Список використаних джерел

1. Klimushin P., Solianyk T., Kolisnyk T., Mozhaev O. Potential application of hardware protected symmetric authentication microcircuits to ensure the security of internet of things. *Advanced Information Systems*. 2021, vol. 5, no. 3, pp. 103-111, DOI: https://doi.org/10.20998/2522-9052.2021.3.14.

2. Mozhaiev M. Sustainability of Open Educational Resources in Forensic Sciences: International Experience/ Karina Palkova, Olena Agapova, Aelita Zīle, Anton Polianskyi, Khosha Vadym, Serafyma Hasparian, Mozhaiev Mykhailo// European Journal of Sustainable Development(2022), 11, 3, 71-80 DOI: https://doi.org/10.14207/ejsd.2022.v11n3p71.

3. Mozhaiev, M., (2022). Devising a procedure for defining the general criteria of abnormal behavior of a computer system based on the improved criterion of uniformity of input data samples./ Semenov, S., Mozhaiev, O., Kuchuk, N., Mozhaiev, M., Tiulieniev, S., Gnusov, Y., Yevstrat, D., Chyrva, Y., Kuchuk, H. EasternEuropean Journal of Enterprise Technologies, 6 (4 (120)), 40–49. DOI: https://doi.org/10.15587/17294061.2022.

4. Гнусов Ю.В., Клімушин П.С., Колісник Т.П., Можаєв М.О. Аналіз систем моделювання мікроконтролерів з додатковими модулями криптографічного захисту інформації. *Вісник Національного технічного університету «ХПІ». Серія: Системний аналіз, управління та інформаційні технології.* 2020,№1(3). С. 79-84.

5. Mykhailo Mozhaiev, Viacheslav Davydov, Zhang Liqiang Analysis and comparative researches of methods or improving the software Advanced Information Systems, 2020 Vol. 4, No. 3, pp. 8-11, DOI: https://doi.org/doi: 10.20998/2522-9052.2020.3.18.

Одержано 26.04.2023

УДК 004.056.5+534.8

МОЖАЄВ Олександр Олександрович,
доктор технічних наук, професор,
професор кафедри кібербезпеки та DATA-технологій факультету № 6
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-1412-2696;

ГНУСОВ Юрій Валерійович,
кандидат технічних наук, доцент,
завідувач кафедри кібербезпеки та DATA-технологій факультету № 6
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-9017-9635;

ЄВСТРАТ Дмитро Іванович,
кандидат технічних наук, доцент,
доцент кафедри інформаційних систем
факультету інформаційних технологій
Харківського національного економічного університету ім. Семена Кузнеця
https://orcid.org/0000-0001-8393-6063

ПРОБЛЕМА ЗАХИСТУ АКУСТИЧНОЇ ІНФОРМАЦІЇ НА КРИТИЧНИХ ІНФРАСТРУКТУРАХ СФЕРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Захист акустичної (мовної) інформації є одним із найважливіших завдань у загальному комплексі заходів щодо забезпечення інформаційної безпеки об’єкта чи установи.

Унікальні особливості мовної інформації (МІ), що циркулює в закритих приміщеннях і поза ними: великий обсяг і оперативність обміну, висока конфіденційність деяких повідомлень, можливість ідентифікації особи людини, яка робить повідомлення, і навіть можливість визначення особистого ставлення до інформації, що озвучується, і складання її психологічного портрета зумовлюють актуальність та надзвичайну важливість вирішення проблеми захисту конфіденційної мовної інформації (КМІ). В інформаційному трафіку мовна інформація, незважаючи на зростання ролі автоматизованих інформаційних систем, як і раніше, відіграє ключову роль (до 80 відсотків від усього потоку інформації) [1, 2]. Особливо це важливо нині за умов військової агресії РФ. Тому останніми роками забезпеченню безпеки акустичної інформації приділяється все більша увага. З одного боку це обумовлено високій полі інформативністю акустичній інформації. З іншого боку, різноманітністю інформаційних загроз у відношенні до акустичної (мовній) інформації і особливостями сценаріїв їх розвитку і реалізації. Все це знайшло своє віддзеркалення у великому різноманітті сучасних методів, алгоритмів, програмних і апаратних засобів захисту акустичної інформації від несанкціонованого доступу. Основними напрямками захисту акустичної інформації вважаються технічний, криптографічний та стеганографічний (стеганофонічний) захист.

Окремим розділом виділено питання захисту акустичної інформації шляхом маскування акустичної інформації на основі сучасних комп'ютерних технологій. Цей напрямок в останні роки набуває все більший практичний інтерес серед виробників програмних засобів. З метою забезпечення основних послуг безпеки аудіо сигналів створюються комплексні програмні системи, розробляються та використовуються нові методи прийому, передачі, обробки та представлення аудіо сигналів.

