КИЇВСЬКА МІСЬКА РАДА
IV сесія IX скликання

Р І Ш Е Н Н Я

12.12.2024 Київ № 477/10285

Про деякі питання забезпечення кібербезпеки в місті Києві

Відповідно до законів України «Про місцеве самоврядування в Україні», «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», частини четвертої та п'ятої статті 5 «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», рішення Київської міської ради від 07 грудня 2023 року № 7516/7557 «Про затвердження Комплексної міської цільової програми «Цифровий Київ» на 2024-2025 роки», з метою забезпечення захисту міських електронних інформаційних ресурсів та міської мережевої інфраструктури від інцидентів кібербезпеки та кібератак Київська міська рада:

ВИРІШИЛА:

1. Затвердити Положення про забезпечення кібербезпеки в 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 (Київською міською державною адміністрацією), 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 та постійну комісію Київської міської ради з питань цифрової трансформації та регулювання надання публічних послуг.

Київський міський голова Віталій КЛИЧКО

КИЇВСЬКА МІСЬКА РАДА
СЕКРЕТАРІАТ
1
УКРАЇНА

ЗАТВЕРДЖЕНО
рішення Київської міської ради
від 14.12.2023 № 477/10285

КИЇВСЬКА МІСЬКА РАДА
СЕКРЕТАРІАТ
1
УКРАЇНА

ПОЛОЖЕННЯ
про забезпечення кібербезпеки в місті Києві

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.

1.2. 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).

1.3. 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 в місті Києві.

2.3. Суб'єктами відносин, задіяними 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).

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 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.

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'єкта кіберзахисту є забезпечення:

1) визначення структурного підрозділу, який виконуватиме функції із забезпечення взаємодії з Центром моніторингу та 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;

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;

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 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 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.

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;

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.

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 із 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, 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.

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 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.

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 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.

4.3. 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 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;

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.

4.10. 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.

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;

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.

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 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 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
Оцінка зрілості архітектури ОК:	**Низька** – ОК побудовано на застарілих рішеннях без урахування сучасних вимог

<table>
<tr><td></td><td colspan="6">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 мети – підвищення зрілості архітектури
Висока – архітектура побудована з урахуванням сучасних вимог до надійності, кіберзахисту та відновлення</td></tr>
<tr><td>Оцінка зрілості архітектури ОК:</td><td>Низька</td><td colspan="2">Середня</td><td colspan="3">Висока</td></tr>
<tr><td></td><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 в залежності від критичності забезпечення надання ОК життєво важливих послуг та функцій):</td><td colspan="6">Використовується бальний принцип за сумою 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, за якого не допускається деградація ОК нижче максимального рівня</td></tr>
<tr><td>Рівень допустимої деградації ОК, % (розраховується у порівнянні зі штатним режимом роботи ОК та в залежності від критичності виконання ОК життєво.</td><td colspan="6">20% для некритичних сервісів
10% для середнього рівня
5% для критичних сервісів</td></tr>
</table>

важливих послуг та функцій);	
Допустимий простій під час штатного режиму роботи ОК, хв	
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 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	
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 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		
Сценарій 2: АВАРІЯ	Масова проблема: часткова чи повна деградація (непрацездатність) ОК, що призводить до неможливості надання послуг унаслідок виходу з ладу одного зі складових ОК, водночас 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 формах		
План аварійного відновлення:	Вказати, чи для всіх вказаних вище ОК / сервісам є плани аварійного відновлення		
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 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 унаслідок виходу з ладу одного зі складових ОК, водночас 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 формах		
План аварійного відновлення:	Вказати, чи за всіма вказаними вище ОК / сервісами є плани аварійного відновлення		
Час відновлення, днів:			
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 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 месенджерів, 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, год:	
Кіберзахист:	
Структурний підрозділ адміністратора ОК, відповідальний за моніторинг та інформування про події кібербезпеки:	
Контакти співробітників кіберзахисту: (прізвище, власне ім'я, по батькові (за наявності) та номер телефону	
Порядок комунікації:	Вказати назви каналів Microsoft Teams чи інших месенджерів, номера телефонів для отримання поточної інформації
Структурний підрозділ адміністратора ОК, відповідальний за	Вказати контакти підрозділу (прізвище, власне ім'я, по батькові (за наявності), номер телефону керівника або відповідальної

реагування на події кібербезпеки	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 цього 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 міського ОК**

Додаток 1.4. **План безперервної діяльності ОК**

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