письмової згоди фізичної чи юридичної особи; розробити кодекс України про захист персональних даних.

Список використаних джерел:

1. Костенко І. В. Проблеми правового захисту персональних даних у діяльності Національної поліції. Юридичний часопис Національної академії внутрішніх справ. 2018. № 1 (15). С. 296–302.
2. Про захист персональних даних. Закон України від 1 черв. 2010 р. № 2297-VI. URL: http://zakon1.rada.gov.ua/laws/show/2297-17.
3. Про Національну поліцію. Закон України від 2 лип. 2015 р. № 580-VIII. URL: http://zakon1.rada.gov.ua/laws/main/580-19.

УДК 004.056

КСЕНІЯ ОЛЕКСАНДРІВНА КРАТАСЮК
курсант 4 курсу факультету №4 Харківського національного університету внутрішніх справ
ВОЛОДИМИР ВОЛОДИМИРОВИЧ ТУЛУПОВ
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

ПИТАННЯ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВТОРГНЕНЬ В СУЧАСНИХ СИСТЕМАХ ВІДЕОСПОСТЕРЕЖЕННЯ

На теперішній час в Україні на державному та регіональних рівнях впроваджуються різні програми, проекти та заходи публічної безпеки. Так, у більшості міст в Україні створюються проекти забезпечення публічної безпеки й порядку та протидії злочинності. Наприклад, у місті Києві в рамках проекту Kyiv Smart City «Безпечне місто» у загальноміській системі відеоспостереження працює 5823 камер та створені програмні модулі розпізнавання обличчя і номерів автомобілів. Також відкрито три ситуаційні центри та налагоджена взаємодія з оперативними частинами МВС та СБУ. У майбутньому до системи підключать пожежну, рятувальну, медичну, дорожню й інші комунальні та державні служби [2].

Серед завдань таких проектів і програм є: удосконалення науково-методичного, матеріально-технічного та інформаційного забезпечення правоохоронних та інших органів, що беруть участь у забезпеченні публічної безпеки та порядку; безперервний моніторинг криміногенної ситуації в області, в т.ч. за рахунок соціологічних технологій та забезпечення своєчасного реагування на негативні зміни; здійснення посиленого контролю за ситуацією у публічних місцях, передусім при проведення заходів за участю значної кількості громадян; запобігання правопорушенням, що вчиняються з використанням телекомунікаційних мереж та мережі Інтернет.

На теперішній час у системі Міністерства внутрішніх справ впроваджено низку аналітичних систем з можливістю проведення глибокого

аналізу великих масивів інформації, включаючи відкриті джерела де на першому рівні є система відеомоніторингу наприклад - єдиний аналітичний сервісний центр (UASC) поліції, створений за прикладом системи безпеки Абу-Дабі при ГУНП в Донецькій області [1, с. 271].

При створенні технічного завдання для проектування оптимальної системи відеоспостереження слід розглянути типові технології побудови таких систем, їх переваги та недоліки.

Кожна мережева відеокамера, якщо ми використовуємо IP-камери має свою власну IP-адресу, обчислювальні функції та вбудоване ПЗ, що дозволяє їй функціонувати як повноцінний мережевий пристрій.

На відміну від аналогової відеокамери, IP-камера не потребує прямого підключення до комп'ютера або до будь-яких інших апаратних або програмних засобів. Її підключення може здійснюватися як за допомогою дротяного з'єднання (по міді або оптичному волокну), так і безпровідного (Wi-Fi, GPRS/EDGE, 3G, 4G, супутниковому зв'язку та ін.). Таким чином, досягається повна або часткова мобільність користувача, який здатний стежити за видаленими об'єктами практично з будь-якої точки земної кулі.

Тому слід виділити наступні переваги таких систем IP – відеоспостереження, а саме:

1. Оператор системи може здійснювати візуальний контроль як локально, так і віддалено (з ПК, мобільного телефону і так далі), здійснювати функції адміністрування системи відеоспостереження використовуючи переваги веб-технологій.

2. Спрощеність та малі витрати на встановлення й монтаж. Мережеві відеосистеми IP не вимагають прокладення додаткового коаксіального кабелю, як в аналогових системах, а підключаються до існуючої локальної мережі відеоспостереження за об'єктом з допомогою безпровідних технологій.

3. Якість відеозображення. В сучасних IP-системах застосовується формат MPEG-4, який дозволяє ефективніше використовувати ресурси мережі в порівнянні з форматом M-JPEG.

4. Можливість передавати по одній лінії зв’язку не лише відеосигнал, але й звук, а також управляти та адмініструвати IP-камери.

5. Гнучкість й масштабованість систем IP- відеоспостереження полягає в можливості будівництва фізично розподілених мереж відеомоніторингу, контролю і дистанційного керування без прив'язки до відстані.

6. Інтеграція з багатьма існуючими на даний момент системами відеоспостереження.

Критеріями вибору на користь IP – камер при проектуванні таких систем на теперішній час також є [3]:

– наявність каналу зв’язку з високою пропускною спроможністю від 100 Мб/с і вище та вільних портів Ethernet;

– за рахунок вбудованих в камери WEB серверів при рішенні завдань моніторингу контрольованого об'єкту (без використання архівної інформації) з використанням мережі Інтернет;

– завдання вимагають високого розділення, при невисоких вимогах до освітленості, розміру кадру та ін. (З дозволом більш 1 Мп).

Виходячи з проведеного аналізу існуючих на ринку готових систем відеоспостереження, найбільш перспективними технологіями відеоспостереження є IP–відеоспостереження, яке легко розгортається та базується на сучасних комп'ютерних мережах стандарту Ethernet.

Нормальне функціонування комп'ютерних мереж та її складових таких як мережеві екрани, брандмауери, фаєрволи, системи резервного копіювання, антивірусні засоби та інші) неможливо без стандартних засобів захисту, тому існує необхідність використання IDS (СВВ – систем виявлення вторгнень), які є основним засобом боротьби з мережними атаками [4].

Системи виявлення вторгнень починають усе ширше впроваджуватися в практику забезпечення безпеки корпоративних мереж які у свою чергу можуть використовувати системи IP-відеоспостереження.

Список використаних джерел:

1. Тулупов В. В., Колісник Т.П. Особливі питання захисту систем IP-відеоспостереження. Актуальні питання протидії кіберзлочинності та торгівлі людьми: зб. матеріалів Всеукр. наук. – практ. конф. (23 листопада 2018 р., м. Харків) / МВС України , Харків. нац. ун-т внутр. справ; Координатор проектів ОБСЄ в Україні. ХНУВС, 2018. С. 270–274.

2. Kyiv Smart City. URL: https://www.kyivsmartcity.com/projects/safe-city.

3. Системи відеоспостереження (CCTV). URL: https://guard-lviv.com.ua/uk/sistemi-videonablyudeniya/index.html.

4. Intrusion Detection System (IDS). URL: https://ru.wikipedia.org/wiki/IDS.

УДК 343.98

ПЕТРО СЕРГІЙОВИЧ КЛІМУШИН
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій і кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ
АРТУР ГЕННАДІЙОВИЧ ПЛАКСЮК
курсант 3 курсу факультету № 4 Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ БІОМЕТРИЧНИХ ДАНИХУ ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Поява біометричних механізмів ідентифікації включає в себе кілька різних технологій, які з певних вимірюваних характеристик з високою часткою ймовірності ідентифікують конкретну людину. До таких технологій належать фото- та відеосистеми розпізнавання осіб, голосів, відбитків пальців, райдужної оболонки, сітківки ока, ДНК та ін. [1].