08/231-969/ПР
04.07.2024

КИЇВСЬКА МІСЬКА РАДА

III сесія IX скликання

РІШЕННЯ

_____№_____ ПРОЄКТ

Про деякі питання забезпечення кібербезпеки у місті Києві

Відповідно до законів України «Про місцеве самоврядування в Україні», «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про основні засади забезпечення кібербезпеки України», постанов Кабінету Міністрів України від 29 березня 2006 року № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах», від 16 травня 2023 року № 497 «Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж», Київська міська рада

ВИРІШИЛА:

1. Затвердити Положення про забезпечення кібербезпеки у місті Києві, що додається.

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.

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 (Київської міської державної адміністрації), протягом одного року з дня прийняття цього рішення 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.

4.2. Затвердження паспортів об'єктів кіберзахисту, визначених у Положенні, затвердженому згідно з пунктом 1 цього рішення.

5. Оприлюднити це рішення в установленому порядку.

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, постійну комісію Київської міської ради з питань цифрової трансформації та регулювання надання публічних послуг.

Київський міський голова Віталій КЛИЧКО

ПОДАННЯ:

Заступник голови з питань здійснення самоврядних повноважень — Петро ОЛЕНИЧ

Директор Департаменту інформаційно-комунікаційних технологій — Вікторія ІЩКОВИЧ

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

ПОГОДЖЕНО:

Перший заступник голови — Микола ПОВОРОЗНИК

Заступник голови — Петро ПАНТЕЛЕЄВ

Заступник голови — Валентин МОНДРИЇВСЬКИЙ

Заступник голови — Вячеслав НЕПОП

Заступниця голови — Ганна СТАРОСТЕНКО

Заступниця голови з питань здійснення самоврядних повноважень — Марина ХОНДА

Заступниця голови з питань здійснення самоврядних повноважень — Олена ГОВОРОВА

Заступник голови з питань здійснення самоврядних повноважень — Костянтин УСОВ

Заступник голови з питань здійснення самоврядних повноважень — Владислав АНДРОНОВ

Заступник голови з питань здійснення самоврядних повноважень — Володимир ПРОКОПІВ

Заступник міського голови – секретар Київської міської ради — Володимир БОНДАРЕНКО

Виконувач обов’язків директора СКП «Київтелесервіс» — Олександр БИСТРУШКІН

Заступник керівника апарату – начальник юридичного управління — Леся ВЕРЕС

Керівник апарату — Дмитро ЗАГУМЕННИЙ

Постійна комісія Київської міської ради з питань транспорту, зв’язку та реклами

Голова — Олексій ОКОПНИЙ

Секретар — Ігор ГАЛАЙЧУК

Постійна комісія Київської міської ради з питань цифрової трансформації та регулювання надання публічних послуг

Голова — Максим НЕФЬОДОВ

Секретар засідання — Ксенія СЕМЕНОВА Михайло Наконечний

Начальник управління правового забезпечення діяльності Київської міської ради — Валентина ПОЛОЖИШНИК

Голова постійної комісії Київради з питань регламенту, депутатської етики та запобігання корупції — Леонід Ємець

ПОЯСНЮВАЛЬНА ЗАПИСКА
до проєкту рішення Київської міської ради
«Про деякі питання забезпечення кібербезпеки у місті Києві»
(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.

Розвиток інформаційних і кібертехнологій та глобальна інформатизація призвели до того, що інформаційна та кіберсфери стали сферами, в яких та через які здійснюються різноманітні деструктивні впливи на усі базові сфери суспільної діяльності (політичну, воєнну, правову, економічну, енергетичну, інфраструктурну, соціальну, духовну, технологічну тощо), що в свою чергу може впливати на безпеку столиці в цілому.

В умовах дії правового режиму воєнного стану, необхідність забезпечення безпеки міських електронних інформаційних ресурсів та міської мережевої інфраструктури від кібератак щодня зростає і є актуальним питанням сьогодення. Кіберзлочинність розвивається дуже швидко і має різноманітні прояви. Найпоширенішими є кібератаки, спрямовані на несанкціонований доступ, блокування доступу до роботи з файлами, викрадення персональних даних, поширення вірусів в комп'ютерних системах і мережах та інше.

У зв'язку з цим, місто Київ, як столиця України, потребує створення й організацію потужної системи кіберзахисту, яка забезпечить здійснення постійного спостереження та контролю за станом захищеності міських електронних інформаційних ресурсів, міської мережевої інфраструктури, суспільства, природного середовища і потенційно небезпечних об'єктів від цілеспрямованого кібервпливу, зокрема з боку російських хакерів.

