– 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].

Всі вони можуть застосовуватися комплексно або окремо і зараз в основному є додатковим чинником безпеки у діяльності правоохоронних органів. Світовий досвід показує, що мультибіометрія (розпізнавання особи відразу за кількома індивідуальними характеристиками – за обличчям, голосом або відбитками пальців) можлива при використанні смартфона як терміналу, через який підтверджується транзакція.

Біометрію вигідно використовувати в комбінації з іншими способами ідентифікації особи без обмежень, оскільки плюси є очевидними: авторизація за біометричними характеристиками відбувається швидко, вона зручна і має високий ступінь захисту. Крім того, саме ідентифікацію за обличчям доцільно застосовувати не тільки для підтвердження доступу до персональних баз даних, а й у внутрішній роботі правоохоронного органу, на-приклад при доступі до службових кімнат.

Для широкого втілення біометричних технологій на всіх рівнях у діяльності правоохоронних органів необхідно формування єдиної бази біометричних даних осіб, але сьогодні така база у необхідному обсязі поки що відсутня. Але прогнози говорять, що в перспективі п'яти-восьми років біометрична ідентифікація стане основним способом підтвердження особи у діяльності правоохоронних органів. Поки ж будуть використовуватися в сукупності кілька способів ідентифікації особи одночасно.

В Україні застосовуються такі біометричні дані (параметри) як відцифровані відбитки пальців рук, відцифроване зображення обличчя. При цьому, *біометрична ідентифікація* – здійснення пошуку за принципом “один до багатьох” шляхом розпізнавання і зіставлення одного або двох біометричних даних (параметрів) особи з біометричними даними (параметрами) осіб у відомчих інформаційних системах суб’єктів національної системи; *біометрична верифікація* – здійснення пошуку за принципом “один до одного” між біометричними даними (параметрами), отриманими від особи в даний момент, і біометричними даними (параметрами), наявними у відомчих інформаційних системах суб’єктів національної системи [1].

У контексті протидії злочинності, переваги застосування документів з персональними біометричними даними забезпечують: більш високий ступінь захисту від підробки; можливість автоматичної перевірки приналежності власника документу, що скорочує час на ідентифікацію особистості, збільшує швидкість даної процедури і виключає суб'єктивізм при оцінці її результатів; значний технологічний потенціал даного документа, тобто на чіп, крім ідентифікаційних даних, можуть записуватися різноманітні інші персональні дані; втрачає сенс підробки та незаконного використання електронних документів з біометричними даними; біометричні персональні дані що збираються при оформленні електронних паспортів можуть застосовуватися в діяльності з розслідування правопорушень [2].

Застосування біометричних технологій є надзвичайно важливими у боротьбі з тероризмом. Це стало зрозуміло з поширенням авіатероризму. На питанні застосування біометричних технологій у боротьбі з тероризмом

зосереджено основні акценти Резолюції 2396 (2017) Ради безпеки ООН. В даний час Інтерпол має біометричні дані більш як 41 000 іноземних бойовиків – терористів.

У 2018 р. в Україні створено національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства (далі – національна система). Суб'єктами національної системи є ДМС, Адміністрація Держприкордонслужби, Національна поліція, МВС, МЗС, закордонні дипломатичні установи, Мінінфраструктури, СБУ, Служба зовнішньої розвідки та Міноборони. Розпорядником системи є ДМС.

Останнім часом значного поширення в світі набувають інформаційно-пошукові системи біометричної ідентифікації особистості по зображенню обличчя за оперативними даними від камер, розміщених у громадських місцях. Ураховуючи це, слід дослідити можливості удосконалення систем автоматизованих інформаційних систем та Інтегрованої інформаційно-пошукової системи органів внутрішніх справ України, що стоять на озброєнні правоохоронних органів України.

Найбільш відомі загрози безпеки для біометричної ідентифікації є: крадіжки біометричної інформації з сервісу авторизації; перехоплення біометричної інформації з мережі; читання біометричної інформації з фізично або програмно зламаного пристрою автентифікації; крадіжка біометричної інформації «з людини »або з носія інформації; зчитування біометричної інформації за допомогою методів соціальної інженерії або підроблених пристроїв; отримання біометричної інформації насильно.

