Міністерство освіти і науки України

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ АВТОМОБІЛЬНО-ДОРОЖНІЙ УНІВЕРСИТЕТ

Матеріали

Всеукраїнської науково-практичної Internet-конференції

«МОДЕЛЮВАННЯ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В НАУЦІ, ТЕХНІЦІ, КІБЕРБЕЗПЕЦІ ТА ОСВІТІ»

15-16 листопада 2022 року
м. Харків, Україна

Харків 2022
Україна

Зміст

ДК 004.056.5:629.3 **doi:**

СИСТЕМА PKES АВТОМОБІЛЯ ТА СПОСОБИ ЇЇ ЗАХИСТУ ВІД ЗЛОВМИСНОГО ВТРУЧАННЯ

Левтеров А.І., Іванов С.М.
Харківський національний автомобільно-дорожній університет

Анотація: Розглянуто систему безключового доступу до автомобіля. Запропоновано нову методику захисту від зловмисників цієї системи введенням до смарт-ключа та іммобілайзера додаткових елементів та розглянуто роботу оновленої системи.
Ключові слова: смарт-ключ, транспондер, іммобілайзер, регістр пам’яті зі зсувом, зондуюча антена, ретранслятор, емулятор, криптопароль.

Вступ

Сучасні автомобілі є найкращим прикладом кіберфізичної системи через інтеграцію обчислювальних компонентів і фізичних систем. Інакше кажучи, автомобілі нашого століття, це комп'ютери, які керують технологічною обвіскою - двигуном і гальмами, фарами і поворотниками, двірниками і кондиціонером, та й рештою теж [1]. Їх сміливо можна порівняти з сучасними комп'ютерами, що мають складну електронну начинку. Але «розумні», машини перетворюються на досить ласу мішень для хакерів [2]. За даними всесвітньої організації *ISO/SAE 21434:2021* кіберзлочинність завдає шкоди світовій економіці на суму 500 млрд. євро щорічно [3].

Аналіз публікацій

Відмички, монтировка та розбите скло – це вже в минулому. Сьогодні для зламу автомобілів все частіше використовуються ноутбуки та спеціальне комп'ютерне обладнання. Наприклад, у Лондоні ще в 2015 році зловмисники, зробивши дублікат радіобрелка для розблокування іммобілайзера, викрали понад 6000 автомобілів. Система безключового доступу до автомобіля (СПДА) стала дуже популярною функцією у багатьох нових автомобілях. Вона дозволяє водієві без використання ключа відчиняти двері і заводити машину завдяки маленькому електронному брелку, що лежить у кишені одягу або в сумці водія, який обмінюється даними по радіохвилях з автомобілем, що дозволяє відкривати двері і запускати двигун і так далі без ключа [2].

Як правило, автовиробники комплектують свої нові автомобілі радіо-брелками (смарт-ключами) (за галузевою термінологією такі системи називаються PKES – Passive Keyless Entry and Start – «пасивний безключовий доступ і запуск двигуна» [4]), які, працюючи по радіоканалу, повідомляють сигналізації машини, що до нею підходить її автовласник. Якщо код у них збігається, сигналізація відключається і у автомобіля автоматично відкриваються двері.

Це посилання передається в ефір на чистоті 125 кГц і, якщо ключ-брелок знаходиться поруч і розуміє мову запиту, він відразу відповідає машині, використовуючи вже свою робочу частоту (433 або 868 МГц). Причому відповідає хитрою цифровою комбінацією, що згенерована за індивідуальним алгоритмом шифрування.

Щоб виключити електронні підтасовки, відповідь від електронного ключа має надійти в режимі реального часу (рахунок затримок ведеться на наносекунди), тому будь-які спроби відкрити машину приречені на провал. Але навіть такі хитромудрі дії не завжди рятують від угону. [3]. Кількість викрадень машин з безконтактною системою доступу зростає у геометричній прогресії [2] і займає третє місце по числу кібератак [4].

Так, згідно з проведеним дослідженням Швейцарським технологічним інститутом вдалося встановити, що сучасні PKES, що дозволяють водієві автоматично відчиняти

двері в машині і запускати двигун без ключа, дуже вразливі для зламу безпосередньо через радіоканал [5].

Щоб протестувати електронний захист автомобілів, фахівці інституту відібрали десять ключів-брелків (від 10 автомобілів) від 8 марок автомобілів. Тестування відбувалося без участі представників автомобільних компаній. Завдяки цьому експерименту Швейцарська команда інженерів продемонструвала конкретний метод, який дозволив їм зламати (відкрити) усі без винятку вибрані автомобілі, які брали участь у цьому випробуванні.

Саме ці тести показали, що смарт-ключи дистанційного відчинення дверей (PKES) при наближенні власника до автомобіля, досить-таки нескладно зламати за допомогою спеціального способу та відповідного обладнання.

Щоб відкрити автомобіль за допомогою сигналу з нерідного ключа автомобільному злодієві знадобиться помічник і спеціальний прилад – ретранслятор (рис.2) [6,7].

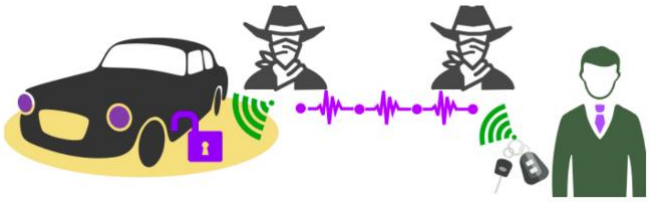


Рис. 2. «Операція» відкриття автомобіля

Помічник під час «операції» знаходиться поряд із власником автомобіля (смарт-ключем). Він встановлює цифровий зв'язок із пристроєм. Його учасник біля автомобіля натискає кнопку відкриття дверей. Сигнал обробляється в ретрансляторі та відправляється помічнику, який, підтримуючи зв'язок із ключем, пересилає сигнал назад. Ця схема спрацьовує практично на будь-яких авто. Схематично це виглядає так (рис. 3, рис. 4) [8].

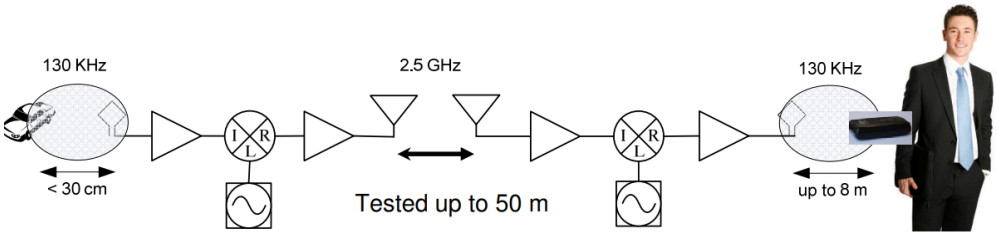


Рис.3. Схема безключового відкриття автомобіля

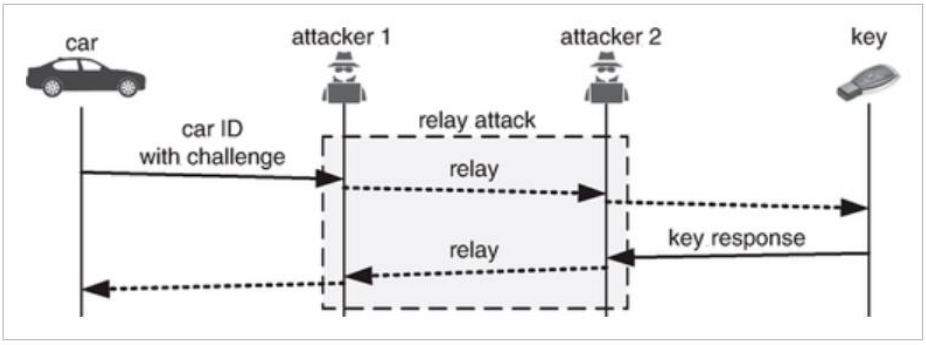


Рис. 4. Схема ретрансляції сигналу між двома зловмисниками

Пристрій коштує пристойних грошей, але успішне викрадення автомобіля все окупає. На рис.5. показано обладнання, яке було представлене на міжнародній виставці, що проходила у Польщі [9].

Виставка була присвячена технологіям відкриття автомобілів без оригінального ключа. На виставці були присутні автомайстри із багатьох Європейських країн.

Рис.5. Комплект обладнання для відкриття автомобілів без оригінального ключа-брелка

Розглянемо проведення «операції» відкриття автомобіля докладніше на конкретному прикладі.

Після включення охоронної сигналізації блоки встановлюють між собою високошвидкісний канал передачі даних, що дозволяє ретранслювати ключові запити автомобіля і віддалено приймати відповіді мітки.

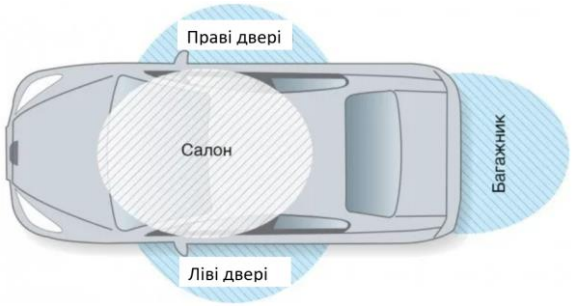


Рис.6. Зондуючі антени, встановлені в автомобілі

Зондуючі антени на 125 кГц встановлені по периметру кузова так, щоб їх діаграми не перекривалися (рис.6) [10]. Завдяки цьому машина завжди знає, звідки відповідає ключ, і дозволяє виконання лише "географічно прив'язаних" команд. Наприклад, двигун запуститься в тому випадку, якщо в радіообміні з ключем буде задіяна антена в спинці сидіння водія, а багажник відкриється лише при успішному опитуванні ключа із заднього сектора.

Для викрадення злочинці використовують спеціальні ретранслятори, які, перехоплюючи сигнал з безконтактних ключів, посилюють спійманий сигнал, а потім передають його на радіоприймач, який у свою чергу ретранслює сигнал на автомобіль (рис.3, рис.4) [8]. Зрештою охоронна система приймає рідний сигнал безконтактного ключа, який може в цей момент перебувати далеко від автомобіля. Наприклад, за допомогою подібних ретрансляторів зловмисники можуть передати сигнал з ключа-брелка, коли водій перебуває на роботі, в кафе, ресторані, магазині, кінотеатрі і т.д. Можна навіть змусити електронний пароль відгукнутися з закритого приміщення.

Ліворуч «емулятор», а праворуч – «зчитувач» (Рис.3), які можуть бути представлені у вигляді нехитрих коробочок. Усередині цих коробочок заховані приймачі та передавачі

на три діапазони (125 кГц, 433 МГц та 900 МГц), смугові фільтри, підсилювачі, процесори, літій-полімерні батареї великої ємності та рамкова антена. Після включення живлення блоки встановлюють між собою високошвидкісний канал передачі даних, який дозволяє ретранслювати ключові запити автомобіля і віддалено приймати відповіді мітки. На рис.7 наведено приклади реалізації протоколів обміну між автомобілем та ключем [11].

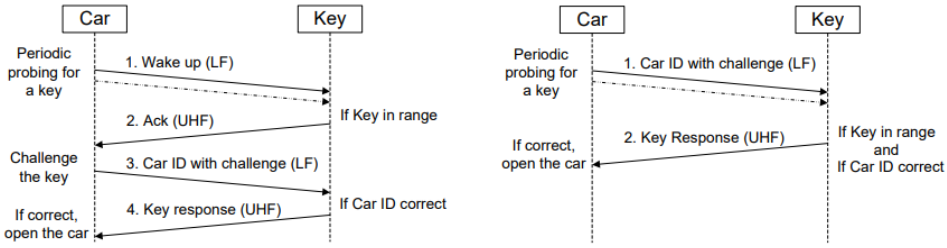


Рисунок 7. Приклади реалізації протоколу системи пасивного доступу без ключа:

a) У типовій реалізації автомобіль періодично прощупує канал на наявність ключа короткими маячками. Якщо ключ всередині діапазону, протокол запиту-відповіді між автомобілем і ключем надає або забороняє доступ (є енергоефективним, оскільки виявлення ключів залежить від дуже коротких маяків);

b) В другій реалізації автомобіль періодично зондує канал безпосередньо за допомогою потужних маяків, які містять автомобіль ідентифікатор. Якщо ключ знаходиться в зоні дії, він безпосередньо відповідає на виклик.

Творці кримінального радіоподовжувача добре знаються на питаннях електромагнітної сумісності. Під час роботи «Довгої руки/ключа» (рис.8) можна говорити по мобільному телефону або, навпаки, включати генератори перешкод стільникового зв'язку для блокування GSM-трафіку систем моніторингу [12].

Це посилання передається в ефір на «транспондерній» частоті 125 кГц і, якщо смарт-ключ знаходиться поруч і розуміє мову запиту, він відразу відповідає машині, використовуючи вже свою робочу частоту (у нас і в Європі це 433 МГц або 868 МГц), наприклад, код відповіді X123.Y456.Z789.

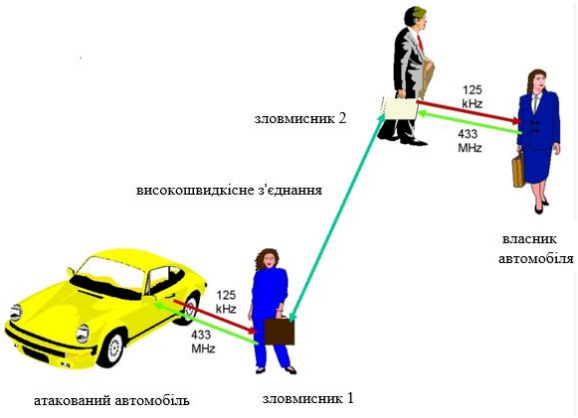


Рис. 8. Схема роботи Relay Station Attack (Технологія довгої руки/ключа)

При цьому не має значення, де знаходиться ключ - чи знаходиться він усередині будівлі, наприклад: будинку, офісу, або в кишені, сумці або файлі власника, вловити сигнал через сканер/підсилювач можна навіть з відстані 8 метрів від ключа. Посилення сигналу настільки сильне, що його можна передати на другий приймач/передавач поруч із автомобілем на відстані до 800 метрів! Автомобіль "думає", що власник відкриває

двері автомобіля заводським смарт-ключом. Перед запуском двигуна система доступу повинна ще раз запросити ключ (через антену в спинці сидіння водія), тому «емулятор» повинен бути поруч. Злодії діють неймовірно швидко. Крадіжка займає в середньому 6 секунд!

Мета і постановка завдання

Метою даної статті є пропозиція методу захисту автомобіля від несанкціонованого безключового доступу.

Відповідно до поставленої мети слід розробити методику і пристрій захисту від зловмисників для цієї системи введенням до смарт-ключа та іммобілайзера додаткових елементів.

Рішення проблеми

Що робити, щоб зв'язати викрадачам їхні довгі руки? Для цього пропонується кілька способів захисту [13].

Найрадикальнішим, мабуть, є відключення системи PKES, витягнувши з смарт-ключа батарейку!

Другий спосіб, після закриття автомобіля ховати брелок від машини в клітину Фарадея: чохол чи футляр з металевим (фольгованим) екраном. Такий притулок для «золотого ключика» можна зробити і самому – хоч би з цигаркової пачки чи рулону побутової фольги. Однак ці обидва способи дуже незручні при їх експлуатації.

Наступні три способи відносяться до системи кодування інформації та паролів. Сигнал від смарт-ключа є своєрідним паролем, що зчитується блоком керування. Ці паролі бувають трьох типів [11]:

- пароль ID (ідентифікаційний);
- змінний пароль;
- шифрований криптопароль.

Ідентифікаційний пароль записаний у чіпі ключа та в блоці іммобілайзера. Він не змінюється і завжди однаковий. Зловмисники можуть перехопити такий сигнал та згенерувати свій. Не найнадійніша система.

Набагато надійніше системи зі змінним паролем. Сигнал із паролем від транспондера приймається блоком керування. Після розпізнавання в блоці керування генерується новий пароль та відправляється назад на транспондер. Однак і в цьому випадку зловмисники можуть перехопити такий сигнал та згенерувати свій.

У найсучасніших іммобілайзерах використовується алгоритм із шифрованим криптопаролем. У транспондері є функція шифрування. Блок управління посилає певний сигнал у транспондер, в якому потім генерується унікальний пароль, який може розпізнати тільки блок управління. Його ще називають «плаваючим» паролем. І хоча цей алгоритм надійніший, його також можна перехопити та розшифрувати.

Тому пропонується наступний простий варіант захисту. Для цього скористаємось малюнками, наведеними в [14, 15], з деякими змінами. У смарт-ключі додатково встановлюється регістр пам'яті зі зсувом та реле для автоматичного відключення живлення смарт-ключа (рис.9).

Рис.9. Смарт-ключ з доданими елементами

Регістр пам'яті зі зсувом додатково встановлюється в замок запалювання з іммобілайзером (рис.10).

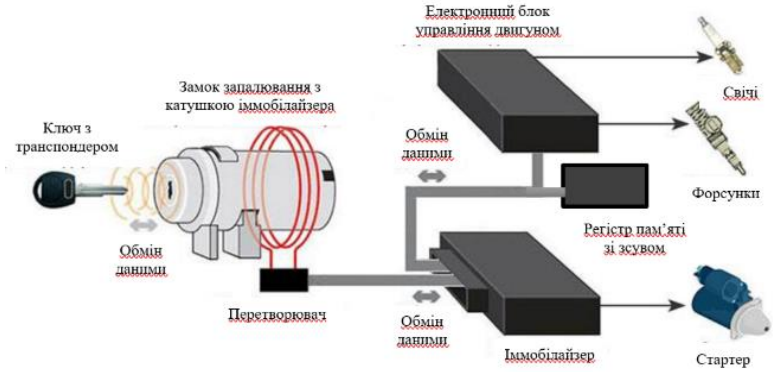


Рис.10. Схема обміну між смарт-ключом та іммобілайзером з доданим елементом

У сервісному центрі обслуговування автомобіля фахівцем центру в регістри пам'яті смарт-ключа та іммобілайзера записується набір (бажано кілька десятків) пар відповідних шифрованих кодів: в іммобілайзер код запиту, смарт-ключ з транспондером код відповіді. Слід зазначити, що водієві необхідно буде раз на два-три місяці заїжджати до центру для зміни бази кодів.

Як це працює? Процедура обміну між смарт-ключом та іммобілайзером з наступним запуском двигуна аналогічна вищеописаному (рис.1). Відмінність полягає в тому, що після виходу водія з автомобіля останній закриває автомобіль натиснувши відповідну кнопку на смарт-ключі. У цей момент з ECU надходить сигнал одночасно на регістри пам'яті смарт-ключа та іммобілайзера на зсув коду на одну позицію, після чого сигнал з ECU надходить на реле, що знаходиться в смарт-ключі, на відключення живлення смарт-ключа автоматично перерветься. Тепер, при використанні технології «Довгої руки/ключа», код смарт-ключа зловмисникам буде недоступний. У кращому випадку зловмисники зможуть зчитати код іммобілайзера, чого недостатньо для відкриття автомобіля.

Щоб здійснити поїздку, водій підходить до припаркованого автомобіля, попередньо примусово натискає спочатку кнопку включення реле на смарт-ключі, яке своїми контактами замикає ланцюг подачі живлення на смарт-ключ (перед реле у смарт-ключі додатково ставиться елемент АБО на два входи: для автоматичного підключення реле з ECU та фізичного підключення водієм натисканням відповідної кнопки на смарт-ключі). Потім водій натискає кнопку для обміну кодами з іммобілайзером. Тепер, навіть якщо зловмисники зчитають коди іммобілайзера і смарт-ключа, водій може бути спокійним тому, що після включення двигуна також відбудеться автоматична зміна кодів в іммобілайзері та смарт-ключі. Зазвичай, при включенні запалювання, іммобілайзер через

кільцеву антену, намотану навколо замку запалення на досить високій частоті запитує дані від регістру пам'яті іммобілайзера. Якщо код упізнано правильно, починається діалог між іммобілайзером та контролером. Він відбувається на низькій частоті. Якщо обмін даними завершився успішно, роботу двигуна дозволено. Найчастіше до вимкнення запалювання регістр пам'яті більше не обпитуватиметься. Після чого командою з ECU відбудеться відключення живлення смарт-ключа і база з кодами смарт-ключа знову буде недоступною.

