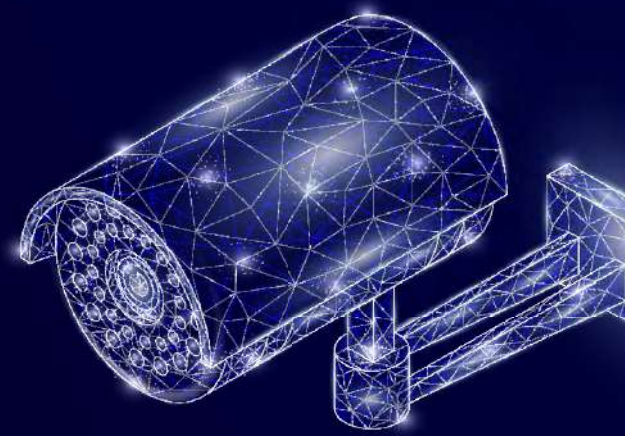
ПОСІБНИК ДЛЯ ОРГАНІВ МІСЦЕВОГО САМОВРЯДУВАННЯ



ВІДЕОСПОСТЕРЕЖЕННЯ У ПУБЛІЧНИХ МІСЦЯХ:

ОСНОВИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Асоціація УМДПЛ UMDPL Association

МІЖНАРОДНИЙ ФОНД ВІДРОДЖЕННЯ

Відеоспостереження у публічних місцях:

основи захисту персональних даних

Посібник для органів місцевого самоврядування

Асоціація УМДПЛ UMDPL Association

Відеоспостереження у публічних місцях: основи захисту персональних даних (посібник для органів місцевого самоврядування)/ В.К. Батчаєв, У.С. Шадська. — К.. Компринт, 2021. —98 с.

Авторський колектив:

Уляна Шадська
Володимир Батчаєв

Дизайн та верстка:

Іван Юрчик

Цей посібник надає можливість посадовим особам органів місцевого самоврядування та підпорядкованих їм установ ознайомитися з ключовими заходами захисту персональних даних, під час їх обробки за допомогою систем відеоспостереження.

Викладені рекомендації базуються на положеннях національного та міжнародного законодавства, що робить цей методичний матеріал актуальним для інших суб'єктів, які використовують подібні системи.

МІЖНАРОДНИЙ ФОНД ВІДРОДЖЕННЯ

Посібник підготовлено за підтримки Міжнародного фонду "Відродження" у межах проєкту «Захист персональних даних в системах відеоспостереження за дотриманням публічного порядку, якими користуються органи місцевого самоврядування». Матеріал відображає позицію авторів і не обов'язково збігається з позицією Міжнародного Фонду «Відродження».

ЗМІСТ

ПЕРЕДМОВА

Ми звикли до того, що камери спостереження стають частиною інфраструктури наших міст, будинків, підприємств. Їх встановлення стає універсальною рекомендацією для всіх, хто хоче посилити захищеність об'єктів та підвищити відчуття безпеки людей. Кількість квадратних метрів публічного простору у населених пунктах, що перебуває поза відеоспостереженням, постійно зменшується. Чи зростає з такою ж динамікою відчуття захищеності?

Таку залежність складно побачити за допомогою доступних соціологічних досліджень. Водночас, складно заперечити той факт, що при розслідуванні багатьох категорій злочинів дані мобільних операторів та інформація з камер спостереження є важливим, а часто основним джерелом первинної інформації для органів досудового розслідування.

За таких обставин, а також враховуючи все більшу технологічну доступність, можна очікувати подальшого розширення застосування відеоспостереження. Проте, чи не варто подивитися на «інший бік медалі» — ризики масового поширення цієї практики без належних гарантій дотримання прав людини?

Право на приватність (повага до приватного та сімейного життя) напряму пов'язано із визначальною цінністю всієї концепції прав людини — людською гідністю. Це право, що належить кожному, передбачає, що людина сама вправі визначати межі допустимого втручання в своє приватне і сімейне життя. Звісно, ширше застосування технологій збору та обробки даних, поєднання інформації з різних джерел без обмежень, — нівелює це право. Неможливо зупинити технологічний прогрес, неможливо відмовитися від переваг, які несуть інформаційні технології. Проте, можна передбачити запобіжники, що дозволить залишити той обсяг приватності, що збереже у кожного відчуття справедливості, захищеності і гідності.

Якщо кінець 18 та 19 століття стали епохою індустріалізації і саме цей процес визначив розвиток країн на наступне століття, то наша епоха має таке саме значення для майбутнього, але джерелом розмежування виступає цифровізація. Окрім технічної інфраструктури, напрям розвитку буде залежати від того, яке місце у її впровадженні будуть займати права людини. Повага до прав людини означає, що треба врахувати застереження, передбачити обмеження застосування технологій, розмежувати публічне та приватне, залишити простір, в якому людина може реалізувати основний зміст права на приватність — «бути залишеною у спокої». Як же цього досягнути?

Асоціації органів місцевого самоврядування, Міністерство розвитку громад та територій України і, звичайно, Міністерство внутрішніх справ мали би разом подбати про належне методичне забезпечення органів місцевого самоврядування рекомендаціями, правилами та політиками застосування систем відеоспостереження для підтримки безпеки у місцевих громадах.

Нажаль, цього поки не сталося, і організації громадянського суспільства почали пропонувати свої ідеї визначення необхідних умов для балансування переваг і ризиків застосування цих технологій. Сподіваюся, ця збірка рекомендацій, підготовлена Асоціацією українських моніторів дотримання прав людини в діяльності правоохоронних органів за підтримки Міжнародного Фонду «Відродження», стане в нагоді всім, хто намагається знайти рішення для своїх громад. А також, додатково стимулюватиме державні структури до розробки необхідних політик, затребуваність яких буде лише зростати.

Роман Романов

Директор програми «Права людини і правосуддя»
Міжнародного Фонду «Відродження»

Розділ 1.

Системи відеоспостереження: функціональні можливості та використання

1.1. Системи відеоспостереження: функціональні можливості та призначення

Системи відеоспостереження поступово стають звичним атрибутом сучасної України. Електронні пристрої здійснюють відеофіксацію за тим, що відбувається на стадіонах, спортивних майданчиках, вулицях, парках, транспортних магістралях, в аеропортах та вокзалах. Інформаційні технології застосовують з метою охорони громадського порядку, контролю безпеки дорожнього руху, захисту власності тощо.

Якщо раніше системи відеоконтролю переважно впроваджувалися у великих містах, то сьогодні такі технології набули популярності й у малих громадах. Камери встановлюють органи державної влади, місцевого самоврядування та приватні особи.

За своїм функціональним призначенням і способом обробки інформації системи відеоспостереження поділяють на такі різновиди:

1. **Системи, що забезпечують візуальний контроль у режимі реального часу.**

   Така функціональна можливість є практично в усіх комплексах міських систем. З огляду на практику інших країн світу, можна припустити, що вона є доцільною лише за наявності достатньої кількості операторів, які постійно відстежуватимуть зображення на моніторах («відеостінах»), що транслюють отриману з відеокамер інформацію у реальному часі.

   Але з цього приводу є дискусії. Деякі фахівці, зокрема представники органів місцевого самоврядування, вважають такий підхід нераціональним і малоефективним, оскільки люди можуть помилятися щодо правильного реагування на отримані відеодані. Оператор, через стомленість або неуважність, може просто не помітити значимої інформації або

невірно проаналізувати її, і в результаті — прийняти помилкове рішення. Також серед аргументів є те, що цілодобове функціонування системи потребує витрат іншого роду — оплата праці кількох змін операторів та проведення комплексу робіт по створенню для них належних умов праці.

2. **Системи з можливістю збереження отриманої з відеокамер інформації.**

   Вказані системи дозволяють не тільки спостерігати за подіями у певному місці, а й накопичувати та зберігати отримане відео протягом необхідного часу. Переваги цього методу роботи у тому, що відеофайлами можна управляти: переглядати, редагувати, збільшувати зображення, робити уривки відео тощо.

   У таких функціональних можливостях, передусім, зацікавлені органи правопорядку, адже збережені відеозаписи можна використовувати під час здійснення оперативно-розшукової діяльності, досудового слідства або у якості доказів при притягненні правопорушників до відповідальності. Разом із тим, місцева влада часто використовує таку інформацію, наприклад, при вирішенні питань, пов'язаних із містобудуванням, розвитком інфраструктури, оптимізацією транспортних потоків, роботою комунальних служб тощо. Системи такого типу також застосовуються на підприємствах, установах та організаціях інших форм власності для охорони території та майна або контролю за дотримання режиму роботи, використанням робочого часу тощо.

3. **Системи із застосуванням можливостей «штучного інтелекту».**

   Ці системи відеоспостереження здатні не лише записувати всі події у секторі спостереження, а й відокремлювати інформацію із загального відеопотоку, аналізувати та структурувати її за визначеними у програмі критеріями. Наприклад,

такі системи використовуються для автоматичного розпізнавання транспортних засобів за державними номерними знаками. Разом із тим, при сучасному програмному та апаратному оснащенні, вони здатні вирішувати завдання більш широкого діапазону — розпізнавати обличчя для подальшої безконтактної ідентифікації особи, встановлювати наявність у зоні контролю певних предметів та речей (наприклад, об'єктом пошуку і відеофіксації може бути особа з великогабаритною сумкою), реагувати на параметри руху чи щільність транспортного потоку, фіксувати перетин віртуальних ліній, здійснювати підрахунок людей та інше.

Так, однією з функцій системи відеоспостереження може бути інформування про скупчення людей, якщо їх кількість у зоні контролю перевищує задане програмою порогове значення. Це дозволяє оперативно встановлювати місця спонтанного виникнення натовпу (масові заворушення чи бійки, стихійні зібрання, наслідки аварії тощо) та своєчасно реагувати на подію в залежності від ситуації. Або є система «Гарпун»,[1] яка за допомогою відеокамер збирає та обробляє інформацію про номерні знаки транспортних засобів, що розшукуються у рамках кримінальних чи виконавчих проваджень, зокрема, у справах про адміністративні правопорушення, а також за ухвалою суду.

[1] «Гарпун» — інформаційна підсистема інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України», призначена для обробки відомостей про транспортні засоби усіх типів та номерні знаки ТЗ, що розшукуються.

1.2. Питання правового врегулювання встановлення систем відеоспостереження

Питання щодо застосування систем відеоспостереження доцільно розглянути у широкому контексті, зокрема, як реагує суспільство у різних куточках світу на розвиток подібних технологій. Адже іноземний досвід також буде впливати на сприйняття розвитку інтелектуальної системи контролю й в Україні.

Якщо подивитися на реакцію щодо переваг та ризиків від використання розумних систем відеофіксації, то суспільство часто демонструє невдоволення контролем за своїми діями і чинить опір цьому. Наприклад, під час протестів у Гонконгу влітку 2019 року, у місті Коулун Бей, демонстранти знесли стовпи з камерами для розпізнавання обличчя. Організатори акцій заявили, що за допомогою цих пристроїв влада збирає дані про активістів та передає їх до правоохоронних служб Китаю для подальшого переслідування. Це одна із причин, чому у мережі інтернет розпочали поширювати рекомендації як унеможливити автоматичну ідентифікацію обличчя — від застосування макіяжу до спеціальних окулярів.

Під тиском суспільної думки, влада у різних країнах була вимушена вдаватись до обмежень, а іноді й до заборони розміщення інтелектуальних мереж відеоспостереження. Так, Європейський Союз розглядає можливість заборони використання технології розпізнавання обличчя у громадських місцях на строк до п'яти років, з метою запобігання зловживанням у цій сфері. «*План ЄС, викладений у 18-сторінковій доповіді, вийшов на тлі глобальної дискусії щодо систем, які керуються штучним інтелектом і широко використовуються правоохоронними органами. Комісія ЄС заявила, що, можливо, доведеться запровадити нові жорсткі правила для зміцнення захисту конфіденційності людини*».[2]

[2] «EU mulls five-year ban on facial recognition tech in public areas», Reuters

В травні 2019 року, у Сан-Франциско (Каліфорнія, США), поліції та іншим муніципальним службам взагалі заборонили використовувати системи відеоспостереження з функцією розпізнавання облич (за винятком камер в аеропортах, на вокзалах і автостанціях) — місцева влада вирішила, що такі технології порушують право мешканців на приватність. Надалі таку ж заборону запровадили в Окленді (Каліфорнія) та Сомервілі (Массачусетс).

Разом із тим, Великобританія, країна з давніми традиціями поваги до приватного життя, має одну з найпотужніших мереж відеонагляду у світі — відповідно до даних «Brookings Institution», лише у Лондоні та його передмістях нараховується 420000 відеокамер. Згідно з дослідженням Британської асоціації індустрії безпеки (BSIA), на кожні 11 осіб, які проживають в країні, встановлено по одній відеокамері спостереження. А у американському місті Бостоні, саме за допомогою систем відеоспостереження викрили виконавців гучного теракту — вибухів під час проведення марафону.

Ці приклади демонструють, що у світі, як і в Україні, триває дискусія щодо доцільного, законного та справедливого підходу використання систем відеоспостереження. З одного боку, протидія злочинності та охорона громадської безпеки за допомогою технічних засобів, може призводити до обмежень права людини на приватність в інтересах усього суспільства в цілому. З іншого — такі обмеження нерідко переростають у грубі порушення цього права, якщо відсутні норми щодо підстав, умов та порядку здійснення відеонагляду, а також механізмів контролю за їх дотриманням.

На міжнародному рівні є вироблені стандарти, які декларують загальні принципи щодо порядку обробки та захисту інформації, отриманої за допомогою технологій. Це означає, що кожна країна повинна самостійно прийняти законодавство, яке регулюватиме цю сферу, та забезпечити баланс інтересів: як окремої особи — у недоторканності приватного життя, так і держави — у створенні належного рівня національної безпеки та добробуту суспільства.

В Україні апаратні комплекси систем відеоспостереження переважно перебувають на балансі органів місцевого самоврядування та підпорядкованих їм комунальних підприємств. Але проблема полягає у тому, що на сьогодні у місцевої влади немає правових підстав встановлювати технічні засоби відеонагляду, не кажучи вже про доступ до баз даних інших органів, наприклад, для впровадження функції розпізнавання обличчя. Муніципальні органи намагаються обґрунтувати правомірність використання таких систем, посилаючись на статтю 38 Закону України «Про місцеве самоврядування в Україні». Проте, незважаючи на її гучну назву — «Повноваження щодо забезпечення законності, правопорядку, охорони прав, свобод і законних інтересів громадян», стаття не містить жодного положення, яке б надавало право місцевій владі використовувати технології для нагляду за життям громади. Також, серед доводів є те, що оскільки вони є представницьким органом громади, то встановлюючи системи, мешканці приймають рішення та інвестують у свою безпеку. У певній мірі це виправдано, враховуючи те, що велика кількість населених пунктів не забезпечена достатньою кількістю правоохоронних служб і жителі громад, дійсно, стають ініціаторами рішення про впровадження відеоконтролю.

