v-ev-008gk

Про затвердження Регламенту використання та функціонування комплексної системи відеоспостереження міста Миколаєва

На виконання рішення Миколаївської міської ради від 25.01.2024 № 28/57 «Про затвердження Положення про комплексну систему відеоспостереження «Безпечне місто Миколаїв», враховуючи Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», рішення Миколаївської міської ради від 23.07.2020 № 57/371 «Про затвердження міської комплексної Програми «Інформатизація та розвиток електронного урядування» на 2020-2022 роки» (із змінами), керуючись ст. 59 Закону України «Про місцеве самоврядування в Україні», виконком міської ради

ВИРІШИВ:

1. Затвердити Регламент використання та функціонування комплексної системи відеоспостереження міста Миколаєва (додається).

2. Контроль за виконанням даного рішення покласти на керуючого справами виконавчого комітету Миколаївської міської ради Волкова А.С.

Перший заступник

міського голови В. ЛУКОВ

ЗАТВЕРДЖЕНО

рішення виконкому міської ради

від\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

№ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

РЕГЛАМЕНТ

використання та функціонування комплексної системи

відеоспостереження міста Миколаєва

1. Загальні положення

1.1. Регламент використання та функціонування комплексної системи відеоспостереження міста Миколаєва (далі – Регламент) розроблений на виконання рішення Миколаївської міської ради від 25.01.2024 № 28/57 «Про затвердження Положення про комплексну систему відеоспостереження «Безпечне місто Миколаїв», згідно із Законами України «Про місцеве самоврядування в Україні», «Про інформацію», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних», «Про електронні документи та електронний документообіг», постанови Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», рішенням Миколаївської міської ради від 23.07.2020 № 57/371 «Про затвердження міської комплексної Програми «Інформатизація та розвиток електронного урядування» на 2020-2022 роки» (із змінами), іншими нормативно-правовими актами, з метою визначення складу та порядку функціонування комплексної системи відеоспостереження (далі – Система), правил користування Системою, суб’єктів отримання інформації із Системи, організації захисту даних в Системі тощо.

1.2. Терміни в Регламенті вживаються в значенні, наведеному в Законах України «Про інформацію», «Про телекомунікації», «Про захист персональних даних», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про електронні документи та електронний документообіг», Положенні про комплексну систему відеоспостереження «Безпечне місто Миколаїв» (далі – Положення).

2. Склад та порядок функціонування Системи

2.1. Система складається з програмних, технічних та програмно- технічних компонентів, які умовно можливо розділити на окремі підсистеми, що є невід’ємними частинами Системи.

2.2. Підсистема засобів відеофіксації (відеокамери) – умовно розділяється на декілька типів – розпізнавання автомобільних номерів, розпізнавання об’єктів, оглядові. Відеокамери працюють в автоматичному режимі та можуть бути переведені в режим ручного керування. Основні функціональні можливості підсистеми засобів відеофіксації (за наявності технічної можливості):

2.2.1. Безперервне збирання відеоінформації в зоні відеоспостереження.

2.2.2. Збирання відеоінформації в залежності від наявності руху об’єктів у зоні відеоспостереження.

2.2.3. Зміна фокусної відстані (за наявності технічної можливості).

2.2.4. Автоматичне та автоматизоване фокусування на рухомих чи нерухомих об’єктах, що знаходяться в зоні відеоспостереження.

2.2.5. Цифрове масштабування (збільшення/зменшення) відеозображення.

2.2.6. Зміна режиму відеозапису день/ніч (керування інфрачервоним фільтром).

2.2.7. Накладання службового тексту та зображення на відеопотік.

2.2.8. Автоматичне протоколювання подій:

- спрацювання сигналу тривоги;

- спрацювання детектора: «день/ніч»;

- спрацювання контролю доступу до відеопотоку, живого перегляду, несанкціоновані дії;

- час: використання розкладу, періодичність; дії по події.

Засоби відеофіксації можуть бути налаштовані відповідно до зазначеного вище функціоналу та до проєктної документації на їх монтаж і забезпечують функціонування в автоматичному режимі.