Висновки

Розглянута методика безключового доступу до автомобіля є більш простою і більш захищеною від зловмисників в зрівнянні з розглянутими аналогами.

Література:

1. By N. Huq, C. Gibson, V. Kropotov, R. Vosseler. Cybersecurity Risk of Connected Cars URL:https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/in-transit-interconnected-at-risk-cybersecurity-risks-of-connected-cars
2. Найкращий друг викрадача – безключовий доступ. Експеримент. URL: https://autogeek.com.ua/luchshiy-drug-ugonshhika-besklyuchevoy-dostup-eksperiment/
3. Колодяжний В.М., Левтеров А.І., Малащук Є.В. Кібербезпека автомобілів: історія цифровізації автомобілів, поточний стан проблеми, цілі сталого розвитку та стандарти. *Вісник ХНАДУ*, вип. 96. 2022. С. 59-65.
4. Ivy Wigmore. Passive keyless entry (PKE). URL: https://www.techtarget.com/whatis/definition/passive-keyless-entry-PKE#:~:text=Passive%20keyless%20entry%20(PKE)%20is,touches%20the%20car%20on%20exit.
5. Keyless entry car thieves. (whichcar.com.au).
6. A. Ranganathan, S. Capkun. Are We Really Close? Verifying Proximity in Wireless Systems. URL: are_we_really_close.pdf (ethz.ch)
7. Secure Proximity Verification (Ranging)URL: https://securepositioning.com/secure-proximity-verification/.
8. A. Francillon, B. Danev, S. Čapkun. Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. URL:Microsoft PowerPoint - PKES_relay.pptx (ndss-symposium.org).
9. Rundgang auf DER „Autoknacker-Messe“. https://www.bild.de/auto/auto-news/diebstahl/autoklau-messe-polen-reportage-38446846.bild.html
10. Abel Valko, Relay Attack Resistant Passive Keyless Entry. Securing PKE Systems with Immobility https://www.kth.se/polopoly_fs/1.987191.1589831618!/valkoabel_47599_2869553_Relay_Attack_Resistant_Passive_Keyless_Entry-1.pdf
11. A. Francillon, B. Danev, S. Čapkun. Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. URL:https://eprint.iacr.org/2010/332.pdf
12. Relay Attack. URL: Relay attack - Wikipedia
13. Skybrake immobilizer: principle of operation, features, installation and dismantling. URL:https://avtotachki.com/en/immobilayzer-skybrake-princip-raboty-osobennosti-ustanovka-i-demontazh/
14. R. Verdult, Flavio D. Garcia, J. Balasch. Gone in 360 Seconds: Hijacking with Hitag2. https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final95.pdf
15. Principle of operation and types of engine blocking relay. https://130.com.ua/en/princip-raboty-i-raznovidnosti-rele-blokirovki-dvigatelja/

УДК 519.63

РОЗВ'ЯЗОК КРАЙОВОЇ ЗАДАЧІ ДЛЯ РІВНЯННЯ ГЕМГОЛЬЦЯ

Колодяжний В.М. докт. фіз-мат. наук, професор
Харківський національний автомобільно-дорожний університет
Лісіна О.О. канд. канд.мат. наук, доцент
Харківський національний університет імені В.Н. Каразіна

Наявність в постановці крайової задачі двох різноманітних видів інформаціх – аналітичної та геометричної – є серйозною проблемою при створенні методів та алгоритмів при розв'язуванні відповідних задач.

Будь який метод повинен враховувати обидва ці підходи визначення інформації, а це потрибує перетворення геометричної інформації в аналітичну (при цьому не всяка кодировкв геометричной інформації може застосовуватись). В таких класичних методах, як наприклад, розділення змінних, інтегральних перетвореннях, форма областей та ділянок їх границь враховуються завдяки відповідному вибору систем координат, у методі комфорних відображень – при побудові відображаючих функцій, у варіаційних методах – при побудові координатних функцій, у сіткових методах – при складанні рівнянь для вузлів, близких до крнауі, інших. Метод скінченних елементів виник в звязку з бажанням як можна більш точно враховувать геометричні форми. Особливо актуальна розробка таких методів розв'язку крайових задач, які би мали універсальний характер і не вимагали застосовань (як правило, від математика) знань тонких питань теорії.

Нехай необхідно обчислити критичні частоти та власні хвилі, які розпространяються в хвильоводах. У випадку розгляданні електромагнітних хвиль вимагається визначити Н-моди, для акустичних хвиль - розповсюдження крутильних коливань в нескінченних стрижнях постійного січення. Крайова задача, яка описує розповсюдження хвиль у хвильоводах, може бути задана наступтим чином. Вимагається знайти власні числа та власні функції для двовимірного рівняння Гемгольця

$$\frac{\partial^2 u}{\partial x^2}+\frac{\partial^2 u}{\partial y^2}+\lambda u=0, \qquad (1)$$

з граничною умовою Діріхле

$$u\big|_{\partial\Omega}=0 \qquad (2)$$

де Ω - область, що відображається на рисунку 1.

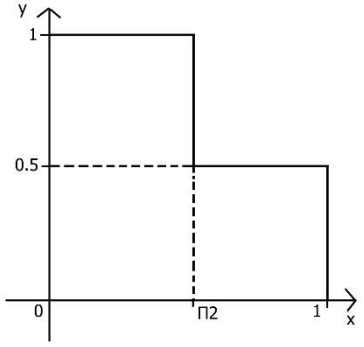


Рисунок 1. Ω - область

Розв'язок даної задачі виконувалась за схемою запрпонованою В.В. Веретельником з застосуванням структурно-варіаційного метода. В комбінації зі структурним методом розглядається варіаційний метод Ритца. Можна показати, що оператор крайової задачі (1)-(2) є додатньо визначеним. Це гарантує збіжність наближеного за Ритцом [4,5] розв'язку до точного узагальненого. Пошук розв'язку задачі (1)-(2) еквівалентнний знаходженню мінімуму
функціоналу

$$\Phi(u) = -\left\{\int_{\Omega} |\nabla u|^2 \, d\Omega\right\} / \left\{\int_{\Omega} |u|^2 \, d\Omega\right\} \qquad (3)$$

локальні мінімальні значення якого дорівнюють шуканим власним значеннм [2]. Функцію будем відшукувати у вигляді

$$u = \sum_{i=0}^{\chi} c_i \Psi_r . \qquad (4),$$

де $\{\Psi_r\}$ точно задовільнює граничним умовам і будується згідно структурі, яка описується у формі $\Psi_i = \omega\varphi_i$. Функція $\omega(x, y)$ задає рівняння границі області Ω: $\omega(x, y) = 0$: функція $\omega(x, y)$ будується за допомогою R-операцій та має вигляд

$$\omega(x, y) = (f_1 \wedge_\alpha f_2) \wedge_\alpha (f_3 \vee_\alpha f_4), \qquad (5)$$

де $f_1 = x(1-x) \geq 0$ – вертікальна; полоса; $f_2 = y(1-y) \geq 0$ – горизонтальна; полоса; $f_3 = \Pi 2 - x \geq 0$ – півплощина, П2 – параметр для оперативного вимірування конфігугації області;. $f_3 = 0{,}5 - y \geq 0$ – півплощина.

Так як оператор крайової задачі (1)-(2) самоспряжний, то його власні числа та функції будуть дійсними. Тому достатьо будувати функції $\Psi_r(x, y)$, що належитимуть класу дійсних функціям.

Підставляя (4) та диференцируючи по c_i приходимо до узагальненій задачі на власні значення:

$$Ax - \lambda Bx = 0 \ , \qquad (6)$$

де A та B - матриці: $A = [a_{ij}]$, $B = [b_{ij}]$, $a_{ij} = \int_{\Omega} \nabla\Psi_i \nabla\Psi_j \, d\Omega$, $b_{ij} = \int_{\Omega} \Psi_i \Psi_j \, d\Omega$ та $x = (c_1, c_2, ...c_n)$. Так як матриці A і B – симетричні та додатньо визначені, то до матриці B – можна застосувати розкладення Холецкого: $B = LL^T$, де L – трикутна матриця. Тоді задачу (6) иожно привести до вигляду $(L^{-1}AL^{-T})(L^T x) = \lambda(L^T x)$, тобто до звичайної проблеми на власні значення:

$$Py = \lambda y . \qquad (7)$$

Власні числа при цьому перетворенні зберігаються, а власний вектор x перетворюється в $y = L^T x$ (L^T визначає матрицю, яка є оберненою до транспонованої матриці L). Задачу (7) можна вирішити одним з стандартних методів. Розв'язок зручно проводити у два етапи: спочатку перетворенням Хаусхолдера привести матрицю P до тридіагольного вигляду, а потім знайти власні числа QL – методом. Якщо треба отриматівласні функції задачі (7) , то треба виконати обернені перетворення отриманого власного вектора тридіагональної матриці.

Використання для розв'язання данної крайової задачі програмуючої системи типу «ПОЛЕ» передбачає завдвння давдання інформації вихідної інформації про задачу у вигляді спеціальних директив [1]. Директиви відокремлюються одна від одною спеціальним розділителем «;» і складаються з ключових слів, допоміжних розподілителів, індефікаторів, числової інформації.

Деякі директиви, наприклад директиви, наприкдад ті, що задають вигдяд рівняння, логістичні формули області, функціональні компоненти та інші мають аналітичні вирази, що визначають вихідну інформацію про крайову задачу. Відповідні директиви , необхідні для завдання крайової задачі (1)-(2) програмуючої системи «ПОЛЕ-3», можна познайомитись
у відповідній літературі.

Література

1. Рвачев В.Л. Теория R-функций и некоторые ее приложения. – Киев: Наук. думка, 1982. – 551 с. 2. Колодяжний В.М. Геометрично структуровані атомарні функції // Доповіді НАН України, № 6, 2003. – С. 12-15. 3. Рвачов В.Л. Експериментальна математика: методологія, проблеми, практика / Рвачов В.Л., Рвачов В.О. – Киев: Товариство "Знання". (Серія VIII, № 8), 1983. – 31 с. 4. Михлин С.Г. Вариационные методы в математической физике. М.: Наука, 1979. – 512 с. 5. Колодяжный В.М. Структурно-вариацинный метод решения краевых задач математической физики. Харьков.: ХАИ, 1981. – 92.

УДК 629.05+681.5+004.32

ІНФОРМАЦІЙНА БЕЗПЕКА НА АВТОМОБІЛІ ТА АВТОМОБІЛЬНОМУ ТРАНСПОРТІ

Кривошапов Сергій Іванович, канд. техн. наук, доцент кафедри «Технічної експлуатації та сервісу автомобілів ім. проф. Говорущенко М.Я.», Харківський національний автомобільно-дорожній університет

Анотація. Вказано на широке використання мікропроцесорних систем керування у сучасному автомобілі. Розглядаються різні канали передачі в цифрових системах управління, які можуть передавати дані всередині системи управління, між системами всередині транспортного засобу чи зв'язувати автомобіль із зовнішніми системами. Наведено основні причини порушення роботи системи керування автомобілем під внутрішнім та зовнішнім впливом. Вказано основні шляхи інформаційних загроз для персональних комп'ютерів та серверів, які використовуються для управління діяльністю підприємства автомобільного транспорту.

Ключові слова: транспорт, автомобіль, інформаційні технології, мережа, система управління, передача даних, кібербезпека, програмне забезпечення

Конструкція сучасного автомобіля все більше використовує електронні компоненти, що базуються на мікропроцесорних системах обробки даних, мережевих технологій прийому та передачі сигналів, комунікаційних систем загальної взаємодії елементів інформаційної системи [1]. В автомобіль широко використовуються мультимедійні технології, взаємодії з хмарними сестрами, телефонні та супутникові канали радіозв'язку, що дозволяють взаємодіяти з дорожньою інфраструктурою та центрами управління.

Для керування двигуном, трансмісією, підвіски, гальмівної системи та рульового керування, освітлення та комфорту використовуються електронні блоки управління (ЕБУ), з'єднані між собою різними каналами передачі даних:

- Controller Area Network (CAN) – об'єднана промислова мережа виконавчих пристроїв та датчиків, розроблена фірмою Bosch у середині 1980-х років;
- FlexRay – високошвидкісна мережа для автомобілів, заснована компаніями Philips спільно з BMW, Daimler, Bosch, General Motors та Volkswagen у 2004 році;
- Local Interconnect Network (LIN) – мережа для управління автомобільними системами низької відповідальності, розроблена консорціумом європейських автовиробників: Audi, BMW, Daimler Chrysler, Motorola, Volkswagen, Volvo та ін. у 1999 році;
- Media Oriented Systems Transport (MOST) – високошвидкісна мультимедійна автомобільна мережа, розроблена Microchip Technology;
- Ethernet – сімейство провідних мереж (LAN, MAN, WAN) передачі даних між комп'ютерами, яка розроблена фірмою Xerox 1973 року;
- Wi-Fi (Wireless Fidelity) – бездротова локальна мережа між пристроями, розроблена CSIRO у 1997 році.

Із зовнішнім світом сучасний автомобіль спілкується через канали супутникового зв'язку, використовує систему глобального позиціонування GPS (Global Positioning System), підтримує стандарти цифрового мобільного зв'язку GSM (Global System for Mobile Communications) та GPRS (General Packet Radio Service), протоколи радіозв'язку Wi-Fi та Bluetooth.

Сигнали від датчиків до мікропроцесора також можуть передаватися за

стандартними протоколами зв'язку:

- I²C (Inter-Integrated Circuit) - послідовний асиметричний канал для зв'язку між інтегральними схемами всередині електронних приладів, розроблений фірмою Philips;
- 1-Wire – двонаправлений однопровідний канал зв'язку для пристроїв із низькошвидкісною передачею даних, розроблений фірмою Maxim Integrated;
- SPI (Serial Peripheral Interface) - послідовний синхронний канал передачі в режимі повного дуплексу;
- UART (Universal Asynchronous Receiver-Transmitter) - двонаправлений канал зв'язку між цифровими пристроями.

Розвиток різних систем комунікації дозволяє оперативно отримувати та передавати інформацію про режим функціонування систем на автомобілі, дані про стан виконавчих елементів, відомості про місцезнаходження автомобіля та ін.

Використання стандартизованих каналів (протоколів) зв'язку дозволяють розширювати можливості інформаційної системи автомобіля без значних витрат на проектування архітектури, використовувати розподілену систему для збору та обробки даних, залучати різних розробників та технології.

Однак через канал зв'язку можуть передаватися помилкові або спотворені дані, які заважатимуть надійній роботі системи керування автомобілем. Порушення можуть відбуватися на сигнальному (невідповідність рівня напруги на лінії), логічному (порушення послідовності передачі даних та сигналів, що управляють передачею) або інформаційному (передача неправильних даних) рівні.

Канали зв'язку можуть бути використані для несанкціонованого доступу до даних, з метою їх перехоплення або цілеспрямованої зміни [2]. Основні види ризику з порушення кібербезпеки на транспортному засобі відображено у документі [3].

Джерелом загрози безпеці може бути внутрішні елементи автомобіля. До автомобіля можуть бути підключені пристрої, які порушують роботу системи керування автомобілем. Також до автомобіля можуть бути підключені пристрої, які виконують, крім основної заявленої функції, приховані функції, які спрямовані на збір даних або порушення роботи систем на автомобілі. Шкідлива програма може видаляти чи спотворювати дані, які передаються між різними блоками керування по шині. Програма може блокувати певні блоки керування або генерувати нові дані, імітуючи роботу блоків керування, яких фізично немає в автомобілі.

Загрозою безпеки може бути зовнішній вплив, спрямований на канал зв'язку транспортного засобу із зовнішнім світом. Зловмисниками може бути організована DoS атака – надходження великої кількості запитів на обслуговування, як правило, з різних джерел, що призводить до порушення роботи сервісу, якій відповідає за обробку повідомлень по каналах зв'язку.

Основна мета зловмисника – отримати привілейований доступ до ядра програмного забезпечення. Тоді шкідлива програма матиме доступ до всіх даних, які не можуть бути виявлені системою безпеки. Шкідлива програма може керувати системою безпеки і змінювати логіку роботи ядра. За певною подією або часом, шкідлива програма може включити свій алгоритм управління, який може призвести до катастрофи.

Розробники шкідливих програм можуть аналізувати та використовувати вразливості програмного забезпечення, встановленого виробником обладнання. Також використовуються вразливість неякісного оновлення, особливо якщо таке оновлення виконується каналами спільного зв'язку.

Передача даних по широкомовних каналах, до яких належить радіозв'язок та Інтернет, може бути перехоплена стороннім програмними або апаратними засобами, які знаходяться в зоні дії мережі. Шляхом запису та подальшого аналізу всього або вибіркового трафіку, зловмисник може отримати відомості про приховану інформацію.

Інтерес представляє коди доступу, паролі та ключі до шифрування даних. Частина даних може бути записана та згодом відтворена у необхідний для зловмисника час.

На інформаційну безпеку впливає людський фактор, який може вносити зміни до електричної схеми плати контролера, перепрограмувати пам'ять блоку управління, встановлювати неперевірені прошивки, підключати сумнівне обладнання та ін.

Аналізуючи дані, отримані шляхом несанкціонованого доступу до каналу передачі, зловмисник може отримати інформацію про транспортний засіб. Інтерес представляють ідентифікатори автомобіля, версії програм і прошивок, режим використання (пробіг, швидкість та напрямок руху), дані з датчиків, журнал відмов, дані поточного стану, параметри конфігурації, дані моніторингу тощо. Метою несанкціонованого доступу може бути конфіденційна інформація про власника: особисті дані, режим роботи та відпочинку, інформація про рахунки, дані про контакти, інформація про місцезнаходження, особисті уподобання та ін.

Часто кібератака на автомобіль здійснюється для його несанкціонованого заволодіння шляхом відключення системи охорони або іммобілайзера, а також інших систем, які дозволяють відстежити або вплинути на роботу викраденого автомобіля.

Впроваджене шкідливе програмне забезпечення може негативно впливати на роботу водія, викликаючи збої в роботу систем автомобіля, виконуючи виведення незрозумілої або неправдивої інформації на панель приладів, зміни налаштування системи забезпечення комфорту, записувати або видаляти коди несправності бортової системи самодіагностики. Небезпечно, якщо порушуватиметься робота тих систем автомобіля, які відповідають за безпеку: система гальмування, кермового керування, світлової сигналізації тощо.

Інформаційна безпека поширюється не тільки на транспортний засіб, але й на сервери та комп'ютери, на яких проводиться обробка транспортної, логістичної та діагностичної інформації. В даний час найкращий захист мають хмарні сервери. Погано можуть бути захищені комп'ютери, які знаходяться на підприємстві автомобільного транспорту, особливо якщо один комп'ютер виконує кілька сервісних функцій (база даних, Веб-сервер, файловий сервер, поштовий сервер і т.п.). На таких підприємствах рідко працюють професійні адміністратори та фахівці кібербезпеки. Тому такі комп'ютери вразливі до поширення вірусів, можуть мати низький захист мережі, на них може бути встановлено не ліцензійне програмне забезпечення, нерідкі випадки поширення шкідливих програм через USB або Інтернет. Метою шахраїв – це персональні та фінансові дані, впровадження модулів для проведення DoS атак, віддалене керування комп'ютером тощо [4].

Широке впровадження інформаційних технологій у всі сфери діяльності, включаючи транспорт, вимагає професійного підходу до забезпечення кібернетичної безпеки на всіх рівнях.