Окрім проблем правового регулювання, вже декілька років тривають дискусії навколо питання щодо власності та доступу до систем. По-перше, у кожному регіоні місцева влада самостійно ухвалює рішення щодо обробки відеопотоків, використовуючи пристрої з різним програмним забезпеченням та технічними характеристиками. Таке різноманіття в обладнанні суттєво ускладнює спроби інтегрувати муніципальні відеосистеми в мережу інформаційних систем, які використовує Національна поліція.

По-друге, доступ правоохоронців до обробки відеозаписів, у більшості випадків, не можливий без попереднього отримання дозволу від власника систем — органів місцевого самоврядування, які не мають єдиного підходу щодо надання правоохоронцям можливості користуватися масивом інформації. У деяких громадах порядок доступу поліцейських до відеоданих встановлюється

актами органів місцевого самоврядування, в інших — взагалі не регламентується й залежить від усталеної практики взаємин місцевих чиновників з правоохоронцями.

Слід зауважити, що в отриманні інформації з систем відеоспостереження часто зацікавлені не тільки правоохоронці, а й ЗМІ, громадські активісти, страхові компанії тощо. Проте, на сьогодні в органах місцевого самоврядування відсутній єдиний алгоритм обміну такою інформацією з третіми особами. В одних містах їх запити на отримання відеозаписів переадресовують для прийняття рішення в поліцію, в інших — надають інформацію без обґрунтованих підстав. Непоодинокими є й факти оприлюднення на вебсайтах або сторінках соціальних мереж муніципальних органів відеозаписів дорожньо-транспортних пригод, випадків отримання громадянами травм, вчинення правопорушень та інших матеріалів, які, на думку публікаторів, викликають у глядача підвищений інтерес. В окремих випадках такий підхід є безпідставним та непропорційним втручанням у приватне життя людини та може призвести до порушення Законів України «Про доступ до публічної інформації» чи «Про захист персональних даних».[3]

Відеозапис завжди є носієм персональних даних у тому випадку, якщо на ньому прямо або опосередковано можна ідентифікувати особу. Водночас, законодавство України гарантує людині дотримання права на невтручання в її особисте життя, окрім випадків, які дуже чітко визначені у законі. Стаття 32 Конституції забороняє «збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом». Закон України «Про захист персональних даних» зобов'язує володільців і розпорядників персональних даних забезпечити їх надійний захист від незаконного доступу, обробки, втрати та знищення.

[3] Детальніше з проблемами функціонування систем відеоспостереження в українських громадах можна ознайомитися в аналітичному звіті Асоціації УМДПЛ «Відеоспостереження за дотриманням публічного порядку в Україні».

У свою чергу, Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», зобов'язує використовувати усі державні інформаційні ресурси із застосуванням комплексної системи захисту, яка має бути підтверджена за державною експертизою (або мати сертифікат відповідності).[4]

Підсумовуючи, необхідно зазначити — інформаційні технології відеоконтролю в Україні будуть продовжувати стрімко розвиватися. Незалежно від подальших змін законодавства щодо повноважень місцевої влади впроваджувати технології, уже сьогодні усі суб'єкти зобов'язані забезпечити виконання вимог щодо захисту персональних даних.

[4] Згідно з даними у дослідженні Асоціації УМДПЛ «Відеоспостереження за дотриманням публічного порядку в Україні», станом на жовтень 2019 року, атестат на відповідність щодо захисту систем відеоспостереження отримано лише в Одесі, а в Києві система відеоспостереження перебувала у процесі атестування.

Розділ 2.

Загальні вимоги до обробки персональних даних у системах відеоспостереження

Українське законодавство напряму не забороняє монтаж систем відеоспостереження у публічних місцях і не встановлює технічних чи інших обмежень у їх експлуатації, але, водночас, регулює можливість використання відзнятого матеріалу. І це цілком зрозуміло, адже такий відеозапис може бути носієм інформації про приватне життя людини, яка потрапила в об'єктив камери.

Що таке «персональні дані»? Отримати відповідь на це питання вкрай важливо, оскільки від правильного розуміння цього та інших пов'язаних з ним термінів і понять, власне й залежить те, наскільки законною у кожному конкретному випадку буде діяльність з обробки отриманої відеоінформації.

2.1. Терміни та правові визначення

Персональні дані[5] — *це відомості чи сукупність відомостей про фізичну особу, які дають можливість прямо або опосередковано її ідентифікувати.*

Персональні дані поділяють на дві категорії: *загальну і особливу*.

До **загальної категорії** відносять інформацію про прізвище та ім'я, дату та місце народження людини, її зображення, сімейний стан, майно, адресу місця проживання, професію тощо.

Особлива категорія розкриває інформацію про расове або етнічне походження, політичні та релігійні переконання, приналежність до політичних партій, наявність судимості за вчинення правопорушення, а також дані, що стосуються здоров'я, статевого життя, біометричних особливостей.

[5] Стаття 2 Закону України «Про захист персональних даних»

А отже, фактично відеозапис із зображенням людини містить персональні дані про неї, адже дозволяє прямо чи опосередковано ідентифікувати її особу за індивідуальними фізіологічними та зовнішніми ознаками — риси обличчя, колір волосся, параметри тіла, голос, хода, одяг й так далі. При цьому, отримання персональних даних загальної категорії часто поєднується з встановленням особливої інформації.

Наприклад, впізнання й персоніфікація особи під час перебування на мирних зібраннях може вказувати на її політичні вподобання, зафіксовані на відео візити до певного медичного закладу свідчити про стан здоров'я, відвідування культових споруд — про ті чи інші релігійні переконання, а одягнена уніформа — про рід професійної діяльності.

Утім, відомості про приватне життя людини можна отримати не лише якщо вона особисто потрапила в об'єктив відеокамери. Розпізнані завдяки відеоспостереженню марка та номерний знак автомобіля дають можливість відслідковувати маршрути її пересування, а відеозапис з камери поблизу місця проживання особи — дати інформацію про коло її друзів та знайомих.

Очевидно, що у загальному діапазоні інформації про людину, сегмент даних, що відносяться до розряду персональних, є надзвичайно великим, а отже й вразливим для ризиків втрати або незаконного поширення.

Суб'єкти відносин, пов'язаних з персональними даними[6] **— це учасники правовідносин, які виникають під час обробки та захисту цих даних.**

Зокрема, **такими учасниками є:**

1. **Суб'єкт персональних даних** — фізична особа, персональні дані якої обробляються і якій належать всі права на ці дані.

[6] Стаття 4 Закону України «Про захист персональних даних»

Зрозуміло, що у складній, а іноді й конфліктній системі взаємин у сфері обігу персональної інформації, пріоритетна роль відводиться саме суб'єкту, оскільки персональні дані є його власністю і саме його права перебувають під загрозою порушення.

2. **Володілець персональних даних** — фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює їх склад, спосіб та порядок обробки, та має у власності відповідне технічне обладнання. Володільцями персональних даних можуть бути підприємства, установи і організації усіх форм власності, органи державної влади чи органи місцевого самоврядування, а також фізичні особи-підприємці.

3. **Розпорядник персональних даних** — фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані. Володілець може доручити розпоряднику обробку персональних даних відповідно до договору, укладеного у письмовій формі. При цьому, розпорядник має обробляти дані лише з метою і в обсязі, визначеними цим договором. Розпорядником персональних даних, які знаходяться у володінні органів державної влади чи органів місцевого самоврядування, крім цих органів, може виступати лише державне або комунальне підприємство, що належить до сфери управління цього органу.

4. **Уповноважений Верховної Ради України з прав людини** (Омбудсман) — здійснює контроль за дотриманням законодавства у сфері персональних даних.

5. **Третя особа** — будь-яка особа (за винятком суб'єкта та Уповноваженого ВРУ з прав людини), якій володілець чи розпорядник передає персональні дані.

Обробка персональних даних[7] — будь-яка дія або сукупність дій з персональних даними, зокрема, збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення.

Отже, можна зробити висновок, що ***використання систем відеоспостереження вважається обробкою персональних даних*** у випадках, коли отримана відеоінформація дає можливість:

- ідентифікувати людину за рисами обличчя, особливостями побудови тіла, фізичними вадами тощо *(пряма ідентифікація)*;
- ідентифікувати людину за допомогою специфічної моделі поведінки, характерних речей чи предметів, майна, що їй належать *(непряма ідентифікація)*. Наприклад, на відеозаписі не проглядається обличчя людини за кермом, але ідентифікацію власника автомобіля дозволяє провести номерний знак транспортного засобу, який він використовує.

2.2. Принципи обробки персональних даних

Новітні технології призвели до переходу людства на принципово новий рівень інформаційної свободи з доступними майже для всіх засобами отримання, коректування, зберігання та використання інформації, для реалізації власних потреб та інтересів. Тому не дивно, що персональні дані, особливо в електронному вигляді, стали надзвичайно затребуваною і, водночас, уразливою для стороннього вторгнення інформацією. У наш лексикон увійшли терміни «хакер», «злам бази даних», «інформаційна загроза», а відеозаписи з моментами приватного життя людини стали інструментом шантажу. Тому законодавством покладено обов'язок на

[7] Стаття 2 Закону України «Про захист персональних даних».

суб'єктів, що збирають та обробляють персональні дані, дотримуватись певних принципів й правил під час їх обробки.

Загальновизнані світові стандарти визначають **сім основних принципів обробки персональних даних**. Вони не встановлюють жорстких обмежень і за своєю сутністю є орієнтирами у загальній стратегії роботи з інформацією та фундаментом для нормативного врегулювання цієї сфери.

1. Законність, справедливість і прозорість.

Законність обробки персональних даних передбачає те, що дані обробляються лише у законний спосіб, для законних цілей і за наявності правових засад для цього, а будь-яка робота з ними, за відсутності легітимних підстав, забороняється.

Справедливість полягає у обов'язковому врахуванні прав суб'єкта персональних даних при їх обробці, унеможливленні завдання шкоди його законним інтересам, а також у запобіганні зловживанням з боку володільця чи розпорядника персональних даних.

Прозорість гарантує кожному отримання інформації про обробку своїх персональних даних та безпосередній доступ до них, адже людина має усвідомлювати не тільки загальносуспільні вигоди від впровадження систем відеоспостереження, а й власні ризики від їх застосування. Володілець персональних даних зобов'язаний пояснювати широкому загалу у доступній формі для чого і яким чином ці дані отримує, як планує використовувати та кому вони можуть бути передані.

2. Обмеження мети.

Персональні дані можуть збиратися лише з конкретною та законною метою і за умов, коли без цих даних досягнення такої мети неможливе. Саме мета має визначати обсяги та спосіб обробки даних, а не навпаки. Приміром, є цілком очевидним, що для забезпечення

протипожежної безпеки, у приміщенні доцільніше встановити систему протипожежної сигналізації, аніж відеоспостереження. Принцип обмеження мети вимагає заздалегідь визначити, обґрунтувати та документально закріпити реальні підстави і мету збору даних, адже у подальшому це стане запобіжником від їх використання у незаконних цілях. Наприклад, якщо система відеоспостереження поблизу інституту встановлена з метою охорони громадського порядку, то отримані відеодані не можуть бути передані керівництву ВУЗу і використовуватися, як засіб контролю за відвідуваністю студентами навчального закладу.

> *«Перш ніж встановити систему відеоспостереження, володілець даних повинен визначити його мету і переконатися, що ця мета є законною. Персональні дані мають збиратися для певних, чітких та законних цілей і не оброблятись способом, несумісним з цими цілями. Неоднозначні або занадто загальні описи на кшталт «для кращого виконання покладених завдань» чи «для безпеки суспільства» є недостатніми. Крім того слід переконатися, що дані згодом не будуть використані для непередбачених цілей або передані непередбаченим розпорядникам, які можуть використовувати їх для додаткових, невідповідних цілей»*, — наголошує Секретаріат Уповноваженого Верховної Ради України з прав людини[8].

3. Мінімізація даних.

Принцип мінімізації, який тісно пов'язаний з принципом обмеження мети, полягає у тому, що обсяг отримуваних даних має бути зменшений до мінімального рівня. Тобто, можна збирати лише ті дані, які забезпечують досягнення цілей їх обробки, і не більше. Це слід враховувати при виборі технічних засобів — діапазон функціональних можливостей системи відеоспостереження (наявність мікрофонів, обсяги архівації даних, здатність до виконання аналітичних функцій)

[8] «Рекомендації органам місцевого самоврядування щодо здійснення відеоспостереження у громадських місцях»

не повинен бути надмірно широким, а визначатись за критерієм мінімальної необхідності для досягнення передбаченої мети. Так, якщо відеокамери встановлюються у сквері для контролю за збереженням зелених насаджень, їм не потрібні вмонтовані мікрофони і функція транслювання звуку оператору, оскільки це призведе до прослуховування розмов відпочиваючих громадян.

4.Точність.

Цей принцип вимагає постійного контролю за точністю, достовірністю та актуальністю отриманих персональних даних. Застаріла або неточна інформація підлягає невідкладному виправленню або знищенню у спосіб, що виключає можливість їх поновлення.

5. Обмеження строку зберігання.

Персональні дані мають зберігатися не довше, ніж це необхідно для досягнення мети їх обробки — як тільки таку мету досягнуто, вони повинні бути видалені чи знищені. Зберігання даних протягом більш тривалого часу допускається виключно з метою реалізації громадських інтересів, у наукових цілях, задля історичних досліджень або формування статистики. Також, у разі необхідності, тривале зберігання даних можна здійснювати після їх знеособлення — тобто приведення даних у вигляд, який не дає можливості ідентифікувати особу. Для відеозаписів це, як правило, редагування зображення шляхом «замилювання» його певних сегментів — обличчя людини, номерного знаку авто, таблички з номером на будинку тощо.

6. Цілісність і конфіденційність (безпека).

Обробка даних повинна здійснюватися у спосіб, який гарантує їх належну безпеку, в тому числі захист від несанкціонованої/незаконної обробки або випадкової втрати.

7. Підзвітність.

Кожен, хто обробляє персональні дані, повинен детально фіксувати та документувати свою діяльність та бути готовим у будь-який час продемонструвати правомірність її здійснення. Зрозуміло, що компетентні органи, відповідно до своїх повноважень, вправі перевіряти стан дотримання законності у цій сфері, але підзвітність — це не лише пред'явлення звітів про роботу контролюючим структурам. Позивною практикою можна вважати, коли володільці систем відеоспостереження систематично і з власної ініціативи звітують перед громадою про заходи у сфері захисту персональних даних. У широкому розумінні, підзвітність — це засіб ознайомлення суспільства з тим, яким чином і наскільки ефективно забезпечується захист зібраної щодо нього інформації. Втім, у такого роду підзвітності зацікавлені не тільки пересічні українці, а й уся держава в цілому, адже порушення законодавства несуть ризики й для національної безпеки країни.