У статті 1 Закону України «Про основні засади забезпечення кібербезпеки України» (далі – Закон про кібербезпеку), який визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки, визначено, що:

кібербезпека - захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;

кіберзахист - сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації,

спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем.

Відповідно до статті 5 Закону 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.

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 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 – 2025 роки, затвердженої рішенням Київської міської ради від 07 грудня 2023 року № 7516/7557, забезпечує створення та впровадження центру моніторингу та кібербезпеки міських сервісів, його технічне обслуговування, моніторинг та підтримку сервісів, розширення та дооснащення, а також супровід мережевої інфраструктури Київської міської ради, виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва тощо.

Крім того, відповідно до пункту 3 розпорядження виконавчого органу Київської міської ради (Київської міської державної адміністрації) від 03 серпня 2018 року № 1394 «Про введення в дослідну експлуатацію корпоративних інформаційних сервісів виконавчого органу Київської міської ради (Київської міської державної адміністрації)» СКП «Київтелесервіс» доручено забезпечити кіберзахист у корпоративних інформаційних сервісах виконавчого органу Київської міської ради (Київської міської державної адміністрації), які використовуються структурними підрозділами виконавчого органу Київської міської ради (Київської міської державної адміністрації), районними в місті Києві державними адміністраціями, підприємствами, установами та організаціями, що належать до комунальної власності територіальної громади міста Києва.

У зв'язку із зазначеним, на базі СКП «Київтелесервіс» створюється центр моніторингу та кібербезпеки міських сервісів, який виконує превентивні заходи та забезпечує оперативне реагування на кіберінциденти, пов'язані з міськими електронними інформаційними ресурсами та міською мережевою інфраструктурою, здійснюватиме підготовку і передачу інформації щодо кіберзахисту до центральних органів державної влади у сфері кібербезпеки, а також з питань запобігання, виявлення кіберінцидентів.

Також СКП «Київтелесервіс» здійснює взаємодію з Адміністрацією Державної служби спеціального зв'язку та захисту інформації України та Службою безпеки України у сфері забезпечення захисту електронних інформаційних ресурсів місцевих органів виконавчої влади та місцевого самоврядування міста Києва.

Крім того, співпрацює з Національним координаційним центром кібербезпеки Ради національної безпеки і оборони України (НКЦК), Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA (далі - CERT-UA).

Законом про кібербезпеку на CERT-UA, що функціонує в складі Державної служби спеціального зв'язку та захисту інформації України, покладено завдання, зокрема щодо:

накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів;

взаємодію з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору;

сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам.

У зв'язку з цим підготовлено проєкт рішення, яким передбачено впровадження інформаційно-комунікаційної системи моніторингу та кібербезпеки (далі – Система) та затвердження Положення про забезпечення кібербезпеки у місті Києві, яке визначає основні засади забезпечення кібербезпеки, порядок підключення об'єктів кіберзахисту до Системи, функціональні можливості, суб'єктів відносин, та інше.

Враховуючи вищевикладене, а також зростаючу кількість ризиків та небезпек, що можуть бути спричинені діями держави-агресора у кіберпросторі, які потребують вжиття заходів кіберзахисту системного характеру, спрямованих на швидке виявлення та захист від інцидентів кібербезпеки 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, що належать до

комунальної власності територіальної громади міста Києва та/або використовуються для задоволення суспільних потреб та/або реалізації правовідносини у сферах електронного урядування, електронних послуг, електронної комерції, електронного документообігу тощо, 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 захист інформації в інформаційно-комунікаційних системах»;

Закону України «Про основні засади забезпечення кібербезпеки України»;

постанови Кабінету Міністрів України від 29 березня 2006 року № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах»;

постанови Кабінету Міністрів України від 16 травня 2023 року № 497 «Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж».

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 забезпечення захисту міських електронних інформаційних ресурсів та міської мережевої інфраструктури від інцидентів кібербезпеки та кібератак.

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 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) в особі Департаменту інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації).

Доповідачем на пленарному засіданні Київської міської ради та особою, відповідальною за супроводження даного проєкту рішення є директор Департаменту інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації) Іцкович Вікторія Євгенівна (тел. 366-86-70).