Для перехоплення мовної інформації передбачуваний "противник" (обличчя або група осіб, зацікавлених в отриманні даної інформації) може використовувати широкий арсенал портативних засобів акустичної мовної розвідки, що дозволяють перехоплювати мовленнєву інформацію по прямому акустичному, віброакустичному, електроакустичному і оптико-акусто-електронному до основних у тому числі ставляться [3,4]:

– портативна апаратура звукозапису (малогабаритні диктофони, магнітофони та пристрої запису на основі цифрової схемотехніки);

– спрямовані мікрофони;

– електронні стетоскопи;

– електронні пристрої перехоплення мовної інформації (заставні пристрої) з датчиками мікрофонного та контактного типів з передачею перехопленої інформації по радіо, оптичному (в інфрачервоному діапазоні довжин хвиль) та ультразвуковим каналам, мережі електроживлення, телефонним лініям зв'язку, сполучним лініям допоміжних технічних засобів або спеціально лініям;

– оптико-електронні акустичні системи та ін.

Метою даного дослідження є аналіз проблеми захисту акустичної інформації на критичних інфраструктурах сфери інформаційної безпеки за допомогою маскування для забезпечення неможливості несанкціонованого доступу до системи.

Для досягання цієї мети потрібно вирішити такі часткові задачі:

– провести аналіз програмно-технічного маскування мови;

– провести дослідження маскування мовних повідомлень з метою введення невпізнання;

– вивчати особливості стиснення мовних повідомлень;

– дослідити методи прихованої передачі акустичної інформації.

В даний час заходи забезпечення безпеки мовного зв'язку можуть бути направлені не тільки на запобігання несанкціонованого знімання акустичної інформації, але і на приховування самого факту її передачі, шляхом використання для цих цілей, стандартних технічних засобів, звичайних, традиційних протоколів інформаційного обміну і загальнодоступних каналів зв'язку.

Останніми роками такий напрям інформаційної безпеки в комп'ютерних телекомунікаційних системах, що одержав назву "стегологія" (іноді "стелсологія"), активно розвивається у всьому світі.

Особливу популярність останнім часом одержала така частина стегології як "стеганографія", що використовується в області приховування конфіденційної інформації в графічних зображеннях, переданих по обчислювальних мережах. У тій же час, прогрес, досягнутий у області розробки пристроїв передачі акустичної інформації, а також в засобах обчислювальної техніки, відкриває нові можливості як для прихованої передачі конфіденційної інформації в аналогових і цифрових аудіо сигналах і мові, так і для прихованої передачі в інформаційних контейнерах різного роду, на основі використання нових технологій мультимедіа, комп'ютерної і стільникової телефонії і т.і. Такий напрям цифрових технологій у області захисту конфіденційної інформації, приховано присутньої всередині або поверх відкрито переданого аудіо сигналу, прийнято зараз називати "стеганофонією".

Сьогодні можна запропонувати наступні вимоги до приховування конфіденційної акустичної інформації і постановці стеганофонічних маркерів в сигналах, масивах і форматів даних різної природи:

– сприйняття сигналів і даних із закладеною в них конфіденційною акустичною інформацією повинне бути практично невідмітним від сприйняття початкового, "відкритого" повідомлення, що міститься в даному сигналі або масиві;

– передані по загальнодоступних каналах зв'язку конфіденційні мовні дані, що маскуються різними сигналами або в неявному вигляді що містяться в їх параметрах, не повинні легко виявлятися в цих сигналах-носіях широко поширеними методами і технічними засобами аналізу, що є в наявності в даний час;

– у ряді додатків постановка і виявлення стеганофонічних маркерів не повинні залежати від синхронізації цих процесів і від наявності яких-небудь еталонів;

– спеціальні методи постановки і виявлення стеганофонічних маркерів повинні реалізовуватися на основі стандартної обчислювальної техніки або спеціальних програмно-апаратних засобах на її основі;

– повинна забезпечуватися можливість закладки і виявлення ознак автентичності в акустичний (мовний) сигнал, що виявляються при незаконному його копіюванні або модифікації незалежно від виду уявлення і передачі цього сигналу (аналогового або цифрового);

– повинна забезпечуватися можливість захована конфіденційної акустичної інформації в масивах даних незалежно від виду представленої в них інформації.

Зображення сонограм можуть бути використані для передачі і зберігання мови на паперових носіях в якості стегомаркерів. При реалізації технологій "мовного підпису", пов'язаних з документом, що захищається, по сенсу і змісту приблизно також як і електронно-цифровий підпис, на стандартний лист паперу може бути нанесено від двох до чотирьох хвилин мови телефонної якості звучання у вигляді різноманітних візерунчастих рисунків. В цьому випадку достовірність документа може бути встановлена не тільки за наявності відповідних підписів і друку, але і за інформацією, що міститься в "мовному підписі", відсканувавши, просинтезував і озвучивши який можливо почути ключові моменти змісту документа, озвучені голосом відповідальної особи.