Дотримання принципу підзвітності допомагає отримати довіру людей, оскільки наочно демонструє — володілець даних поважає приватне життя громадян, знає та сумлінно виконує вимоги законодавства, працює над зниженням ризиків його порушення, не відмовляється від діалогу з суспільством і готовий нести відповідальність за власні прорахунки.

На практиці принцип підзвітності реалізується у різні способи, серед яких слід виокремити створення окремої вебсторінки на офіційному сайті з найбільш затребуваною та актуальною інформацією. На сторінці доцільно помістити:

- карту з позначенням місць розташування відеокамер;
- відомості про технічні характеристики використовуваного обладнання;
- звіти щодо вжитих заходів із захисту інформації;

- повідомлення про виникнення загроз (кібератаки, несанкціонований витік тощо) та шляхи їх усунення;
- перелік нормативно-правових актів, що регламентують роботу з персональними даними (політики приватності);
- контакти посадових осіб, на яких офіційно покладено відповідальність за роботу з персональними даними;
- номер відповідного телефону «гарячої лінії»;
- онлайн форум для обговорення проблем використання систем відеоспостереження та отримання скарг і пропозицій громадян.

Підсумовуючи, можна зауважити, що всі сім вказаних принципів тісно пов'язані і доповнюють один одного, утворюючи єдину концепцію дотримання прав і свобод людини при обробці персональних даних.

2.3. Базові вимоги до обробки персональних даних

Необхідно розуміти, що за своїм визначенням суб'єкт персональних даних не може виступати у ролі порушника законодавства у цій сфері, оскільки саме йому належать всі права на свої дані. Водночас, володільці персональних даних, які фактично розпоряджаються чужою нематеріальною власністю, повинні діяти вкрай виважено й обережно, аби не потрапити у категорію порушників закону.

У правовідносинах, пов'язаних з обігом персональних даних, саме їх володільці та розпорядники є стороною, на яку покладений обов'язок зі створення доволі складного механізму захисту законних інтересів фізичних осіб, дані яких обробляються.

Високий рівень безпеки роботи з персональними даними передбачає необхідність попереднього виконання цілого комплексу правових, організаційних і технічних заходів, при цьому всі вони однаково значущі і нехтування якоюсь окремою вимогою може звести нанівець позитивні результати від реалізації інших. Отже, плануванню та прийняттю управлінських рішень має передувати чітке усвідомлення вимог до обробки персональних даних.

Визначимо такі **базові вимоги** з урахуванням положень статті 6 Закону України «Про захист персональних даних»:

1. Обробка даних має здійснюватися з метою забезпечення виконання законів чи інших нормативно-правових актів та відповідати законодавству про захист персональних даних.
2. Робота з персональними даними проводиться відкрито й прозоро з демонстрацією широкому загалу її правомірності.
3. Цілі обробки персональних даних повинні бути законними, конкретно сформульованими і визначеними до початку їх збору.
4. Суб'єкти персональних даних мають знати і не заперечувати щодо конкретних цілей та способу обробки цих даних.
5. Персональні дані мають бути точними, достовірними та своєчасно оновлюватися відповідно до поставлених цілей їх обробки.
6. Обробка персональних даних повинна здійснюватися із застосуванням засобів та у спосіб, що відповідають меті обробки.
7. При зміні цілей або способу обробки персональних даних, необхідно оримати згоду на це від осіб, дані яких обробляються.
8. Забороняється обробка конфіденційних персональних даних особи без отримання її попередньої згоди на це (крім встановлених законом випадків).

9. Термінова обробка персональних даних, яка викликана необхідністю захисту життєво важливих інтересів особи, допускається без її згоди, але лише до моменту, коли таке погодження стане можливим.
10. Обсяги накопичуваних персональних даних, їх склад, зміст та термін зберігання обмежуються рамками конкретної мети їх обробки і не мають бути надлишковими чи розширеними задля реалізації невизначених цією метою потреб.
11. Допускається тривале зберігання персональних даних в історичних, статистичних або наукових цілях, але за умови забезпечення їх належного захисту.

Вказані вимоги є універсальними і **не поширюються лише на випадки,** коли обробка даних здійснюється:

- фізичною особою виключно для особистих чи побутових потреб;
- виключно для журналістських та творчих цілей, за умови забезпечення балансу між правом на повагу до особистого життя та правом на свободу вираження поглядів.[9]

Слід додати, що працюючи з будь-якою інформацією завжди треба враховувати її категорію. Наприклад, якщо здійснюється обробка особливої категорії даних,[10] то необхідно про це повідомити Уповноваженого Верховної Ради України з прав людини (порядок здійснення такого повідомлення вказаний на сторінці офіційного сайту Уповноваженого).[11]

[9] Стаття 25 Закону України «Про захист персональних даних»

[10] Нагадаємо, до них відносяться біометричні та генетичні дані, дані про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також відомості, що стосуються здоров'я і статевого життя.

[11] Офіційний сайт Омбудсмана *http://www.ombudsman.gov.ua/ua/page/zpd/*

2.4. Підстави для обробки персональних даних

Стаття 11 Закону України «Про захист персональних даних» визначає перелік підстав для обробки персональних даних:

1. згода суб'єкта персональних даних;
2. дозвіл на обробку персональних даних, який надано відповідно до закону виключно для здійснення його повноважень;
3. укладення та виконання правочину, стороною якого є суб'єкт персональних даних або який укладено на його користь чи для здійснення заходів, що передують укладенню правочину на вимогу суб'єкта персональних даних;
4. захист життєво важливих інтересів суб'єкта персональних даних;
5. необхідність виконання обов'язку володільця персональних даних, який передбачений законом;
6. необхідність захисту законних інтересів володільця персональних даних або третьої особи, якій передаються дані, крім випадків, коли потреби захисту основоположних прав і свобод суб'єкта персональних даних у зв'язку з обробкою його даних переважають такі інтереси.

У контексті визначення підстав для роботи систем відеоспостереження аналіз змісту цієї статті дозволяє дійти до наступних висновків:

1. **Органи місцевого самоврядування є суб'єктом владних повноважень.** Відповідно до статті 19 Конституції України, органи місцевого самоврядування, їх посадові особи, зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України.

   З огляду на це положення, місцева влада може здійснювати обробку персональних даних (будь-яка дія або сукупність дій) лише за наявності повноважень, законної підстави й обґрунтованої мети та у спосіб, передбачений законом.

Тобто, не потрібно отримувати згоду суб'єкта персональних даних у тих випадках, коли дозвіл на збір інформації буде прямо передбачений законом. Разом з тим, недостатньо мати повноваження, має бути обґрунтована мета та чітка процедура.

2. **Підстави «необхідність виконання обов'язку, який передбачений законом» та «необхідність захисту законних інтересів».**

   Вказані підстави можуть застосовуватись органами місцевого самоврядування для обробки відеозаписів лише з певними застереженнями, оскільки запропоновані у статті формулювання мають загальний характер і напряму не визначають практичні цілі застосування систем відеоспостереження. Проблема поглиблюється й тим, що у Законі «Про місцеве самоврядування в Україні» відсутні норми, безпосередньо пов'язані з положеннями Закону «Про захист персональних даних», зокрема і щодо використання відеонагляду.

   Часто місцева влада для впровадження систем відеоспостереження обирає підставу *«захист життєво важливих інтересів»*, що є некоректним. Під *«життєво важливими інтересами»* слід розуміти не загальну безпеку громади, а тільки ті інтереси, які безпосередньо пов'язані з питаннями врятування життя і здоров'я людини. Наприклад, ця підстава актуальна у випадку, коли вкрай необхідно отримати персональні дані людини у медичних цілях, а вона не може дати згоду на це через свій безпорадний стан. У міжнародних актах визначені й інші можливості застосування підстави *«захист життєво важливих інтересів»*, коли обробка персональних даних здійснюється для моніторингу розвитку епідемій, під час ліквідації стихійного лиха або катастрофи тощо.

Час від часу у ЗМІ інформують українців про факти торгівлі персональними даними, отриманими через системи відеоспостереження. Наприклад, сторонні особи за грошову винагороду отримали

з відеосистеми «Безпечне місто» інформацію про маршрути пересування першого заступника директора Державного бюро розслідувань.[12] У квітні 2019 року зловмисник намагався скоїти замах на високопосадовця Міністерства оборони України, встановивши вибухівку на його автомобіль. Як було встановлено слідством, до витоку інформації щодо автомобіля та місць його можливого перебування призвели дії посадової особи, яка надала своєму знайомому пароль та віддалений доступ до комп'ютера, на якому був встановлений ключ до бази даних «Безпечне місто».[13]

Враховуючи вищенаведене, ініціативи з впровадження систем відеоспостереження завжди супроводжуються певними ризиками судових позовів і штрафів, відсутність яких наразі викликана лише низькою правовою обізнаністю громадян щодо інструментів захисту своїх прав у сфері персональних даних. Тому керівництво установ має бути зацікавлене у дотриманні вищенаведених принципів і вимог до захисту персональних даних під час їх обробки. Тим самим забезпечити справедливу рівновагу між правом людини на повагу до її приватного життя і інтересами охорони громадського порядку.

2.5. Відповідальність за порушення законодавства про захист персональних даних

Відповідно до статті 22 Закону України «Про захист персональних даних», контроль за додержанням законодавства у цій сфері здійснюють Уповноважений Верховної Ради України з прав людини (надалі — Уповноважений) та суди.

[12] «Медіакілери торгували конфіденційними відео з камер стеження Києва», — Інтернет-видання «*Texty.org.ua*»

[13] «До вибуху автівки спецслужбовця у Києві причетний правоохоронець», — Інтернет-видання «Українська правда».

Порушення законодавства про захист персональних даних тягне за собою відповідальність, встановлену законом[14]. Зокрема відповідальність передбачена:

- Кримінальним кодексом України (статтями 182 «Порушення недоторканності приватного життя» та 359 «Незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації»)
- Кодексом України про адміністративні правопорушення (статтею 188-39 «Порушення законодавства у сфері захисту персональних даних»).

(Детальне роз'яснення положень законів дивіться у Додатку 2).

Кодекс України про адміністративні правопорушення (КУпАП) передбачає покарання у вигляді адміністративного штрафу як за ігнорування вимог Уповноваженого, так і за недодержання порядку захисту персональних даних.

[14] стаття 28 Закону України «Про захист персональних даних»

Розділ 3.

Організація захисту персональних даних у системах відеоспостереження

3.1. Загальні вимоги. Технічні та організаційні заходи

Щороку у світі з'являються нові сценарії використання систем відеоспостереження для покращення якості та безпеки життя. Збільшення спектру їх можливого використання, постійне вдосконалення та здешевлення обладнання стимулює поширення технологій відеонагляду і в Україні — наразі мережу відеоспостереження може дозволити собі навіть місто з порівняно невеликим бюджетом.

Проте, незважаючи на все різноманіття існуючих типів і незалежно від цільового призначення чи рівня модернізації систем, до них висувається одна загальна вимога — оброблювальні за їх допомогою персональні дані мають бути надійно захищені від загрози стороннього втручання та протиправного розповсюдження.

Захист систем відеоспостереження необхідний для:

- запобігання витоку інформації;
- недопущення знищення, перекручення, копіювання, несанкціонованого блокування персональних даних;
- запобігання неавторизованому підключенню та іншому несанкціонованому доступу до масиву даних;
- забезпечення вичерпного, цілісного, достовірного характеру персональних даних у телекомунікаційних мережах та інформаційних ресурсах;
- дотримання законодавства, що регламентує використання інформаційних систем та програм для обробки персональних даних.

Враховуючи таке широке коло та різнобічність завдань, захист персональних даних має забезпечуватись єдиним комплексом організаційних і технічних заходів, без виконання яких будь-яке використання систем відеоспостереження не допускається.

Умовно такі заходи можна поділити на **три основні блоки:**

1. Заходи, що в цілому визначають загальні процедури роботи з персональними даними.
2. Заходи, що забезпечують безпеку даних під час їх обробки безпосередньо в системах відеоспостереження.
3. Заходи з моніторингу стану захищеності персональних даних та порядку здійснення внутрішнього контролю за дотриманням законності під час їх обробки.

Основні положення щодо **технічних заходів безпеки** визначені у Законі «Про захист інформації в інформаційно-телекомунікаційних системах».

Закон вимагає використовувати усі державні інформаційні ресурси із застосуванням комплексної системи захисту, яка має бути підтверджена висновком державної експертизи (або мати сертифікат відповідності). Відповідальність за забезпечення захисту інформації в системі покладається на власника системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом. Власник системи утворює службу захисту інформації або призначає осіб, на яких покладається відповідний обов'язок.[15] По суті, йдеться про використання сучасного спеціального обладнання та програмного забезпечення, яке дозволяє мінімізувати уразливість системи до зламу, запобігає зчитуванню паролів, захищає від «захвату» серверів, унеможливлює керування діями відеокамери стороннім оператором, вберігає дані від спотворення тощо. Оскільки обробка даних здійснюється з використанням можливостей та ресурсів Інтернету, а це завжди створює ризики витоку інформації, набувають надзвичайної актуальності і питання «кібербезпеки».

[15] Стаття 9 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах»

До основних технічних компонентів систем відеоспостереження можна віднести:

- відеокамери;
- пристрої зберігання відеоархіву (відеореєстратори або сервери, які отримують від камер потоки відео та записують його на жорсткі диски);
- програмне забезпечення — сукупність програм, необхідних для експлуатації систем відеоспостереження;
- мережеве обладнання — комутатори, маршрутизатори та інші пристрої, які створюють мережу відеонагляду та ін.

Захист має охоплювати всі без виключення технічні засоби, задіяні в обробці персональних даних, незалежно від їх типу і функціонального призначення: відеокамери, магнітні, оптичні, лазерні або інші носії електронної інформації, інформаційні масиви та бази даних, операційні системи, телекомунікаційні мережі та їх елементи тощо.

