v-ev-001

Про затвердження Регламенту використання та функціонування комплексної системи відеоспостереження «Безпечне місто Миколаїв»

Відповідно до 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-комунікаційних системах», рішення міської ради від 23.07.2020 року № 57/371 «Про затвердження міської комплексної Програми «Інформатизація та розвиток електронного урядування» на 2020-2025 роки» (із змінами), керуючись статтею 59 Закону України «Про місцеве самоврядування в Україні», виконком міської ради

ВИРІШИВ:

1. Затвердити Регламент використання та функціонування комплексної системи відеоспостереження «Безпечне місто Миколаїв» (додається).

2. Рішення виконавчого комітету Миколаївської міської ради від 14.02.2024 № 231 «Про затвердження Регламенту використання та функціонування комплексної системи відеоспостереження міста Миколаєва» визнати таким, що втратило чинність.

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

Міський голова О. СЄНКЕВИЧ

ЗАТВЕРДЖЕНО

рішення виконкому міської ради

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

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

РЕГЛАМЕНТ

використання та функціонування комплексної системи

відеоспостереження «Безпечне місто Миколаїв»

1. Загальні положення

1.1. Регламент використання та функціонування комплексної системи відеоспостереження «Безпечне місто Миколаїв» (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», відповідно до Законів України «Про місцеве самоврядування в Україні», «Про інформацію», «Про електронні комунікації», «Про захист інформації в інформаційно-комунікаційних 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, електронних комунікаційних та інформаційно-комунікаційних системах», рішення Миколаївської міської ради від 23.07.2020 № 57/371 «Про затвердження міської комплексної Програми «Інформатизація та розвиток електронного урядування» на 2020-2025 роки» (із змінами), інших нормативно-правових актів, з метою визначення складу та порядку функціонування комплексної системи відеоспостереження «Безпечне місто Миколаїв» (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 електронні комунікації», «Про захист персональних даних», «Про захист інформації в інформаційно-комунікаційних 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 можна 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 смузі 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 смузі руху;

- з’їзд з головної дороги на другорядну.

2.8.3.8. Фіксація знаходження транспортного засобу в пішохідній зоні.

3. Порядок надання, блокування, припинення доступу до Системи

3.1. Доступ до Системи надається розпорядником на підставі заявки про отримання доступу до комплексної системи відеоспостереження «Безпечне місто  Миколаїв» (далі – заявка) за формою, наведеною у додатку 1. У разі погодження заявки, розпорядник Системи протягом доби направляє її адміністратору Системи для здійснення останнім фактичного підключення користувача до Системи.

3.2. Рівні доступу до Системи та порядок їх надання.

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

3.2.1.1. мінімальний 1 (передбачає доступ до онлайн-трансляції зображення з підсистеми засобів відеофіксації);

3.2.1.2. мінімальний 2 (передбачає доступ до онлайн-трансляції зображення з підсистеми засобів відеофіксації, відтворення раніше записаного відео, окремих функцій підсистеми відеоаналітики, в частині пошуку подій, пов’язаних з людьми, транспортними засобами) (детальний перелік функцій відеоаналітики, до яких надається доступ, наведено в додатку 1);

3.2.1.3. загальний (передбачає доступ до онлайн-трансляції зображення з підсистеми засобів відеофіксації, відтворення раніше записаного відео, окремих функцій підсистеми відеоаналітики, в частині пошуку подій, пов’язаних з людьми, всіх функцій підсистеми відеоаналітики, що стосується транспортних засобів, без права обробки інформації в Системі) (під обробкою інформації в Системі слід розуміти дії користувача, спрямовані на створення окремих відрізків із загального відеопотоку (відеофайлів), їх завантаження та/або експорт на зовнішні носії);

3.2.1.4. розширений (передбачає доступ до онлайн-трансляції зображення з підсистеми засобів відеофіксації, відтворення раніше записаного відео; всіх функцій підсистеми відеоаналітики, можливість обробки (створення, завантаження, експорт) інформації в Системі.

3.2.2. Для кожного з рівнів можуть бути накладені обмеження щодо кількості та переліку відеокамер, на які поширюється доступ. Рівень доступу до Системи відеоспостереження визначається розпорядником на підставі заявки (додаток 1).