Література

1. Мигаль В.Д. Інтелектуальні системи в технічній експлуатації автомобілів: монографія. Х.: Майдан, 2018. 262 с.
2. Колодяжний В.М., Левтеров А.І., Малащук Є.В. Кібербезпека автомобілів: історія цифровізації автомобілів, поточний стан проблеми, цілі сталого розвитку та стандарти, Вісник ХНАДУ, Вип. 96, 2022, С. 59-65.
3. Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system, UN Regulation No. 155. URL: https://eur-lex.europa.eu/eli/reg/2021/387/oj.
4. Диогенес Ю., Озкайя Э. Кибербезопасность: стратегии атак и обороны, ДМК Пресс, 2020, 326 с.

УДК 656.051

ОГЛЯД ТЕХНІЧНИХ ЗАСОБІВ ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ У ВІДЕОРЯДІ КАМЕР ВІДЕОСПОСТЕРЕЖЕННЯ ТРАНСПОРТНИХ СИСТЕМ

Симбірський Геннадій Дмитрович, доцент,
Харківський Національний автомобільно-дорожній університет

Анотація. *Проведений огляд систем детектування аномалій в відеоряді камер відеоспостереження автотранспортного комплексу. Досліджено склад сучасних систем відеоспостереження та систем детектування аномалій в відеоряді на їх основі. Розроблено функціональну схему такої системи на базі інтелектуальної IP відеокамери. Представлена класифікація систем детектування аномалій у відеоряді камер відеоспостереження.*

Ключові слова: *аномалії відеоряду, системи детектування аномалій, класифікація систем детектування аномалій у відеоряді, інтелектуальні камери відеоспостереження.*

Відеоспостереження – це процес спостереження за об’єктами та процесами, що реалізується із застосуванням оптико-електронних пристроїв, призначених для візуального контролю та автоматичного аналізу [1]. Для контролю різноманітних процесів та об’єктів з метою запобігання широкому спектру ризиків та небезпек сьогодні широко використовуються системи відеоспостереження, тобто комплекс технічного обладнання та програмного забезпечення, що призначений для моніторингу перебігу та поведінки цих процесів та об’єктів.

Такими процесами та об’єктами можуть бути, наприклад, автомобілі, що рухаються по вулиці або по заміській трасі, дорожнє покриття під час контролю його стану та якості, система охорони, в тому числі кібербезпека, будь-якого дорожньо-транспортного об’єкту чи транспортного засобу.

Щодо аномалій у відеоряді камер спостереження, то вони можуть належати до корисної інформації, тобто бути свідченням якихось порушень у нормальному перебігу спостережуваних процесів. В цьому випадку реєстрація або детектування аномалій і є основною метою відеоспостереження. Наприклад, при відеоспостереженні за транспортним потоком на перехресті нормальним перебігом подій буде безпечний рух автомобілів, а ось аномалією у відеоряді камер спостереження буде зіткнення автомобілів, тобто дорожньо-транспортна пригода. Аномалії у відеоряді камер спостереження можуть бути також обумовлені, наприклад, несправностями апаратури або перешкодами в тракті передавання сигналу від відеокамер. Тому одним з важливих завдань системи детектування аномалій у відеоряді камер відеоспостереження є вміння вилучати зайву чи непотрібну інформацію з відеоряду.

Метою даного дослідження є огляд систем виявлення аномалій у відеоряді камер відеоспостереження, встановлених в транспортних системах.

У промисловості камери спостереження можуть використовуватись для централізованого стеження за виробничим процесом або у разі наявності середовища, небезпечного для людини. Системи відеоспостереження можуть знімати безперервно або вмикатись лише за заданою подією. Досконаліші системи стеження з використанням відеореєстраторів дозволяють створювати записи, які зберігатимуться роками, з різною якістю та з додатковими можливостями (такими як виявлення рухів та оповіщення через електронну пошту) [2].

Відеоряд є продуктом дії відеокамер систем спостереження і відноситься до часових рядів, дослідженню яких, в тому числі, і їх аномалій, присвячено чимало робіт. А от досліджень аномалій власне у відеорядах не так вже і багато.

Зазвичай відеоряд розглядається як послідовність кадрів, і суттєві зміни від одного кадру до іншого можуть вказувати на виникнення нових ситуацій, і це розглядається як вихід із стану стабільності, тобто як аномалія [1]. Інших визначень, що є аномалією у відеорядах, ми в україномовному та російськомовному інтернеті не знайшли. Тобто зрозуміло, що аномалія у відеоряді це щось відмінне від його загального характеру. Можливо, подальші дослідження дозволять дати ще одне визначення аномалії у відеорядах.

Нами був проведений аналіз чималої кількості наукових робіт, в яких розглядаються проблеми, пов'язані з дослідженням відеорядів. Це не тільки відеокамери, що використовуються для відеоспостереження у системах безпеки, але й ті відеокамери, що використовуються у багатьох інших сферах людської діяльності. Це оборона, промисловість, медичні дослідження, сільське господарство, різноманітні наукові дослідження, у тому числі космічні, та багато інших.

Великий обсяг відеоданих, які продукуються останнім часом та невпинно продовжують продукуватися, потребують автоматизованої обробки із залученням потужних комп'ютерів, спеціалізованого програмного забезпечення та новітніх інтелектуальних інформаційних технологій. Зараз роль людини в аналізі відеоряду с точки зору пошуку аномалій практично зведена до мінімуму. Це пояснюється і великим обсягом відеоданих, що потребують аналізу, і низькими можливостями людини порівняно з обчислювальною технікою (швидкість роботи, особливості зору та інше).

В рамках поставленої задачі дослідження нас цікавлять технології, системи і методи, що були запропоновані та розроблені для отримання, обробки та аналізу відеорядів та зображень, включаючи задачі машинного зору, класифікація зображень, детектування об'єктів та аномалій, сегментація зображень, тощо. Не дуже багато зустрілося наукових робіт на цю тему, в яких би систематизувалися та класифікувалися ці вищезгадані технології, системи і методи. Однією з таких робіт є дослідження [1], завдання якого (серед інших) його автори оголосили як аналіз існуючих рішень в області відеоспостереження та суміжних областей.

В [1] вказано, що всі системи відеоспостереження, незалежно від виду, включають такі технічні компоненти: блок живлення, кабель, жорсткий диск для запису і зберігання відеосигналу з камер, монітор, відеореєстратор або комп'ютер для локального перегляду та зберігання відеозапису, Інтернет для використання відеореєстратора з хмарним сервісом при перегляді відеозапису в онлайн режимі.

Сучасну систему відеоспостереження та систему виявлення аномалій в відеоряді на її основі можна представити у вигляді наступної функціональної схеми (рис. 1).

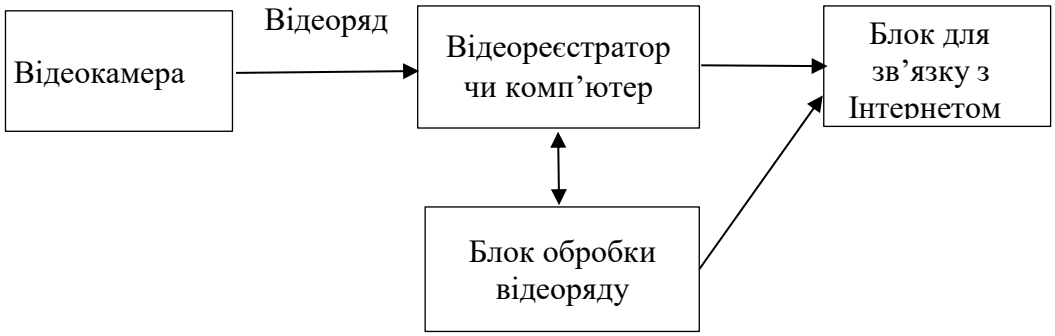


Рис. 1. Функціональна блок-схема системи детектування аномалій в відеоряді

Система детектування аномалій в відеоряді чи система відеоспостереження функціонує наступним чином. Відеоряд, тобто корисний сигнал від відеокамери, який є результатом відеоспостереження, потрапляє до відеореєстратора чи комп’ютера для реєстрації, подальшої обробки та зберігання.

Відеореєстратор – це електронний пристрій, призначений для запису, зберігання та відтворення відеоінформації [3]. Він схожий по будові з комп'ютером або відеосервером і містить у своєму складі аналого-цифровий перетворювач (АЦП), процесор, жорсткий диск та інші компоненти. Для управління відеореєстратором на ньому встановлена спеціалізована операційна система. Перед записом оцифровані відеозображення, як правило, піддаються компресії для зменшення займаного місця на жорсткому диску. Практично всі відеореєстратори можуть працювати як з монохромними, так і з кольоровими відеозображеннями. Багато відеореєстраторів мають можливість підключення до комп'ютерної мережі для передачі відеозображень на комп'ютери віддалених користувачів.

У випадку використання відеореєстратора обробка відеоряду здійснюється у блоці обробки відеоряду. Цей процес обробки відеоряду з метою виявлення загроз чи аномалій у сукупності з відповідним програмним забезпеченням називається відеоаналітикою і може реалізовуватися як окремими пристроями, так і програмним забезпеченням комп’ютера чи відеореєстратора. Результати роботи відеоаналітики чи сам відеоряд можуть бути передані до мережі Інтернет за допомогою блоку для зв’язку з Інтернетом.

Треба відмітити, що важко відокремити системи детектування аномалій в відеоряді від самої системи відеоспостереження, тому далі в цьому розділі будемо вести мову про системи відеоспостереження в цілому. Тим більше, що технічний рівень людства в цілому і, зокрема, радіоелектроніки та обчислювальної техніки дозволяє чи дозволить в близькому майбутньому об’єднати різні функціональні блоки системи, що зображена на рис.1, без істотного збільшення габаритів. Це буде показано далі.

На рис. 2 наведемо приклад функціональної блок-схеми системи детектування аномалій в відеоряді для випадку об’єднання функціональних блоків.

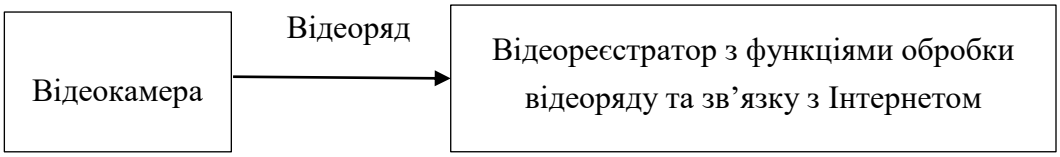


Рис. 2. Функціональна блок-схема системи детектування аномалій в відеоряді з об’єднаними блоками

Зараз на ринку пристроїв для відеоспостереження з’явилися автономні керовані роботизовані поворотні Internet Protocol (IP) камери відеоспостереження, які дають можливість видалено повертати об'єктиви по горизонталі і вертикалі для збільшення обсягу контрольованого простору, наприклад, Hikvision DS-2DF8C448I5XS-AELW [4].

Управління такою відеокамерою здійснюється в додатку для смартфонів та планшетів або ж у програмному забезпеченні для самої системи відеоспостереження. Такі пристрої є бездротовими і можуть передавати відео онлайн через Інтернет у реальному часі, а також записувати архів в хмарну область або на карту пам'яті обсягом до 256 Гб.

Це сучасний самодостатній інструмент для відеоспостереження, який має програмне відеоаналітичне забезпечення і не потребує додаткового обладнання. Відеокамери спостереження такого типу, що виробляються відомими фірмами, коштують 100 тисяч гривень і більше за штуку. Тому такі камери поки не дуже поширені, але практика

доводить, що згодом такі пристрої подешевшають та будуть широко використовуватись в системах відео спостереження.

Поки що дослідникам та фірмам і установам, що займаються впровадженням систем відеоспостереження, доводиться вибирати пристрої, які складають такі системи, в залежності від фінансової спроможності замовника та обсягу його вимог до завдань системи відеоспостереження.

Для роботизованої IP відеокамери з відеоаналітикою функціональна блок-схема системи детектування аномалій в відеоряді має наступний вигляд (рис.3):

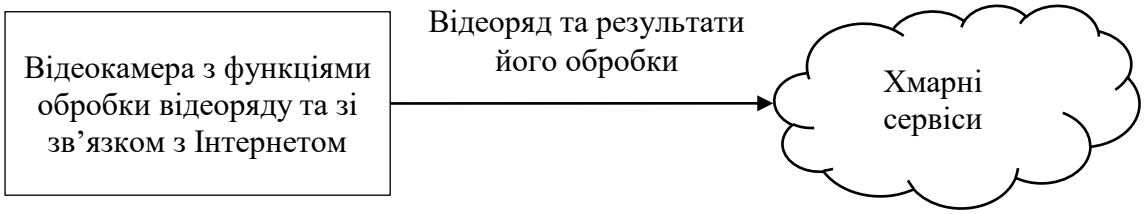


Рис. 3 - Схема системи детектування аномалій в відеоряді з об'єднаними функціональними блоками

Бачимо, що така відеокамера об'єднує функції декількох блоків системи, яка зображена на рис. 1. Такий пристрій для відеоспостереження самостійно може зберігати певний обсяг відеоінформації, може передавати її для зберігання по хмарним технологіям. Ця відеокамера також може обробляти отриману відеоінформацію по певним алгоритмам самостійно (в рамках своїх можливостей), а може передавати її для хмарних обчислень, якщо потрібні більш потужні обчислювальні ресурси.

Вищезазначені найсучасніші системи детектування аномалій в відеоряді – це все ж таки справа майбутнього. Тому задача класифікації дещо простішої традиційної техніки, яка зараз переважним чином використовується у системах детектування аномалій в відеоряді у нинішній час, продовжує бути актуальною.

Прийнято виділяти кілька типів класичних систем відеоспостереження [1] в залежності від використовуваного технічного оснащення [5].

1) Аналогові системи. Склад комплектуючих: AHD/HD-CVI/HD-TVI камера відеоспостереження, цифровой відеореєстратор (Digital Video Recorder (DVR)).

2) Цифрові системи. В їх основу покладено IP-технології. Абревіатура IP (Інтернет-протокол - Internet Protocol, англ.) зазначає збірку правил, за якими потрібно використовувати технологію інтернет для обміну інформацією між комп'ютерними мережами. Мається на увазі використання IP відеокамер спільно з мережевими комутаторами. Склад комплектуючих: IP камера відеоспостереження, мережевий відеореєстратор (Network Video Recorder (NVR)) та мережевий комутатор для підключення відеокамер і відеореєстраторів до мережі Інтернет.

3) Змішані (гібридні) системи. Принцип їх роботи засновано на прийомі відеозображення з аналогових камер та на оцифруванні зображення для подальшого використання.

Аналогові системи не дуже сучасні, проте іноді використання цього типу систем є обґрунтованим [5].

Цифрові системи сьогодні є більш перспективними в порівнянні з аналоговими системами: покращена якість відеозображення, гнучкість і легка масштабованість, можливість глибокого аналізу і віддаленого налаштування, простота інтеграцій в існуючу комп'ютерну мережу.

Гібридні системи є поки що найбільш поширеними. В них якість одержуваного зображення поступається системам з цифровим форматом, але інші параметри роботи

систем цього типу нічим не відрізняються від аналогічних характеристик цифрових систем, а це дає можливість створювати надійні і багатофункціональні системи змішаного типу.

Спробуємо наочно представити класифікацію систем детектування аномалій у відеоряді, базуючись на зазначених вище класах цих систем (рис. 4).

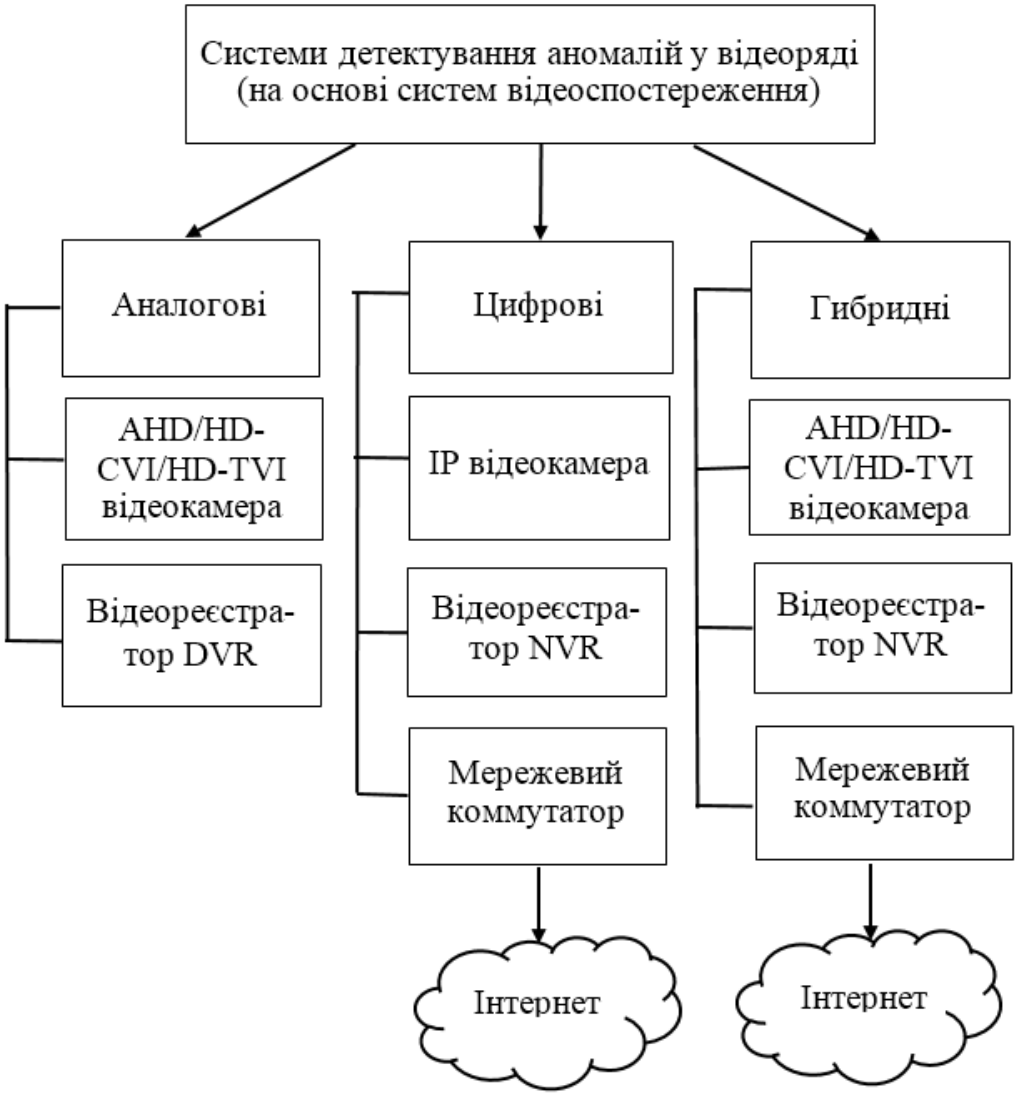


Рисунок 4. Схема класифікації систем детектування аномалій у відеоряді камер спостереження

Відмітимо, що сучасні системи відеоспостереження обов'язково використовують Інтернет і для цього мають в своєму складі або відеокамери та відеореєстратори для отримання, запису і збереження відеозображення, а також маршрутизатор та блок управління всіма відеокамерами, або одну мережеву IP-відеокамеру для невеликих територій чи локальних завдань. Для передачі відеоінформації одночасно з декількох пунктів система відеоспостереження може складатися з декількох мережевих відеокамер.

Таким чином, проведений вище аналіз показує, що для сучасних відеокамер для спостереження огляд систем детектування аномалій в відеоряді тотожній огляду методів виявлення аномалій в відеоряді камер спостереження. Всі наведені вище схеми

функціонально не відрізняються, але з невпинним розвитком оптики, електроніки та обчислювальної техніки поступово змінюється апаратний склад систем детектування аномалій у відеоряді камер відеоспостереження.