При цьому, особливу увагу слід приділяти закупівлі виключно ліцензійного програмного продукту (так званий «піратський» є ненадійним і несе численні загрози) та виваженому вибору його виробника. «Донедавна досить широко використовувались програми від російської компанії Axxon Soft, але у грудні 2018 року Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ звернувся до Асоціації міст України з листом про припинення практики розгортання систем відеоспостереження на базі російського програмного забезпечення, оскільки це створює передумови до проведення підривної діяльності спецслужбами РФ та може використовуватись з метою отримання інформації з обмеженим доступом. Проте й досі в різних тендерах, що стосуються створення систем відеоспостереження переважно в малих містах, періодично перемагають компанії, пов'язані з Axxon Soft та іншими російськими виробниками

програмних продуктів. Ця ситуація потребує пильної уваги з боку СБУ», — вказують у своєму дослідження експерти Асоціації УМДПЛ.[16]

Більше того, у статті 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» визначено, що жоден з елементів системи не може бути розташований на територіях України, на яких органи державної влади України тимчасово не здійснюють своїх повноважень, на територіях держав, визнаних Верховною Радою України державами-агресорами, на територіях держав, щодо яких застосовані санкції відповідно до Закону України «Про санкції», та на територіях держав, які входять до митних союзів з такими державами.

Не менш важливим є й вибір виробника застосовуваних для відеонагляду технічних пристроїв. «Окремим проблемним моментом є те, що в переважній більшості органів місцевого самоврядування для встановлення систем відеоспостереження закуповують обладнання китайської фірми HikVision, яка, судячи з усього, контролюється урядом КНР і перебуває у переліку торговельних санкцій США поруч з продукцією фірми Huawei. Причиною потрапляння до цього списку називають міркування національної безпеки США та інформацію про існування закладених урядом Китаю механізмів прихованого отримання доступу до цих систем», — зазначається у цьому ж дослідженні.

До питань технічного захисту даних також відносяться постійний контроль за працездатністю системи та її своєчасне обслуговування, автоматичний облік підключених засобів відеофіксації та всіх дій операторів у системі, фільтрування можливості доступу персоналу до певних персональних даних в залежності від встановленого рівня доступу та інше.

[16] «Відеоспостереження за дотриманням публічного порядку в Україні», сайт Асоціації УМДПЛ

Організаційні заходи безпеки є не менш важливою складовою захисту інформації. Вони передбачають прийняття та закріплення у внутрішніх документах низки управлінських рішень, спрямованих на неухильне дотримання принципів обробки персональних даних та виконання вимог законодавства щодо їх захисту.

Зокрема, такі рішення повинні визначати:

- порядок доступу до приміщень з технічним обладнанням (серверні, ситуаційні центри тощо);
- заходи по захисту цих приміщень від незаконного проникнення;
- оптимальний режим роботи з персональними даними;
- порядок отримання персоналом допуску до обробки тієї чи іншої категорії даних;
- порядок передачі таких даних розпорядникам чи третім особам;
- заходи з професійної підготовки персоналу щодо виконання вимог закону;
- заходи з контролю за всіма етапами обробки даних та роботою залученого до цього процесу персоналу.

3.2. Цілі обробки персональних даних та технічні параметри обладнання

Впровадженню заходів безпеки при обробці персональних даних має передувати попередня аналітична робота з ***визначення цілей такої обробки*** та підбору найбільш оптимальних ***технічних характеристик*** використовуваного обладнання.

Цілі обробки персональних даних в системах відеоспостереження.

Чітке усвідомлення того, навіщо здійснюється відеонагляд, вкрай необхідне для реалізації принципу *«обмеження мети»*[17], який сприяє забезпеченню справедливості, законності й прозорості обробки персональних даних та визначає необхідний рівень їх захисту. Системи відеоспостереження повинні використовуватись для досягнення заздалегідь визначених реальних цілей, при цьому такі цілі мають бути максимально конкретизованими, досяжними та викладеними у внутрішніх документах (політиках), що регулюють роботу з персональними даними. Крім цього, мета їх обробки має бути не тільки чітко визначена та сформульована, а й очевидна для всіх, в тому числі для суб'єктів персональних даних і третіх осіб. Навіть невелика організація, система діловодства якої не передбачає значного обігу документації, при роботі з персональними даними повинна вказувати цілі їх обробки в окремій довідці, яка видається з цього приводу зацікавленим фізичним особам.

Закріплення конкретної мети обробки даних у внутрішніх документах є своєрідним запобіжником від того, що персональні дані зможуть бути використані для досягнення сторонніх цілей. Зрозуміло, що такий підхід вимагає регулярного моніторингу і інспектування діяльності систем відеоспостереження, аби завжди бути впевненим — визначені й задекларовані початкові цілі їх функціонування з часом не змінились.

Використання відеонагляду для реалізації додаткових чи нових завдань можливе, **якщо:**

[17] Про принцип «обмеження мети» детальніше розповідається у п.2.2 розділу 2 цього Посібника

1. **Нова мета обробки персональних даних сумісна з метою первинною.**

   У такому випадку нова правова підстава для роботи з даними не потрібна, проте оцінювання того, чи дійсно оновлена мета сумісна з початковою, має бути повним й об'єктивним. Для цього необхідно взяти до уваги наступні фактори:

   - наскільки первинна мета пов'язана з новою;
   - контекст, у якому початково оброблялися персональні дані;
   - специфіку та характер даних (наприклад, наскільки вони є важливими, конфіденційними, уразливими тощо);
   - вірогідність настання негативних наслідків для осіб, чиї дані обробляються;
   - можливість гарантування належного рівня захисту обробки нової інформації.

2. **З'явилась правова норма, яка вимагає чи дозволяє обробку даних з новою метою.**

   Наприклад, через відповідні зміни у законодавстві повноваження органу збільшені і він отримав право виконувати додаткові функції, пов'язані з обробкою персональних даних.

Місця розміщення відеокамер та технічні параметри обладнання.

Визначення місць монтажу відеокамер та технічні параметри всіх компонентів системи відеоспостереження мають відповідати цілям її використання й забезпечувати мінімальне втручання у приватне життя людини, яка потрапила у зону відеонагляду.

Для цього слід звернути увагу на **наступні нюанси:**

1. **Розміщення та кількість відеокамер.**

   Розташування відеокамер здійснюється таким чином, щоби

під спостереженням перебував лише той мінімальний сегмент публічного місця, контролювати який необхідно для досягнення цілей роботи системи. Надмірно великий сектор огляду може призвести до порушень права громадян на приватність — наприклад, на відеозаписі буде проглядатись подвір'я приватного будинку. При орієнтуванні камер у просторі, слід враховувати ракурс здійснюваного відеонагляду — за відсутності потреби у ідентифікації фізичних осіб, висота розміщення та кут нахилу відеокамер не повинні сприяти зайвій деталізації зовнішності людини та її фізіологічних особливостей. Наприклад, відеокамери поблизу пляжів доцільно розміщувати і орієнтувати у спосіб, що унеможливлює потрапляння в об'єктив кабінок для переодягання.

2. **Технічні параметри і функціональні можливості обладнання.**

Правило «доцільної мінімізації» застосовується і при виборі обладнання для систем відеоспостереження. Технічні характеристики та спеціальні можливості відеокамер (якість створюваного зображення, наявність вбудованого ZOOM-об'єктива та мікрофона, здатність до «нічного бачення», «повороту» та підтримки Wi-Fi), а також параметри іншого обладнання (ресурс сервера, аналітична складова системи тощо) повинні слугувати лише досягненню мети відеоконтролю і не створювати передумов для зловживань. Так, свого часу в Англії відбувся судовий процес над операторами камер вуличного спостереження, які могли фокусувати їх великим планом на жінок у квартирах і у ванних кімнатах.[18]

Раціональне розміщення камер, їх оптимальна кількість і виважений підбір технічного обладнання дозволяють запобігти отриманню сторонньої та надлишкової інформації, що, в

[18] «Камери в громадських місцях і право на недоторканність особистого життя», сайт «Радіо Свобода»

свою чергу, дає можливість сконцентрувати роботу систем відеоспостереження виключно на виконанні поставлених цілей.

Узагальнимо та підведемо підсумки:

при запровадженні систем відеоспостереження питання забезпечення захисту даних необхідно враховувати під час:

- визначення цілей відеофіксації;
- визначення місць, які підлягають відеоконтролю;
- визначення необхідного класу відеосистеми та структури мереж;
- виборі необхідного обладнання (в тому числі його виробника);
- безпосереднього монтажу всіх складових системи відеоспостереження;
- встановлення правил доступу до роботи системи;
- визначення алгоритмів контролю за роботою системи та обслуговуючим персоналом.

3.3. Аналіз процесів обробки персональних даних

Для забезпечення вимог законодавства про захист персональних даних, необхідно провести попереднє дослідження існуючого в органі чи установі порядку їх обробки як в цілому, так і безпосередньо в інформаційних системах відеоспостереження. Кожен етап роботи з даними має бути підданий всебічному правовому аналізу на предмет відповідності вимогам чинного законодавства, в тому числі мають бути перевірені на повноту й змістовність внутрішні директивні документи, що регламентують обіг та захист інформації в органі. Подібний аналіз дозволяє визначити приблизний

перелік основних процесів з обробки даних, який у подальшому можна коригувати як з метою оптимізації цих процесів, так і у зв'язку зі змінами у законодавстві або отриманням органом додаткових повноважень.

По кожному процесу обробки персональних даних необхідно визначити:

- мету обробки персональних даних;
- вид та категорії даних, що обробляються (з прив'язкою до мети обробки);
- правову підставу обробки даних (з прив'язкою до мети обробки);
- способи обробки персональних даних (автоматизована, паперова або змішана);
- перелік інформаційних систем, в яких обробляються дані;
- перелік місць та терміни зберігання носіїв таких даних;
- перелік осіб, задіяних до обробки персональних даних;
- інші заходи з обробки даних в рамках процесу (реєстрація, накопичення, зміна, знеособлення, передача, знищення та інше).

Слід зауважити, що необхідні для проведення такої роботи відомості можуть бути отримані під час співбесід з особами, які працюють з інформаційними системами та безпосередньо залучені до процесів обробки даних.

3.4. Підготовка організаційно-розпорядчих документів

Обробка персональних даних — це процес, який складається з певних етапів, що має регулюватися відповідними внутрішніми організаційно-розпорядчими документами. При цьому, кожен з таких документів має забезпечувати вирішення конкретного завдання та призначатись для певного кола осіб, уповноважених ухвалювати рішення або вчиняти ті чи інші дії на його виконання. Сукупність цих взаємопов'язаних документів і є тим правовим інструментом, який забезпечує дотримання норм законодавства.

До переліку таких документів можна віднести:

- Політику щодо обробки персональних даних[19];
- Правила обробки персональних даних[20];
- Правила розгляду запитів суб'єктів, чиї дані обробляються;
- Правила здійснення внутрішнього контролю за процесами обробки та захисту даних;
- Правила роботи зі знеособленими даними;
- Перелік посад працівників, які здійснюють обробку даних;
- Перелік (вид та категорія) персональних даних, що обробляються;
- Перелік місць зберігання матеріальних носіїв персональних даних;

[19] Документ, розроблений володільцем або розпорядником персональних даних, який визначає заходи з захисту даних, зважаючи на існуючі потенційні та реальні ризики.

[20] Чіткі внутрішні правила щодо організації та забезпечення усього циклу обробки даних (збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення тощо).

- Посадові інструкції осіб, відповідальних за організацію обробки даних;
- Типове зобов'язання про нерозголошення й забезпечення безпеки персональних даних;
- Типове зобов'язання працівника про припинення обробки персональних даних у разі розірвання з ним трудового договору;
- Типова форма згоди фізичної особи на обробку персональних даних;
- Порядок доступу до приміщень, де ведеться обробка персональних даних;
- Правила щодо передачі персональних даних третім особам або їх поширення.

Цей перелік не є вичерпним. Зміст пакету необхідної службової документації залежить від специфіки діяльності та повноважень органу, набору функцій та модернізації комплексу інформаційних систем, кількості персоналу, залученого до роботи з системами тощо. Як правило, керівництво органу самостійно вирішує як організувати менеджмент управління даними, зокрема, які необхідні положення тощо. Є приклади, коли усі перелічені вище документи формують в одне керівництво. Інші ж вважають, що такий підхід не ефективний.

Але в будь-якому випадку, при розробці внутрішніх документів, які регулюють процедури обробки та захисту даних, слід брати до уваги:

- категорію персональних даних та специфіку операцій з їх обробки;
- рівень складності інформаційних систем та програм, задіяних у процесі обробки даних;
- наявність персоналу з технічного обслуговування систем, який в силу цього має доступ до даних;

- специфіку форми персональних даних (цифровий відеозапис), що створює загрози їх спотворення, підміни, несанкціонованого перегляду тощо;
- специфіку функціонування каналів передачі даних, що створює загрози їх перехоплення;
- процедури накопичення, архівування та зберігання даних у електронному вигляді;
- «кіберзагрози», зумовлені використанням Інтернету під час передачі даних;
- інші ризики, які можуть виникнути в інформаційних системах відеоспостереження.

Головні принципи та правила роботи з персональними даними в органі визначає і закріплює окремий розпорядчий акт — ***«Політика обробки персональних даних»***. Вказаний документ регламентує дії персоналу, задіяного у процесах обробки, а також встановлює алгоритми взаємин володільця персональних даних з їх розпорядниками, суб'єктами та третіми особами.

Політика обробки даних в інформаційних системах відеоспостереження повинна передбачати, як мінімум:

- опис технічних характеристик систем відеоспостереження;
- роз'яснення законної підстави та обґрунтованої мети використання систем;
- опис того, як працюють системи;
- види та категорії персональних даних, їхні локалізації та операції, що проводяться над ними;
- конфігурацію інформаційних систем, а також програм, задіяних у процесі обробки даних;
- список осіб, які мають доступ до персональних даних та адміністративних підрозділів;

- список авторизованих користувачів в інформаційних системах;
- докладний опис критеріїв, відповідно до яких будуть доступні персональні дані;
- повноваження та обов'язки осіб, які мають доступ до системи;
- механізм здійснення заходів безпеки;
- порядок доступу третіх осіб до даних систем відеоспостереження;
- права суб'єктів персональних даних;
- форми ведення реєстру, в якому обробляються дані;
- ризики, які можуть виникнути у системах відеоспостереження;
- особу, відповідальну в органі за безпеку персональних даних;
- періодичність проведення перевірок стану дотримання правил безпеки при обробці персональних даних;
- форму звітів за результатами перевірок та про інциденти порушення безпеки;
- заходи з виявлення випадків несанкціонованого доступу та/або обробки даних;
- термін зберігання персональних даних та порядок їх видалення.

З метою забезпечення принципів «прозорості» і «підзвітності», Політика обробки персональних даних та інші документи у цій сфері повинні бути оприлюднені на офіційному сайті органу та доступні для ознайомлення у інший спосіб (розміщені на інформаційних стендах, надруковані у вигляді брошур та інше).

Слід додати, що розпорядчі документи, при необхідності, можуть врегульовувати правила обробки персональних даних окремо для кожного етапу такої обробки або окремо для кожного структурного підрозділу, який бере у ній участь.