2.3. Підсистема засобів обробки відеоінформації– програмно-технічний комплекс, який умовно може бути розділений на компоненти за функціоналом, що забезпечують:

2.3.1. онлайн-трансляцію зображення з підсистеми засобів відеофіксації;

2.3.2. зберігання загальної відеоінформації протягом 30 діб;

2.3.3. запис відеоінформації та відеоданих;

2.3.4. маркування відеоінформації та відеоданих;

2.3.5. можливість відображення інформації із засобів відеофіксації, дати та часу, назви відеокамери та іншої службової інформації Системи;

2.3.6. групування відображення інформації з підсистеми засобів відеофіксації за різноманітними критеріями (пресети);

2.3.7. відображення засобів відеофіксації на мапі;

2.3.8. пошук збереженої відеоінформації та відеоданих за календарем та тривожними подіями;

2.3.9. можливість перегляду архіву з декількох відеокамер одночасно;

2.3.10. експорт відеоданих.

2.4. Підсистема засобів передачі відеоінформації **–** сукупність програмно-технічних засобів, що забезпечують передачу відеоінформації з підсистеми засобів відеофіксації до підсистеми засобів обробки відеоінформації та підсистем робочих місць Адміністратора, Розпорядника та Користувачів, та являє собою відокремлений сегмент муніципальної мережі передачі даних та/або ізольований сегмент загальнодоступної мережі передачі даних.

2.5. Підсистема робочих місць Користувачів – сукупність програмно- технічних засобів, що забезпечують суб’єктам використання функціональних можливостей Системи відповідно до Положення, Регламенту та отриманих прав доступу:

2.5.1. можливість виведення на робочих місцях Користувачів зображення з будь-якої відеокамери Системи;

2.5.2. можливість зміни потоку відеоданих відеокамери у вікні зображення на робочому місці (у разі збереження більше ніж одного потоку);

2.5.3. перегляд зображень з відеокамер зі зменшеною та збільшеною швидкістю (до 16-кратної швидкості) на робочих місцях;

2.5.4. можливість конфігурування розкладок відеокамер на робочих місцях та створення шаблонів розкладок;

2.5.5. можливість керування роботизованими відеокамерами.

2.6. Підсистема робочих місць Адміністратора, Розпорядника- сукупність програмно-технічних засобів, що забезпечують працездатність, технічну підтримку та експлуатацію Системи.

2.7. Підсистема колективної роботи з відеозображенням, що створюється та накопичується в Системі – сукупність технічних та програмно – технічних засобів, що забезпечує можливість цілодобового контролю та оперативне реагування на штатні/позаштатні ситуації на території міста.

2.7.1. Можливість керування відображенням інформації на екрані колективної роботи.

2.7.2. Трансляція відеозображення до віддалених робочих місць з можливістю дистанційного конфігурування відображення.

2.8. Підсистема відеоаналітики– сукупність програмних засобів, що на основі відеоданих, отриманих з підсистеми засобів відеофіксації та опрацьованих в підсистемі обробки відеоінформації дозволяють в автоматичному режимі (без участі людини) отримати та виявити ознаки нестандартних подій, що можуть бути віднесені до правопорушень відповідно до норм чинного законодавства. Програмні засоби підсистеми відеоаналітики можуть працювати як разом, так і окремо.

2.8.1. Два основні об’єкти роботи підсистеми відеоаналітики – це події, пов’язані із людьми та транспортними засобами. За функціональними можливостями відеоаналітики можна поділити на два типи:

- відеоаналітика з пошуку подій, пов’язаних з людьми;

- відеоаналітика з пошуку подій, пов’язаних з транспортними засобами.

2.8.2. Відеоаналітика з пошуку подій, пов’язаних з людьми, може забезпечувати виконання наступних функцій:

2.8.2.1. фіксація потрапляння людини в зону, заборонену для людей, на постійній або тимчасовій основі;

2.8.2.2. фіксація масового скупчення людей, поблизу громадських та соціально значимих будівель, транспортної інфраструктури;

2.8.2.3. підрахунок кількості людей, що зайшли в певні будівлі. Аналіз проходження за часовими характеристиками.