Для кращого розуміння можна сказати, що зараз обчислювальні та комунікативні (мережеві) можливості IP-відеокамер кращі, ніж у потужних комп'ютерів 2000-х років. Ті блоки у складі таких систем, що потребували для експлуатації систем відеоспостереження окремих корпусів та багатьох кабелів, перетворились на невеликі мікропроцесорні плати, що легко вмонтовуються до корпусів IP-відеокамер. Але ж і нові методи обробки результатів відеофіксації (а це здебільшого методи, що пов'язані з використанням нейронних мереж) потребують значно більших обчислювальних потужностей. Тут у нагоді стають мережеві можливості IP-відеокамер та хмарні сервіси, за допомогою яких по новим мережевим технологіям зберігаються і обробляються величезні обсяги зафіксованих даних.

Список літератури

1. Рувінська В.М., Девятков В.В. Відеоспостереження для систем безпеки: моделі, методи та запропоновані рішення. *Інформатика та математичні методи в моделюванні*. 2021. Том 11. № 4. С. 331-342.
2. Відеоспостереження. URL: https://uk.wikipedia.org/wiki/%D0%92%D1%96%D0%B4%D0%B5%D0%BE%D1%81%D0%BF%D0%BE%D1%81%D1%82%D0%B5%D1%80%D0%B5%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F (дата звернення: 01.11.2022).
3. Відеореєстратор. URL: https://uk.wikipedia.org/wiki/%D0%92%D1%96%D0%B4%D0%B5%D0%BE%D1%80%D0%B5%D1%94%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%BE%D1%80 (дата звернення: 01.11.2022).
4. Роботизированная камера SpeedDome Hikvision DS-2DF8C448I5XS-AELW(T5) DarkFighter с лазерной подсветкой. URL: https://vario.com.ua/ptz-robotizirovannaya-kamera-speeddome-hikvision-ds-2df8c448i5xs-aelwt5-darkfighter-s-lazernoy-podsvetkoy/?gclid=Cj0KCQjw4omaBhDq ARIsADXULuUk4Pc554R11Rizwk_Fe8MZ6JRxC8HQB-AIl-2Jn7yc-Jp0fShCu6QaAlqCEALw_wcB (дата звернення: 01.11.2022).
5. Особливості камер відеоспостереження. URL: https://worldvision.com.ua/ru/kak-vybrat-naruzhnuu-kameru-rabotaushchuu-ot-batarei/ (дата звернення: 01.11.2022).

УДК 378:004

ОСОБЛИВОСТІ ПІДГОТОВКИ БАКАЛАВРІВ З КІБЕРБЕЗПЕКИ У ВІТЧИЗНИНИХ ТА ЕВРОПЕЙСЬКИХ ВИШАХ

Шевченко В.О. к.т.н., доцент каф. інформатики та прикладної математики, Харківський національний автомобільно-дорожній університет
Трунов С.В. ст.лаборант каф. інформатики та прикладної математики, Харківський національний автомобільно-дорожній університет

Анотація. В статті проаналізовані освітні програми вітчизняних та зарубіжних вищих навчальних закладів, що готують бакалаврів за спеціальністю «Кібербезпека», зроблена порівняльна характеристика освітніх послуг, представлені висновки щодо підвищення якості підготовки фахівців з кібербезпеки.

Ключові слова: кібербезпезка, автомобільна кібербезпека, ВНЗ, освітня програма, знання, вміння, якість підготовки.

Фахівець з кібербезпеки – це сучасна професія, яка користується поширеним попитом як в нашій країні, так і в інших. Згідно статистичних даних, що опубліковані у листопаді 2021 року журналом Cybersecurity Ventures, який є провідним світовим дослідник глобальної кіберекономіки у м. Нью Йорк, США, в 2021 році світ мав нестачу фахівців у галузі кібербезпеки в 3,5 мільйона [1].

Але доцент кафедри інформаційної безпеки КПІ та керівник проекту "Кібер Академія" по співпраці між бізнесом та вищими навчальними закладами у сфері кібер-освіти Олексій Барановський стверджує, що із 900 молодих українських IT-спеціалістів лише десять обирають своєю спеціальністю кібербезпеку. Чому при такому попиті на фахівців, наша молодь не працює за фахом? Олексій Барановський вважає, що причина цього у системі нашої освіти [2].

Спробуємо розібратися в цій проблемі. Для цього порівняємо що і як викладають майбутнім кібербезпечникам у ВНЗ різних країн.

Були переглянуті сайти 52 вітчизняних [3] та 20 зарубіжних ВНЗ [4], де готують фахівців з кібербезпеки на рівні бакалавр. На жаль, жоден ВНЗ не навчає спеціалістів з автомобільної кібербезпеки. Можливо, диференціація за різними спеціалізаціями відбувається на рівні магістерської підготовки, але метою дослідження є огляд освітніх послуг на рівні бакалавр, тому магістерські програми не розглядалися. Огляд освітніх програм підготовки магістрів за спеціальністю «Кібербезпека» буде темою наступного дослідження. Тому за неможливістю провести аналіз підготовки бакалаврів з кібербезпеки автомобільного транспорту, дослідження було проведено у загальній сфері підготовки бакалаврів з кібербезпеки.

Також з усіх переглянутих сайтів освітні програми були доступні на сайтах 27 вітчизняних та 10 зарубіжних ВНЗ. Тому порівняльна характеристика була проведена за даними 37 ВНЗ.

Як порівняльні вибрані три параметри, за якими оцінюється кібербезпечник як фахівець:

1 – вміння програмувати та читати програмні коди;

2 – вміння володіти веб-технологіями;

3 – знання баз даних [5-7].

Одиницею виміру якості підготовки бакалаврів вибраний кредит. Зараз усі вищі навчальні заклади як в Україні, так і за кордоном, працюють за кредитно-модульною або кредитно-трансферною системою навчання, що дозволяє оцінити об’єм навчальних послуг безпосередньо у кредитах.

Розглянемо об’єм навчальних послуг, що пропонується різними вишами по кожному з вибраних параметрів.

Перше вміння – вміння програмувати - вважається головним критерієм рівня підготовки фахівця з кібербезпеки. Тобто фахівець-кібербезпечник повинен володіти кількома сучасними мовами програмування. В моєму дослідженні я не мала за ціль порахувати скільки мов програмування вивчають студенти протягом всього навчання. Мною було визначено, скільки кредитів відведено на вивчення різних мов програмування взагалі по кожному ВНЗ. Результати класифіковані на групи залежно від кількості кредитів та наведені в табл. 1, 2. Також в таблицях наведені відсоткові співвідношення між кількістю кредитів.

Таблиця 1 Загальна кількість кредитів на вивчення мов програмування у вітчизняних ВНЗ

Кредити на програмування				
немає	≤ 5	≤ 10	≤ 15	>15
4	2	10	4	7
Відсотки				
15%	7%	37%	15%	26%

Таблиця 2 Загальна кількість кредитів на вивчення мов програмування у зарубіжних ВНЗ

Кредити на програмування			
≤ 5	≤ 10	≤ 15	>15
0	0	4	6
Відсотки			
0%	0%	40%	60%

Згідно результатам дослідження, що представлені в табл. 1, зовсім не передбачають вивчення мов програмування при підготовці бакалаврів з кібербезпеки 15 відсотків ВНЗ в Україні. Це зовсім незрозумілий та неочікуваний мною результат. Як в сучасному світі можна захищати інформацію, запобігати різних кібератак, якщо не володіти жодною мовою програмування, не розуміти жоден програмний код? Звичайно, студенти подібних ВНЗ вивчають інші спеціальні предмети, такі, як криптозахист та кодування інформації та ін., але від фахівця з кібербезпеки чекають поглибленого знання технологій програмування, що неможливо придбати без вивчення спеціальних дисциплін з програмування.

Зовсім інша картина спостерігається за результатами дослідження викладання мов програмування у зарубіжних ВНЗ, що наведені в табл. 2. Всі зарубіжні ВНЗ викладають студентам різні мови програмування, при цьому я не знайшла жодного ВНЗ, де кількість кредитів на програмування була менше 10. А більшість закордонних ВНЗ (60%) пропонує студентам на вивчення мов програмування більше 15 кредитів. Моє дослідження також показало, що ця цифра значно більше 15, мова йде про 40 – 60 кредитів на 3 роки підготовки бакалаврів. Тобто за кордоном студенти вивчають різні технології програмування увесь час навчання у ВНЗ.

Далі проаналізуємо, скільки часу у кредитах пропонується на вивчення мережних технологій. Дані дослідження по розподілу кредитів на вивчення мережних технологій наведені в табл.3, 4.

Таблиця 3 Загальна кількість кредитів на вивчення мережних технологій у вітчизняних ВНЗ

Кредити на мережні технології				
немає	≤ 5	≤ 10	≤ 15	>15
5	6	9	5	2
Відсотки				
19%	22%	33%	19%	7%

Таблиця 4 Загальна кількість кредитів на вивчення мережних технологій у зарубіжних ВНЗ

Кредити на мережні технології				
немає	≤ 5	≤ 10	≤ 15	>15
1	2	1	3	3
Відсотки				
10%	20%	10%	30%	30%

За даними табл. 3 та табл. 4 можна зазначити, що декількох вітчизняних, так само і в зарубіжних ВНЗ, програми не передбачають вивчення мережних технологій. Можна допустити, що студенти вивчають веб-технології у межах інших дисциплін, але щоб це довести треба провести додаткове дослідження.

В табл. 5, 6 наведені дані дослідження кількості кредитів на вивчення баз даних студентами спеціальності «Кібербезпека».

Таблиця 5 Загальна кількість кредитів на вивчення баз даних у вітчизняних ВНЗ

Кредити на бази даних				
немає	≤ 5	≤ 10	≤ 15	>15
14	5	8	0	0
Відсотки				
52%	19%	30%	0%	0%

Таблиця 6 Загальна кількість кредитів на вивчення баз даних у зарубіжних ВНЗ

Кредити на бази даних				
немає	≤ 5	≤ 10	≤ 15	>15
1	1	5	3	3
Відсотки				
10%	10%	50%	30%	30%

З табл. 5 видно що освітні програми більше половини досліджених вітчизняних ВНЗ (52%) не передбачають вивчення баз даних. Для зарубіжних ВНЗ (табл. 6) цей показник складає 10%. У ВНЗ, в яких вивчають бази даних, пропонується на ці дисципліни переважно по 10 кредитів як у вітчизняних, так і у зарубіжних ВНЗ.

Таким чином, очевидно, що найбільші розбіжності між освітніми послугами вітчизняних та зарубіжних ВНЗ ми маємо у сфері викладання технологій програмування. Можна припустити, що випускники вітчизняних ВНЗ спеціальності «Кібербезпека» не працюють за фахом, бо не мають достатній рівень знань та вмінь в області програмування.

Література

1. Cybersecurity Jobs Report: 3.5 Million Openings In 2025. URL: https://cybersecurityventures.com/jobs/ (дата звернення 25.10.2022).

2. Навчання кібербезпечників: застарілі програми і проблеми зі спеціалізацією. URL: https://24tv.ua/ru/navchannya_kiberbezpechnikiv_zastarili_programi_i_problemi_zi_spetsializatsiyeyu_n1320757 (дата звернення 25.10.2022).
3. Education.ua. Кібербезпека. URL: https://www.education.ua/universities/?speciality=627 (дата звернення 26.10.2022).
4. Keystone. Bachelor studies. Cybersecurity https://www.bachelorstudies.com/Bachelor/Cyber-Security/Europe/ (дата звернення 27.10.2022).
5. Хто такий фахівець з кібербезпеки та як ним стати? URL: https://te.itstep.org/blog/who-is-a-cybersecurity-specialist (дата звернення 25.10.2022).
6. How To Learn Cybersecurity on Your Own [Get Started Guide]. URL: https://www.springboard.com/blog/cybersecurity/how-to-learn-cybersecurity (дата звернення 25.10.2022).
7. Cyber Security Specialist job description. URL: https://resources.workable.com/cyber-security-specialist-job-description (дата звернення 25.10.2022).

УДК

ЗАДАЧА ІНТЕГРАЦІЇ ЗЕМЕЛЬНОГО ТА МІСТОБУДІВНОГО КАДАСТРІВ

К. О. МЕТЕШКІН, д.т.н., професор кафедри земельного адміністрування та геоінформаційних систем, ХНУМГ ім. О. М. Бекетова.
Л. О.МАСЛІЙ, старший викладач кафедри земельного адміністрування та геоінформаційних систем, ХНУМГ ім. О. М. Бекетова.

На даний момент в Україні існує тринадцять галузевих кадастрів та дев'ятнадцять реєстрів у різних сферах. Відомо, що кадастри належать до класу спеціалізованих геоінформаційних систем, які вирішують низку важливих та актуальних завдань, зокрема, пов'язаних із земельними відносинами в Україні [1]. До яких належать завдання оцінки земель, управління земельними і майновими ресурсами, формування та супровід містобудівного кадастру та інших кадастрів природних ресурсів.

Аналіз та детальне вивчення продуктивності та ефективності функціонування деяких кадастрів, які діють в Україні, показує, що окремі завдання, пов'язані з інформаційним пошуком та управлінням територій, займають багато часу і в деяких випадках не вирішуються без участі експертів. Тому що існуюча законодавча та нормативна база України, яка визначає набори геопросторових даних земельного, містобудівного та інших кадастрів, створює ситуацію коли відсутня система в організації збору, зберігання і забезпечення доступу до просторових даних, що призводить до неефективних відносин щодо їх створення, розповсюдження, обміну та спільного використання геопросторової інформації між відповідними установами.

Наприклад, відбувається включення до складу геопросторових даних одного галузевого кадастру геопросторових даних інших кадастрів. У цій ситуації інформація може пересікатися, накладатися або дублюватися.

В свою чергу сьогодні найпоширенішими є геоінформаційні системи земельного та містобудівного кадастрів. Відсутність загальної системи у роботі із інформацією про нерухомість призводить до неефективного використання земельно-майнових ресурсів, а роздільне ведення земельного й містобудівного кадастрів та реєстру прав на нерухоме майно ускладнюють створення єдиної земельної політики, процесів підготовки загальних рішень і надання послуг. У зв'язку з поділом адміністрування державних реєстрів інтеграція даних стає неможливою. Ці та інші існуючі проблеми не призводять до ефективного управління земельними і майновими ресурсами в Україні [2].

Тому постає задача інтеграції даних земельного та містобудівного кадастрів. Різноманітність та різнотипність даних різних кадастрів ускладнює експертну оцінку та впливає на достовірність та точність вирішення поставленої задачі. Суттєвим недоліком стану управління земельними і майновими ресурсами в Україні є розділене ведення двох систем: кадастрової системи та системи реєстрації нерухомого майна, підпорядкованих різним відомствам.

Звідси випливає, що необхідно, по-перше, розробити процедуру інтеграції даних різних кадастрів, а також створити моделі знань, які б пропонували користувачеві відповідні рішення. Для цього на основі гранично-узагальненої моделі геоінформаційної системи керування (рис. 1), побудованої на основі кадастрів, запропоновано процедуру інтеграції типових шарів баз геоданих різнотипних кадастрів.

На рисунку 1 позначено літерами *І* – інформація, *Д* – директиви (команди), *О* – обмеження та припущення, *К1* – кадастр, наприклад земельний, *К2* – кадастр, наприклад містобудівний, *К3* – кадастр, наприклад водних ресурсів. Символом *Σ* показано процедуру інтеграції даних різних кадастрів.

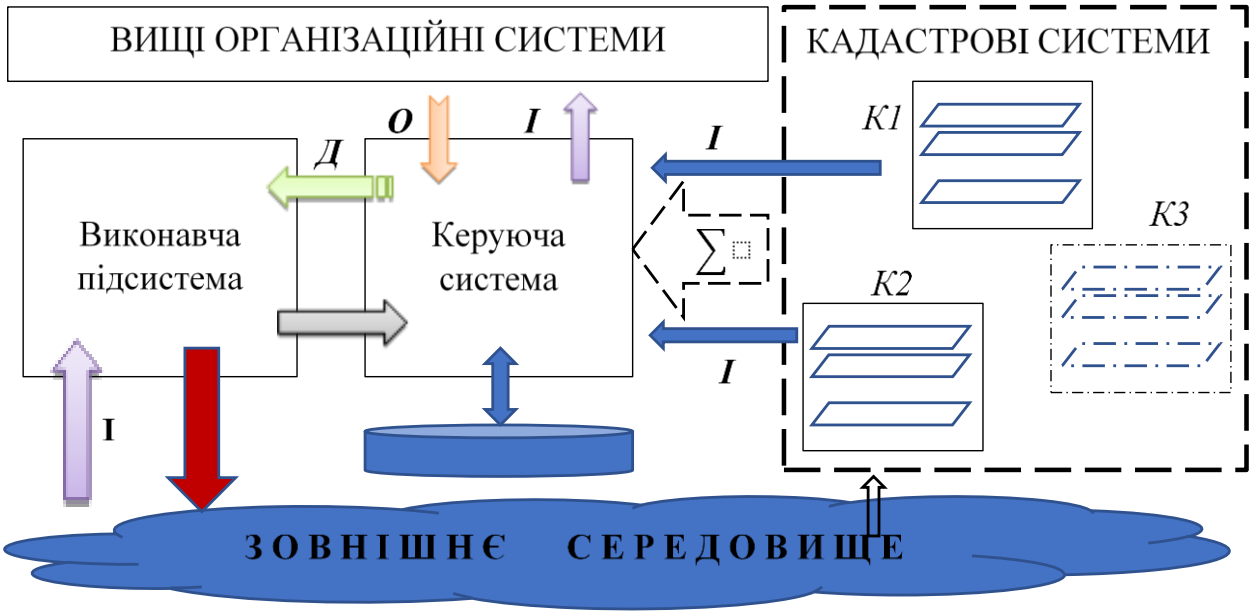


Рисунок 1 – Гранично узагальнена модель інформаційно-керуючої системи, побудованої на основі кадастрів

Як, приклад, для інтеграції типових шарів беремо бази геоданих земельного кадастру *К1* та містобудівного кадастру *К2* (рис.2). Згідно цього рисунку, для вирішення деякої задачі управління територіями, необхідно використовувати дані двох кадастрів, які сформовані для актуальних шарів *К1* і *К2*. Щоб вирішувати такі задачі необхідно розробити спеціальну базу даних та систему управління, в якій можна було б отримати інтегральний результат $\mathbb{N} = K1 \cup K2$.

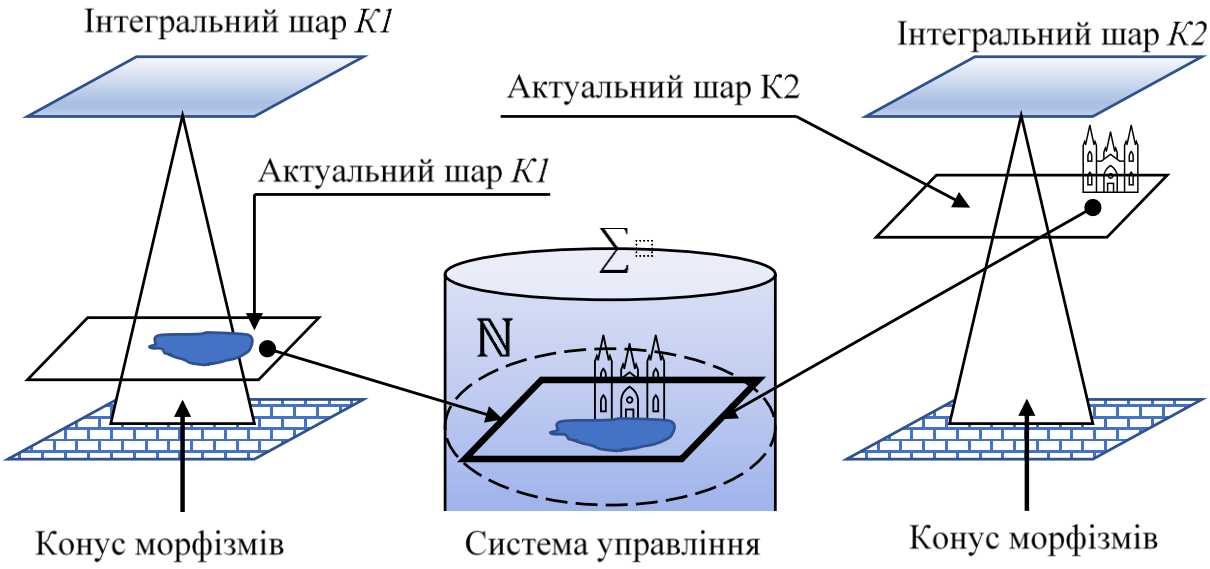


Рисунок 2 – Ілюстрація процесу інтеграції даних двох актуальних шарів *К1* та *К2*

Атрибутивні дані, що лежать в основі конусу морфізмів, відображаються в тому чи іншому типовому шарі кадастру *К1* і *К2* і утворюють інтегральні шари, відповідно.

