлення, днів:			
Порядок інформування:	Вказати хто, кого та в який спосіб інформує		
Час	Хто	Кого	Метод
30хв			
60хв			
2 год			
4 год			
8 год			
Альтернативний сценарій дій на час відновлення сервісу:	Описати інструкцію щодо дій виконавців, які мають бути виконані під час відновлення штатного режиму роботи для зменшення негативного ефекту від непрацездатності ОК		
Моніторинг:			
Режим моніторингу штатного режиму роботи ОК:	Вказати поточний режим моніторингу працездатності (24/7, 8/7, 8/5) чи інше		

Відповідальний за моніторинг: (прізвище, власне ім'я, по батькові (за наявності) та номер телефону)	Контакти відповідального за моніторинг штатного режиму роботи ОК	
Схема моніторингу:	Описати окремим додатком, як здійснюється моніторинг працездатності, які технічні та програмні засоби задіяні, за допомогою яких інструментів	
Порядок обміну інформацією:	Вказати назви каналів зв'язку Microsoft Teams чи інших месенджерах, номера телефонів для отримання поточної інформації щодо працездатності	
Частота звітування щодо працездатності ОК:		
Супровід та адміністрування ОК:		
Назва структурного підрозділу адміністратора ОК, відповідального за супровід ОК:		
Прізвище, власне ім'я, по батькові (за наявності) та номер		

телефону керівника структурного підрозділу:	
Прізвище, власне ім'я, по батькові (за наявності) та номер телефону заступника керівника структурного підрозділу:	
Прізвище, власне ім'я, по батькові (за наявності), номер телефону керівника та номер телефон адміністраторів супроводу:	
Підрядник з підтримки роботи ОК:	
Контакти підрядника (прізвище, власне ім'я, по батькові (за наявності), номер телефону керівника або відповідальної особи підрядника):	
Режим взаємодії з підрядником:	

Дані про укладення договору з підтримки роботи ОК: (номер, предмет договору, ціна тощо)	
Дата укладення договору:	
Дата закінчення терміну дії договору:	
Режим підтримки:	
Час реагування підрядника, хв:	
Контрактний час усунення проблеми, годин:	
Кіберзахист:	
Структурний підрозділ адміністратора ОК, відповідальний за моніторинг та інформування про подій кібербезпеки:	
Контакти співробітників кіберзахисту: (прізвище, власне ім'я, по батькові (за	

наявності) та номер телефону	
Порядок комунікації:	Вказати назви каналів Microsoft TEAMS чи інших месенджерах, номера телефонів для отримання поточної інформації
Структурний підрозділ адміністратора ОК, відповідальний за реагування на події кібербезпеки	Вказати контакти підрозділу (прізвище, власне ім'я, по батькові (за наявності), номер телефону керівника або відповідальної особи), що несе відповідальність за усунення подій кібербезпеки та виконання рекомендацій щодо кіберзахисту ОК.
Короткий опис заходів кібербезпеки для ОК	Вказати об'єм заходів кібербезпеки, які виконуються для даної ОК
Регламент взаємодії:	Порядок взаємодії підрозділу кіберзахисту та супроводу, зробити стислий опис
Відновлення, тестування, аудит планів аварійного відновлення робити ОК:	
Тип перевірки	«стендові випробування» (імітаційний стенд) або офлайн-тестування (в умовах реального часу)

Частота перевірки	
Дата останньої перевірки	
Дата наступної перевірки	

Додаток 1.1. **Архітектура ОК**

Додаток 1.2. **Схема резервного копіювання**

Додаток 1.3. **Схема моніторингу міської ОК**

Додаток 1.4. **План безперервної діяльності ОК**

Додаток 1.5. **План аварійного відновлення штатного режиму роботи ОК**

Заступник голови Київської міської державної адміністрації Валентин МОНДРИЇВСЬКИЙ

Довідка

до проєкту рішення Київської міської ради «Про внесення змін до рішення Київської міської ради від 12 грудня 2024 року № 477/10285»

Проєкт рішення розроблено Департаментом інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації).