2.8.3. Відеоаналітика з пошуку подій, пов’язаних з транспортними засобами, може забезпечувати виконання наступних функцій:

2.8.3.1. Класифікація і розпізнавання транспортних засобів за наступними критеріями:

- державний номер транспортного засобу (у тому числі іноземні);

- тип транспортного засобу (легковий автомобіль, вантажний автомобіль, автобус та ін.);

- колір транспортного засобу;

- інше.

2.8.3.2. Фіксація подій під час руху автомобільного транспорту:

- здійснення обгону в забороненому місці;

- перетин суцільної смуги;

- перетин суцільної подвійної смуги;

- інші.

2.8.3.3. Фіксація блокування транспортним засобом дорожніх ділянок, зупинка та стоянка в забороненому місці.

2.8.3.4. Контроль правильності паркування, підрахунок транспортних засобів в місцях паркування.

2.8.3.5. Фіксація зупинки транспортного засобу в полосі руху або в іншій визначеній зоні.

2.8.3.6. Автоматичне сповіщення Системи при виявленні вантажівки в зоні для легкових автомобілів.

2.8.3.7. Підрахунок кількості (як абсолютної, так і за одиницю часу) транспортних засобів, які перетнули встановлену ділянку:

- проїзд по всій дорозі або полосі руху;

- з’їзд з основної дороги на другорядну.

2.8.3.8. Фіксація знаходження транспортного засобу в пішохідній зоні.

3. Порядок надання доступу до Системи

3.1. Рівні доступу до Системи та їх надання

3.1.1. У Системі передбачено декілька рівнів розмежування доступу для користувачів, а саме:

3.1.1.1. Перегляд інформації в режимі онлайн.

3.1.1.2. Перегляд інформації в режимі відтворення раніше записаного відео.

3.1.1.3. Пошук інформації за критеріями.

3.1.1.4. Експорт відеоінформації в зовнішні формати для подальшого її використання.

3.1.1.5. Інше.

3.1.2. Для кожного з рівнів можуть бути накладені обмеження щодо кількості відеокамер, на які поширюється доступ. Рівень доступу до Системи відеоспостереження визначається розпорядником. Про прийняте рішення запитувач та адміністратор повідомляються письмово.

3.1.3. Обліковий запис Користувача в Системі створюються Адміністратором Системи за допомогою захищених відповідним чином програмно-технічних засобів адміністрування Системи. При створенні облікового запису Користувача системи система створює індивідуальне системне ім’я (логін) та індивідуальний пароль Користувача системи, який має бути змінений самим Користувачем.

3.1.4. Пароль Користувачу в Системі призначається Адміністратором Системи у відповідності до розділу 9 цього Регламенту.

3.2. Блокування доступу Користувача Системи.

3.2.1. При порушенні Користувачем вимог цього Регламенту, Положення, доступ Користувача до Системи блокується Адміністратором Системи до з’ясування причин і усунення недоліків. При цьому посадовій особі користувача, відповідальній за роботу в Системі, направляється електронний лист з повідомленням про факт порушення і відключення Користувача.

3.2.2. Доступ до Системи може бути блокований Адміністратором Системи без попереднього повідомлення Користувача.

3.2.3. Повторне підключення Користувача проводиться після з’ясування причин і усунення недоліків за письмовим клопотанням керівника органу (підприємства, установи, організації) Користувача.

3.2.4. У разі необхідності, при тривалій відсутності Користувача на робочому місці (відпустка, відрядження, хвороба тощо), керівник відповідного органу Користувача, має надати інформацію Адміністратору про необхідність тимчасового блокування доступу до Системи. У разі необхідності надання тимчасового доступу іншому Користувачеві, направити звернення Розпоряднику на тимчасовий доступ іншого Користувача, ознайомленого з цим Регламентом та Положенням (у зверненні додатково зазначається термін, на який має надаватись доступ).

3.2.5. Для запобігання можливості підбору пароля, при введенні неправильного пароля 5 разів, обліковий запис Користувача автоматично блокується.

3.2.6. Розблокування облікового запису здійснюється Системою автоматично не раніше ніж через 15 хвилин.