Враховуючи, що атрибутивні дані можуть відображатися на багатьох шарах того чи іншого кадастру та утворювати інтегральний шар кожного *K1* і *K2*, то за аналогією з результатами досліджень у роботі [3] можна вважати ці конуси Гіперконусами морфізмів. Тоді у формальному вигляді можна записати наступний вираз, позначивши Гіперконуси морфізмів *K1* наступним чином:

$$\amalg^{\nabla} K1 \subseteq \left\{\left\{\{D_1 \supset D_2\} \supset, \dots, \supset D_i\right\} \supset, \dots, \supset D_n\right\} \times \left\{R_1^{\uparrow}, R_2^{\uparrow}, \dots, R_i^{\uparrow}, \dots, R_n^{\uparrow}\right\}.$$

Аналогічну формулу можна записати і для Гіперконусу морфізмів *K2*, де D_i – атрибутивні дані для формування кадастру *K1* і *K2*, відповідно.

Згідно вищесказаного випливає, що така процедура інтеграції може бути реалізована, якщо Гіпреконуси морфізмів відображають на тих або інших шарах однотипні дані або дані з однієї предметної області. У нашому випадку атрибутивні дані різні за своєю суттю. Отже, в системі управління необхідно передбачити спеціальні моделі, які могли б маніпулювати різнотипними даними. Таку можливість забезпечує такий формалізм, як «кореспонденція». У алгебрі відносин така процедура позначається наступним чином:

$$K1 \xrightarrow{Kor} \mathbb{N} \xleftarrow{Kor} K2.$$

На наш погляд, такі відносини можна реалізувати, використовуючи відомі моделі уявлення знань, такі як продукційні або фреймові моделі.

Таким чином сформульовано задачу створення інтеграційних процедур різних кадастрів.

1 Закон України Про Державний земельний кадастр. Верховна Рада України, 2011. URL:https://zakon.rada.gov.ua/laws/show/3613-17#Text (дата звернення: 07.10.2022).

2. Шипулін В. Д. Інтегрована інформаційна система нерухомості. Концепція для України : монографія / В. Д. Шипулін ; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. – Харків : ХНУМГ ім. О. М. Бекетова, 2021. – 90 с. ISBN 978-966-695-518-3

3. Метешкин К. А. Кибернетическая педагогика: теоретические основы управления образованием на базе интегрированного интеллекта. Монография / К.А. Метешкин. – Харьков: Международный Славянский университет, 2004. – 400 с.

4. Постанова Кабінету Міністрів України Про затвердження Порядку ведення Державного земельного кадастру. Кабінет Міністрів України, 2012. URL: https://zakon.rada.gov.ua/laws/show/1051-2012-%D0%BF#Text (дата звернення: 10.10.2022).

5. ДБН Б.1.1-16:2013 «Склад та зміст містобудівного кадастру» [Чинний від 01−09−2013]. – Київ : Міністерство регіонального розвитку, будівництва та житлово-комунального господарства України від № 73, 51 стор.

6. Постанова Кабінету Міністрів України Про містобудівний кадастр. Кабінет Міністрів України, 2011. URL: https://zakon.rada.gov.ua/laws/show/559-2011-%D0%BF#Text (дата звернення: 20.09.2022).

УДК 656.051

ЗАСТОСУВАННЯ ВІДЕОАНАЛІТИКИ В СИСТЕМАХ ВИЯВЛЕННЯ АНОМАЛІЙ У ВІДЕОРЯДІ

Симбірський Геннадій Дмитрович, доцент,
Харківський національний автомобільно-дорожній університет

Анотація. *Проведений аналіз використання відеоаналітики для виявлення аномалій в відеоряді камер відеоспостереження транспортних систем. Досліджено склад сучасних інтелектуальних систем відеоспостереження та систем детектування аномалій в відеоряді на їх основі. Розроблено функціональну схему такої системи на базі інтелектуальної IP відеокамери.*

Ключові слова: *аномалії відеоряду, відеоаналітика, системи детектування аномалій, інтелектуальні камери відеоспостереження.*

Відеоспостереження – це процес спостереження за об’єктами та процесами, що реалізується із застосуванням оптико-електронних пристроїв, призначених для візуального контролю та автоматичного аналізу [1]. Для контролю різноманітних процесів та об’єктів з метою запобігання широкому спектру ризиків та небезпек сьогодні широко використовуються системи відеоспостереження, тобто комплекс технічного обладнання та програмного забезпечення, що призначений для моніторингу перебігу та поведінки цих процесів та об’єктів.

Такими процесами та об’єктами можуть бути, наприклад, автомобілі, що рухаються по вулиці або по заміській трасі, дорожнє покриття під час контролю його стану та якості, система охорони будь-якого об’єкту, в тому числі, система “Розумний дім” та багато чого іншого. Тобто, зараз відеоспостереження використовується без перебільшення в усіх сферах людського життя та діяльності.

Аномалії у відеоряді камер спостереження за транспортними системами - це такий стан спостережуваного об’єкту, що значно відрізняється від нормального перебігу подій та процесів. Для транспортних систем звичний чи штатний перебіг подій – це рівномірний транспортний потік. Тому в цьому випадку аномалії у відеоряді камер спостереження є свідченням якихось порушень у нормальному перебігу спостережуваних процесів, тобто дорожньо-транспортних пригод. Своєчасне детектування аномалій дозволить вчасно реагувати на такі виклики та мінімізувати можливі збитки та шкоду здоров’ю людей. В такий ситуації реєстрація або детектування аномалій і є основною метою відеоспостереження.

Аномалії у відеоряді камер спостереження можуть бути також обумовлені, наприклад, несправностями апаратури або перешкодами в тракті передавання сигналу від відеокамер. Тому одним з важливих завдань систем детектування аномалій у відеоряді камер відеоспостереження є вміння відділяти корисну інформацію від непотрібної.

Метою даного дослідження є розгляд можливості використання сучасних методів відеоаналітики для пошуку та обробки аномалій у відеоряді камер відеоспостереження.

З розвитком мікропроцесорної техніки та хмарних технологій зберігання і обробки інформації важко відокремити системи детектування аномалій в відеоряді від систем відеоспостереження. Ми вважаємо, що з подальшим розвитком радіоелектроніки, інформаційних технологій, обчислювальних потужностей сучасних мікропроцесорів та математичного моделювання кожна система відеоспостереження одночасно буде і системою детектування аномалій в відеоряді.

Сучасні інтелектуальні відеокамери, наприклад, відеокамера Hikvision DS-2DF8C448I5XS-AELW [2], самі являють собою систему детектування аномалій у відеоряді, а відмінності однієї системи детектування аномалій у відеоряді від іншої, це відмінності між собою методів виявлення таких аномалій.

Можна підсумувати, що інтелектуальні відеокамери самі становляться системами детектування аномалій у відеоряді за рахунок наступних чинників:

- наявність у відеокамери модуля для первинної обробки результатів відеоспостереження;
- наявність у відеокамери модуля для зв'язку з Інтернетом, тобто можливості користування хмарними технологіями та сервісами для зберігання та обробки інформації.

Відомі два типи задач, що пов'язані з пошуком аномалій [3] у відеорядах.

1) Виявлення викидів, що визначаються як спостереження, що значно відрізняються від інших. Алгоритми для визначення таких викидів намагаються знайти, на якій ділянці відеоряду знаходиться основна маса даних. Аномальні спостереження заважають використанню цих даних і перед машинним навчанням їх прибирають. Процедуру виявлення таких аномалій називають Outlier detection (виявлення викидів).

2) Виявлення аномальної поведінки в ситуації, коли є спостереження, що описують звичайні стани системи, а при появі нових даних потрібно визначити, чи є вони аномальними. Такий підхід називають Novelty detection (виявлення новизни). Він найбільше підходить для аналізу відеоряду і встановлення, чи є аномалії в новому кадрі порівняно з попередніми.

Одним із самих простих підходів, що використовуються при відеоспостереженні, є відеодетекція [1]. Відеодетектор попіксельно порівнює наступний кадр з попереднім або з групою кадрів і сигналізує про змінення статичних картинок. При цьому визначають заздалегідь, чи враховувати більше або менше змін у глибині кольору, чи виключати реакції на певні зони в кадрі, визначають площу змін. Самим суттєвим недоліком відеодетекції є низька перешкодостійкість. Якщо у зоні відеодетекції, для прикладу, знаходяться гілки, що гайдаються від вітру, то точність значно знижується. І це потребує безвідривного ручного контролю у реальному часі або тривалого перегляду відеоархівів, щоб відстежити важливі події. Такі перешкоди у фіксуємому відеоряді є великою проблемою у процесі відеоспостереження.

Тобто до проблеми величезного обсягу відеоінформації, що неупинно накопичується у процесі відеоспостереження, додається проблема аналізу цієї відеоінформації. До того ж, цей аналіз потрібен бути проведений здебільшого в реальному часі, тобто під час спостережень.

Ми підійшли до моменту, коли потрібно ввести нове для цього дослідження поняття. Це відеоаналітика або аналіз відеоконтенту (Video content analysis або video content analytics (VCA)) — можливість автоматичного аналізу відеоряду для виявлення та визначення часових і просторових подій [3].

Відеоаналітика порівнює не статичні картинки і не пікселі як такі, а зміни характеру активності [1]. Вона працює з динамікою, знаходить новий рух на фоні інших рухів. Коли об'єкт потрапляє в кадр або починає рухатися, аналізується і запам'ятовується його характер активності, що стає ознакою ідентичності даного об'єкта. Реакція наступає при зміні цієї закономірності руху чи на появу іншого характеру руху на кадрі, і навіть їх комбінацій при накладенні. Одне з найактуальніших завдань у системах відеоспостереження – скорочення обсягу марної інформації, видалення непотрібних даних, на відміну від інших підходів відеоаналітики, коли розпізнається потрібна для людини інформація.

Цій меті служить так звана відеосемантика [1] – «короткий логічний виклад відеоінформації шляхом розкладання її на семантичні одиниці (відеосюжети), кожен з

яких має свій закінчений зміст, що відрізняється і від попереднього, і від наступного відеосегмента» [4]. Відеосемантика спрацьовує не при кожному хитанні гілочки з останнього прикладу, а тільки один раз, коли змінилася погода, ставши вітряною. Наступні коливання не будуть зареєстровані, як не важлива інформація. При цьому технологія «коротких даних» вкорочує все, зокрема і самі перешкоди. У панелі видачі результатів буде повідомлення про хитання гілочки, але один раз за час вітряної погоди, це в тисячі разів менше кількох годин постійного відеозапису, зав'язаного на стандартну відеодетекцію.

Одна з перших систем відеоспостереження, що працювала по технології «коротких даних» була технологія автоматизованого спостереження під назвою Annotation of Critical Evidence (ACE) Surveillance (спостереження як анотація критичних доказів, ACE Surveillance) [4]. Вона займається вилученням та обробкою анотованих критичних ділянок відеоспостереження. Технологія ACE складається з модуля ACE Capture (захоплення) та модуля ACE Browser (браузер). ACE Capture працює наступним чином: відеосигнал з камери постійно обробляється на комп'ютері. При виявленні нового об'єкта або активності програмне забезпечення запускає сигнал тривоги. Критичні моментальні знімки даних автоматично фіксуються та зберігаються. Кожний такий знімок забезпечений текстовими анотаціями (пояснювальними підписами), що допомагають зрозуміти дані та підвищують керованість архівними даними.

Анотації до знімків включають: місцезнаходження та розмір об'єкта, що рухається, напрямок, звідки з'явився об'єкт та його швидкість. Браузер ACE відповідає за підготовку, ефективний перегляд і пошук архівних даних. Така структура системи має за мету спростити виявлення аномальних подій в величезній кількості даних відеоспостереження, що зберігаються.

Інший автор [5] дає інше визначення цьому новому науково-технічному напрямку. Відеоаналітика – це апаратно-програмне забезпечення або технологія, що використовує методи комп'ютерного зору для автоматизованого збору даних на підставі аналізу потокового відео (відеоаналізу), яка спирається на алгоритми обробки зображення і розпізнавання образів, що дозволяють аналізувати відео без прямої участі людини.

В принципі ці два визначення не протирічать одне одному. Оба констатують автоматичний характер обробки та аналізу відеоінформації з використанням обчислювальної техніки. Останнім часом використанню відеоаналітики в системах відеоспостереження приділяється дуже велика увага.

Зробимо спробу розібратися в тому, як відеоаналітика співвідноситься з пошуком аномалій у відеоряді камер спостереження. В [5] наведені базові функції відеоаналітики, на яких побудована її робота:

1) Виявлення об'єктів (object detection). Виявлення об'єктів у полі зору відеокамери проводиться за допомогою відеодетекторів руху, до того ж можливий аналіз декількох об'єктів. Якщо рух не є достатньою ознакою для локалізації об'єкта в кадрі, то іноді використовуються шаблони, у тому числі ознаки Хаара, які нам відомі з проблематики комп'ютерного зору.

2) Стеження за об'єктами (object tracking). Алгоритми стеження дозволяють отримати траєкторію руху об'єкта як у полі зору однієї камери, так і по результатам стеження декількома камерами. Наприклад, так визначаються автомобілі, що рухаються з підвищеною швидкостю.

3) Класифікація об'єктів (object classification). Системи відеоаналітики класифікують об'єкти. Наприклад, типовий класифікатор об'єктів, використовуючи ознаки форми і абсолютні розміри, розподіляє об'єкти на групи: людина, групи людей, транспортний засіб.

4) Ідентифікація об'єктів (object identification). Ідентифікація об'єктів є найбільш складним компонентом систем відеоаналітики. Сучасні системи відеоспостереження,

обладнані блоком відеоаналітики, дозволяють ідентифікувати людей за біометричними ознаками особи, або транспортні засоби за номерними знаками.

5) Виявлення (розпізнавання ситуацій). Діючи за певними алгоритмами та використовуючи ті ж операції, що в пунктах 1-4, відеоаналітичне програмне забезпечення дозволяє не лише виділяти об’єкти з потокового відео, але і розпізнавати тривожні ситуації на основі аналізу поведінки цих об’єктів. Така ситуаційна відеоаналітика може автоматично детектувати, наприклад, перетин сигнальної лінії, падіння людей, заборонену парковку, пожежі, тощо.

Наведені вище базові функції відеоаналітики для систем відеоспостереження потребують для своєї реалізації різноманітних методів. Останніми роками з’явилося доволі багато таких методів. В наступному розділі зробимо спробу їх класифікувати та проаналізувати особливості застосування.

Останній пункт вищенаведених базових функцій відеоаналітики майже повністю відповідає тим задачам, які стоять перед системами детектування аномалій у відеоряді камер спостереження. Хоча все залежить від мети створення чи придбання кожної конкретної системи відеоспостереження. З клієнтом чи з замовником такої системи обговорюються її задачі. Треба підібрати такий метод виявлення аномалій у відеоряді камер відеоспостереження чи сукупність методів, щоб він чи вони були здатні вирішувати поставлені безпекові задачі.

Вважаючи на відомості про використання програмних чи апаратних блоків відеоаналітики в системах детектування аномалій у відеоряді камер відеоспостереження наведемо функціональну схему такої системи для інтелектуальної системи детектування аномалій в відеоряді взагалі і для випадку використання теж інтеллектуальної IP-відеокамери (рис. 1).

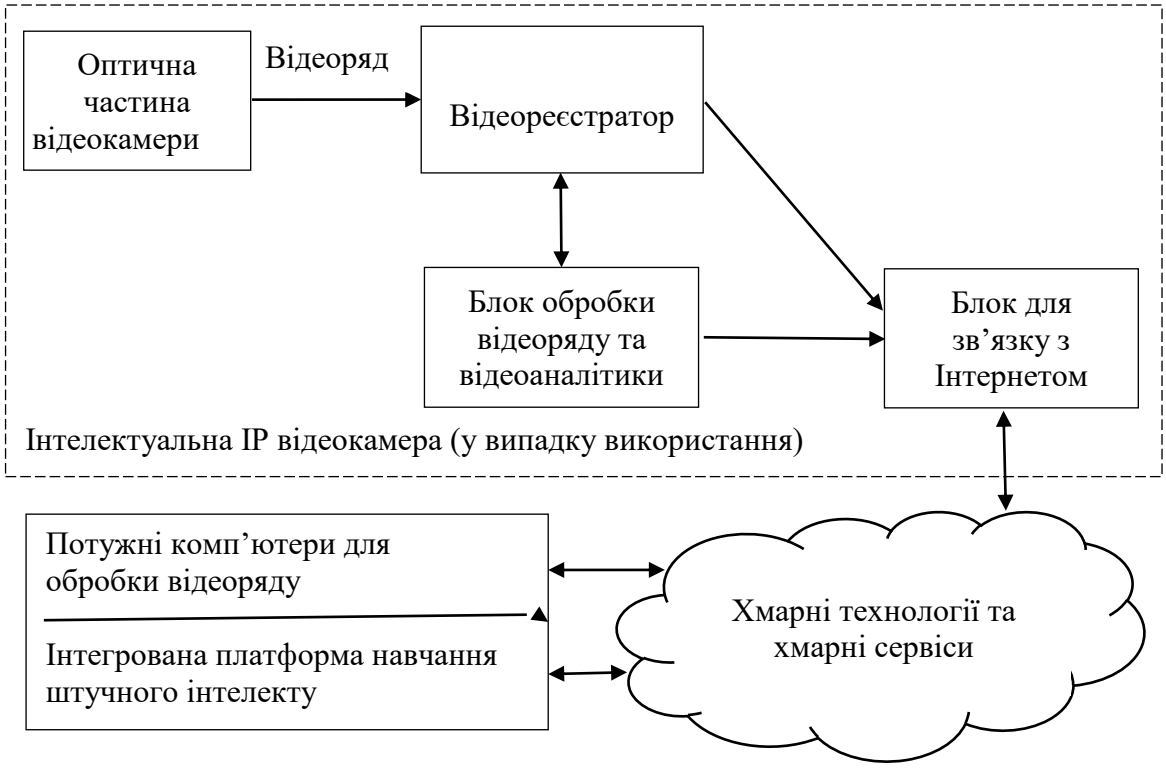


Рисунок 1 - Функціональна схема використання відеоаналітики в інтелектуальній системі детектування аномалій в відеоряді

Функціональна блок-схема інтелектуальної системи детектування аномалій в відеоряді камер відеоспостереження, що зображена на рис. 1, має універсальний характер. Вона показує склад системи детектування аномалій, яка базується на звичайній відеокамері. В цьому випадку сигнал з відеокамери, тобто відеоряд, передається на відеореєстратор для зберігання та подальших операцій. Після відеореєстрації сигнал з відеокамери передається до блоку обробки чи, якщо потрібно, до Інтернету для більш глибокої обробки, для подальшого аналізу чи зберігання. В залежності від задач системи та наявності певної апаратури в кожному конкретному випадку може бути свій склад системи детектування аномалій в відеоряді.