В цілому, застосування біометрії не вирішить проблем надійності ідентифікації для систем з великою кількістю користувачів, але може підвищити достовірність ідентифікації при доступі до критично важливих систем як частини системи контролю і управління фізичним доступом або в якості додаткового фактору автентифікації.

Для середніх і великих правоохоронних органів поліції, а також для об'єктів з максимальною вимогою до безпеки рекомендується використовувати райдужну оболонку в якості засобу біометричного доступу. Для об'єктів з кількістю персоналу до декількох сотень чоловік оптимальним буде доступ за відбитками пальців. Для інформаційних систем з великою кількістю користувачів створення систем доступу на основі біометрії не виправдано економічно. Для таких систем можна використовувати біометричні характеристики з національної бази даних (наприклад, паспорта нового типу) як додатковий фактор.

**Список використаних джерел:**

1. Положення про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства. Затверджено постановою КМУ від 27 грудня 2017 р. № 1073. URL: http://zakon.rada.gov.ua/laws/show/1073-2017-п

2. Філіппов С. О. Біометричні технології: значення для протидії транскордонній злочинності. Вісник Національної академії Державної

прикордонної служби України. Серія : Юридичні науки. 2018. Вип. 2. URL: http://nbuv.gov.ua/UJRN/vnadpcurn_2018_2_6.

УДК 621.34
**ОЛЕКСАНДР СЕРГІЙОВИЧ ТКАЧЕНКО**
студент 3 курсу факультету №6 Харківського національного університету внутрішніх справ
**ВОЛОДИМИР ВОЛОДИМИРОВИЧ ТУЛУПОВ**
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій факультету № 4 Харківського національного університету внутрішніх справ

## ПИТАННЯ БЕЗПЕКИ ПРИ ВИКОРИСТАННІ СУЧАСНОГО СТАНДАРТУ LTE

У розвинених країнах світу продовжується перехід до інформаційної сервісно-технологічної економіки. На теперішній час в Україні використовується стандарт зв'язку четвертого покоління LTE (Long Term Evolution), який вважається перспективним. За даними компанії HUAWEI, LTE забезпечує швидкість до 326,4 Мбіт/с від базової станції до користувача і до 172,8 Мбіт/с у зворотному напрямку.

Метою створення стандарту LTE є збільшення можливостей високошвидкісних систем мобільного зв'язку, зменшення вартості передачі даних, можливість надання широкого спектру недорогих послуг.

Мобільний зв'язок четвертого покоління передбачає використання цілого спектру технологій, які раніше розвивалися паралельно. Всі вони внесли свій внесок у специфікацію LTE реалізованої в двох основних варіантах технологій: з дуплексним частотним поділом LTE-FDD (Frequency Division Duplex) і часовим поділом LTE-TDD (Time Division Duplex).

З точки зору безпеки таких LTE мереж враховуючи різні технології ускладнює пошук її вразливостей. В мережах 4G весь трафік проходить через єдину архітектуру EPC (Evolved Packet Core) за протоколом IP.

З фізичної точки зору в мережах LTE використовуються великі смуги частот, високорівнева модуляція сигналу, технологія MIMO (Multiple Input Multiple Output) яка дозволяє збільшити смугу пропускання каналу, при якому для передачі даних використовуються дві і більше антени і така ж кількість антен для прийому. Разом вони забезпечують адекватну завадостійкість, високі швидкості передачі даних і ємність мережі. Важливою особливістю мережі 4G є те, що з її архітектури зникло поняття контролера радіомережі (RNC), який в 3G виконував основну функцію з управління комунікаційними ресурсами. Тому базові станції в LTE стали більш інтелектуальними і самостійними – вони отримали можливість маршрутизувати трафік, що дозволило організовувати з'єднання між абонентами безпосередньо, минаючи ядро мережі. Щоб звести до мінімуму атаки на конфіденційну інформацію, базова станція повинна забезпечити