Директор Департаменту
інформаційно-комунікаційних технологій
виконавчого органу Київської
міської ради (Київської міської
державної адміністрації) Вікторія ІЦКОВИЧ

ЗАТВЕРДЖЕНО

рішення Київської міської ради
від_____№_____

ПОЛОЖЕННЯ
про забезпечення кібербезпеки у місті Києві

І. Загальні положення

1.1. Положення про забезпечення кібербезпеки у місті Києві (далі – Положення) розроблено з метою забезпечення кібербезпеки у 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.

1.2. 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 (Київської міської державної адміністрації).

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.

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.

2.2. У розумінні цього Положення 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 у місті Києві.

2.3. Суб'єктами відносин, задіяними у 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).

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.

2.5. Власником об'єкта кіберзахисту є територіальна громада міста Києва в особі Київської міської ради, 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.

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).

2.7. Завданнями розпорядника та/або адміністратора об'єкту кіберзахисту є забезпечення:

1) Визначення структурного підрозділу, який виконуватиме функції із забезпечення взаємодії з Центром моніторингу та кібербезпеки з питань кіберзахисту об'єкту або посадової (службової) особи з цих питань.

2) Розроблення, затвердження, підтримки в актуальному стані документів, необхідних для забезпечення кібербезпеки відповідного об'єкту кіберзахисту, у тому числі, але не виключно паспорту об'єкта кіберзахисту.

3) Функціональності, безперервності роботи, відновлюваності, цілісності та стійкості відповідного об'єкту кіберзахисту.

4) Систематичного проведення аналізу вразливостей, ідентифікованих Центром моніторингу та кібербезпеки, впровадження оновлень програмного забезпечення, спрямованих на усунення вразливостей 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.

7) Підключення відповідного об'єкта кіберзахисту до інформаційно-комунікаційної системи моніторингу та кібербезпеки (далі – Система), у порядку визначеному цим Положенням, створення облікових записів з 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 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'єкту 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'єкту кіберзахисту.

13) Проведення оцінки ризиків кібербезпеки об'єкту кіберзахисту відповідно до стандартів, обов'язковість застосування яких встановлена нормативно-правовими актами.

14) Створення та зберігання резервних копій інформації відповідного об'єкту кіберзахисту в установленому порядку та своєчасної заміни відповідних компонентів об'єкту 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'єкту 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, в 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.

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'єкту 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 законодавства.

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, здійснюється 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.

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.

3.2. 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).

2) Моніторинг, виявлення та сповіщення про підозрілу поведінку, що може бути пов'язана з кіберінцидентом та кібератакою щодо об'єктів кіберзахисту.

3) Автоматизація заходів із запобігання, виявлення та реагування на кіберінциденти та кібератаки, усунення їх наслідків.

4) Здійснення аналізу та моделювання поведінки зловмисника відповідно до життєвого циклу відомих (типових) вивчених кіберінцидентів та кібератак.

5) Систематизація, узагальнення інформації та перетворення її у формат, придатний для проведення подальшого аналізу ефективності заходів з реагування на кіберінциденти та кібератаки, 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.

7) Проведення пошуку та виявлення вразливостей об'єктів кіберзахисту.

8) Захист кінцевих точок від шкідливого програмного забезпечення.

9) Забезпечення електронної взаємодії з об'єктами кіберзахисту.

10) Захист інформації від несанкціонованого доступу, модифікації (зміни) шляхом здійснення відповідних організаційних і технічних заходів, впровадження 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.

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.

3.5. Адміністратором Системи є Центр моніторингу та кібербезпеки, який забезпечує:

1) Створення, адміністрування, безперебійне функціонування та підтримку працездатності Системи.

2) Модернізацію Системи, за попереднім погодженням з 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, в 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.

3.6. Складовими Системи є:
центральна підсистема;
підсистеми;
модулі.

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 додатку до цього Положення.

У разі потреби, Центр моніторингу та кібербезпеки може витребувати у 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, паспорту 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.

4.4. У разі підтвердження технічної відповідності, 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.

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.

4.7. Підключення Центром моніторингу та кібербезпеки об'єктів кіберзахисту до Системи відбувається у 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;

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 обліковим записам 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:

оброблювати 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.

4.10 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 за рахунок інтеграції передачу в режимі реального часу інформації щодо ідентифікованих кіберінцидентів.

V. Вимоги до паспорта об'єкта кіберзахисту

5.1. Паспорт об'єкта кіберзахисту:

задокументований у паперовій та у електронній формі;

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;

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 наступними напрямками: 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.

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.

Київський міський голова Віталій КЛИЧКО

Додаток до Положення

ФОРМА ПАСПОРТУ
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 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.