Сучасні інтелектуальні камери відеоспостереження можуть також мати вбудовані функції відеоаналітики. Перевага тут полягає в тому, що такі можливості аналітики у відеокамерах не залежать від смуги пропускання мережі та часу відгуку сервера. Таке рішення вигідне там, де потрібна висока оперативність та негайний відгук. Відеодані в цьому випадку зберігаються на самих відеокамерах і можуть бути вилучені для аналізу будь-коли через віддалену програму-клієнт. В тому випадку, якщо для спостереження використовується інтелектуальна IP відеокамера, вона об'єднує в собі декілька блоків зі схеми 1.6 (пунктирна лінія). Первинна обробка може бути виконана самою камерою (блок обробки відеоряду та відеоаналітики). Якщо ж потрібні більш потужні обчислювальні ресурси, наприклад, у випадку використання нейронних технологій, то використовуються хмарні ресурси.

У будь-якому варіанті використання наведена на рис. 1 система детектування аномалій в відеоряді камер відеоспостереження належить до систем інтелектуальної відеоаналітики (Intelligent Video System (IVS)). Є різні типи інтелектуального відео у сфері IVS: від простих пристроїв, які реєструють будь-який рух взагалі, що вбудовані в нижній щабель цифрових відеокамер, до розвинених систем, котрі класифікують об'єкти та їх поведінку, компенсуючи помилкові тривоги. Деякі системи відеоспостереження та детектування аномалій у відеоряді інтелектуальні за рахунок використання інтелектуальної відеокамери, а деякі – за рахунок їх глибокого навчання у нейронних мережах. Тобто методів використання відеоаналітики для виявлення аномалій у відеоряді камер відеоспостереження чимало, і для їх успішного використання потрібен відповідний аналіз цих методів.

Список літератури

1. Рувінська В.М. Відеоспостереження для систем безпеки: моделі, методи та запропоновані рішення / В.М. Рувінська, В.В. Девятков // Інформатика та математичні методи в моделюванні. – 2021. – Том 11, № 4. – С. 331-342.

2. PTZ роботизированная камера SpeedDome Hikvision DS-2DF8C448I5XS-AELW(T5) DarkFighter с лазерной подсветкой https://vario.com. ua/ptz-robotizirovannaya-kamera-speeddome-hikvision-ds-2df8c448i5xs-aelwt5-darkfighter-s-lazernoy-podsvetkoy/ ?gclid=Cj0KCQjw4omaBhDqARIsADXULuUk4Pc554R11Rizwk_Fe8MZ6JRx C8HQB-AIl-2Jn7yc-Jp0fShCu6QaAlqCEALw_wcB.

3. Відеоаналітика.https://uk.wikipedia.org/wiki/%D0%92%D1%96%D0%B4%D0%B5%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D1%96%D1%82%D0%B8%D0%BA%D0%B0

4. Gorodnichy D.O., Mungham T. Automated video surveillance: challenges and solutions. ACE Surveillance (Annotated Critical Evidence) case study NATO SET-125 Symposium Sensor and Technology for Defence against Terrorism. 2008. URL: https://www.researchgate.net/publication/229040125_Automated_video_surveillance_challenges_and_solutions_ACE_Surveillance_Annotated_Critical_Evidence_case_study.

5. Мусієнко Д.І. Проблеми сучасних систем відеоаналітики / І.Д. Мусієнко // Сучасна спеціальна техніка. – 2014. – № 2 (37). – С. 75-81.

УДК 005.7:519.8

ШЛЯХИ ПОБУДОВИ СИСТЕМ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ АПРІОРНОЇ НЕВИЗНАЧЕНОСТІ

Борисенко Леся Андріївна
студентка V курсу факультету Інфокомунікацій
Харківський національний університет радіоелектроніки, Україна
Добринін Ігор Станіславович
кандидат технічних наук, доцент, доцент кафедри інфокомунікаційної інженерії імені В.В. Поповського
Харківський національний університет радіоелектроніки, Україна

Анотація. У статті відображена важливість розробки та впровадження системи менеджменту інформаційної безпеки. Визначено доцільний математичний апарат для прийняття рішень в умовах апріорної невизначеності. Запропоновано підхід до побудови системи менеджменту інформаційної безпеки в умовах апріорної невизначеності.

Ключові слова: інформаційна безпека, невизначеність, оптимальна стратегія, система менеджменту інформаційної безпеки, теорія ігор.

Забезпечення системи захисту інформації є однією з найважливіших актуальних проблем сьогодення. Стрімкий розвиток суспільства призвів до широкого використання в усіх сферах діяльності швидкодіючих інформаційних систем та технологій. Одночасно збільшилися загрози для інформації, тяжкість наслідків реалізації яких посприяли оновленню розуміння захисту інформації, який полягає у забезпеченні цілісності, доступності та конфіденційності інформації. Сучасне підприємство має на увазі не тільки організацію робочого процесу та документообігу, а й захист конфіденційної інформації, що циркулює у певному приміщенні. Її витік може призвести до серйозних наслідків: втрата таємниць компанії, санкції контролюючих органів, погіршення іміджу компанії, втрата особливо важливої інформації. Саме тому для попередження витоку конфіденційної інформації та уникнення вищеперерахованих наслідків, кожна компанія та підприємство має подумати про проблему витоку інформації та організувати на своїй території систему протидії намірам зловмисників.

Впровадження системи менеджменту інформаційної безпеки (далі – СМІБ) є стратегічним рішенням організації. На проектування СМІБ компанії впливають потреби та цілі підприємства, вимоги безпеки, використовувані процеси, а також масштаби діяльності і структура організації. Загальноприйнятим є факт, що стандарт ISO/IEC 27001:2013 містить кращі практики і принципи з управління інформаційною безпекою компанії, впровадження яких дозволить забезпечити захист від сучасних інформаційних ризиків. Проте ті організації, які не стикались із загрозами втрати конфіденційних даних, мають повну невизначеність у побудові СМІБ. З огляду на це, метою статті була поставлена розробка шляху побудови систем менеджменту інформаційної безпеки в умовах апріорної невизначеності.

Система менеджменту інформаційної безпеки – це частина загальної системи управління, що базується на аналізі ризиків і призначена для проектування, реалізації, контролю, супроводження та вдосконалення заходів у галузі інформаційної безпеки. Вона повинна забезпечувати гарантію досягнення таких цілей, як забезпечення конфіденційності критичної інформації, неможливості виникнення несанкціонованого доступу до критичної інформації, цілісності інформації та пов’язаних з нею процесів (створення, введення, обробки і виведення) і ряду інших цілей [1].

Незамінним елементом на шляху створення цілісної системи менеджменту інформаційної безпеки виступає сімейство міжнародних стандартів ISO 27000, а саме ISO/IEC 27001:2013 та ISO/IEC 27003:2017. Вони забезпечують такі питання, як політика та організація інформаційної безпеки, процеси СМІБ, визначення статусу заходів щодо забезпечення інформаційної безпеки, використання зовнішніх та внутрішніх аудитів для визначення відповідності СМІБ, а також розглядають підходи до управління ризиками, активами та інформаційною безпекою відповідно до законодавства.

Взагалі розробка та впровадження системи менеджменту інформаційної безпеки – відповідальний та достатньо довготривалий процес, що охоплює декілька етапів, перелічені нижче.

1) Прийняття рішення керівництвом компанії про створення системи менеджменту інформаційної безпеки.

2) Підготовка до створення СМІБ. Цей етап включає в себе створення команди, яка буде відповідати за впровадження системи менеджменту інформаційної безпеки, ознайомлення цих співробітників з нормативно-методичним забезпеченням, а далі – вибір галузі діяльності компанії, яка буде охоплена системою менеджменту інформаційної безпеки.

3) Аналіз різноманітних ризиків. Цей етап повинен відображати результати проведення таких процесів:

- ідентифікація активів у межах обраної частини діяльності;
- визначення цінності ідентифікованих активів;
- ідентифікація загроз та вразливостей для ідентифікованих активів;
- оцінка ризиків для можливих випадків успішної реалізації загроз інформаційній безпеці щодо ідентифікованих активів;
- вибір критеріїв прийняття ризиків;
- підготовка плану обробки ризиків [2].

Отже, зазначений етап включає процес оцінки ризиків інформаційної безпеки, спрямований на ідентифікацію ризиків, пов'язаних із втратою конфіденційності, цілісності та можливості застосування інформації в рамках галузі дії системи менеджменту інформаційної безпеки.

4) Розробка політики системи менеджменту інформаційної безпеки на основі результатів аналізу попередніх етапів.

5) Впровадження системи менеджменту інформаційної безпеки в експлуатацію. При впровадженні СМІБ у роботу компанії повинні бути задіяні всі розроблені методи та методики, які здатні реалізувати та досягти первинно обрані цілі.

Очевидно, що етап аналізу ризиків є найважливішим для розробки ефективної системи менеджменту інформаційної безпеки, але в умовах апріорної невизначеності, з якою стикається доволі широкий пласт компаній, майже неможливо правильно та чітко оцінити ризики виникнення тієї чи іншої загрози. Отже, однією з головних проблем прийняття рішень у умовах апріорної невизначеності є її власне розкриття. У дослідженні операцій розроблено спеціальні математичні методи, призначені для кількісного обґрунтування рішень в умовах невизначеності.

Вагомим внеском у виборі засобів захисту конфіденційних даних при розробці системи менеджменту інформаційної безпеки є результати математичних перетворень. Перелік останніх, в свою чергу, визначається за допомогою підсумку аналізу наявних ризиків та уразливостей активів.

Для того, щоб знайти оптимальний математичний апарат, який може стати в нагоді у пошуку найкращої стратегії при побудові СМІБ в умовах апріорної невизначеності, досліджено метод аналізу ієрархій, теорію корисності, а також теорію ігор, яка має досить широку класифікацію. Перелічені математичні методи мають безліч переваг та можуть бути застосовані при прийнятті рішень у розробці системи

менеджменту інформаційної безпеки. Але слід відмітити, що вищезазначені теорії, окрім однієї, засновані на виборі певних критеріїв, на знаннях про визначені ризики та загрози, що має організація. Таким чином, при дослідженні теорії ігор був відокремлений розділ, що стосується ігор з природою, в яких усвідомлено діє тільки один гравець, а інший – навмання. Природа не має на меті отримання виграшу, що і відрізняє цей тип ігор від інших. Отже, в якості шляху побудови СМІБ в умовах апріорної невизначеності, буде використана теорія ігор ходом природи. Слід зазначити, що природа – узагальнене поняття супротивника, який не переслідує власних цілей у конфлікті. Відповідно, в іграх з природою задача вибору оптимальної стратегії для гравця з одного боку полегшується, а з іншого – ускладнюється через дефіцит інформації про поведінку природи.

Взагалі, управління інформаційною безпекою певною мірою і є грою – уповноважена особа компанії захищається від атак зловмисника, а той, в свою чергу, шукає слабкі сторони в системі захисту інформації організації для отримання власної вигоди. Як правило, при побудові СМІБ переважна кількість рішень приймається в умовах невизначеності. Саме тому є важливим дослідження математичних апаратів, які можуть надати інформацію для прийняття доцільних рішень.

Прийняття рішення в умовах апріорної невизначеності полягає у визначенні найбільш оптимальної стратегії, успіх реалізації якої залежить від певних невизначених факторів, що не відомі в момент прийняття рішення. Як було визначено, допоміжним математичним апаратом в цьому питанні виступає теорія ігор ходом природи. Її використання передбачає застосування таких критеріїв оптимальності, як критерій оптимізму, песимізму, Лапласа, Вальда, Севіджа та Гурвіца [3]. Обґрунтувати використання критеріїв оптимальності досить легко, оскільки причина полягає в неможливості передбачити наслідки вибору певного засобу захисту адміністратором безпеки в умовах апріорної невизначеності. Вибір комбінацій критеріїв оптимальності залежить від політики компанії, для якої розробляється система менеджменту інформаційної безпеки, яка може бути більш оптимістична або більш песимістична з елементами обережності вибору.

Отже, запропонований підхід може бути використаний компаніями, які мають на меті захистити свої активи для знаходження балансу інтересів бізнесу та інформаційної безпеки, а також для підвищення довіри зацікавлених сторін, але стикнулися зі станом невизначеності при побудові СМІБ.

Список джерел:

1. Система управління інформаційною безпекою як ключовий чинник успішності організації [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://ua.ikmj.com/isms/.

2. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements [Електронний ресурс]. – 2013. – Режим доступу до ресурсу: https://www.iso.org/standard/54534.html.

3. Критерії опимальності в умовах повної невизначеності [Електронний ресурс] – Режим доступу до ресурсу: https://lubbook.org/book_411_glava_7_Tema_7._Pravove_reguljuvannja_.html.

4. Ігри з природою в умовах невизначеності [Електронний ресурс] – Режим доступу до ресурсу: https://moodle.kstu.ru/mod/book/view.php?id=11481.

5. Сааті Т. Прийняття рішень. Метод аналізу ієрархій / Т. Сааті. – М.: Радио и связь, 1993. – 278 с.

6. Вертакова Ю. В. Теорія корисності та її використання для пошуку рішення [Електронний ресурс] / Ю. В. Вертакова. – 2005. – Режим доступу до ресурсу: https://laws.studio/upravlencheskie-resheniya-uch/teoriya-poleznosti-ispolzovanie-dlya-poiska-25828.html.

UDC 624

GEOMETRIC MODELLING AND ITS APPLICATION TO DESIGN HIGHWAYS

Levterov A. I., Professor, PhD in Technical Science, Head of Department of Informatics and Applied Mathematics Kharkiv National Automobile and Highway University,
Plekhova H. A., Assistant Professor, PhD in Technical Science (Transport Systems), Assistant Professor of Department of Informatics and Applied Mathematics, Kharkiv National Automobile and Highway University,
Kostikova M. V., Assistant Professor, PhD in Technical Science, Assistant Professor of Department of Informatics and Applied Mathematics, Kharkiv National Automobile and Highway University

Abstract. Mathematical models to solve optimization connection problems in nonsimply connected regions under typical technological restrictions on geometric and topological parameters of routes, first of all, on curvature and the number of bends, have been investigated and developed. The models are linked with the extant and prospective topogeodesic models of the polygonal images of territories.

Key words: mathematical model, optimization problem, restriction, topological parameter, construction norm and rule, homotopy, accuracy.

The object of the research is the mathematical models of problems to search for optimal networks and routes that come into existence during the automation of design and control taking into consideration a landscape under the restrictions on the form, mutual location and other connection parameters. The subject of the research is the development of a mathematical model to solve the problem of the search of optimum routes and connecting networks in nonsimply connected regions under restrictions on curvature, the number of bends and other geometric topological connection parameters that reflect typical technological requirements. This paper uses the following methods of research: optimization techniques, computational approaches, computational geometry, mathematical modelling and combinatorial topology approaches. As of topological parameters, this paper provides their decomposition as a system of basic and standard problems; basic optimization problems are posited.

The most effective approach to solve analogous problems, which are NP-complete, even for a case of bends in a convex area, is developed in the papers of Yu. H. Stoyan and S. V. Smelyakov [1 – 4]. It is the synthesis of combinatorial and variational optimization methods within a framework of a hierarchical system of models. Low-level models are oriented to solve basic problems for the search of an optimum route, using variational methods, which have been developed by M. M. Moiseyev, S. V. Smelyakov and N. Z. Shor. High-level models are oriented to examine the homotopic families of highways and networks on the basis of the discrete optimization methods that have been developed in the papers of V. I. Mykhalievych, I. V. Sergiyenko, Yu. H. Stoyan, S. V. Yakovlev and others [5 – 7]. The impossibility of the complete formalization of requirements for CN&S – construction norms and standards – (as a consequence of their inconsistency and not complete strictness of formulae) and the subordinate character of connection problems in relation to the problems of the normalization of regions causes a need for their solution in two modes – optimization and imitation when a decision-making person is involved in the process of the interactive solution of connection problems.

The objective of this paper is the development of a mathematical model to solve the optimization connection problems in nonsimply connected regions under typical technological restrictions on geometrical and topological route parameters, first of all, on curvature and the number of bends. The model should be in conformity with the extant and prospective

topogeodesic models of a polygonal territory image; optimization methods should guarantee the effective solution of the main classes of applied problems and allow natural integration in the extant and prospective systems of design and control.

To attain the objective, it is necessary to solve the following tasks:

- to sort out the major criteria and restrictions that are linked with geometric and topological route parameters that will be under consideration to design connections and on this basis to posit the main optimization problem;

- to develop the general model of connection problems that ensures the statement of the main types of route optimization and modelling problems using the functional classes of lines and allows augmentation and integration into existing systems.

In accordance with requirements for the accuracy of obtainable solutions and the computational effectiveness of the methods of their construction as well as with extant world tendencies to use polygonal terrain models in topogeodesic provision systems, the region models and optimization methods to solve connection problems should use the polygonal models of a nonsimply connected region that is specified for route connections rather than the grid models that are used in modern systems like ReCAD, CREDO. So, the region is calculated as follows:

$$F = Cl\left[\frac{F_0}{\left(\bigcup_{i=1}^{nF} F_i\right)}\right], \qquad (1)$$

where CI – a closing operation; F_0 – the overall area that is used to examine modelling problems; F_i, $(i = 1, 2, \ldots, n_F)$ – the simply connected regions that are mutually crossed ("prohibited zones" for routing) in the simply connected region F_0 on the plane.

The general mathematical feature of even routes (highways, railroads and tramlines) is a requirement for the continuity and limitedness of curvature. The requirement has to be fulfilled to guarantee transport traffic safety and the lack of impact blows. In connection with it, the construction norms and standards read that highway center lines will be presented as splines

$$p = S_1\, r_1\, C_1\, R_1\, S_2\, r_2\, C_2\, R_2 \ldots S_m\, r_m\, C_m\, R_m\, S_{m+1}, \qquad (2)$$

where S_i – legs; C_i – arcs of circles; r_i, R_i – the connecting curves that can be presented by the fragments of clotoids and cubic parabolas, m – the number of the fragments of respective curves.

The analysis of CN&S shows that the majority of technological restrictions for transport and engineer networks under investigation can be reduced to the following main classes of geometric and topological restrictions: Q_1 – restrictions on maximum length of straight legs; Q_2 – restrictions on the angle of turn α, $\alpha \in \left(-90^\circ, 90^\circ\right)$, in vertices; Q_3 – restrictions on a functional class of smooth curves: $\tilde{W}$, SC, SKC, SPC; Q_4 – conditions on ends (to determine tangents and their length in the points of *A* and *B*); Q_5 – junctions with allowable sections; Q_6 – junctions to coordinate flows in terms of direction; Q_7 – junctions to provide their reach; Q_8 – junctions to boundaries and routes; Q_9 – the topological structure of a sought network (connectivity, cycles).

According to CN&S, the choice of the route of a pipeline, highway etc. should be made with the help of mathematical methods on the basis of one or some optimum criteria (for example, curves should be designed with as large radii as possible). In so doing, criteria, as a rule, are expressed by the geometric parameters of routes and the topological parameters of networks, and some of them can be nonadditive. Among the main geometric parameters of the route p, it is necessary to indicate length $l(p)$, the quantity $m(p)$ of circle insertions and their curvature radii $\{p_i\}_{i=1,\, m(p)}$ (or – for a bandy line – the quantity of bends $n(p)$ and turning angles $\{\varphi_i\}_{i=1,\, m(p)}$), the location of the route p in the region F. They influence the cost of the construction $c(p)$, maintenance charges $e(p)$, manufacturability $t(p)$ and reliability $b(p)$ that is one of the most important and the product of the possible analogues of reliability

$$\begin{cases} b_m(p) = \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right), (p_i \geq 1) \text{ for } m > 0; \\ b_d(p) = \prod_{j=1}^{d} (1 - g_i)^{k_j}; \\ b_l(p) = \frac{1}{l(p)}, (l(p) \geq 1). \end{cases} \tag{3}$$

To summarise, the general problem to optimize connections (GPOC) taking into consideration the introduced criteria and restrictions can be posited as follows.