Правила роботи зі знеособленими даними необхідні лише у випадку, коли орган дійсно працює з ними. Бажано, щоби за цей напрямок були призначені відповідальні особи. Також в організаційно-розпорядчих документах встановлюються вимоги до пропускного режиму, охорони приміщень зі спеціальним обладнанням, порядку ведення відповідних журналів (реєстрів, книг) тощо. Вся документація щодо обробки персональних даних має бути змістовною, вичерпною, актуальною та регулярно оновлюватися.

3.5. Дотримання прав суб'єктів персональних даних

Сьогодні системи відеоспостереження є невід'ємною частиною масштабних проєктів із забезпечення комфортного життя громад (програми *«Безпечне місто»* та *«Розумне місто»* і вважаються індикаторами сучасного підходу до вирішення питання безпеки населення. Проте, це не повинно створювати передумов для порушення законних прав і інтересів окремих громадян.

На відміну від відеонагляду в офісах чи на територіях з обмеженим доступом, при розташуванні систем відеоспостереження у публічних місцях неможливо заздалегідь визначити коло носіїв персональних даних (фізичних осіб, транспортних засобів тощо), які можуть стати об'єктами відеофіксації. В той же час, як вже вказувалось, стаття 32 Конституції України гарантує кожному право на приватність і забороняє «збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом». З огляду на це, використання систем відеоспостереження вимагає особливо ретельного підходу до забезпечення прав осіб, чиї персональні дані стають об'єктом обробки.

Таке твердження відповідає чинним на сьогодні міжнародним стандартам — пункт 12 Резолюції ПАРЄ 1604 (2008) «Відеоспосте-

реження в публічних місцях» сповіщає: *«кожен, хто живе або проходить через зону відеоспостереження, має право знати про це і мати доступ до всіх записів зі своїм зображенням. Країни-члени Ради Європи мають захищати це право законом»*.

Стаття 8 Закону України *«Про захист персональних даних»* проголосила особисті немайнові права фізичної особи на свої персональні дані *«невід'ємними і непорушними»* та вказала, що **суб'єкт персональних даних має право:**

1. знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження (перебування) володільця чи розпорядника персональних даних або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом;
2. отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким вони передаються;
3. мати доступ до своїх персональних даних;
4. отримувати не пізніш як за тридцять календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи обробляються його персональні дані, а також отримувати зміст таких персональних даних;
5. пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх даних;
6. пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних, якщо ці дані обробляються незаконно чи є недостовірними;
7. на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є

недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи;

8. звертатися зі скаргами на обробку своїх даних до Уповноваженого Верховної Ради України з прав людини або до суду;
9. застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних;
10. вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди;
11. відкликати згоду на обробку своїх персональних даних;
12. знати механізм автоматичної обробки персональних даних;
13. на захист від автоматизованого рішення, яке має для нього правові наслідки.

В той же час, використання систем відеоспостереження для обробки персональних даних зумовлює певні особливості у способах реалізації окремих із наведених прав.

Попередження про відеоспостереження.

Люди, які перебувають у зоні відеоконтролю, мають бути заздалегідь проінформовані про те, що їх дії фіксує система відеоспостереження, а також знати, хто є її володільцем та де, при необхідності, можна переглянути зроблені відеозаписи і ознайомитись зі встановленим порядком їх обробки й захисту.

Таке інформування повинно бути комплексним: на офіційному сайті органу публікуються відомості про місця розташування камер («карта мереж відеонагляду»), а у зонах, охоплених відеоспостереженням, розміщується необхідна кількість відповідних попереджувальних знаків (піктограм). Знаки повинні бути візуально сприйнятливими, мати необхідну текстову інформацію і розташовуватись так, щоб особа могла побачити їх ще до того, як потрапить у зону

спостереження. Вказані заходи забезпечують необхідну відкритість та прозорість збору даних, як того вимагає чинне законодавство.

На жаль, проведений моніторинг показав, що наразі муніципальні органи на місцях часто ігнорують необхідність виконання цих доволі простих правил. *«З усіх відвіданих міст тільки у Житомирі практично під кожною камерою є попередження про здійснення відеоспостереження. При цьому, відповідні таблички містять інформацію про власника системи (Житомирська міська рада), адміністратора системи (КП «Міський інформаційний центр»), міську цільову програму, в рамках якої встановлено систему відеоспостереження («Безпечне місто»), а також контактний телефон, за яким можна звернутися у випадку виникнення питань. В Києві та Одесі попереджувальні знаки розміщуються не у кожної камери, хоча у столиці подібні роботи ведуться і планується встановити близько 3 тисяч табличок-попереджень. У Тростянці Сумської області та Маріуполі в деяких місцях розміщені таблички, втім, вони не містять жодної довідкової інформації про суб'єкт здійснення відеоспостереження. В інших відвіданих містах знаків про ведення відеоспостереження побачити не вдалось»*, — вказують на масштаби проблеми експерти.[21]

Безумовно, що використання відеонагляду у такий спосіб є порушенням законодавства, оскільки приховане відеоспостереження *«за особою, річчю або місцем»* можуть здійснювати лише правоохоронні структури і тільки у рамках кримінального провадження під час розслідування тяжких злочинів.

Необхідно пам'ятати і про те, що для публічного відеоспостереження заборонено використовувати спеціальні технічні засоби — устаткування, апаратуру, прилади, пристрої та інші вироби, спеціально створені, розроблені, запрограмовані або модернізовані для виконання завдань з приховуваного від людини отримання інформації. Відеокамера може бути віднесена до спеціального

[21] «Відеоспостереження за дотриманням публічного порядку в Україні», сайт Асоціації УМДПЛ

технічного засобу за певними конструктивними особливостями і якісними характеристиками, зокрема, у випадку мінімізації її розмірів, виконання у вигляді побутового предмету, пристосованості до швидкого або замаскованого розміщення на об'єкті тощо. Показово, що стаття 359 Кримінального кодексу України «Незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації» встановлює кримінальну відповідальність не тільки для осіб, які здійснюють приховане відеоспостереження з використанням цих засобів, а й для їх продавців.

Доступ особи до своїх персональних даних.

Закон України «Про захист персональних даних» не тільки гарантує право на доступ до своїх персональних даних, а й визначає засади отримання такого доступу — ***безоплатність*** *(стаття 19 Закону)* та ***невідкладність*** *(стаття 17 Закону)*. Отже кожна особа, при бажанні, повинна отримати можливість безперешкодно переглянути зроблене системою відео з її участю, при цьому плата за такі дії не береться, а відстрочення доступу особи до відео не допускається.

Крім цього, фігурант відеозапису має право отримати його копію, а також іншу інформацію, в тому числі щодо:

- мети, порядку та виду обробки своїх персональних даних;
- технічних параметрів системи відеоспостереження, як джерела збору персональних даних;
- своїх прав, як суб'єкта персональних даних;
- обов'язків володільця системи відеоспостереження у зв'язку з обробкою даних;
- порядку доступу до персональних даних та їх передачі третім особам;
- умов захисту даних;
- термінів зберігання даних, порядку їх видалення тощо.

Порядок надання доступу до персональних даних необхідно врегулювати відповідним внутрішнім документом, у якому визначити процедуру отримання інформації особами, чиї дані обробляються.

3.6. Професійна підготовка

Самі собою системи відеоспостереження не є загрозою для інформаційної безпеки — лише цілі та спосіб їх використання людиною можуть призвести до порушення законних прав та інтересів людини. Судження на кшталт «це відео з вулиць міста нікому не цікаве» є апріорі помилковим, адже у сучасному світі саме інформація вважається найбільш цінним ресурсом. Розуміючи значущість персональних даних, зловмисники вдаються до вторгнення у створювані системами інформаційні бази з метою викрадення, знищення, корегування чи підміни відеозаписів, змінюють налаштування або режим роботи обладнання для забезпечення їх роботи у власних незаконних інтересах.

Також часто деякі представники місцевої влади аргументують тим, що функціональні можливості встановлених камер не дозволяють ідентифікувати особу. Справа у тому, що камера — це пристрій, який безперервно пише інформацію про інфраструктуру певної місцевості, переміщення і скупченні людей, машин, військової техніки та інших об'єктів. Пристрій може бути встановлено як в парку, так і на режимному об'єкті, що, в результаті, показує цілісну картинку. Тому це вже вагомий аргумент того, що системи потрібно захищати від зловмисників і всіляко припиняти соціальну інженерію.

Працівники й працівниці мають не тільки знати вимоги внутрішніх розпорядчих актів, що встановлюють режимні обмеження та визначають порядок обробки інформації у системах, а й вільно орієнтуватись у положеннях національного та міжнародного законодавства у сфері захисту персональних даних. Навчальні за-

ходи необхідно планувати заздалегідь відповідно до попередньо розробленого графіку, а кожен факт проведення заняття має бути зафіксований у документах (план заняття, конспект, списки учасників тощо).

Вкрай важливо уникнути поверхового ставлення до навчання — у колективі всі мають усвідомити, що подібні заняття є важливою складовою підвищення професійного рівня і проводяться у їхніх інтересах. Під час занять потрібно акцентувати увагу слухачів на тому, що у надійному захисті персональних даних зацікавлене не тільки керівництво органу, а й вони самі і тому необхідність виконання заходів безпеки не повинна сприйматися як додаткове навантаження, безглузда та формальна повинність. Учасники та учасниці навчання мають чітко зрозуміти, що кожен випадок порушення норм законодавства про захист персональних даних може завдати серйозної шкоди установі, в якій вони працюють (репутаційні втрати, штрафи, судові позови).

Окрему увагу слід приділяти розбору конкретних прикладів порушення правил обігу персональних даних — кожний такий факт повинен стати предметом правового аналізу та обговорення на заняттях. Формуванню необхідного обсягу знань сприяє і направлення працівників на відповідні курси, їх участь у тренінгах чи семінарах, проведення занять із запрошенням фахівців, перевірка рівня професійної підготовки за допомогою тестування тощо. Правова грамотність, усвідомлення важливості застосування отриманих знань на практиці та мотивація до цього всього колективу дозволять отримати бажаний результат.

3.7. Особа, відповідальна за захист персональних даних

Стаття 24 Закону України *«Про захист персональних даних»* покладає на володільця персональних даних, в тому числі і на орган

місцевого самоврядування, обов'язок створити структурний підрозділ або призначити **відповідальну особу**, яка буде організовувати роботу, пов'язану із захистом персональних даних при їх обробці. Інформація про такий підрозділ чи відповідальну особу направляється Уповноваженому Верховної Ради України з прав людини, який, в свою чергу, забезпечує її оприлюднення.

Закон не висуває конкретних вимог до посади, рівня освіти, кваліфікації такої відповідальної особи, лише зазначає, що вона:

1. інформує та консультує володільця або розпорядника персональних даних з питань додержання законодавства про захист персональних даних;
2. взаємодіє з Уповноваженим Верховної Ради України з прав людини та визначеними ним посадовими особами його секретаріату з питань запобігання і усунення порушень законодавства про захист персональних даних.

Отже, при визначенні кандидатури відповідальної особи керівництво органу може приймати рішення на власний розсуд, але з урахуванням наступних нюансів:

- для уникнення конфлікту інтересів, особа має підпорядковуватись безпосередньо керівнику установи;
- особа повинна мати необхідні повноваження й ресурси для виконання покладених функцій з контролю за обробкою даних, а також виявлення та профілактики порушень у цій сфері;
- при необхідності, особа може доручити виконання частини своїх функцій іншим працівникам та працівницям органу.

Призначення відповідальної особи варто оформити відповідним наказом, з яким вона ознайомлюється під підпис. Факт покладання на особу нових обов'язків потрібно закріпити документально — зазначити це у її трудовому договорі та посадових обов'язках, а також у Політиці щодо обробки персональних даних в органі.

До функціональних обов'язків відповідальної особи доцільно віднести:

- контроль за проведенням заходів щодо захисту персональних даних;
- ведення обліку процесів обробки персональних даних та обліку осіб, які задіяні у цих процесах;
- створення, ведення та підтримання в актуальному стані відповідної документації;
- організацію та здійснення внутрішнього контролю за дотриманням законодавства про захист персональних даних;
- організацію та контроль за проведенням у колективі занять з тематики обробки та захисту персональних даних, а також оцінюванням отриманих знань;
- організацію прийому та розгляд звернень (запитів) суб'єктів персональних даних, а також запитів третіх осіб і Уповноваженого Верховної Ради України з прав людини;
- підготовку та своєчасну актуалізацію внутрішніх організаційно-розпорядчих документів у сфері захисту персональних даних;
- організацію та безпосередню участь у проведенні службових перевірок за фактами порушень вимог до обробки й захисту персональних даних, а також інших інцидентів інформаційної безпеки;
- підготовку органу до перевірок з боку контролюючих інстанцій та організаційне сприяння здійсненню таких перевірок (підготовку необхідних документів, інформації тощо);
- взаємодію з Уповноваженим Верховної Ради України з прав людини, іншими державними органами контролю та неурядовими громадськими організаціями у питаннях забезпечення прав, свобод і законних інтересів громадян під час обробки персональних даних.

Слід зауважити, що наведений перелік обов'язків не є вичерпним. У кожному окремому випадку для відповідальної особи необхідно визначити той обсяг повноважень, що дозволяє гарантувати належну обробку та надійний захист даних.


and let thy feet
millenniums hence
be set in midst of knowledge

Розділ 4.

Внутрішні процедури щодо безпеки даних

4.1. Загальні заходи

З одного боку, законодавство[22] покладає на володільців, розпорядників та третіх осіб обов'язок захищати персональні дані від незаконної обробки, доступу, випадкової втрати чи знищення, а з іншого — не деталізує правові інструменти та механізми здійснення такого захисту. За цих умов, перед кожним суб'єктом, постає важливе завдання: розробити власну політику безпеки, яка би передбачала реалізацію комплексу технічних й організаційних заходів із захисту персональних даних на всіх етапах їх обробки — отримання, накопичення, зберігання, використання, надання третім особам.

Немає єдиного універсального алгоритму впровадження таких заходів, адже процес їх розроблення вимагає врахування багатьох специфічних факторів — від мети здійснення відеоспостереження до кількості задіяного персоналу. Проте, у будь-якому випадку, ці заходи мають сприяти виконанню першочергових завдань, а саме:

- передбачити організаційно-технічні рішення, які мінімізують несанкціоноване втручання у роботу систем;
- звести до мінімуму ризики порушення законодавства під час роботи з даними;
- забезпечити прозорість їх обробки на всіх етапах;
- надати громадянам можливість контролювати обробку свої даних.