<table>
<tr><td></td><td colspan="6">Середня – ОК побудовано на сучасних рішеннях, але не всі аспекти супроводу, кіберзахисту та відновлення враховано. Потрібне доопрацювання для досягнення мети – підвищення зрілості архітектури.
Висока – архітектура побудована з урахуванням сучасних вимог до надійності, кіберзахисту та відновлення</td></tr>
<tr><td rowspan="2">Оцінка зрілості архітектури ОК:</td><td>Низька</td><td colspan="2">Середня</td><td colspan="3">Висока</td></tr>
<tr><td>+</td><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td>Характеристики ОК:</td><td colspan="6"></td></tr>
<tr><td rowspan="12">БАЛ критичності: (розраховується у залежності від критичності забезпечення надання ОК життєво важливих послуг та функцій)</td><td colspan="6">Використовується бальний принцип по сумі показників, таких як:</td></tr>
<tr><td colspan="6">Фактори впливу /1 – відсутній, 5 – значний/</td></tr>
<tr><td>Кількість користувачів</td><td>+</td><td>+</td><td>+</td><td>+</td><td>+</td></tr>
<tr><td>Репутаційні втрати</td><td>+</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Фінансові втрати</td><td>+</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Безпека громадян</td><td>+</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Транспорт</td><td>+</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Енергетика</td><td>+</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Довкілля</td><td>+</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Житлово-комунальна сфера</td><td>+</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Втрата керованості (управління) містом</td><td>+</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Загальний бал:</td><td colspan="5">(середній бал всіх оцінок)</td></tr>
<tr><td>Режим роботи ОК:</td><td colspan="6">Вказати режим, при якому не допускається деградація ОК нижче максимального рівня</td></tr>
<tr><td>Рівень допустимої деградації ОК, %: (розраховується у порівнянні з штатним режимом роботи ОК та в залежності від критичності виконання ОК життєво важливих послуг та функцій)</td><td colspan="6">20% для некритичних сервісів;
10% для середнього рівня;
5% для критичних сервісів.</td></tr>
<tr><td>Допустимий простій під час штатного режиму роботи ОК, хв</td><td colspan="6"></td></tr>
</table>

Допустимий простій під час режиму мінімального навантаження ОК, хв			
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			
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**

Довідка
до проєкту рішення Київської міської ради «Про деякі питання забезпечення кібербезпеки у місті Києві»

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

Проєктом рішення зокрема передбачається затвердити Положення про забезпечення кібербезпеки у місті Києві та впровадити інформаційно-комунікаційну систему моніторингу та кібербезпеки.

З нормативно-правових актів зазначених в преамбулі проєкту рішення, як правові підстави для видання рішення, не вбачається повноважень Київської міської ради затверджувати Положення про забезпечення кібербезпеки у місті Києві та впроваджувати інформаційно-комунікаційну систему моніторингу та кібербезпеки.

Заступник керівника апарату-
начальник юридичного управління Леся ВЕРЕС

«01» липня 2024 року

Андрій Ковальов 202 74 87

КИЇВСЬКА МІСЬКА РАДА
Управління правового забезпечення діяльності Київської міської ради
вул. Хрещатик, 36, м. Київ, 01001, тел.: (044) 202 70 19
Контактний центр міста Києва: (044) 15 51, e-mail: jurist@kmr.gov.ua, сайт: kmr.gov.ua,
код ЄДРПОУ 22883141

20.11.2024 № 08/230-1454 На № _____ від _____

Голові постійної комісії Київської міської ради з питань транспорту, зв'язку та реклами Олексію ОКОПНОМУ

Зауваження
до проєкту рішення Київської міської ради від 04.07.2024 №08/231-969/ПР
«Про деякі питання забезпечення кібербезпеки у місті Києві»

Управлінням правового забезпечення діяльності Київської міської ради опрацьовано поданий проєкт рішення, з приводу чого зазначаємо таке.

Проєктом рішення пропонується затвердити Положення про забезпечення кібербезпеки у місті Києві та здійснити низку організаційно-правових заходів щодо впровадження інформаційно-комунікаційної системи моніторингу та кібербезпеки.

1. Зауважуємо, що преамбулі проекту рішення як на правову підставу його прийняття містяться посилання на закони України «Про місцеве самоврядування в Україні», «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про основні засади забезпечення кібербезпеки України», постанови Кабінету Міністрів України від 29 березня 2006 року № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах», від 16 травня 2023 року № 497 «Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж».