General problem to optimize connections. The given region F has both a set of points $\{A_i\}_{i=1,\, N}$ and some networks $\{S_j\}_{j=1,,\, M}$. It is required to connect these points and networks with the connecting network s^*, which consists of the lines of the given functional class $S\Theta C$ to meet the specified restrictions Q of the type $Q_1 - Q_9$, and it will be the most effective one in the meaning of the given optimum principle $R(s)$.

Taking into account the above-mentioned effectiveness of the decomposition of GPOC, which is based on the reduction of this problem to a system of basic problems on the continual families of routes that allow an exact solution, we can have the main typical optimization problem (MOP) to search for an optimum way in the class of route equivalence $[\tau]$ on a given functional class of lines $P(A,B)$ with the set ends of A and B under respective reduction of restrictions Q^*:

Main optimization problem. Calculate

$$\underset{p \in P_{tQ}(A,B)}{arg\, extr}\, R(p). \tag{4}$$

This paper further posits informational and computational requirements to models to calculate the specified problems.

The problem of the global and local decomposition and regularization of GPOC on the basis of its reduction to a system of the homogeneous basic problems of type (4) is considered. It guarantees constructive regularization and an effective computational approach to solve a general problem to optimize connections, using discrete and continual models and methods. The two-level FL model by Yu. H. Stoyan and S. V. Smelyakov is used to do it. On the top topological level the structure of this model is determined by an algebraic exfoliation of lines on the classes of the equivalence of routes and networks and on the geometric level by the consideration of the demanding functional class of lines in each class. Restrictions can be imposed on components on both levels. Since the variety F in form (1) has the homotopical

nature of the type of disk with $n_F \geq 0$ holes, the structure of the homotopical model of lines consists of the free group $C_{(nF)}$, which discretizes the continuous families of routes.

The network $\Gamma = \{\gamma_i\}_{i=1,m}$ in the region *F* is a set of rectifiable curves that are limited in number. They are non-selfintersecting and have no common points except ends. The review of the connected combinations of the types of networks, graphs etc. brings about the problems of three classes: the search of optimum networks on the topological level with no account taken of the geometry of the region *F*; the optimization of the contributions of an abstract model in the region *F* and the structure of an optimum network in the region *F*. To solve these problems, we can introduce the concept of the abstract network $s^* = (V^*, R^*)$ as the end connected abstract simplical complex $K = (V^*, R^*)$. The implementation of the abstract network by the geometric complex $s = (V, R)$ is a geometric network. The networks $s_1 = (V_1, R_1)$ and $s_2 = (V_2, R_2)$ are homotopical in F if their abstract analogues have the isomorphism $\omega : s_1 \to s_2$ under which the correspondence of 0-simplexes means the combination of apexes in *F* and the correspondence of 1-simplexes means their belonging to one class of route equivalence in *F*; the networks s_1 and s_2 are free homotopical if they are homotopical with accuracy to the shift of 0-simplexes in *F* and deformatively equivalent if they are isomorphic and homotopical and their various edges can have common points only in the basic apexes which they connect. It should be noted that network isomorphism saves algebraic invariants for basic apexes but it does not take into account the structure of the region *F* with enclosures in it. Homotopy saves network homotopy but it does not contribute to their isomorphism due to the emergence of additional apexes. Network deformity keeps homotopical invariants.

The geometric model of routes is the functional classes of lines $\Lambda = \{S, SC, SKC, SPC, W, \tilde{W}\}$ in the region F that have a spline image (2). Topological restrictions can be applied to them as well. The introduction of the models of networks and lines allows us to reduce the GPOC to the system of the basic problems of type (2) on various functional classes of lines and standard problems on the same classes that reflect the combination of restrictions that are typical for applied problems and are reduced to basic problems.

The hierarchical mathematical model of a common connection problem has been developed. The essense of it is the search of optimum connections (routes and connecting networks) in nonsimply connected regions. The problem comes into existence when designing transport and engineer networks and controlling vehicle traffic on cross-country terrain. In the framework of the model this problem is reduced to a system of basic and standard problems to search optimum routes. The use of this hierarchical structure of models in the systems of decision-making allows us to solve the problem of the adequate modelling of connections in nonsimply connected regions in terms of accuracy, computational effectiveness and absence of informational redundancy for all functional classes of bendy and even lines $\{S, SC, SKC, SPC\}$, which are regulated by CN&S, under restrictions on curvature and other geometric and topological parameters of routes.

References

1. Плехова А. А., Смеляков С.В. Моделирование коммуникационных сетей с учетом ландшафта при разнородных критериях и ограничениях. *Информационные системы. Сборник научных трудов.* 1998. Вып. 3 (11). С. 143-146.

2. Стоян Ю. Г., Яковлев С. В. Математические модели и оптимизационные методы геометрического проектирования. К.: Наук. думка, 1986. 268 с.

3. Смеляков С. В., Стоян Ю. Г. Моделирование пространства путей в задачах построения оптимальных траекторий, *Ж. вычисл. матем. и матем. физ.* 1983. Том 23, № 1. С. 73-82.

4. Смеляков С. В., Плехова А. А. Построение кратчайшей трассы в неодносвязной области при ограничениях на кривизну и класс кривых. *Информационные системы. Сборник научных трудов*. 1999. Вып. 1 (12). С. 170-175.

5. Сергиенко И. В., Шило В. П. Задачи дискретной оптимизации: проблемы, методы исследования, решения. К.: Наук. думка, 2003. 264 с.

6. Плехова А. А. Модель и метод решения задачи поиска оптимального соединения при ограничении на кривизну. *Радиоэлектроника и информатика*. 1998. № 3. С. 56-59.

УДК 656.051

АНАЛІЗ ПІДХОДІВ ВИЯВЛЕННЯ АНОМАЛЬНОЇ ПОВЕДІНКИ ЛЮДИНИ В РЕАЛЬНОМУ ЧАСІ У ВІДЕОПОСЛІДОВНОСТІ

Фастовець В.І., доцент,
Харківський національний автомобільно-дорожній університет
магістр факультету Інфокомунікацій
Харківський національний університет радіоелектроніки, Україна
Радівілова Т.А. , професор кафедри інфокомунікаційної інженерії імені В.В. Поповського
Харківський національний університет радіоелектроніки

Анотація. *Проведений огляд систем моніторингу поведінки людей в відеоряді камер відеоспостереження. Досліджено склад сучасних систем відеоспостереження та наведені приклади використання таких систем. Проведено аналіз існуючих систем комп'ютерного зору.*

Ключові слова: інтелектуальні камери відеоспостереження, Системи аналізу відеоконтенту, сегментації зображень.

У наш час дуже важливим стає питання моніторингу поведінки людей у громадських місцях та попередження злочинних дій. Для цього використовуються системи відеоспостереження в комплексі із системами біометричної ідентифікації особи.

Використання таких систем дає можливість встановити особу на основі її характерних біометричних даних та аналізу візуального образу людини. Основними перевагами таких систем є висока точність і ефективність розпізнавання обличчя, сітківки ока і відбитків пальця для запобігання різним видам шахрайства та злочинних дій, щоб довести причетність до злочинів затриманих осіб, а також у сфері митного контролю та перетину кордону.

На рис. 1.1 показано приклад практичного використання технологій комп'ютерного зору щодо розпізнавання обличчя та відбитків пальців.

Рисунок 1.1 – Результат розпізнавання об'єктів системою біометричного аналізу

Одним із сценаріїв методів розпізнавання обличчя є порівняння зображень обличчя, одержаного з системи відеоспостереження, та цифрового фото, наприклад, із закордонного паспорту. У 2017 році в одному з аеропортів Франції була встановлена система PARAFE - впроваджена система розпізнавання образів. Така інтелектуальна

система відеоспостереження дозволяє пришвидшити потік людей при перетині кордону, і може замінити систему біометричної ідентифікації за відбитком пальця.

Для моніторингу ситуації при проведенні різних масових громадських заходів доречним є застосування камер на безпілотних літальних апаратах(БПЛА) та використання програмного забезпечення розпізнавання обличчя. Сучасні БПЛА можуть переносити об'єктив камери вагою до 10 кг і забезпечувати ідентифікацію особи з відстані до 900 м та висоти до 100 м.

Системи аналізу відеоконтенту повинні мати інтелектуальні складові, що володіють функцією оповіщення, яка повинна працювати у режимі реального часу і формувати сигнал тривоги у випадку виявлення у відеопотоці заданого об’єкту.

Інтелектуалізовані системи опрацювання відео широко використовуються у банківській сфері (ідентифікація особи за її обличчям).

Зараз реалізовано алгоритми штучного інтелекту для забезпечення достовірності виявлених об’єктів та уникнення шахрайства, пов’язаного із статичним зображенням. Ці алгоритми аналізують рух очей, повертання голови у різні сторони, і навіть зміну емоцій, для встановлення справжності особи шляхом аналізу.

Такий алгоритм перевірки та ідентифікації особи реалізовано у мобільному додатку Дія. Він дає можливість використовувати ідентифікаційні дані особи та згенерувати унікальний цифровий підпис.

Серед найбільш високо технологічних компаній, таких як Google, Microsoft, Amazon, Apple та Facebook великої актуальності набули проекти аналізу об’єктів на зображеннях. Так, у 2014 році був розроблений алгоритм «GaussianFace», що забезпечує точність розпізнавання об’єктів у відеопотоці на рівні 98%, в той час, як точність розпізнавання образів людиною можна оцінити у 97%. Реалізація цього алгоритму потребує великого об’єму дискового простору і оперативної пам’яті, а також спеціалізованих процесорних ядер.

В свою чергу, компанія Facebook у 2014 створила сервіс DeepFace, який дає можливість виконувати порівняння зображень обличчя і визначати приналежність його власнику з точністю до 97%.

Компанія Google у 2015 році реалізувала програмний сервіс FaceNet. Даний сервіс використовує нейромережу, навчання якої виконано на загальнодоступному наборі даних «Labeled Face Wild – LFW». Точність розпізнавання образів, яка була досягнута при використанні FaceNet, становить 99,6%. Технологія FaceNet інтегрована у сервіс Google Photos і застосовується при впорядкуванні зображень з можливістю порівняння з базою даних зображень людей. З’явилась і відкрита версія FaceNet під назвою OpenFace.

Компанія Amazon розробила програму розпізнавання обличчя Rekogmination, яка використовує програмно-апаратні ресурси хмарних сервісів та одночасно може розпізнати до 100 осіб, які знаходяться в межах однієї територіальної області та порівнювати їх з існуючими записами зображень, які містяться у базі даних. Кількість записів у базі даних становить понад десять мільйонів зображень обличь.

Сервіс Thales, запропонований на основі програмного комплексу LFIS, призначеного для розпізнавання зображень, демонструє точність ідентифікації людини на рівні 99,44% з швидкістю менш ніж 5 секунд [1].

Одним з методів, що використовуються в інтелектуальних системах відеоспостереження, є сегментація зображень, основна метою якої є спрощення представлення зображення при його аналізі.

Під час проведення процедури сегментації виконується декомпозиція зображення і виділення контурів об’єктів на різних його частинах (об’єктах) за різними областями, які мають подібні атрибути та властивості.

В процесі аналізу зображення першим кроком, без якого реалізація технік комп’ютерного зору була б практично неможливою, є сегментація. графічних об’єктів,

виявлених у відеопотоці. Сегмегтація дозволяє групувати специфічні пікселі зображення, призначити їм мітки та класифікувати інші пікселі у відповідності до цих маркерів.

Мітки, згенеровані у результаті сегментації, можна використовувати у машинному навчанні нейромережі при використанні алгоритмів навчання з вчителем або без нього.

Сегментація зображень є фундаментальним аспектом в області комп'ютерного зору і має багато застосувань у різних галузях та сферах:

1) Розпізнавання обличчя. Наприклад, у смартфонах iPhone присутня технологія розпізнавання обличь, яка реалізує функції передових систем безпеки, і будується на використанні сегментації зображень для ідентифікації власника. Для того, щоб будь-яка інша особа, крім власника, не могла отримати доступ телефону, смартфон ідентифікує унікальні риси обличчя;

2) Google та інші пошукові системи, які пропонують засоби пошуку на основі зображень, використовують методи сегментації зображень для ідентифікації об'єктів, присутніх на зображенні-запиті, і порівняння з зображеннями, які вони знаходять у результаті пошуку;

3) Візуалізація у медичній галузі. Сегментація зображень має багато застосувань у медичній сфері. Вона допомагає визначити уражені ділянки, ідентифікувати ракові клітини, запускати віртуальне моделювання хірургічних операцій та здійснювати навігацію в межах операції, спланувати лікування.

4) Ідентифікація номерних знаків. Багато світлофорів і камер використовують ідентифікацію номерних знаків, наприклад, для стягнення штрафів. Система дорожнього руху за допомогою технології ідентифікації номерних знаків може розпізнавати автомобіль та отримувати інформацію про його власника. Така система використовує сегментацію зображення, щоб відокремити номерну табличку та її інформацію від решти об'єктів, присутніх у полі зору.

Окрім того, сегментація зображень використовується у сільському господарстві, безпеці, виробництві, та багатьох інших секторах. Наприклад, у виробництві методи сегментації зображень використовуються для знаходження неякісних продуктів. Тут алгоритм фіксує лише необхідні компоненти з зображення об'єкта та класифікує їх як несправні чи оптимальні. Таким чином, система знижує ризик людських помилок і робить процес тестування більш ефективним.

Підходи щодо сегментації зображень можна класифікувати за параметрами наступним чином:

1) Класифікація, заснована на підходах до реалізації. Всі алгоритми сегментації зображень працюють на основі ідентифікації об'єкта. Спочатку ідентифікують об'єкт, а потім різні його компоненти. Таким чином, цей різновид класифікації проводиться на основі того, як методи сегментації зображень ідентифікують об'єкти, тобто яким чином групують подібні пікселі та відокремлюють їх від різнорідних.

Існує два підходи до виконання такої ідентифікації:

– Підхід на основі виявлення подібності. Метод дозволяє виявити схожі пікселі на зображенні відповідно до вибраного порогу, об'єднання зон, зменшення чи розширення області. Алгоритми класифікації користуються цим підходом для виявлення ознак і розділення сегментів зображення. Цей метод використовується в кластеризації та подібних алгоритмах машинного навчання для детектування невідомих функцій або ознак.

- Підхід на основі границь (виявлення розривів). Цей підхід є протилежним до підходу на основі виявлення подібності при ідентифікації об'єктів. На відміну від алгоритму визначення подібності, коли шукають пікселі зі схожими характеристиками,

підхід на основі границь виконує пошук пікселів, які відрізняються один від одного. Виявляють край різнорідних пікселів і відповідно відокремлюють їх від решти зображення.

2) Класифікація на основі техніки сегментації. Існує два глобальних підходи, що реалізують різні техніки сегментації і які включають в себе різні методи сегментації зображень:

– Алгоритми на основі аналізу структури. Особливістю цих алгоритмів є наявність структурних елементів зображення (пікселі, гістограми, щільність пікселів, розподіл кольору та інша відповідна інформація). Також необхідно володіти інформацією про структурні дані щодо області зображення, яку потрібно відокремити від нього і на основі цих даних алгоритм може виявити об’єкт.

– Стохастичні техніки. Стохастичні алгоритми потребують інформації не про структуру необхідної ділянки зображення, а про дискретні значення пікселів зображення. Завдяки цьому вони не вимагають багато інформації для сегментації зображень. У випадках, коли доводиться працювати з кількома зображеннями, доречне використання стохастичних алгоритмів. До цієї категорії надежать такі алгоритми машинного навчання, як кластеризація K-середніх і алгоритми ANN.

– Гібридні техніки. Ці алгоритми використовують як стохастичні, так і структурні методи, наприклад, для виконання сегментації зображення вони використовують структурну інформацію необхідної області та інформацію про дискретні пікселі всього зображення.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Кузин Л.Т. Розрахунок та проектування дискретних систем управління.-Л.: ГН ТИМЛ, 2012.- 648 с.

3. RASPBERRY1 PI 3 MODEL B+. URL: https://www.digikey.com/en/products/detail/raspberry-pi/RASPBERRY-PI-3-MODEL-B/8571724 (дата звернення 01.10.2022 р).

4. Detecting Objects in Images [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: http://luthuli.cs.uiuc.edu/~daf/cv2e-site/detectingextracts.pdf.

УДК 656.072; 656.015; 519,12.176

АНАЛІЗ ТА МОДЕЛЮВАННЯ ОСВОЄННЯ ПАСАЖИРОПОТОКІВ НА МАРШРУТАХ ГРОМАДСЬКОГО ТРАНСПОРТУ ТРАНСПОРТНИХ СИСТЕМ МІСТ

Левтеров А. І., проф. каф. інформатики та прикладної математики ХНАДУ,
Козачок Л. М., ст.. викладач каф. Інформатики та прикладної математики ХНАДУ.

Анотація: проведено огляд відомих методів та принципів застосування певних груп методів для вирішення задачі організації роботи на маршруті громадського міського транспорту, а саме для розподілу змін роботи транспортних засобів по перевезенню пасажирів, застосовано ці методи для обстеження пасажиропотоків, що стало вхідними даними для моделювання та прогнозування об’ємів перевезень на маршрутах.

Ключові слова: транспортні системи міст, часові ряди, математичне моделювання, технологічні процеси, інформаційні технології, комп’ютерні системи.

Введення.

У ході розгляду різноманітних підходів до поліпшення роботи пасажирського транспорту у містах та методів, спрямованих на це, звернемо увагу на відповідні варіанти удосконалення управління перевезеннями пасажирів на маршрутах. У якості таких регуляторів можуть бути використані наступні показники: зменшення інтервалів між виходами на маршрут для виконання перевезень конкретними транспортними засобами, розробка розкладів, які враховують удосконалення якості роботи на маршруті, залучення інших видів транспортних засобів з певною пасажиромісткістю. Коректування та створення нових графіків роботи маршруту, нових розкладів обслуговування пасажирів транспортними засобами рухомого складу також мають спиратися на змінення інтервалів руху на маршруті, на змінення часу початку та закінчення роботи по перевезенню пасажирів [2]. Велике значення у цих розробках набуває урахування змін пасажиропотоку на маршруті та дослідження побудованої за необхідними об’ємами перевезень епюри інтенсивності пасажиропотоку та кількості транспортних засобів, що працюють на маршруті [4].

Таким чином, побудова розкладів, що спираються на змінення часу роботи транспортних засобів на маршруті в залежності від кількості пасажирів, які використовують автобусний пасажирський транспорт в певні періоди часу та на певних ділянках є перспективним напрямком розвитку методів управління та врегулювання роботи маршрутів транспортних систем міст.

В багатьох наукових роботах також останнього часу надані розробки нових ефективних методів та інструментів управління пасажирськими перевезеннями, які спрямовані на мінімізацію часу обслуговування, досягнення максимального показника задоволення потреб пасажирів у транспорті на необхідних, економічно активних ділянках транспортної мережі міста та на мінімізацію затрат при використанні транспортних засобів на маршруті, тобто і на енергозбереження ресурсів економіки міст [1].

Провівши огляд відомих методів та принципів застосування певних груп методів для вирішення різних видів задач, для вирішення задачі організації роботи на маршруті, а саме для розподілу змін роботи транспортних засобів по перевезенню пасажирів я зупинила свій вибір на рахувально-табличному методі обстеження пасажиропотоків.

Розклад роботи автобусів на маршруті по обслуговуванню пасажирів.

$Z = \{z_1, z_2, \dots, z_N\}$ – розклад, який являє собою та надає проміжки часу обслуговування. Мається на увазі обслуговування пасажирів на маршруті певним автобусом при чому z_N є моментом часу відправлення на маршрут N-го автобусу, який відраховується від моменту часу виходу першого автобусу на маршрут. Також час початку та закінчення обслуговування пасажирів на маршруті z_1 та z_N задані спочатку, де N–кількість автобусів, працюючих на маршруті.