Змінами до рішення Київської міської ради від 12 грудня 2024 року № 477/10285 «Про деякі питання забезпечення кібербезпеки в місті Києві» (далі – Рішення) передбачається змінити його заголовок на «Про деякі питання забезпечення кібербезпеки інформаційних (автоматизованих), електронних комунікаційних та інформаційно-комунікаційних систем, що належать до комунальної власності територіальної громади міста Києва».

Також проєктом рішення передбачається внести зміни до Положення про забезпечення кібербезпеки в місті Києві, яке затверджено Рішенням.

Зокрема передбачається змінити його назву на «Положення про забезпечення кібербезпеки інформаційних (автоматизованих), електронних комунікаційних та інформаційно-комунікаційних систем, що належать до комунальної власності територіальної громади міста Києва».

Зазначені у преамбулі проєкту рішення нормативно-правові акти не містять положень, які визначають повноваження Київської міської ради затверджувати будь-які положення у сфері кібербезпеки та кіберзахисту.

Натомість, частиною п’ятою статті 5 Закону України «Про основні засади забезпечення кібербезпеки України» визначено, що суб'єкти забезпечення кібербезпеки (до яких належать зокрема органи місцевого самоврядування) у межах своєї компетенції:

1) здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях;

2) здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

3) здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз;

4) розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту;

5) забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління;

6) здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору.

Заступник керівника апарату –
начальник юридичного управління Леся ВЕРЕС
« 16» червня 2026 року

КИЇВСЬКА МІСЬКА РАДА

Окопному О. Ю.
Нефьодову М. Є.
Положишник В.О.

Ємцю Л.О.

Прошу розглянути проєкт рішення від 19.06.2026 № 08/231-477/ПР в установленому порядку.

Тхорику С. М.

Прошу опрацювати в межах компетенції управління.

Омельченко А. В.

Для контролю за проходженням та тиражування.

Юнаковій С. М.
Павлову Ю. С.

Віталій КЛИЧКО

"19" червня 2026 року
№ 08/231-477/ПР

08/231-477/ПР
19.06.2026

УКРАЇНА

ВИКОНАВЧИЙ ОРГАН КИЇВСЬКОЇ МІСЬКОЇ РАДИ
(КИЇВСЬКА МІСЬКА ДЕРЖАВНА АДМІНІСТРАЦІЯ)

вул. Хрещатик, 36, м. Київ, 01044, тел. (044) 202 71 29, (044) 202 75 58, факс 202 76 41, e-mail: kmda@kma.gov.ua
Контактний центр міста Києва (044) 15 51 Код ЄДРПОУ 00022527
E-mail для електронних звернень громадян: zvernen@kma.gov.ua

18.06.2026 № 009-24р

на № _____ від _____

Київська міська рада

СУПРОВІДНИЙ ЛИСТ

Відповідно до статей 26, 29 Регламенту Київської міської ради, затвердженого рішенням Київської міської ради від 4 листопада 2021 року № 3135/3176, глави 3 розділу VIII Регламенту виконавчого органу Київської міської ради (Київської міської державної адміністрації), затвердженого розпорядженням виконавчого органу Київської міської ради (Київської міської державної адміністрації) від 08 жовтня 2013 року № 1810 за поданням виконавчого органу Київської міської ради (Київської міської державної адміністрації) направляю проєкт рішення Київської міської ради «Про внесення змін до рішення Київської міської ради від 12 грудня 2024 року № 477/10285» (далі – проєкт рішення).

У відповідності до пункту 3.4 глави 3 розділу VIII Регламенту виконавчого органу Київської міської ради (Київської міської державної адміністрації), затвердженого розпорядженням виконавчого органу Київської міської ради (Київської міської державної адміністрації) від 08 жовтня 2013 року № 1810 інформую, що відповідальним за представлення та супроводження проєкту рішення на всіх стадіях розгляду є:

директор Департаменту інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації) Вікторія ІЦКОВИЧ, 366-86-75, 366-86-72.

Текст проєкту рішення у паперовому вигляді відповідає проєкту в електронному вигляді на USB носії.

193088

Додатки:
- проєкт рішення на 9 арк.;
- пояснювальна записка на 4 арк.;
- порівняльна таблиця на 37 арк.;

- додатки на ___1___ арк.;
- електронна версія зазначеного.

Керівник апарату Дмитро ЗАГУМЕННИЙ

Іцкович Вікторія
Петровська Діана