Відповідно до частини першої статті 38 Закону України «Про правотворчу діяльність» преамбула – це вступна частина нормативно-правового акта, в якій можуть визначатися передумова прийняття нормативно-правового акта, роз'яснюватися мета і підстава його прийняття, визначатися основні завдання, на виконання яких спрямована його дія, інші важливі для суб'єкта

правотворчості обставини, що впливають на прийняття цього нормативно-правового акта.

Відповідно до пункту 2.2. розділу 2 Методичних рекомендацій з оформлення проєктів рішень Київської міської ради та дотримання правил нормопроєктувальної техніки, доведених до відома розпорядженням Київського міського голови від 05.11.2024 № 1055 (далі - Методичні рекомендації) преамбула проєкту рішення повинна мати посилання на відповідну структурну одиницю компетенційного нормативно-правового акта (акта, що передбачає відповідні повноваження).

При цьому слід мати на увазі, що компетенційний акт - це акт, що містить пряму вказівку на повноваження суб'єкта нормотворення (Київської міської ради) щодо прийняття рішення з відповідного питання.

Разом з тим, преамбула проєкту рішення містить лише загальні посилання на правові акти та не містить посилання на конкретну норму, яка надає повноваження Київській міській раді щодо прийняття відповідного рішення.

Водночас правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки визначені Законом України «Про основні засади забезпечення кібербезпеки України» (далі – Закон України).

Відповідно до частини четвертої статті 5 Закону України, органи місцевого самоврядування визначені суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки.

Відповідно до частини п'ятої цієї ж статті Закону України, суб'єкти забезпечення кібербезпеки у межах своєї компетенції: здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях; здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків; здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз; розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту; забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління; здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору.

Враховуючи вищевикладене рекомендуємо у преамбулі проєкту рішення слова: «Про основні засади забезпечення кібербезпеки України» замінити словами: «частин четвертої та п'ятої статті 5 Закону України «Про основні засади забезпечення кібербезпеки України».

Крім того зауважуємо, у преамбулі проєкту рішення не зазначена мета прийняття цього проєкту рішення.

Відповідно до пункту 2.2. розділу 2 Методичних рекомендацій, преамбула проєкту рішення дає стислу інформацію про необхідність та мету прийняття цього проєкту рішення і підлягає врахуванню при його роз'ясненні та застосуванні.

Як вбачається із пояснювальної записки до проєкту рішення місто Київ, як столиця України, потребує створення й організації потужної системи кіберзахисту, яка забезпечить здійснення постійного спостереження та контролю за станом захищеності міських електронних інформаційних ресурсів, міської мережевої інфраструктури, суспільства, природного середовища і потенційно небезпечних об'єктів від цілеспрямованого кібервпливу, зокрема з боку російських хакерів.

Зважаючи на викладене, рекомендуємо преамбулу проєкту рішення після слів: «Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж» доповнити словами: «з метою забезпечення здійснення постійного спостереження та контролю за станом захищеності міських електронних інформаційних ресурсів, міської мережевої інфраструктури, суспільства, природного середовища і потенційно небезпечних об'єктів від цілеспрямованого кібервпливу».

2. Відповідно до пункту 1.2 розділу I проєкту Положення про забезпечення кібербезпеки в місті Києві (далі – Положення), що пропонується затвердити, 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 (Київської міської державної адміністрації).

Відповідно до пункту 2.2 розділу II проєкту Положення у розумінні цього Положення 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 у місті Києві.

Водночас пунктом 1 проєкту рішення передбачається затвердити Положення про забезпечення кібербезпеки у місті Києві.

Зауважуємо відповідно до статті 1 Закону України «Про столицю України - місто-герой Київ», місто Київ відповідно до Конституції України є столицею України.

Місто Київ як столиця України є: політичним та адміністративним центром держави; місцем розташування резиденції глави держави - Президента України, Верховної Ради України, Кабінету Міністрів України, Конституційного Суду України, Верховного Суду України, центральних органів державної влади; духовним, культурним, історичним, науково-освітнім центром України; місцем розташування дипломатичних представництв іноземних держав та міжнародних організацій в Україні. Місто Київ є місцем розташування Київської обласної ради та Київської обласної державної адміністрації та їх органів. Місто Київ є місцем розташування відповідних органів виконавчої влади і місцевого самоврядування.

Також варто зазначити, що назва проєкту рішення «Про деякі питання забезпечення кібербезпеки в місті Києві» не відповідає змісту положень проєкту рішення та проєкту Положення.