3.2.7. З метою недопущення доступу сторонніх осіб під паролем Користувача, який тимчасово перервав роботу у Системи, Система автоматично здійснює його тимчасове блокування через 1 хвилину після початку перерви у роботі.

3.3. Припинення доступу.

3.3.1. Доступ Користувача до Системи припиняється на підставі письмового звернення керівника відповідного органу, установи, організації, підприємства комунальної форми власності Розпоряднику Системи із зазначенням облікового запису Користувача, доступ якого до Системи припиняється.

3.3.2. Доступ Користувача до Системи може бути припинений за рішенням Розпорядника, про що Користувач повідомляється письмово заздалегідь.

3.3.3. При припиненні доступу Користувача до Системи його обліковий запис в Системі припиняється, вся інформація, пов’язана з Користувачем в Системі, видаляється.

3.4. Відмова в доступі до Системи.

3.4.1. У доступі до Системи відеоспостереження запитувачу може бути відмовлено в разі немотивованого звернення щодо надання доступу або інформаційного продукту (інформації) з Системи, невідповідності статусу запитувача/користувача нормам Положення та цього Регламенту, відсутності технічної можливості та інше.

3.4.2. Про відмову в доступі запитувач повідомляється письмово.

4. Правила користування Системою

4.1. Загальні правила та вимоги користування Системою.

4.1.1. Для доступу до Системи кожному Користувачеві присвоюються персональний обліковий запис і пароль.

4.1.2. При звільненні Користувача блокується доступ до його облікового запису в Системі.

4.1.3. На вмотивований письмовий запит керівника Користувача на адресу Адміністратора Системи, останнім може бути наданий аналіз дій підпорядкованого запитувачу Користувача, що має доступ до Системи.

4.2. При роботі з Системою Користувач зобов’язаний:

4.2.1. Виконувати вимоги Положення та цього Регламенту, з урахуванням вимог організації парольного захисту.

4.2.2. Використовувати отриману з Системи інформацію відповідно до заявленої мети та виключно у службових цілях.

4.2.3. Самостійно змінювати пароль на доступ до Системи, з дотриманням вимог організації парольного захисту, викладених в розділу 8 цього Регламенту.

4.3. При роботі з Системою Користувачу забороняється:

4.3.1. Поширювати (або розголошувати) власні засоби ідентифікації у Системі іншим особам.

4.3.2. Допускати користування власними засобами ідентифікації у Системі іншими особами.

4.3.3. Здійснювати дії у Системі від чужого імені.

4.3.4. Зберігати пароль у загальнодоступному місці.

4.3.5. Використовувати для аутентифікації чужі облікові дані (ім’я Користувача і пароль) або програми для їх підбору або злому.

4.3.6. Передавати інформацію третій стороні, крім випадків, передбачених законом.

5. Суб’єкти отримання інформації з Системи

та порядок надання доступу до інформації з Системи

5.1. Суб’єкти отримання інформації з Системи.

5.1.1. Запитувачами інформації з Системи, які мають право у встановленому законодавством та Положенням порядку отримувати з Системи інформаційний продукт (інформацію), є юридичні та фізичні особи.

5.1.2. Юридичним особам інформація з Системи може бути надана про об’єкти права власності юридичної особи (при наявності підтвердження права власності) або в інших випадках, передбачених чинним законодавством.

5.1.3. Фізичним особам інформація з Системи може бути надана про об’єкти права власності фізичної особи (при наявності підтвердження права власності) або в інших випадках, передбачених чинним законодавством.

5.2. Порядок звернення за отриманням інформації з Системи.

5.2.1. Для отримання інформації з Системи запитувач надсилає до Розпорядника письмовий запит, форма якого наведена в додатку 2 до цього Регламенту.

5.2.2. Розпорядник Системи у термін до п’яти робочих днів розглядає запит та у разі наявності підстав для надання інформації записує інформацію на електронний носій запитувача та передає її запитувачу разом із супровідним листом, в якому зазначається назва файлу з відеоконтентом, його формат, розмір, час та дата відеозйомки, номер камери та місце її знаходження.

5.2.3. Інформація з камер відеоспостереження, надана на запит від юридичних та фізичних осіб, обліковується Адміністратором та зберігається протягом одного року.