Як вже зазначалось раніше, всі процедури, правила й заборони щодо роботи з персональними даними мають бути прописані в організаційно-розпорядчих документах органу (положення, регламенти, інструкції тощо). Пакет таких внутрішніх директивних

[22] Стаття 24 Закону України «Про захист персональних даних»

документів необхідно підготувати ще до встановлення систем відеоспостереження, адже їх монтаж має здійснюватися з урахуванням заздалегідь визначених вимог до їх безпечного використання, а не навпаки, коли правила по убезпеченню даних «підганяються» під вже готові системи. Завжди слід пам'ятати, що кращий спосіб знизити ризики — це передбачити і не створювати їх. Власне у цьому і полягає суть концепції «Privacy by design», яка є частиною європейського права щодо захисту прав фізичних осіб при обробці їх персональних даних. Відповідно до неї, володілець систем відеоспостереження завчасно, на ранній стадії їх проєктування, зобов'язаний розробити та забезпечити функціонування механізмів захисту персональних даних в усіх операціях системи, пов'язаних із їх обробкою.

Зокрема, при розробці заходів із захисту інформації ще ***на початковому етапі необхідно визначити***:

1. Потенційні загрози для персональних даних та можливі джерела їх виникнення — без цього неможливе подальше планування заходів з усунення таких небезпек. Експерти вказують на існування багатьох способів незаконно «витягнути» дані з інформаційних систем, серед яких найбільш поширеними є:
    - заборонене копіювання даних;
    - проникнення в комп'ютери інших користувачів, іноді, з використанням чужих засобів ідентифікації (логінів, паролів, смарт-карт);
    - застосування програмних пасток;
    - використання дефектів програм і операційних систем;
    - застосування шкідливих програм;
    - нелегітимне підключення до мережі;
    - розкрадання носіїв даних;
    - фотографування екрану.

Визначення й формулювання загроз дасть можливість:

- провести загальний аналіз захищеності систем;
- здійснити модернізацію систем з метою мінімізації та (або) нейтралізації встановлених загроз;
- розробити інструменти запобігання несанкціонованому впливу на технічні засоби систем;
- вдосконалити методи контролю за захищеністю даних у системах.

2. Ризики спричинення шкоди, яку може бути заподіяно внаслідок порушення заходів безпеки під час обробки даних. Витік конфіденційної інформації про певну людину може призвести до серйозних інцидентів — від загрози її життю й здоров'ю до заподіяння матеріальної чи моральної шкоди. Тому дуже важливо завчасно прорахувати такі ризики, в залежності від роду отримуваної інформації та ступеню її конфіденційності, що дозволить запровадити співвідносні ризикам заходи безпеки.

3. Об'єкти в інформаційних системах, що підлягають захисту. В першу чергу до таких об'єктів слід віднести:

- персональні дані, що обробляються в інформаційній системі відеоспостереження;
- інформаційні ресурси систем (файли, відеоархіви, бази даних й т.д.);
- обчислювальну техніку та апаратне забезпечення, задіяне у процесах обробки даних;
- програмне (вбудоване, системне або прикладне) забезпечення, за допомогою якого здійснюється обробка даних в інформаційних системах;
- документацію, у тому числі технічну, справи чи облікові журнали, картотеки, реєстри, відео-, фото,- та інші матеріали, у яких зафіксована чи відображена інформація, що захищається;

- канали (лінії) зв'язку, включаючи кабельні системи;
- мережевий трафік;
- приміщення, в яких здійснюється обробка даних, знаходяться чи зберігаються ресурси інформаційних систем.

4. Оптимальні технічні параметри компонентів систем відеоспостереження, які повинні мати запобіжники від несанкціонованого доступу до інформації. При цьому, не слід обмежуватись аналізом характеристик лише відеокамер, оскільки до технічних засобів обробки персональних даних в інформаційних системах можна віднести:

- автоматизовані робочі місця користувачів з різними рівнями доступу (правами);
- термінальні станції (програмно-апаратні комплекси, які дозволяють здійснювати доступ користувачів до інформаційних систем);
- серверне обладнання (операційні системи фізичних серверів, віртуальних серверів, системи управління базами даних тощо), призначене для зберігання даних в інформаційних системах;
- мережеве та телекомунікаційне обладнання.

5. Технічні рішення, необхідні для захисту персональних даних, порядок та строки їх реалізації. Як правило, такі рішення передбачають:

- проектування системи захисту, розробку робочої та експлуатаційної документації;
- закупівлю, поставку, встановлення і налаштування технічних, програмних та програмно-технічних засобів захисту інформації;
- проведення дослідницької експлуатації засобів захисту

інформації в комплексі з іншими технічними й програмними засобами та відпрацювання технологічного процесу обробки даних;

- здійснення аналізу вразливості компонентів системи захисту даних та вжиття заходів щодо усунення виявлених недоліків у її роботі (при необхідності);
- визначення способу автоматичної фіксації будь-якого стороннього втручання у роботу систем відеоспостереження, в тому числі й несанкціонованого доступу до бази з відеоданими;
- проведення попередніх та приймальних випробувань системи захисту персональних даних перед її введенням в експлуатацію.

6. Заходи з нормативного, кадрового та режимного врегулювання питань інформаційної безпеки. До таких заходів можна віднести:

- підготовку пакета організаційно-розпорядчих документів щодо захисту інформації;
- встановлення форми реєстрації осіб, які офіційно отримували доступ до відеозаписів з персональними даними (хто, коли, з якою метою і на яких підставах);
- встановлення форм обліку зібраної або переглянутої відеоінформації із зазначенням цілей та підстав;
- визначення основних напрямків та методів здійснення контролю за роботою персоналу, який працює з персональними даними у системах відеоспостереження;
- складання переліку посадових осіб, на яких доцільно покласти відповідальність за захист персональних даних, в тому числі й за законність їх передачі та використання третіми особами;

- запровадження процедури ознайомлення персоналу з вимогами інформаційної безпеки при обробці даних, а також надання зобов'язання про нерозголошення відомостей, які стали відомі в результаті здійснення відеоспостереження;
- встановлення обмеженого режиму доступу до приміщень з технічним обладнанням;
- визначення оптимальних місць розташування «відеостін» з моніторами, для унеможливлення несанкціонованого перегляду зображень сторонніми особами.

Варто звернути увагу, що це далеко не повний перелік необхідних заходів. Цей Посібник, втім, як і будь-який інший, не може містити всеосяжних й вичерпних настанов за всіма аспектами захисту даних у різних ситуаціях та обставинах. А отже, при необхідності вирішення складних проблем, пов'язаних з безпекою обробки даних, доцільно додатково звернутись за консультаціями до фахівців у відповідній сфері.

4.2. Реєстр обробки даних у системі відеоспостереження

Технічні характеристики системи відеоспостереження повинні передбачати можливість фіксації всіх дій (їх сукупності) з обробки персональних даних, зокрема, по їх збиранню, реєстрації, накопиченню, зберіганню, адаптуванню, зміні, поновленню, використанню, передачі, поширенню, знеособленню та знищенню. Якщо система з тих чи інших причин не передбачає автоматичної фіксації, то реєстр обробки даних і будь-яка дія, в тому числі передача персональних даних третій особі, мають бути обов'язково зафіксовані іншим чином — в електронному та/або паперовому вигляді.

Реєстр обробки даних повинен включати, щонайменше, такі пункти:

- місце розміщення камери, дату й час отримання відеозапису;

- ім'я та посаду особи, яка здійснює обробку даних;
- інформацію про вид цієї обробки (збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення).

У випадку ***передачі даних третім особам*** у реєстрі фіксується:

- установчі дані особи (ім'я, посада та організація), яка запитує інформацію;
- повноваження, мета та підстави запиту третьої особи;
- стислий опис змісту переданих даних та їх обсяг;
- дата, час та спосіб передачі інформації;
- ім'я та посада відповідальної особи, яка поширила дані з систем відеоспостереження.

Особливу увагу необхідно звернути на те, що у реєстрі, крім офіційних дій з персональними даними, мають неодмінно **обліковуватись факти стороннього втручання** у роботу відеосистеми — всі спроби несанкціонованого отримання доступу до даних та інші інциденти безпеки відображаються у реєстрі незалежно від того, були вони успішними чи ні.

4.3. Накопичення та строк зберігання персональних даних

Під накопиченням персональних даних у системах відеоспостереження слід розуміти не лише формування бази відеофайлів, а й весь комплекс дій з їх відбору, систематизації та подальшого зберігання, під час якого має забезпечуватись цілісність отриманих даних та відповідний режим доступу до них[23].

[23] Стаття 13 Закону України «Про захист персональних даних»

Стаття 15 Закону України «Про захист персональних даних» вказує, що персональні дані підлягають видаленню або знищенню у разі:

1. закінчення строку зберігання, встановленого законом або згодою суб'єкта персональних даних на їх обробку;
2. припинення правовідносин між суб'єктом персональних даних та володільцем чи розпорядником, якщо інше не передбачено законом;
3. видання відповідного припису Уповноваженим Верховної Ради України з прав людини або визначеними ним посадовими особами секретаріату;
4. набрання законної сили рішенням суду щодо видалення або знищення персональних даних.

Персональні дані, зібрані з порушенням вимог цього Закону, підлягають видаленню або знищенню у встановленому законодавством порядку.

Слід зазначити, що нормативно-правові акти не встановлюють конкретних строків зберігання різних типів персональних даних — їх володільцю надається право самостійно визначити та обґрунтувати тривалість періоду перебування даних у його розпорядженні. Проте, це не означає, що інформацію з відеокамер спостереження можна накопичувати та архівувати про всяк випадок.

Нагадаємо, що одним з основних загальних принципів обробки персональних даних є принцип *«обмеження строку зберігання»*[24]. Він повною мірою поширюється і на правила зберігання даних у системах відеоспостереження — якщо відеозаписи дозволяють

[24] Пункт 2.2. «Принципи обробки персональних даних» розділу 2 цього Посібника

прямо чи опосередковано ідентифікувати людину-суб'єкта персональних даних, то вони зберігаються не довше, ніж це необхідно для досягнення цілей їх отримання та обробки. Такі вимоги є цілком логічними, оскільки довготривале зберігання даних завжди множить ризики їх втрати чи умисного викрадення.

Відеозаписи з камер спостереження можуть зберігатися більш тривалий час, якщо це необхідно для формування статистики, проведення наукових чи історичних досліджень або для забезпечення суттєвих інтересів громади. Термін зберігання відеоданих також може бути продовжений з метою розслідування зафіксованого інциденту безпеки, наприклад спроби передати окремі відеофайли стороннім особам. У будь-якому випадку можливі причини збільшення терміну зберігання записів повинні обумовлюватись у внутрішній політиці безпеки персональних даних, а реєстр дій з їх обробки має зберігатися і після видалення даних з системи відеоспостереження.

В інформаційних системах найбільш оптимальним варіантом реалізації принципу «обмеження строку зберігання» є застосування програм, які автоматично видаляють інформацію після завершення фінального етапу їх обробки чи визначеного терміну зберігання. Крім цього, автоматизація процесу знищення вже непотрібних відеозаписів дозволяє раціонально використовувати обсяги пам'яті на електронних носіях інформації, сприяє ефективному використанню робочого часу персоналом та мінімізує фактор «помилки виконавця».

4.4. Ідентифікація й автентифікація користувачів

При вирішенні завдань надійного збереження персональних даних у системах відеоспостереження, варто звернути увагу на питання щодо захисту цих систем від несанкціонованого досту-

пу. Для запобігання таким ситуаціям, доступ до роботи у системі відеоспостереження має отримати вузьке коло працівників, які мають відповідну кваліфікацію, і, відповідно до своїх службових обов'язків, несуть відповідальність за дотримання норм законодавства при роботі з персональними даними. Особи, які працюють із системами відеонагляду, можуть виконувати різні завдання — від спостереження за подіями на моніторах до технічного обслуговування чи програмного забезпечування діяльності системи, а тому і їх повноваження як користувачів доцільно розмежовувати відповідно до характеру покладених завдань. Вказане досягається наданням персоналу різних прав доступу у систему.

Для будь-якого входу у систему відеоспостереження, незалежно від категорії доступу, користувач повинен підтвердити своє право на це — пройти ***процедури ідентифікації та автентифікації***. *Ідентифікація* — це пред'явлення користувачем системі своїх індивідуальних та унікальних ідентифікаторів, як правило, логіну (реєстраційне ім'я) та паролю входу. В свою чергу *автентифікація* — це процедура впізнання системою наданих ідентифікаторів. Простіше кажучи, користувач через комп'ютер вводить у систему свій логін та пароль, отримавши які система проводить автентифікацію, порівнюючи їх з логіном та паролем, наявними у її базі даних, аби переконатися у тому, що користувач є тим, за кого себе видає. У випадку збігу, автентифікація вважається успішною, після чого система проводить авторизацію користувача та допускає його до роботи.

Правила безпеки під час використання пароля передбачають:

- збереження його конфіденційності;
- відсутність відображення пароля на екрані під час його введення;
- заборону використання одного пароля кількома користувачами;
- зміну пароля у випадку наявності ознак можливої компрометації системи або пароля;

- блокування доступу після кількох спроб невірного введення пароля;
- зберігання історії попередніх призначених для користувача паролів у формі hash (за попередній рік) і запобігання їхньому повторному використанню.

Ввівши логін та пароль входу у систему, користувач створює власний ***обліковий запис***. За допомогою таких записів відслідковується всі дії користувача у системі: час входу та виходу з неї, адресу використаного для цього комп'ютера, інтенсивність перебування у системі та проведені у ній операції. Для контролю облікових записів користувачів доцільно використовувати автоматизовані засоби реєстрації їх створення, активації, зміни, відключення тощо.

Так, ***реєстрація спроб входу/виходу*** користувачів із системи повинна фіксувати:

1) дату і час спроби входу/виходу;
2) ідентифікатор користувача;
3) результат спроби: успішна чи невдала.

Реєстрацію виконаних операцій необхідно здійснювати за такими параметрами:

1) дата і час виконання операції (найменування операції);
2) ідентифікатор користувача;
3) зміст операції (перегляд, коригування, запис, видалення і т. ін.);
4) результат спроби виконати операцію: успішна чи невдала.

Реєстрація зміни права доступу користувача має відобразити:

1) дату і час зміни повноважень;
2) ідентифікатор адміністратора, що здійснив зміни;
3) ідентифікатор користувача, його нові повноваження (рівень доступу) і статус.