3.2.3. Порядок отримання доступу до Системи уповноваженими особами підприємств, установ або організацій, а також порядок оформлення відповідних заявок може бути регламентований внутрішніми розпорядчими документами таких суб’єктів, що не суперечать положенням цього Регламенту. Для забезпечення належної організації доступу до Системи, копії таких документів надаються розпоряднику Системи.

3.2.4. Для доступу до Системи кожному користувачеві присвоюються персональний обліковий запис і пароль.

3.2.5. Обліковий запис користувача в Системі створюється адміністратором Системи за допомогою захищених відповідним чином програмно-технічних засобів адміністрування Системи. При створенні облікового запису користувача, система створює індивідуальне системне ім’я (логін) та індивідуальний пароль користувача Системи, який має бути змінений самим користувачем після здійснення першого входу до Системи.

3.2.6. Пароль користувачу в Системі призначається адміністратором Системи у відповідності до розділу 9 цього Регламенту.

3.3. Блокування доступу користувача до Системи.

3.3.1. При порушенні користувачем вимог цього Регламенту, Положення, доступ користувача до Системи блокується адміністратором Системи до з’ясування причин і усунення недоліків. При цьому на адреси електронної пошти користувача Системи та органу (підприємства, установи, організації) або уповноваженого підрозділу органу (підприємства, установи, організації), які вказані в заявці, невідкладно направляється лист з повідомленням про факт порушення і блокування користувача.

3.3.2. Доступ до Системи може бути блокований адміністратором Системи без попереднього повідомлення користувача.

3.3.3. Повторне підключення користувача проводиться після з’ясування причин і усунення недоліків на підставі листа (в довільній формі), за підписом керівника органу (підприємства, установи, організації) користувача або керівника уповноваженого підрозділу органу (підприємства, установи, організації).

3.3.4. У разі необхідності, при тривалій відсутності користувача на робочому місці (відпустка, відрядження, хвороба тощо), на підставі листа (в якому зазначається період блокування доступу користувача) за підписом керівника органу (підприємства, установи, організації) або керівника уповноваженого підрозділу органу (підприємства, установи, організації) адміністратор проводить тимчасове блокування доступу користувачу до Системи. Повторне підключення користувача проводиться відповідно до пункту 3.3.3. Регламенту.

У разі необхідності надання тимчасового доступу іншому користувачеві, необхідно направити заявку (додаток 1)розпоряднику на тимчасовий доступ іншого користувача, ознайомленого з цим Регламентом та Положенням (у заявці обов’язково зазначається термін, на який має надаватись доступ).

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

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

3.4. Припинення доступу.

3.4.1. Доступ користувача до Системи припиняється на підставі листа (в довільній формі) за підписом керівника органу (підприємства, установи, організації) до розпорядника Системи із зазначенням облікового запису користувача, доступ якого до Системи необхідно припинити.

3.4.2. При звільненні користувача з роботи на підприємстві, установі, організації, невідкладно, але не пізніше 2 календарних днів, за підписом керівника відповідного підприємства, установи, організації до розпорядника Системи направляється лист про необхідність блокування доступу користувача до його облікового запису в Системі та припинення доступу до Системи.

При отриманні такого листа розпорядник Системи протягом доби направляє його адміністратору Системи для блокування та припинення доступу користувача в Системі.

3.4.3. Доступ користувача до Системи може бути припинений за рішенням розпорядника, про що користувач повідомляється письмово заздалегідь.

3.4.4. При припиненні доступу користувача до Системи його обліковий запис в Системі припиняється, вся інформація, пов’язана з користувачем в Системі, зберігається не менше 120 діб, після чого повинна бути видалена адміністратором Системи.

3.5. Відмова у доступі.

3.5.1. У доступі до Системи посадовій (службовій) особі (користувачу) може бути відмовлено в разі недотримання вимог Регламенту, в частині заповнення та направлення розпоряднику Системи заявки, згідно з додатком 1**,** невідповідності статусу посадової (службової) особи (користувача) нормам Положення, Регламенту, відсутності технічної можливості та інше.

3.5.2. У разі прийняття рішення про відмову у доступі до Системи, розпорядник протягом 1 доби направляє службовий лист керівнику відповідного органу (підприємства, установи, організації), яким ініційовано надання доступу посадовій (службовій) особі (користувачу) з мотивованою відмовою у такому доступі та обґрунтуванням підстав для прийняття вказаного рішення.