5.2.4. У разі відсутності підстав або технічної можливості для надання інформації з Системи Розпорядник відмовляє запитувачу, про що повідомляє його письмово.

5.3. Адміністратор у жодному випадку не несе відповідальності за використання запитувачем інформаційного продукту з Системи, а також за настання небажаних запитувачу наслідків отримання (використання) інформаційного продукту з Системи, як і за ненастання наслідків, на які розраховував запитувач.

6. Технічна підтримка Системи

6.1. Розпорядник і Адміністратор Системи здійснюють моніторинг працездатності Системи та її компонентів.

6.2. Моніторинг працездатності Системи здійснюється Адміністратором на регулярній основі за допомогою системи автоматичного моніторингу та/або власними силами.

6.3. Система автоматичного моніторингу має передбачати фіксацію зміни стану компонентів Системи (доступність активного мережевого обладнання з відповідних серверів у складі Системи), якість та параметри встановленого мережевого зв’язку та фіксувати їх у вигляді журналів роботи Системи, які мають зберігатись в електронному вигляді не менше одного року.

6.4. У разі виявлення недоліків у роботі Системи Адміністратор оперативно усуває недоліки власними силами або із залученням сторонніх виконавців на договірних засадах.

6.5. Адміністратор зобов’язаний перевірити інформацію про недоступність елементів Системи та, у разі наявності недоліків у роботі Системи, усунути їх.

6.6. Обслуговування Системи здійснює Адміністратор власними силами та залученими силами на договірних засадах. Терміни виконання регламентних робіт визначаються відповідно до технічних вимог до обладнання, що входить до складу Системи.

6.7. Розпорядник Системи на регулярній основі здійснює аналіз роботи Системи та вживає заходів, направлених на її удосконалення, підвищення якості її роботи та розвиток. З цією метою проводить роботи із вдосконалення роботи Системи власними силами або із залученими силами на договірних засадах.

6.8. За необхідності Розпорядник та Адміністратор вносять пропозиції Власнику щодо удосконалення і розвитку Системи та виділення на це відповідного фінансування.

6.9. Користувачі Системи мають право надавати пропозиції щодо удосконалення роботи Системи.

7. Захист інформації в Системі

7.1. Ідентифікація, автентифікація, авторизація.

7.1.1. Ідентифікація в Системі відбувається шляхом введення Користувачем логіна та пароля з метою отримання доступу до Системи.

7.1.2. Автентифікація здійснюється Системою автоматично після введення Користувачем логіна та пароля.

7.1.3. Авторизація здійснюється після проходження Користувачем автентифікації, у результаті чого йому надаються права на виконання регламентованих дій у Системі.

7.2. Захист даних у Системі.

7.2.1. Розпорядник (Адміністратор) Системи забезпечує цілісність інформації в Системі шляхом:

- використання відповідних програмно-апаратних рішень, що забезпечують цілісність даних в Системі;

- визначення рівнів доступу до інформації в Системі Користувачам Системи;

- постійного контролю за працездатністю Системи та своєчасністю її технічного обслуговування;

- контролю за здійсненням фіксації та збереженням в автоматичному режимі всіх дій суб’єктів відносин в Системі щодо роботи з даними в Системі;

- обліку підключених засобів відеофіксації в Системі.

7.2.2. Розпорядник (адміністратор) Системи забезпечує побудову системи технічного захисту інформації та підтримує її в актуальному стані на всіх стадіях життєвого циклу Системи. Передача інформації між Користувачами та сервером Системи здійснюється за допомогою захищених каналів зв’язку із застосуванням шифрування передачі даних.

7.3. Облік дій Користувачів.

7.3.1. Дії Користувача в Системі фіксуються автоматично у відповідних електронних журналах. Для цього в автоматичному режимі зберігається інформація про:

- Користувача інформації в Системі, дату та час входу (виходу) до Системи;

- перегляд ним даних в режимі реального часу або архіву;

- будь-яку передачу (копіювання) ним даних з Системи.

8. Організація парольного захисту Системи

8.1 Загальні вимоги.