У ролі ідентифікаторів користувача можуть застосовуватись не тільки логіни та паролі, а й мікропроцесорні карти або цифровий підпис. Але у будь-якому випадку, всі особи, які отримали доступ до обробки даних у системах відеоспостереження, включно з персоналом технічної підтримки, адміністраторами мережі, системними адміністраторами бази даних тощо, повинні мати свої унікальні індивідуальні ідентифікатори. Це надає можливість посилити контроль за діями персоналу у системі відеоспостереження і, при необхідності, встановити особу порушника правил обробки персональних даних. Коли посадова особа з тих чи інших причин вже не виконує обов'язків, пов'язаних з доступом до обробки персональних даних, її коди ідентифікації повинні бути невідкладно заблоковані. Те саме треба зробити при встановлені фактів зловживання користувачем правом доступу у систему відеоспостереження, а також, якщо коди передавались стороннім особам або не використовувались протягом тривалого часу.

4.5. Заходи фізичної безпеки

Безпека інформації у будь-якій інформаційній системі не в останню чергу залежить від оточення, в якому ця система функціонує, а тому комплексний захист персональних даних у системах відеоспостереження повинен передбачати заходи з *фізичної безпеки*, які спрямовуються на запобігання несанкціонованого доступу до службових приміщень, а також на збереження засобів обробки інформації.

До заходів фізичної безпеки відносяться:

1. ***Нормативне врегулювання.*** В органі мають бути розроблені та затверджені внутрішні документи, які визначають режимні правила та процедури під час обробки персональних даних.

2. *Режим доступу до приміщень.* Вхід до приміщень, де обробляється інформація з відеосистем, дозволяється лише особам, які мають відповідний рівень доступу. Особа може увійти до приміщення лише після проходження нею процедури ідентифікації і перевірки наявних для цього повноважень. Списки осіб, які отримали той чи інший рівень доступу, затверджуються керівником органу та своєчасно оновлюються.
3. *Моніторинг фізичного доступу до приміщень.* Доступ до приміщень має відслідковуватися за допомогою пристроїв відеоспостереження та сигналізації. При цьому доцільно застосовувати автоматизовані засоби, що розпізнають і фіксують порушення доступу до приміщень та повідомляють про них.
4. *Контроль за відвідувачами.* Всі відвідувачі підлягають реєстрації у відповідних журналах чи електронному реєстрі, із збереженням даних про них не менше, ніж протягом одного року. Для проведення реєстрації у приміщенні має бути виділена окрема зона. Відвідувачі отримують доступ до приміщень лише у робочий час, увесь період їх перебування на об'єкті вони супроводжуються особою з числа персоналу, яка контролює їх дії.
5. *Захист обладнання.* Обладнання має бути захищене так, щоби мінімізувати ризики несанкціонованого доступу до нього. Наприклад, слід унеможливити фотографування або перегляд сторонніми особами зображення на моніторах, зняття відеоінформації з комп'ютерів на флеш-накопичувач та інше. Має бути заборонено виносити з приміщень носії інформації та засоби обробки персональних даних. Кожна така спроба повинна бути зареєстрована і стати підставою для службового розслідування.

Крім цього, захист інформації передбачає виконання заходів, не пов'язаних напряму з можливістю стороннього втручання — протипожежний захист, захист від екологічних та техногенних катастроф, захист від перебоїв у подачі електроенергії тощо.

4.6. Доступ до персональних даних третіх осіб

Записи з систем відеоспостереження доволі часто стають предметом інтересу третіх осіб, які не беруть безпосередньої участі у їх обробці. Для вирішення питання можливості надання третім особам відеозаписів, насамперед слід встановити, чи містять вони персональні дані, а також з'ясувати наміри щодо їх подальшого використання. Це необхідно, оскільки умови та процедура надання третім особам доступу до персональних даних здійснюється їх володільцем не на власний розсуд, а лише у визначений законодавством спосіб та при наявності відповідних правових підстав.

Передусім, слід пам'ятати: **обов'язок забезпечити належний захист персональних даних у випадку їх поширення чи передачі, покладається на сторону, яка їх поширює чи передає.** Таким чином, коли муніципальний орган передає відеозапис з персональними даними, то саме цей орган несе повну відповідальність за те, яким чином цей запис буде використано у подальшому та чи не призведе це до порушення законодавства. Стаття 16 Закону України «Про захист персональних даних» наголошує: «доступ до персональних даних третій особі не надається, якщо зазначена особа відмовляється взяти на себе зобов'язання щодо забезпечення виконання вимог цього Закону або неспроможна їх забезпечити».

Ця ж стаття вказує, що «*порядок доступу до персональних даних третіх осіб визначається умовами згоди суб'єкта персональних даних на їх обробку, надану володільцю персональних даних, або відповідно до вимог закону*».

Передавання персональних даних третім особам здійснюється на офіційний запит останніх, при цьому у запиті, відповідно до статті 16 вищевказаного Закону, мають бути зазначені:

1. прізвище, ім'я та по батькові, місце проживання (місце перебування) і реквізити документа, що посвідчує фізичну особу, яка подає запит (для фізичної особи — заявника);
2. найменування, місцезнаходження юридичної особи, яка подає запит, посада, прізвище, ім'я та по батькові особи, яка засвідчує запит; підтвердження того, що зміст запиту відповідає повноваженням юридичної особи (для юридичної особи - заявника);
3. прізвище, ім'я та по батькові, а також інші відомості, що дають змогу ідентифікувати фізичну особу, стосовно якої робиться запит;
4. відомості про базу персональних даних, стосовно якої подається запит, чи відомості про володільця чи розпорядника даних;
5. перелік персональних даних, що запитуються;
6. мета та/або правові підстави для запиту.

Строк вивчення запиту на предмет його задоволення не може перевищувати *десяти робочих днів* з дня його надходження. Протягом цього строку орган має повідомити особу, яка подала запит, чи буде його задоволено або чому запитувані персональні дані не підлягають наданню (із зазначенням підстави). Запит ***задовольняється протягом тридцяти календарних днів*** з дня його надходження, якщо інше не передбачено законом.

Відстрочення доступу до персональних даних третіх осіб допускається у разі, якщо дані не можуть бути надані протягом тридцяти календарних днів з дня надходження запиту. При цьому, згідно зі статтею 17 Закону України «*Про захист персональних даних*», загальний термін вирішення питань, порушених у запиті, не може перевищувати ***сорока п'яти календарних днів***. Повідомлення про відстрочення доводиться до відома третьої особи, яка подала запит, у письмовій формі з роз'ясненням порядку оскарження такого рішення.

У повідомленні про відстрочення зазначаються:

- прізвище, ім'я та по батькові посадової особи;
- дата відправлення повідомлення;
- причина відстрочення;
- строк, протягом якого буде задоволено запит.

Ця ж стаття вказує, що ***третій особі може бути відмовлено у наданні персональних даних***, якщо доступ до них заборонено згідно із законом. Відмова оформлюється відповідним повідомленням, у якому зазначаються:

- прізвище, ім'я, по батькові посадової особи, яка відмовляє у доступі;
- дата відправлення повідомлення;
- причина відмови.

Рішення про відстрочення або відмову у доступі до персональних даних може бути оскаржено до Уповноваженого Верховної Ради України з прав людини або суду.

Порядок передачі персональних даних правоохоронним органам роз'яснений у листі Представника Уповноваженого Верховної Ради України з прав людини від 28.12.2015 року «Щодо правових підстав передачі персональних даних правоохоронним органам»[25], в якому вказується: *«належною підставою для отримання правоохоронними органами доступу до персональних даних в рамках кримінального провадження є ухвала слідчого судді, суду про тимчасовий доступ до речей і документів. Усі інші запити на доступ до персональних даних мають розглядатися індивідуально з огляду на повноваження запитувача, підстави запиту, обсяг запитуваної інформації тощо»*.

[25] *http://www.ombudsman.gov.ua/ua/publication/petition/schodo-pravovix-pidstav-peredachi-personalnix-danix-pravooxoronnim-organam/*

Доступ третіх осіб до персональних даних може бути платним — оплаті підлягає робота, пов'язана з обробкою персональних даних, консультуванням та організацією доступу до них.

Володілець персональних даних ***протягом десяти робочих днів*** має повідомити суб'єкта персональних даних про їх передачу третій особі, якщо цього вимагають умови його згоди або інше не передбачено законом. Проте, ***таке повідомлення не здійснюються***:

1) у разі передачі персональних даних за запитами при виконанні завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом;
2) під час виконання органами державної влади та органами місцевого самоврядування своїх повноважень, передбачених законом;
3) якщо персональні дані обробляються в історичних, статистичних чи наукових цілях;
4) коли суб'єкт персональних даних ще під час їх збору був повідомлений про третіх осіб, яким можуть бути передані його дані.

Під ***поширенням персональних даних*** розуміють дії з передавання відомостей про фізичну особу за її згодою. Стаття 14 Закону України «*Про захист персональних даних*» встановлює наступні правила їх поширення:

- поширення персональних даних без згоди суб'єкта персональних даних або уповноваженої ним особи дозволяється у випадках, визначених законом, і лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту та прав людини;
- виконання вимог встановленого режиму захисту персональних даних забезпечує сторона, що поширює ці дані;
- сторона, якій передаються персональні дані, повинна попередньо вжити заходів щодо забезпечення вимог законодавства про їх захист.

На завершення можна додати, що одним зі способів уникнути порушень при поширенні відеозаписів є проведення їх знеособлення.

4.7. Інциденти безпеки та їх адміністрування

Захист персональних даних у системах відеоспостереження передбачає роботу з виявлення та реєстрації інцидентів інформаційної безпеки, а також здійснення профілактичних заходів з їх попередження. Під терміном ***«інцидент безпеки»*** розуміють подію небажаного чи неочікуваного характеру, яка здатна негативно вплинути на інформаційну безпеку в системі, зруйнувати або знизити рівень захищеності персональних даних. До інцидентів безпеки можна віднести будь-які негативні випадки, що загрожують процесам обробки відеозаписів — від залишення користувачем на робочому місці папірця з паролем входу у систему до хакерської атаки для знищення відеофайлів.

Серед найбільш поширених видів інцидентів безпеки, можна виділити:

- неавторизований або несанкціонований доступ третіх осіб до інформаційної системи;
- відмова обладнання через причини технічного характеру;
- порушення роботи програмного забезпечення;
- недотримання персоналом режимних правил обробки, зберігання, передачі інформації;
- виявлення фактів зовнішнього моніторингу або встановлення контролю над роботою системи чи окремих її елементів;
- ураження вірусами або іншими шкідливими програмами;
- будь-яка компрометація системи, наприклад, «зламування» та оприлюднення пароля облікового запису;

- порушення порядку взаємодії з Інтернет-провайдерами, хмарними сервісами та іншими постачальниками телекомунікаційних послуг.

Оскільки за визначенням інцидентом безпеки є несанкціонована подія (дія) під час обробки персональних даних, виникає потреба у чіткому розмежуванні подій (дій) на дозволені та заборонені. Наприклад, вхід у систему відеоспостереження під обліковим записом іншого співробітника є очевидним інцидентом безпеки, але він не буде зафіксований як інцидент, якщо це офіційно не заборонено і персонал вважає таку поведінку загальноприйнятою у зв'язку з дефіцитом кадрових ресурсів. Частина інцидентів може бути малопомітними, проте вони не повинні залишатися поза увагою, адже частота появи і загальна кількість інцидентів є одним із показників ефективності захисту персональних даних. В окремих випадках почастішання таких подій може свідчити про умисну атаку на систему відеоспостереження і вимагати невідкладного підвищення рівня її захисту.

Враховуючи це, всі зафіксовані інциденти безпеки мають бути класифіковані за ступенем загрози, описані, піддані всебічному аналізу для розроблення заходів з усунення причин їх виникнення у подальшому. Такі завдання досягаються адмініструванням інцидентів безпеки, механізм здійснення якого встановлюється відповідним внутрішнім документом — регламентом.

Адміністрування інцидентів безпеки.

Адміністрування інцидентів інформаційної безпеки базується на наступних діях:

1. *Встановлення* — з урахуванням викладених у регламенті критеріїв, визначається, чи є певна подія (дія) інцидентом безпеки.

2. *Реагування* — в особливих випадках інциденти безпеки вимагають невідкладного реагування, наприклад, відключення обладнання, блокування передачі інформації чи припинення контакту з провайдером. Причини для такого реагування, механізм здійснення та відповідальні за його оперативну реалізацію повинні бути заздалегідь визначені у регламенті.

3. *Оповіщення* — якщо подія (дія) ідентифікована як інцидент, персонал інформує про нього, за встановленою регламентом формою, відповідну посадову особу (керівника органу, начальника служби безпеки тощо).

4. *Реєстрація* — факт встановлення інциденту безпеки фіксується офіційно у реєстрі, журналі або у інший спосіб, передбачений регламентом.

5. *Усунення причин і наслідків* — вжиття невідкладних заходів з припинення впливу інциденту безпеки на обробку персональних даних та відновлення їх належного захисту. При цьому слід враховувати те, що такі заходи не повинні знищувати докази, які необхідні для проведення розслідування причин виникнення інциденту та дозволяють виявити винуватця.

6. *Розслідування* — вивчення умов та обставин, що зумовили або сприяли виникненню інциденту безпеки. Під час розслідування потрібно:
   - встановити причини виникнення інциденту і недоліки у директивних документах, які зробили його можливим;
   - зібрати і оформити докази та інші фактичні дані, які підтверджують факт інциденту;
   - встановити мотиви скоєння інциденту та винуватих осіб, чиї умисні дії або халатність призвели до інциденту;
   - виявити замовника інциденту та можливу причетність до нього сторонніх осіб;
   - встановити наслідки інциденту та нанесену ним шкоду.

В рамках розслідування перевіряються реєстри, журнали обліку, аналізуються дії користувачів і адміністраторів, які мали доступ до систем в період виникнення інциденту безпеки, та здійснюються інші необхідні дії із встановлення істини. За результатами розслідування готується протокол або акт комісії, а у випадку, коли в інциденті встановлені ознаки скоєння правопорушення, про нього повідомляються правоохоронні органи, куди передаються матеріали розслідування.

7. *Превенція* — реалізація заходів, які унеможливлюють або мінімізують ризики повторного виникнення подібної ситуації. Крім того, з урахуванням обставин виникнення інциденту безпеки та його наслідків, приймається рішення про застосування до винуватців заходів дисциплінарного впливу згідно із законодавством про працю.

8. *Аналітика* — ґрунтовний аналіз інциденту безпеки, на підставі якого здійснюється загальне вдосконалення захисту персональних даних у системі відеоспостереження.

4.8. Внутрішній контроль та аудит заходів безпеки персональних даних

Надійний захист персональних даних у системах відеоспостереження неможливий без здійснення внутрішнього контролю, який часто залишається поза увагою, і цей напрямок управлінської діяльності сприймається як формальний обов'язок. Проте, таке судження є помилковим, оскільки належним чином вибудована система внутрішнього контролю дозволяє отримати реальне уявлення про стан безпеки персональних даних у системах відеоспостереження, сприяє своєчасному виявленню, усуненню й попередженню порушень та загроз у цій сфері.