4. Правила користування Системою

4.1. При роботі з Системою користувач зобов’язаний:

4.1.1. виконувати вимоги Положення та цього Регламенту, з урахуванням вимог організації парольного захисту;

4.1.2. використовувати отриману з Системи інформацію відповідно до заявленої мети та виключно у службових цілях;

4.1.3. самостійно змінювати пароль на доступ до Системи, з дотриманням вимог організації парольного захисту, викладених в розділі 9 цього Регламенту.

4.2. При роботі з Системою користувачу забороняється:

4.2.1. поширювати (або розголошувати) власні засоби ідентифікації у Системі іншим особам;

4.2.2. допускати користування власними засобами ідентифікації у Системі іншими особами;

4.2.3. здійснювати дії у Системі від чужого імені;

4.2.4. зберігати пароль у загальнодоступному місці;

4.2.5. використовувати для автентифікації чужі облікові дані (ім’я користувача і пароль) або програми для їх підбору або злому;

4.2.6. передавати інформацію третій стороні, крім випадків, передбачених законом.

4.3. На письмовий запит керівника органу (підприємства, установи, організації) користувача на адресу адміністратора Системи, останнім може бути наданий аналіз дій підпорядкованого запитувачу користувача, що має доступ до Системи, або користувача, доступ до Системи якого припинено.

5. Суб’єкти та порядок отримання 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 або користувача з розширеним рівнем доступу (за умови, що користувач та запитувач інформації є посадовими особами однієї організації, установи, підприємства), запит про отримання інформації з комплексної системи відеоспостереження «Безпечне місто Миколаїв» (далі – запит), форма якого наведена в додатку 2.

5.2.2. Розпорядник Системи (у визначених випадках – користувач з розширеним рівнем доступу) у термін до 5 робочих днів розглядає запит та у разі наявності підстав надає інформацію запитувачу.

5.2.3. Інформація з камер відеоспостереження, надана адміністратором Системи на запит, обліковується та зберігається протягом 1 року.

5.2.4. Порядок обліку та зберігання даних, сформованих і наданих користувачем з розширеним рівнем доступу на виконання запиту, може бути регламентований внутрішніми розпорядчими документами підприємства, установи або організації.

5.2.5. У разі відсутності підстав або технічної можливості для надання інформації з Системи розпорядник Системи (у визначених випадках – користувач з розширеним рівнем доступу) відмовляє запитувачу, про що повідомляє його письмово.

5.3. Розпорядник, адміністратор (у визначених випадках – користувач з розширеним рівнем доступу) 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 заходи, направлені 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. Адміністратор Системи забезпечує побудову комплексної системи захисту інформації (відповідно до розділу 8 Регламенту) 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. Експлуатація Системи з наданням доступу віддаленим користувачам до побудови комплексної системи захисту інформації забороняється.

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. Створення комплексної системи захисту інформації

8.1. Загальні положення.

Створення комплексної системи захисту інформації (КСЗІ) необхідне для забезпечення захисту інформації, що обробляється в інформаційних системах. Це дозволить уникнути її втрати, пошкодження чи несанкціонованого доступу. При створенні КСЗІ Адміністратор Системи спирається на вимоги чинних нормативно-правових актів України.

8.2. Основні етапи створення КСЗІ.

Створення КСЗІ передбачає кілька важливих кроків:

8.2.1. Підготовчий етап:

- аналіз інформаційної системи, визначення її структури та типів інформації, які потребують захисту.

- формування переліку необхідних засобів та процедур захисту інформації.

8.2.2. Проєктування:

- розробка технічного завдання, яке чітко описує, як саме створюватиметься і працюватиме КСЗІ;

- створення проєктної документації, що описує деталі реалізації системи захисту.

8.2.3. Впровадження і тестування:

- реалізація спроєктованих рішень;

- встановлення і налаштування програмного забезпечення та обладнання;

- перевірка роботи системи, усунення помилок та недоліків.

8.2.4. Оцінка і введення в експлуатацію:

- проведення незалежної експертизи та отримання відповідних сертифікатів відповідності.

- запуск системи у повноцінну роботу.

8.3. Документація.

У процесі створення КСЗІ обов’язково готується така документація:

- технічне завдання;

- проєктна документація;

- інструкції з експлуатації;

- організаційні документи, що регламентують використання КСЗІ.

8.4. Вимоги до безпеки та організаційні заходи.

Система має гарантувати:

- контроль доступу та ідентифікацію користувачів;

- захист від комп’ютерних вірусів і кібератак;

- реєстрацію всіх важливих подій.