Неспівпадіння озвучених відомостей з інформацією, що міститься в документі, говорить про його фальсифікацію. Підроблювати ж "мовний друк" або "мовний підпис" практично неможливо. Відмітимо, що така дешева технологія "мовного підпису" може бути реалізована на стандартній офісній техніці: комп'ютер із звуковою картою плюс принтер і сканер.

Таким чином, виходячи з вищесказаного, можна вважати, що одним з перспективних напрямів захисту акустичної інформації в каналах зв'язку і виділених приміщеннях, можна рахувати створення і розвиток комп'ютеризованих систем маскування мови наряду або при сумісному використанні з традиційними технологіями смислового захисту акустичної інформації, а саме, засекречуванням мовних сигналів на основі криптографічних алгоритмів.

Вибір конкретних методів і засобів маскування мови як одного з видів смислового захисту акустичної інформації, залежатиме від практичних вимог, що пред'являються до системи мовного захисту і технічних характеристик каналу передачі акустичної інформації.

В сучасних системах безпеки мовного зв'язку комп'ютерні технології цифрової обробки сигналів і зображень знаходять все більш широке застосування. Основними вимогами сьогоднішнього дня, що пред'являються до систем , які забезпечують захист акустичної інформації у комп'ютерних системах критичного застосування , є швидкість і ефективність виконання різних процедур обробки мовного сигналу з використанням стандартних недорогих технічних засобів комп'ютерної телефонії, а саме: персонального комп'ютера, звукової карти, пристрою стику з телефонною лінією і-або модему. Задовольнити цим вимогам можна, застосовуючи цифрові методи динамічного спектрального аналізу – синтезу мовних і аудіо сигналів.

Приведені приклади використання запропонованого підходу стосовно рішення найбільш поширених задач забезпечення безпеки мовних повідомлень показали його високі потенційні можливості при здійсненні різних, навіть дуже складних і нових алгоритмів обробки аудіо сигналів, які вже сьогодні застосовні для створення комп'ютерних систем захисту мовних повідомлень в загальнодоступних каналах зв'язку. Даний підхід може стати базовим при проектуванні нових систем безпеки акустичної інформації і оцінці ефективності використання пристроїв захисту мовних повідомлень, які вже існують на ринку спецтехніки.

Подальші дослідження бажано провести по аналізу можливого використання методів синтезу великих ансамблів квазіортогональних дискретних сигналів з поліпшеними ансамблевими, структурними і кореляційними властивостями для забезпечення вищих показників захищеності акустичних каналів у комп'ютерних системах критичного застосування.

Список використаних джерел

1. Косенко В. В. Принципи і структура методології ризик-адаптивного управління параметрами інформаційнотелекомунікаційних мереж систем критичного застосування. *Сучасний стан наукових досліджень та технологій в промисловості.* Харків. 2017. № 1 (1). С. 46–52.

2. Kosenko V. Mathematical model of optimal distribution of applied problems of safety-critical systems over the nodes of the information and telecommunication network. *Advanced Information Systems*. 2017, vol. 1, no. 2, pp. 4–9. DOI: https://doi.org/10.20998/2522-9052.2017.2.01.

3. Karen Bailey, Kevin Curran. Steganography. – BookSurge Publishing, 2005 г. 118 с.

4. Johnson N., Duric Z., Jajodia S. Information Hiding: Steganography and Watermarking – Attacks and Countermeasures, New York. – NY.: Kluwer Academic Pub, 2000.

Одержано 26.04.2023

УДК 343

НАГОРНИЙ Михайло Олександрович,
курсант 1 курсу факультету № 4
Харківського національного університету внутрішніх справ;

РОГ Вікторія Євгенівна,
старший викладач кафедри протидії кіберзлочинності факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-7443-5125

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ДІЯЛЬНОСТІ ПОЛІЦІЇ

Сучасні інформаційні технології стали необхідністю в будь-якій сфері життя, в тому числі і в діяльності поліції. Сьогодні від застосування сучасних ІТ- технологій залежить ефективність та успішність роботи правоохоронних органів. Розглянемо та проаналізуємо основні сучасні інформаційні технології, які використовуються в діяльності поліції.

Однією з головних технологій, яку використовує поліція, є *електронні бази даних*. У них зберігається інформація про злочини, злочинців, свідків, потерпілих, а також інші важливі дані. За допомогою таких баз даних, правоохоронні органи можуть швидко знаходити необхідну інформацію та аналізувати її.

Іншою важливою технологією, яка використовується в діяльності поліції, є *відеоспостереження*. Завдяки відеокамерам, які встановлюються на вулицях, в громадських місцях та на транспорті, правоохоронні органи можуть контролювати ситуацію в режимі реального часу, а також здійснювати пізніше аналіз зареєстрованих відеозаписів. Таким чином, відеоспостереження дозволяє зменшити кількість злочинів та забезпечує швидке розкриття злочинів.

GPS-навігація також є важливою технологією для поліції. Її використовують для відстеження руху автомобілів поліції та їх переміщення, а також для швидкої