Внутрішній контроль дозволяє оцінити:

- відповідність процесів обробки персональних даних вимогам законодавства та внутрішніх розпорядчих документів;
- ефективність запровадженої системи захисту даних;
- стан дотримання внутрішньої політики органу при роботі з персональними даними;
- повноту виконання завдань обробки даних та досягнення поставлених цілей;
- доцільність, у тому числі й економічну, використаних ресурсів і засобів обробки персональних даних та їх захисту;
- правильність та результативність раніше прийнятих управлінських рішень.

Внутрішній контроль може здійснюватися керівництвом установи, окремою відповідальною особою або затвердженим колегіальним органом (наприклад, комісією). Разом з тим, у проведенні контролю не повинні брати участь посадові особи, які тим чи іншим чином зацікавлені у його результатах.

До основних ***складових внутрішнього контролю*** за станом захисту персональних даних можна віднести:

- перевірку коректності процесів обробки персональних даних;
- перевірку стану реалізації організаційних і технічних заходів із захисту персональних даних;
- перевірку своєчасності внесення змін до проектної, експлуатаційної та організаційно-розпорядчої документації щодо забезпечення безпеки даних в системах відеоспостереження;
- перевірку обліків та реєстрів, пов'язаних з обробкою персональних даних;

- перевірку повноти виконання персоналом вимог до захисту безпеки даних;
- аналіз стану захищеності інформації, яка обробляється в системах;
- розроблення та впровадження заходів із усунення виявлених порушень правил роботи з персональними даними та їх наслідків.

Робота з організації, впровадження та оцінювання якості внутрішнього контролю має носити плановий характер, для чого відповідальна особа розробляє та затверджує у керівника органу відповідний план. План може складатися на поточний рік у довільній формі і повинен визначати: об'єкти контролю (процеси, підрозділи, системи тощо); заходи та періодичність (терміни) їх проведення; способи та інструменти виконання передбачених заходів; відповідальних осіб.

У плані доцільно передбачити заходи, що дозволяють перевірити:

- наявність класифікації інформації, що обробляються в системах;
- правові підстави обробки персональних даних;
- законність реальних цілей обробки та їх відповідність офіційно проголошеним;
- загальний стан дотримання прав суб'єктів персональних даних;
- внутрішню документацію, яка врегульовує процеси обробки даних;
- порядок обліку авторизованих користувачів у системі;
- форму і повноту ведення електронних реєстрів;
- критерії, за якими здійснюється доступ персоналу до персональних даних;

- дотримання персоналом «парольної безпеки» та встановлених процедур доступу (ідентифікації й автентифікації) у системи відеоспостереження;
- відповідність рівнів допусків співробітників їх повноваженням;
- технічні ресурси та програми, які використовуються у процесах обробки;
- порядок та умови використання технічних засобів захисту інформації під час обробки даних;
- механізми виявлення випадків несанкціонованого доступу до обробки персональних даних;
- порядок фіксації інцидентів безпеки при обробці персональних даних;
- терміни зберігання персональних даних (відповідно до наказу Міністерства юстиції України від 12.04.2012 №578/5);
- порядок видалення та знищення відеозаписів із системи відеоспостереження;
- порядок зберігання та знищення носіїв персональних даних;
- стан резервного копіювання програмних засобів, архівів, реєстрів, журналів, інформаційних активів, які використовуються і створюються в процесі експлуатації систем відеоспостереження;
- регулярність оновлення засобів антивірусного захисту (актуальність вірусних баз);
- обізнаність персоналу з вимогами законодавства та внутрішніх директивних документів, що регламентують обробку та захист персональних даних;
- наявність та актуальність повідомлення Уповноваженого ВРУ з прав людини про здійснення обробки чутливої категорії даних;

- дотримання вимог законодавства під час надання відповідей на звернення суб'єктів персональних даних та третіх осіб;
- порядок поширення та/або передачі персональних даних третім особам;
- ефективність застосування заходів фізичної безпеки (режим доступу у службові приміщення, справність систем сигналізації, внутрішнього відеомоніторингу та інше).

В той же час, окремі перевірки можуть проводитись і поза планом, передусім, як засіб реагування на неординарні ситуації. Рішення про створення комісії та проведення позапланової перевірки обов'язково ухвалюється для розслідування інциденту інформаційної безпеки або у випадку виявлення недоліків у захисті персональних даних зовнішніми контролюючими органами.

Як **інструменти здійснення внутрішнього контролю** слід використовувати:

- опитування та співбесіди з персоналом;
- огляд робочих місць працівників, використовуваного ними обладнання та програмного забезпечення;
- перевірку відповідних реєстрів та службової документації;
- тестування технічних засобів обробки та захисту персональних даних;
- штучне моделювання інцидентів інформаційної безпеки та виникнення виняткових ситуацій.

За результатами кожної перевірки готується відповідний звіт, у якому зазначаються:

- вид перевірки (планова / позапланова), підстави та цілі її проведення;
- перелік проведених під час перевірки заходів;

- опис встановлених порушень та недоліків, стислий аналіз причин їх наявності;
- висновок про стан безпеки персональних даних та рекомендації з усунення виявлених прорахунків.

Звіт з результатами перевірки передається керівництву органу для реагування.

Ефективним засобом контролю за дотриманням норм законодавства при обробці персональних даних є ***зовнішній аудит інформаційної безпеки***, який дає можливість більш об'єктивно оцінити рівень захисту даних у системах відеоспостереження та визначити потенційні загрози для них. Аудит полягає у ґрунтовному вивченні стану безпеки інформації у системі за допомогою фахівців, які надають відповідні консалтингові послуги. Чисельність та склад групи фахівців залежить від мети і завдань аудиту, а також від технічних і програмних особливостей системи відеоспостереження.

Форми й методи проведення аудиту можуть бути різними, проте у будь-якому випадку вони завжди відповідають наступному алгоритму:

- визначення цілей та рамок здійснення аудиту;
- формування завдань та розроблення регламенту з їх виконання;
- безпосереднє проведення аудиту;
- узагальнення та аналіз отриманих даних;
- підготовка рекомендацій за результатами аналізу;
- оформлення аудиторського звіту.

Одним із найбільш важливих завдань аудиту є оновлення переліку подій, які визнаються інцидентами безпеки, та отримання рекомендацій щодо засобів і методів з їх запобігання. З результатами та висновками аудиту інформаційної безпеки ознайомлюється лише певне коло осіб, зокрема ініціатори його проведення (ке-

рівництво органу, служба безпеки чи інформаційних технологій), оскільки отримана, узагальнена та проаналізована під час аудиту інформація також потребує захисту від несанкціонованого доступу.

Додаток 1

Джерела правового регулювання захисту персональних даних

1. Стаття 32 Конституції України.
2. Стаття 12 Загальної декларація прав людини.
3. Стаття 17 Міжнародного Пакту про громадянські і політичні права ратифікованого Указом Президії Верховної Ради УРСР №2148-VIII (2148-08) 1973 року).
4. Стаття 8 Конвенції про захист прав людини і основоположних свобод.
5. Конвенція Ради Європи про захист осіб у зв'язку автоматизованою обробкою персональних даних. В липні 2010 року Україна ратифікувала Конвенцію Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додатковий протокол до неї.
6. Директива №2002/58/ЄС Європейського Парламенту і Ради ЄС «Про обробку персональних даних та захист таємниці сектора електронних комунікацій».
7. Директива №95/46/ЄС Європейського Парламенту і Ради ЄС «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року.
8. Закон України «Про захист персональних даних».

9. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».

10. Стаття 188-39 «Порушення законодавства у сфері захисту персональних даних» та стаття 188-40 «Невиконання законних вимог Уповноваженого Верховної Ради України з прав людини» Кодексу України про адміністративні правопорушення.

11. Стаття 182 «Порушення недоторканності приватного життя» Кримінального кодексу України.

12. Рішення Конституційного Суду України №2-рп/2012 від 20 січня 2012 року.

13. Типовий порядок обробки персональних даних (затверджений наказом Уповноваженого Верховної Ради України з прав людини «Про затвердження документів у сфері захисту персональних даних» від 08.01.2014 №1/02-14).

14. Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних.

15. Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації.

Додаток 2

**Положення норм законів,
що регулюють відповідальність
у сфері захисту персональних даних**

Стаття 188-39 КУпАП. Порушення законодавства у сфері захисту персональних даних.

Неповідомлення або несвоєчасне повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних або про зміну відомостей, які підлягають повідомленню згідно із законом, повідомлення неповних чи недостовірних відомостей —

тягнуть за собою накладення штрафу на громадян від ста до двохсот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян — суб'єктів підприємницької діяльності — від двохсот до чотирьохсот неоподатковуваних мінімумів доходів громадян.

Невиконання законних вимог (приписів) Уповноваженого Верховної Ради України з прав людини або визначених ним посадових осіб секретаріату Уповноваженого Верховної Ради України з прав людини щодо запобігання або усунення порушень законодавства про захист персональних даних —

тягнуть за собою накладення штрафу на громадян від двохсот до трьохсот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян — суб'єктів підприємницької діяльності — від трьохсот до однієї тисячі неоподатковуваних мінімумів доходів громадян.

Повторне протягом року вчинення порушення з числа передбачених частинами першою або другою цієї статті, за яке особу вже було піддано адміністративному стягненню, —

тягне за собою накладення штрафу на громадян від трьохсот

до п'ятисот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян — суб'єктів підприємницької діяльності — від п'ятисот до двох тисяч неоподатковуваних мінімумів доходів громадян.

Недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних, —

тягне за собою накладення штрафу на громадян від ста до п'ятисот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян — суб'єктів підприємницької діяльності — від трьохсот до однієї тисячі неоподатковуваних мінімумів доходів громадян.

Повторне протягом року вчинення порушення, передбаченого частиною четвертою цієї статті, за яке особу вже було піддано адміністративному стягненню, —

тягне за собою накладення штрафу від однієї тисячі до двох тисяч неоподатковуваних мінімумів доходів громадян.

У контексті взаємин володільців персональних даних з Уповноваженим, буде доречним нагадати й про те, що будь-яке невиконання законних вимог Уповноваженого або його представників карається накладенням штрафу на посадових осіб від ста до двохсот неоподатковуваних мінімумів доходів громадян *(стаття 188-40 КУпАП. «Невиконання законних вимог Уповноваженого Верховної Ради України з прав людини»)*.

Слід зазначити, що за певних обставин порушення порядку обробки персональних даних конфіденційного характеру може призвести до **кримінальної відповідальності** за статтею 182 Кримінального кодексу України (КК України).

Стаття 182 КК України. Порушення недоторканності приватного життя

Незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації, крім випадків, передбачених іншими статтями цього Кодексу, —

> караються штрафом від п'ятисот до однієї тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або арештом на строк до шести місяців, або обмеженням волі на строк до трьох років.

Ті самі дії, вчинені повторно, або якщо вони заподіяли істотну шкоду охоронюваним законом правам, свободам та інтересам особи, —

> караються арештом на строк від трьох до шести місяців або обмеженням волі на строк від трьох до п'яти років, або позбавленням волі на той самий строк.

Примітка. Істотною шкодою у цій статті, якщо вона полягає у заподіянні матеріальних збитків, вважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян.

У науково-практичному коментарі[26] до вказаної статті наголошується, що предметом злочину є саме конфіденційна інформація про особу. Зміст такої інформації складають відомості про приватне життя особи, зокрема і інформація про освіту, сімейний стан, релігійність, стан здоров'я, майновий стан та інші персональні дані людини. Під приватним життям розуміється сфера життєдіяльності окремої особи, яка включає в себе її зв'язки з іншими людьми, приватні справи, сімейні стосунки тощо, тобто все, що пов'язане з її способом життя і не має публічного характеру. Закон зобов'язує зберігати в таємниці відомості про громадян, які стали відомі у зв'язку із здійсненням професійної чи службової діяльності.

[26] Мельник М.І., Хавронюк М.І., «Коментарі до Кримінального кодексу України», «Народний правовий портал»

Конфіденційною не може визнаватися інформація, яка вже раніше була оприлюднена шляхом публікації, повідомлення в засобах масової інформації чи іншим способом.

Варто мати на увазі, що за законом інформація з обмеженим доступом може бути поширена без згоди її власника, якщо ця інформація є суспільно значимою, тобто якщо вона є предметом громадського інтересу і якщо право громадськості знати цю інформацію переважає право її власника на її захист. Поширення такої інформації, незважаючи на її конфіденційність, не утворює складу злочину, передбаченого статтею 182 КК України.

Порушення недоторканності приватного життя можуть проявлятися у наступних формах:

1) незаконне збирання конфіденційної інформації про особу;
2) незаконне зберігання такої інформації;
3) незаконне її використання;
4) незаконне поширення конфіденційної інформації про особу;
5) поширення її у публічному виступі, творі, що публічно демонструється, чи в засобах масової інформації.

Усі ці дії утворюють склад злочину, передбаченого ст. 182, лише у випадку, **якщо вони здійснюються без згоди особи, якої вони стосуються**.

Збирання конфіденційної інформації про особу передбачає її отримання у будь-який спосіб.

Під *зберіганням* слід розуміти збереження та накопичення конфіденційної інформації у певному місці на будь-яких носіях (паперових, електронних, відео тощо). Незаконним слід визнавати і зберігання зібраної у встановленому законом порядку інформації понад визначені терміни.

Використання конфіденційної інформації про особу — це користування за власним розсудом відомостями, які становлять особисту чи сімейну таємницю особи, для задоволення певної потреби чи одержання вигоди.

Під *поширенням* конфіденційної інформації слід розуміти повідомлення будь-яким способом (усно, письмово, друкованим способом, за допомогою комп'ютерної мережі тощо) такої інформації невизначеному числу осіб (хоча б одній людині).

Публічний виступ — це виступ на заходах публічного характеру (зборах, конференціях, з'їздах, мітингах, симпозіумах, круглих столах тощо).

Поширення її у творі, що публічно демонструється, означає повідомлення конфіденційної інформації про особу у плакатах, гаслах, картинах, фотографіях тощо, які виставлені для публічного ознайомлення, демонстрацію відео тощо.

Збирання, зберігання, використання або поширення конфіденційної інформації про особу вважається незаконними тоді, коли ці дії здійснюються з порушенням встановленого законом порядку. Поширення її у публічному виступі, творі, що публічно демонструється, чи в засобах масової інформації є незаконним завжди, коли це здійснюється без згоди особи, якої вона стосується.

У разі, коли недоторканність приватного життя була порушена службовою особою в результаті службової недбалості, *то за наявних для того підстав вчинене може бути кваліфіковане за статтею 367 КК України «Службова недбалість»*.