8.1.1. Цей Розділ визначає вимоги до складності, терміну дії, використання паролів Користувачів Системи, а також організаційно-технічні заходи для забезпечення процесів генерації, зміни та припинення дії паролів в Системі.

8.1.2. Ці Вимоги є обов’язковими для всіх Користувачів Системи в рамках виконання своїх посадових обов’язків.

8.2. Вимоги, що пред’являються до складності паролів.

8.2.1. В якості пароля повинна вибиратися послідовність символів, що забезпечує малу ймовірність її підбору і вгадування.

8.2.2. Довжина пароля повинна бути не менше 8 символів.

8.2.3. Пароль повинен складатися з символів будь-яких 4-х з наступних груп:

- символів латинського алфавіту або кирилиці в нижньому регістрі (а-z, а-я);

- символів латинського алфавіту або кирилиці у верхньому регістрі (А-Z, А-Я);

- цифр (0-9);

- спеціальних символів і символів пунктуації (~ @ # $% & \* () {} [] - + = \_ \ | / " ‘:;, -).

8.2.4. Забороняється використовувати в якості пароля:

- «порожній» пароль (який не містить жодного символу);

- пароль, що співпадає з ім’ям облікового запису;

- прості паролі типу «123», «111», «ааа» і їм подібні;

- імена і дати народження свої і своїх родичів;

- клички домашніх тварин;

- номери автомобілів, телефонів, табельні номери;

- іншу інформацію, яку можна вгадати, ґрунтуючись на загальновідомій інформації про Користувача.

8.2.5. Не рекомендується використовувати в якості пароля імена власні.

8.3. Вимоги, що пред’являються до введення паролів.

8.3.1. Введення пароля повинен здійснюватися з урахуванням регістру (верхній/нижній) і поточної розкладки (російська, англійська, українська) клавіатури, в яких пароль було поставлено.

8.3.2. Під час введення паролів необхідно виключити можливість його підглядання сторонніми особами (людина за спиною, спостереження людиною за рухом пальців в прямої видимості або відбитому світлі) або технічними засобами (відеокамери, фотоапарати тощо).

8.4. Порядок призначення і зміни паролів Користувача Системи.

8.4.1. Початковий пароль облікового запису призначається Адміністратором Системи під час створення облікового запису Користувача в Системі відповідно до Вимог, що пред’являються до введення паролів. Початковий пароль повідомляється Користувачеві.

8.4.2. Користувач зобов’язаний змінити свій особистий пароль при першому вході в Систему.

8.4.3. Планова зміна особистих паролів всіх Користувачів повинна проводитися не рідше 1 разу на 45 діб, але не частіше 2 разів на добу. Не допускається використання останніх п’яти паролів, використаних з цим обліковим записом раніше. Після закінчення терміну дії пароля підключення Користувача до Системи блокується до зміни пароля.

8.4.4. Позапланова зміна особистого пароля Користувача Системи в разі підозри або відомого факту його компрометації повинна проводитися Користувачем негайно.

8.4.5. У разі регулярного блокування облікового запису через неправильне введення пароля, адміністратор Системи має право вимагати від Користувача письмових пояснень причин, що призводять до блокування облікового запису.

9. Облік та маркування засобів відеофіксації в Системі.

Спосіб інформування про здійснення відеоспостереження

9.1. Облік засобів відеофіксації здійснюється Адміністратором відповідно до правил обліку матеріальних цінностей.

9.2. Маркування засобів відеофіксації , у тому числі тих, що знаходяться у володінні інших осіб, та інтегровані в Систему, здійснюється Адміністратором Системи із використанням програмно-технічних засобів, що дає змогу ідентифікувати відеозаписи відповідно до апаратних засобів, якими вони були зроблені.

10. Підключення до Системи засобів відеофіксації,

що знаходяться у володінні інших осіб

10.1. Технічна інтеграція із Системою засобів відеофіксації, що знаходяться у володінні інших осіб, до Системи здійснюється на підставі відповідної угоди (договору), що укладається між Розпорядником Системи та власником засобів відеофіксації. В угоді зазначається, які саме засоби відеофіксації підключаються, на яких умовах, з якою метою і на який термін, обов’язки і права власника та Розпорядника Системи.