9. Організація парольного захисту Системи

9.1. Загальні вимоги.

9.1.1. 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.

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

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

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

9.2.2. Довжина пароля повинна бути не менше 8 символів.

9.2.3. 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 (~ @ # $% & \* () {} [] - + = \_ \ | / « ‘:;, -).

9.2.4. 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.

9.2.5. Не рекомендується використовувати в якості пароля імена власні.

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

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

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

9.4. Порядок призначення і зміни паролів користувача Системи.

9.4.1. 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.

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

9.4.3. 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.

9.4.4. Позапланова зміна особистого пароля користувача Системи в разі підозри або відомого факту його компрометації повинна проводитися користувачем негайно.

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

10. Облік та маркування засобів відеофіксації в Системі.

Спосіб інформування про здійснення відеоспостереження

10.1. Облік засобів відеофіксації здійснюється адміністратором відповідно до правил обліку матеріальних цінностей.

10.2. 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.

10.3. Інформування про здійснення відеоспостереження здійснюється відповідно до вимог Закону Уураїни «Про захист персональних даних».

11. Підключення до Системи засобів відеофіксації,

що знаходяться у володінні інших осіб

11.1. Технічна інтеграція із Системою засобів відеофіксації, що знаходяться у володінні інших осіб, здійснюється на підставі відповідної угоди, договору, меморандуму, що укладається між розпорядником Системи та власником засобів відеофіксації. В угоді, договорі, меморандумі зазначається, які саме засоби відеофіксації підключаються, на яких умовах, з якою метою і на який термін, обов’язки і права власника та розпорядника Системи.

11.2. Порядок надання, припинення, блокування, доступу до Системи власників засобів відеофіксації, зазначених в пункті 11.1 цього розділу, здійснюється на умовах, визначених в укладених між розпорядником Системи та власником засобів відеофіксації угодах, договорах, меморандумах, з урахуванням положень цього Регламенту.

12. Відповідальність

12.1. Користувачі несуть персональну відповідальність за виконання вимог цього Регламенту.

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

12.3. За порушення вимог цього Регламенту користувач несе відповідальність в порядку, передбаченому чинним законодавством.

12.4. 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

ЗАЯВКА

про отримання доступу до комплексної системи відеоспостереження

«Безпечне місто Миколаїв»

Прошу надати працівникові \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

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

(назва підприємства (установи, організації); код ЄДРПОУ)

доступ до комплексної системи відеоспостереження «Безпечне місто Миколаїв».