Зважаючи на викладене, з урахуванням того, що на території міста Києва, окрім об'єктів комунальної власності, розташовані і інші об'єкти, зокрема, органи державної влади, формулювання «забезпечення кібербезпеки в місті Києві», тобто яке передбачає поширення на всі об'єкти розташовані у місті Києві, не відповідає повноваженням Київської міської ради.

З огляду на викладене, рекомендуємо у назві та у пункті 1 проєкту рішення, у назві та у пункті 1 розділу І проєкту Положення слова «у місті Києві» – виключити.

3. У пункті 2.5 розділу ІІ проєкту Положення зазначено, що власником об'єкта кіберзахисту є територіальна громада міста Києва в особі Київської міської ради, 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.

Пунктом 3.3 розділу ІІІ проєкту Положення пропонується, що власником Системи є територіальна громада міста Києва в особі Київської міської ради.

Зауважуємо, що статтею 1 Закону України «Про місцеве самоврядування в Україні» визначено, що право комунальної власності - право територіальної громади володіти, доцільно, економно, ефективно користуватися і розпоряджатися на свій розсуд і в своїх інтересах майном, що належить їй, як безпосередньо, так і через органи місцевого самоврядування.

Частина п'ята статті 16 Закону України «Про місцеве самоврядування в Україні» передбачає, що від імені та в інтересах територіальних громад права суб'єкта комунальної власності здійснюють відповідні ради.

Зважаючи на викладене, положення пункту 2.5 розділу II та пункту 3.3 розділу III проєкту Положення не узгоджуються зі змістом норм Закону України «Про місцеве самоврядування в Україні».

З урахуванням викладеного, рекомендуємо:

- у пункті 2.5 розділу II проєкту Положення слова: «в особі Київської міської ради» замінити словами: «від імені та в інтересах якої права суб'єкта комунальної власності здійснює Київська міська рада та відповідно управління».

- у пункті 3.3 розділу III проєкту Положення слова: «в особі Київської міської ради» замінити словами: «від імені та в інтересах якої права суб'єкта комунальної власності здійснює Київська міська рада».

4. Як вбачається із пункту 3 пояснювальної записки до проєкту рішення, «Реалізація цього рішення не передбачає використання додаткових коштів бюджету міста Києва.

Водночас, пунктом 6.1 проєкту Положення, передбачено, що «Фінансування забезпечення, функціонування, адміністрування та модернізації системи здійснюється за рахунок коштів бюджету міста Києва на відповідні роки та інших незаборонених джерел».

Згідно з частиною восьмою статті 26 Регламенту Київської міської ради, затвердженого рішенням Київської міської ради від 04.11.2021 № 3135/3176, у випадку внесення на розгляд Київради проєкту рішення Київради, прийняття якого призведе до зміни показників бюджету міста Києва (надходжень бюджету та/або витрат бюджету), суб'єкт подання зобов'язаний додати до пояснювальної записки фінансово-економічне обґрунтування та пропозиції щодо джерел покриття цих витрат.

5. До матеріалів проєкту рішення додано Довідку юридичного управління виконавчого органу Київської міської ради (Київської міської державної адміністрації) від 01.07.2024.

Відповідно до частини другої статті 26 Регламенту Київської міської ради, затвердженого рішенням Київської міської ради від 4 листопада 2021 року № 3135/3176 проєкти рішень Київради, суб'єктом подання яких є виконавчий орган Київради (Київська міська державна адміністрація), підписуються посадовими особами, визначеними Регламентом виконавчого органу Київради (Київської міської державної адміністрації). У випадку наявності зауважень або будь-яких інших посилань на наявність недоліків проєкту рішення Київради, наданих посадовими особами та/або структурними підрозділами виконавчого органу Київради (Київської міської державної адміністрації), до проєкту рішення

Київради суб'єктом подання додається письмова інформація щодо врахування зауважень, недоліків або недоцільність їх урахування із зазначенням мотивів.

При цьому, відповідну інформацію щодо врахування зауважень, викладених у довідці, або недоцільність їх урахування із зазначенням мотивів до матеріалів проєкту рішення не додано.

Враховуючи вищевказане, рекомендуємо доопрацювати проєкт рішення в межах можливостей та процедур, передбачених Регламентом Київської міської ради, затвердженим рішенням Київської міської ради від 04.11.2021 № 3135/3176 та відповідно відобразити у проєкті рішення відповідні положення.

Начальник управління Валентина ПОЛОЖИШНИК

Тетяна Мороченець