11. Відповідальність

11.1. Користувачі несуть персональну відповідальність за виконання вимог цього Регламенту та Порядку.

11.2. Користувачі несуть персональну відповідальність за власні дії чи їх відсутність у Системі.

11.3. За порушення вимог цього Порядку та Регламенту Користувач несе відповідальність в порядку, передбаченому чинним законодавством.

11.4. Власник, Розпорядник, Адміністратор Системи не несуть відповідальності за шкоду, спричинену Користувачу у зв’язку з використанням Системи та/ або інформаційного продукту з Системи.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Додаток 1

до Регламенту

Звернення

про отримання доступу до комплексної системи

відеоспостереження «Безпечне місто Миколаїв»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_назва підприємства (установи, організації) запитувача, або викладається на бланку підприємства (установи, організації)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_адреса запитувача

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_контактний телефон заявника, адреса електронної пошти тощо

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_мета і підстави для отримання доступу до системи

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_до яких камер відеоспостереження потрібен доступ і в якому режимі (доступ в режимі реальному часу або до архіву)

Повідомляємо про те, що попереджені про неприпустимість використання записів камер системи відеоспостереження не за призначенням, а також неприпустимість їх публічного розповсюдження.

Повідомлені про вимоги положень Законів України «Про інформацію», «Про захист персональних даних» та відповідальність за їх недотримання (порушення).

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 посада підпис ПІП/б

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

дата

Додаток 2

до Регламенту

ЗАПИТ

на отримання доступу до інформаційного продукту (інформації)

з комплексної системи відеоспостереження «Безпечне місто Миколаїв»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_назва підприємства (установи, організації) запитувача

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_адреса запитувача

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_контактний телефон заявника, адреса електронної пошти тощо

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_мета і підстави для отримання інформаційного продукту із Системи, визначені законодавством

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_дата та орієнтовний проміжок часу запитуваних записів

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ адреса (вулиця, перехрестя вулиць) камер відеоспостереження, з яких запитується інформація

Повідомляємо про те, що попереджені про неприпустимість використання записів камер системи відеоспостереження не за призначенням та всупереч означеній вище меті, а також неприпустимість публічного розповсюдження отриманого інформаційного продукту.

Повідомлені про вимоги положень Законів України «Про інформацію», «Про захист персональних даних» та відповідальність за їх недотримання (порушення).

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 посада підпис ПІП/б

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

дата

v-ev-008gk 19.12.2023

Пояснювальна записка

до проєкту рішення виконкому Миколаївської міської ради

«Про затвердження Регламенту використання та функціонування комплексної системи відеоспостереження міста Миколаєва»

1. Суб’єкт подання проєкту: відділ стандартизації та впровадження електронного врядування Миколаївської міської ради в особі начальника відділу Канарського Дмитра Андрійовича.
2. Розробник проекту: головний спеціаліст відділу стандартизації та впровадження електронного врядування Миколаївської міської ради Бондарєва Інеса Миколаївна, тел.: 063 141 80 35.
3. Опис рішення: затвердити Регламент використання та функціонування системи відеоспостереження міста Миколаєва з метою підвищення безпеки громадян, забезпечення оперативного реагування на надзвичайні та аварійні ситуації, відсічі збройної агресії Російської Федерації проти України і забезпечення національної безпеки, усунення загрози небезпеки державної незалежності.
4. Правове обґрунтування: Закон України «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних», «Про інформацію», постанови Кабінету Міністрів України від 29 березня 2006 року № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», рішення Миколаївської міської ради від 23.07.2020 № 57/371 «Про затвердження міської комплексної Програми «Інформатизація та розвиток електронного урядування» на 2020-2022 роки» (із змінами).
5. Необхідність: з метою підвищення безпеки громадян, забезпечення оперативного реагування на надзвичайні та аварійні ситуації, відсічі збройної агресії Російської Федерації проти України і забезпечення національної безпеки, усунення загрози небезпеки державної незалежності України, її територіальної цілісності.

Начальник відділу Дмитро КАНАРСЬКИЙ

Бондарєва т. +380 63 141 80 35