|  |  |
| --- | --- |
| ПІП/б працівника (або присвоєний порядковий номер) |  |
| Назва посади працівника, підрозділ\* |  |
| Адреса підприємства (установи, організації) |  |
| Контактний номер телефону працівника |  |
| Адреса електронної пошти працівника |  |
| Контактний номер телефону органу (підприємства, установи, організації) або його уповноваженого підрозділу |  |
| Адреса електронної пошти органу (підприємства, установи, організації) або його уповноваженого підрозділу (для повідомлення про блокування користувача у разі порушення вимог Регламенту, Положення) |  |
| ПІП/б відповідальної особи уповноваженого підрозділу за зберігання персональних даних користувача |  |
| Правові підстави для отримання доступу до інформації в Системі |  |
| Мета отримання доступу до Системи |  |
| Період надання доступу | Постійний – Тимчасовий –  з \_\_\_.\_\_\_.20\_\_ по \_\_\_.\_\_\_.20\_\_ |
| Об’єкти відеоспостереження, визначені в Положенні про КСВ «Безпечне місто Миколаїв» |  |
| Територіальна приналежність | місто – район у місті – \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  інше – \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Рівень доступу | Перелік повноважень в Системі |
| Мінімальний 1 – | Доступ до функцій відеоспостереження: |
| Перегляд онлайн-трансляції зображення з підсистеми засобів відеофіксації |
| Доступ до функцій відеоаналітики не надано |
| Мінімальний 2 – | Доступ до функцій відеоспостереження: |
| Перегляд онлайн-трансляції зображення з підсистеми засобів відеофіксації |
| Перегляд відеозаписів в режимі відтворення раніше записаного відео (пошук збереженої інформації по подіях) |
| Доступ до функцій відеоаналітики: |
| Пошук подій, пов’язаних з людьми (підрахунок кількості людей на об’єкті відеоспостереження, в т.ч. за певний проміжок часу) |
| Пошук подій, пов’язаних з транспортними засобами в обсязі:  - перегляд фіксацій подій під час руху автомобільного транспорту;  - перегляд фіксацій блокування транспортним засобом дорожніх ділянок, зупинки та стоянки в забороненому місці;  - контроль правильності паркування, підрахунок транспортних засобів в місцях паркування;  - перегляд фіксацій зупинки транспортного засобу в смузі руху або в іншій визначеній зоні;  - отримання автоматичного сповіщення Системи при виявленні вантажівки в зоні для легкових автомобілів;  - підрахунок кількості (як абсолютної, так і за одиницю часу) транспортних засобів, які перетнули встановлену ділянку (проїзд по всій дорозі або смузі руху; з’їзд з основної дороги на другорядну);  - перегляд фіксацій знаходження транспортного засобу в пішохідній зоні |
| Загальний – | Доступ до функцій відеоспостереження: |
| Перегляд онлайн-трансляції зображення з підсистеми засобів відеофіксації |
| Перегляд відеозаписів в режимі відтворення раніше записаного відео (пошук збереженої інформації за календарем та подіями) |
| Доступ до функцій відеоаналітики: |
| Пошук подій, пов’язаних з людьми |
| Пошук подій, пов’язаних з транспортними засобами |
| Розширений – | Доступ до функцій відеоспостереження: |
| Перегляд онлайн-трансляції зображення з підсистеми засобів відеофіксації |
| Перегляд відеозаписів в режимі відтворення раніше записаного відео (пошук збереженої інформації за календарем та подіями) |
| Доступ до функцій відеоаналітики: |
| Пошук подій, пов’язаних з людьми |
| Пошук подій, пов’язаних з транспортними засобами |
| Інформування щодо подій, пов’язаних з людьми або транспортними засобами |
| Обробка інформації в Системі – створення, завантаження, експорт інформації (відеозаписів, файлів у форматі csv, pdf, xls тощо) на зовнішні носії, у випадках, передбачених Регламентом) |

З вимогами положень Законів України «Про інформацію», «Про захист персональних даних», Положенням про КСВ «Безпечне місто Миколаїв» та Регламентом використання та функціонування КСВ «Безпечне місто Миколаїв» (зі змінами), ознайомлений

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

(дата) (підпис працівника) (власне ім’я, прізвище)

Надаю згоду на обробку вказаних у даній заявці моїх персональних даних, у зв’язку з наданням доступу до КСВ «Безпечне місто Миколаїв».

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

(дата) (підпис працівника) (власне ім’я, прізвище)

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

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

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

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

(посада керівника підприємства, (підпис) (власне ім’я, прізвище)

установи, організації)

\*поле не обов’язкове для заповнення працівниками державних органів, які виконують правоохоронні функції

Додаток 2

до Регламенту

ЗАПИТ

про отримання інформації з комплексної системи

відеоспостереження «Безпечне місто Миколаїв»

1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(найменування підприємства (установи, організації) запитувача, код ЄДРПОУ,

або викладається на бланку підприємства (установи, організації);

прізвище, ім’я та по батькові і реквізити документа, що посвідчує фізичну особу,

яка подає запит (для фізичної особи).

2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(адреса запитувача)

3. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(контактний номер телефону запитувача, адреса електронної пошти)

4. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(мета та правові підстави для запиту)

5.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(опис відомостей, які необхідно отримати, із зазначенням дати, періоду часу,

адреси, об’єктів)

Додатки:

Згоду на обробку персональних даних, у зв’язку з виконанням запиту, надано \_\_\_\_\_\_\_\_\_\_\_\_\_\_

(підпис)

З вимогами положень Законів України «Про інформацію», «Про захист персональних даних» та відповідальність за їх недотримання (порушення) ознайомлений (-а).

Про неприпустимість використання записів з камер системи відеоспостереження не за призначенням, а також неприпустимість їх публічного розповсюдження, попереджений (-а).

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

(посада керівника підприємства, (підпис) (власне ім’я, прізвище)

установи, організації)

\_\_\_\_\_.\_\_\_\_\_.20\_\_\_\_

(для юридичної особи)

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

(підпис) (власне ім’я, прізвище)

\_\_\_\_\_.\_\_\_\_\_.20\_\_\_\_

(для фізичної особи)