Знаходження значень змінних, які будуть рішенням задачі.

$t \in T$є значеннями, що належать скінченій множині усіх значень інтервалів часу та являють собою проміжки часу, що проходять між двома послідовними зупинками автобусу:

$$t_1 < t_2 < \cdots < t_M\,, |T| = M,\ t_{i+1} - t_i = 1, \forall i = \overline{1, M-1}\,.$$

Множина зупинок на маршруті.

Припустимо, що кількість пасажирів, які обслуговуються за інтервали часу $t_i, i = \overline{1, M}$, розподілена рівномірно. Множину зупинок позначимо $b_j \in \{b_1, b_2, \dots, b_J\}, j = \overline{1, J}$.

Максимальна пасажиромісткість являє собою максимальну кількість пасажирів, яка перевозиться однім автобусом, та позначається $p_i\,, i = \overline{1, N}$. Також для розгляду завдань можна використовувати поняття бажаної пасажиромісткості, яке було введено Ceder A. [2].

Тобто для вивчення роботи по обслуговуванню на маршруті системи міського пасажирського транспорту та постановці задачі оптимізації вводяться умови з системи обмежень у певному часовому стані $\omega \in \Omega$ на певному часовому етапі $q \in Q$ та у певному проміжку часу $t \in T$.

Основною задачею згладжування часового ряду є отримання ряду з найменшим випадковим розкиданням рівнів, що дозволяє на основі візуального аналізу зробити висновок щодо наявності тренду та його характерним особливостям. Суть згладжування полягає у заміні фактичних рівнів часового ряду розрахунковими рівнями, які представляють собою середні значення, та схильні до коливань. Це сприяє найбільш чіткому проявленню розвитку тренду.

При побудові однопараметричної моделі, яка є лінійною та використовує експоненціальне згладжування коефіцієнтів, оцінки коефіцієнтів знаходяться за наступними формулами:

$$a_0(t) = a_0(t-1) + a_1(t-1) + (1-\beta)^2 e(t)$$

$$a_1(t) = a_1(t-1) + (1-\beta)^2 e(t),$$

це однопараметрична модель з параметром β .

При побудові двопараметричної моделі оцінки коефіцієнтів знаходяться за наступними формулами:

$$a_0(t) = \alpha_1 y(t) + (1-\alpha_1)\big(a_0(t-1) + a_1(t-1)\big)$$
$$a_1(t) = \alpha_2\big(a_0(t) - a_0(t-1)\big) + (1-\alpha_2)a_1(t-1)$$

це двопараметрична модель з параметрами α_1 та α_2 .

Моделювання об’єму перевезень на маршруті громадського пасажирського транспорту.

Проведемо моделювання часового ряду значень пасажиропотоку за двопараметричною моделлю. Ми отримаємо згладжуваний ряд за процедурою експоненціального згладжування, значення якого будуть наближені до даного ряду

значень пасажиропотоку, отриманого при обстеженні маршруту, при цьому згладжувальний ряд буде мати тенденцію (тренд) – основну складову, таку ж, як у вхідного ряду.

Далі записана функція від чотирьох параметрів (m=4), сума квадратів відхилень значень ряду за моделлю та вхідних значень ряду початкової вибірки, отриманої методами обстеження пасажиропотоку.

Мінімізуючи цю функцію отримаємо початкові значення параметрів моделі:

$$\begin{pmatrix} \alpha \\ \beta \\ Y \\ T \end{pmatrix} := \text{Minimize}(R, \alpha, \beta, Y, T) \qquad \begin{pmatrix} \alpha \\ \beta \\ Y \\ T \end{pmatrix} = \begin{pmatrix} 0 \\ 0.427 \\ 4.3 \times 10^3 \\ 10.083 \end{pmatrix}$$

$$R(\alpha, \beta, Y, T) = 2.669 \times 10^3$$

Згладжування значень ряду для знаходження основної тенденції (тренду) за допомогою адаптивного алгоритмічного моделювання з двома параметрами, початкові значення яких ми знайшли вище, виходячи з того, щоб сума квадратів відхилень була найменшою, буде виконуватись наступним чином.

Початкові значення моделі згладжування:

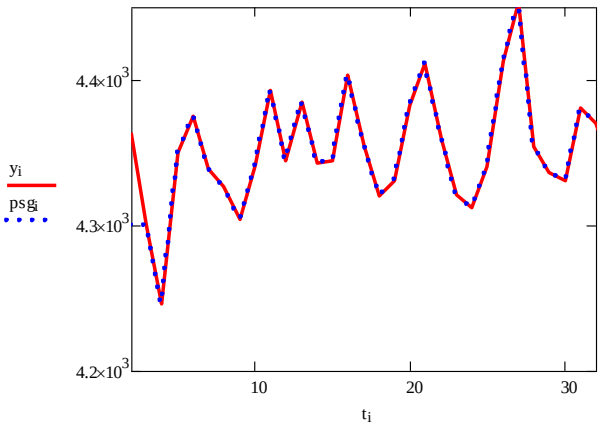
$T := 10.083 \quad Y := 4300$

Початкові значення параметрів моделі:

$\alpha := 0 \quad \beta := 0.427$

За допомогою системи комп'ютерної математики Mathcad ми запрограмували обчислення згладжених значень часового ряду та побудували графік спостережувальних y_i та згладжених psg_i рівнів ряду залежно від часу.

$$psg_i := \left| \begin{array}{l} psg_1 \leftarrow Y \\ \text{for } i \in 1 .. isg - 1 \\ \quad \left| \begin{array}{l} psg_{i+1} \leftarrow \alpha \cdot (psg_i + T_i) + (1 - \alpha) \cdot y_{i+1} \\ T_{i+1} \leftarrow (1 - \beta) \cdot (psg_{i+1} - psg_i) + \beta \cdot T_i \end{array} \right. \\ psg_i \end{array} \right.$$

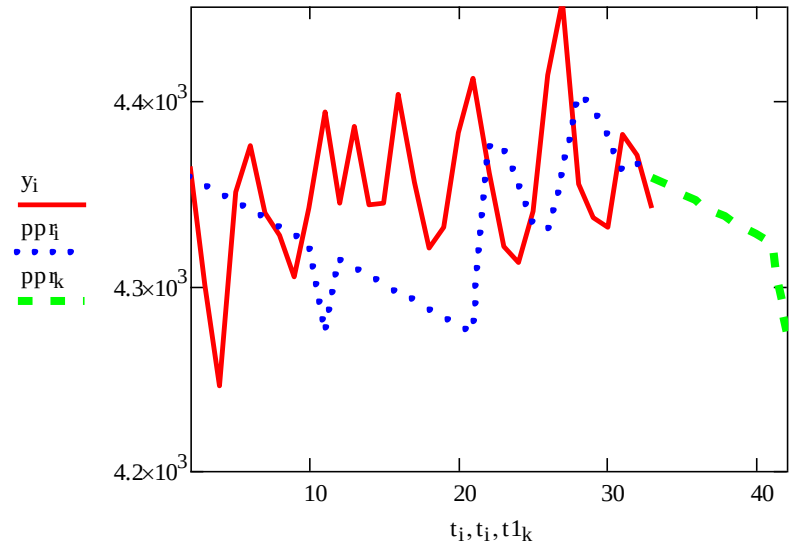


Ми провели навчання моделі, що створюється, з її пристосуванням до досліджуваних значень за методом двопараметричного адаптивного алгоритмічного моделювання для знаходження коефіцієнтів моделі a_0 та a_1 та подальшого прогнозування значень досліджуваної величини. По першим п'яти точкам залежності спостережу вальних значень від часу, використовуючи метод найменших квадратів знаходимо початкові значення коефіцієнтів, як коефіцієнтів рівняння апроксимуючої прямої як рівняння лінії регресії залежності значень об'єму пасажиропотоку від часу.

По отриманим значенням коефіцієнтів моделювання на останньому кроці навчання моделі, що відповідає часу останнього спостережуваного значення, можна спрогнозувати пасажиропотік на декілька кроків за часом вперед.

$ppr_k =$

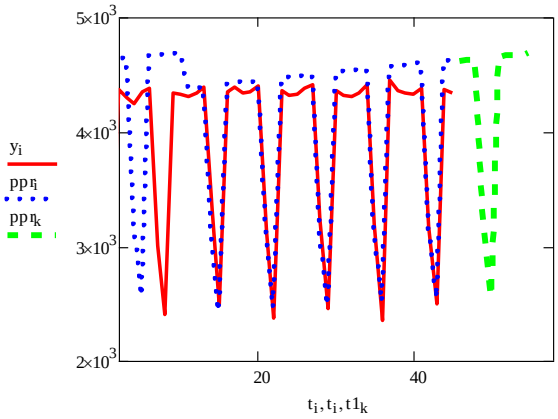
$4.358 \cdot 10^3$
$4.354 \cdot 10^3$
$4.349 \cdot 10^3$
$4.345 \cdot 10^3$
$4.34 \cdot 10^3$
$4.336 \cdot 10^3$
$4.331 \cdot 10^3$
$4.327 \cdot 10^3$
$4.323 \cdot 10^3$
$4.274 \cdot 10^3$



Далі при моделюванні об'ємів перевезень потрібно урахувати періодичну компоненту часового ряду. Для цього візьмемо візьмемо мультиплікативну періодичну модель часового ряду та застосуємо для моделювання та прогнозування двопараметричне адаптивне алгоритмічне програмування.

$$f_i := \left| \begin{array}{l} f_1 \leftarrow 0.55 \\ \text{for } i \in 2..n \\ \quad \left| \begin{array}{l} f_i \leftarrow 0.69 \quad \text{if } \frac{i}{7} - \text{floor}\left(\frac{i}{7}\right) = 0 \\ f_i \leftarrow 1 \quad \text{otherwise} \end{array} \right. \\ \text{for } i \in 2..n \\ \quad f_i \leftarrow 0.55 \quad \text{if } \frac{i-1}{7} + \left(-\text{floor}\left(\frac{i-1}{7}\right)\right) = 0 \\ f_i \end{array} \right.$$

$$ppr_k := \left| \begin{array}{l} \tau \leftarrow 0 \\ ppr_0 \leftarrow y_{45} \\ \text{for } k \in 1..10 \\ \quad \left| \begin{array}{l} ppr_k \leftarrow (model0 + model1 \cdot \tau) \cdot f_{(t1_k)} \\ \tau \leftarrow \tau + 1 \end{array} \right. \\ ppr_k \end{array} \right.$$



Висновки.

Побудова розкладів організації роботи транспортних засобів на громадських пасажирських маршрутах, що полягає у визначенні змін роботи автобусів, спирається на визначенні часу роботи в залежності від кількості пасажирів, які використовують автобусний транспорт в певні періоди часу та на певних ділянках, що є перспективним напрямком розвитку методів управління та врегулювання роботи маршрутів транспортних систем міст. У ході виконання наведених вище алгоритмів ми отримаємо адаптивні моделі дослідження та прогнозування пасажиропотоку, що використовуються при плануванні роботи громадського міського транспорту.

Література.

1. Левковець П.Р., Мороз М.М., Кобилецький Р.В. Удосконалення логістичного управління перевезень пасажирів. *Вісник КДПУ імені Михайла Остроградського.* 2007. Вип. 6 (47). С. 113-115.
2. Ceder A. Planning and Evaluation of Passenger Ferry Service in Hong Kong. *Transportation.* 2006. Vol. 33. P. 133–152.
3. Ceder A., Voß S., Daduna J. Efficient Timetabling and Vehicle Scheduling for Public Transport. Computer-Aided Scheduling of Public Transport. *Lecture Notes in Economics and Mathematical Systems.* 2001. Vol. 505. P. 37-52.
4. Горбачов П.Ф., Любий Є.В. Моделювання попиту на перевезення населення малих міст маршрутним пасажирським транспортом: монографія. Харків: ХНАДУ, 2014. 257 с.
5. Alvarez A., Casado S., Gonzalez Velarde J., Pacheco J. A computational tool for optimizing the urban public transport. *Journal of Computer System Sciences International.* 2010. Vol. 49(2). P. 244-252.
6. Zadeh L.A. Fuzzy sets. *Information and Control*. 1965. Vol. 8(3). P. 338-353.

УДК 621.391: 004.056.5

АНАЛІЗ МЕТОДІВ КЛАСИФІКАЦІЇ ВРАЗЛИВОСТЕЙ ТА ЗАГРОЗ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Румянцева Ольга Володимирівна
студентка VI курсу факультету Інфокомунікацій
Харківський національний університет радіоелектроніки, Україна
Пшеничних Сергій Васильович
кандидат технічних наук, старший науковий співробітник, доцент кафедри інфокомунікаційної інженерії
імені В.В. Поповського
Харківський національний університет радіоелектроніки, Україна

Анотація. У тезах розглядаються відомі методи класифікації вразливостей та загроз інформаційної системи, які можна використовувати для нейтралізації виявлених уразливостей за рахунок налаштування засобів захисту, резервування, розробки організаційних заходів. Також класифікація дозволяє чітко визначити, чому саме має протистояти система захисту інформації.

Ключові слова: інформаційні технології, інформаційна система, система захисту інформації, вразливість, загроза.

У сучасних умовах розвитку інформаційних технологій при створенні інформаційних систем (ІС) для комерційних чи державних організацій обов'язково створюється система захисту інформації (СЗІ). На етапі проектування ІС виникає питання ефективності СЗІ, створеної за тим чи іншим проектом. Вирішення завдання формального порівняння кількох проектів СЗІ для вибору найкращого викликає певні складнощі.

Крім того, існує безліч сучасних міжнародних та вітчизняних стандартів та нормативних документів у галузі інформаційної безпеки, що розглядають питання оцінки ефективності СЗІ або визначають вимоги до її функціональності. У цих документах, як правило, як критерій ефективності використовується наявність тих чи інших засобів захисту інформації або вимоги до їх параметрів і не враховується, що є можливості подолання даних засобів за рахунок наявності в них та ІС тих чи інших вразливостей. Таким чином, актуальним є завдання вибору оптимального проекту СЗІ за критерієм ефективності, що враховує наявність вразливостей та взаємозв'язків між ними.

Процес функціонування типової організації полягає у постійній обробці великих обсягів інформації, їх аналізі, прийнятті рішень та управлінської діяльності. Для автоматизації процесів функціонування типової організації створюється ІС.

Під ІС розуміється організаційно впорядкована сукупність документів (масивів документів) та інформаційних технологій, у тому числі з використанням засобів обчислювальної техніки та зв'язку, що реалізують процеси збирання, накопичення, обробки, пошуку та розповсюдження інформації [1].

Процес реалізації загрози ІС пов'язаний з послідовним використанням вразливостей. Вразливості існують у різних структурних елементах ІС та програмної або апаратної складової елементів ІС.

Для дослідження процесів безпеки інформації досліджується структура ІС, її складові та їх взаємодія. ІС різняться залежно від масштабів, способу організації чи сфери діяльності. Відповідно, для побудови моделей, що відображають особливості структури та функціонування досліджуваної ІС необхідно визначити до якого класу належить типова ІС організації.

Основу ІС складають територіально розподілені комп'ютерні системи (обчислювальні мережі) елементи яких розташовані в окремих будівлях, на різних поверхах цих будівель і пов'язані між собою транспортним середовищем, яке використовує фізичні принципи («вита пара», оптико-волоконні канали, радіоканал і т.д.). Основу апаратних (технічних) засобів таких систем складають електронно-обчислювальні машини (ЕОМ) або групи ЕОМ, периферійні, допоміжні пристрої та засоби зв'язку, що сполучаються з ЕОМ.

У процесі функціонування ІС часто виникають загрози безпеці інформації. Під загрозою безпеці інформації, при цьому, розуміється подія або дія, яка може спричинити зміну функціонування ІС, пов'язану з порушенням захищеності інформації, що обробляється [2]. Джерелами виникнення загроз можуть бути форс-мажорні обставини, збої у роботі обладнання, помилки персоналу та, безумовно, навмисні дії зловмисників.

Для запобігання реалізації загроз створюються комплексні системи захисту інформації (КСЗІ). Під КСЗІ розуміється комплекс організаційних, інженерно-технічних, технічних і програмних заходів спрямованих на підтримку захищеності інформації [3].

КСЗІ інформаційних систем створюються згідно з директивно заданою для цієї організації концепцією захисту інформації. Концепція задає регламент використання комплексу взаємообґрунтованих та узгоджених нормативно-організаційних і технічних заходів щодо запобігання витоку інформації при її обробці, зберіганні та передачі [4].

При розробці проектів систем захисту інформації важливим завданням є визначення вразливостей існуючої інформаційної системи та передбачуваних до застосування засобів та методів захисту. Це необхідно для нейтралізації виявлених вразливостей за рахунок, наприклад, налаштування засобів захисту, резервування, розробки організаційних заходів та інш. Для більш повного аналізу виявлених вразливостей проводиться їх класифікація. При цьому існує безліч підходів до класифікації вразливостей, в яких використовується безліч класифікаційних параметрів, таких як:

— етап життєвого циклу інформаційної системи, у якому впроваджується вразливість;

— рівень в інфраструктурі інформаційної системи;

— рівень небезпеки вразливості;

— причина виникнення;

— особливості вразливості;

— місцезнаходження.

Аналіз наведених підходів до класифікації показує наступне:

— класифікація за етапом життєвого циклу, на якому виникає вразливість, зачіпає всі можливі вразливості ІС. Однак її практичне застосування може бути скрутним, тому що вона є надмірно узагальненою. Відповідно, класи, що виходять, будуть занадто великими;

— класифікація за рівнем в інфраструктури ІС зосереджується на програмних та програмно-апаратних засобах захисту та ігнорує організаційні та технічні засоби захисту та їх вразливості;

— класифікація за рівнем небезпеки зосереджується виключно на вразливості програмного забезпечення, залишаючи поза розгляду вразливості інших складових системи захисту інформаційної системи;

— різні підходи до класифікації через виникнення об'єднує те, що всі вони зосереджені на описі вразливостей операційних систем та програмного забезпечення і, відповідно, не розглядають вразливості організаційних, технічних та апаратних засобів та методів захисту інформації.

— класифікація організації, MITRE за різними особливостями властивих вразливостей (список CWE) також стосується лише вразливості програмного забезпечення [5];

— класифікації за місцезнаходженням поділяють вразливості щодо того, в якій частині ресурсів інформаційної системи вони знаходяться (програмної чи апаратної), відповідно до класифікації не зачіпають вразливостей пов'язаних з помилками в організації захисту інформації.

Основним критерієм порівняння для класифікації вразливостей, з практичної точки зору, є максимальне охоплення класифікацією вразливостей ІС.

Таким чином, класифікація тільки за однією класифікаційною ознакою призводить або до того, що розглядається лише частина вразливостей інформаційної системи, або до того, що вразливості розбиваються на надмірно великі класи, елементи яких (тобто вразливості) можуть сильно відрізнятися один від одного.

Отже, переважно використовувати такі класифікації, які розглядали одночасно кілька класифікаційних ознак. До таких класифікацій належать: класифікація вразливостей Landwehr'a [6] та узагальнена класифікація вразливостей [7]. Перевагою узагальненої класифікації є те, що вона розглядає і вразливості організаційного захисту, хоча й не наводить їх докладнішої класифікації. Таким чином, узагальнена класифікація вразливостей охоплює практично всі аспекти проблеми вразливостей ІС. У свою чергу, недостатня подробиця того чи іншого підкласу може бути вирішена його розширенням. Відповідно, дана класифікація найбільше підходить для практичного застосування.

Також важливим завданням при розробці систем захисту є визначення загроз для інформаційної системи, що захищається, що дозволяє чітко визначити чому саме повинна протистояти система захисту. Як наслідок, також необхідно проводити класифікацію загроз.

Аналіз літератури показує, що є безліч підходів до класифікації загроз. При цьому в цих підходах до класифікації простежується неоднозначність визначення загрози безпеці інформації. Існує два визначення загрози безпеці інформації. Під загрозою безпеки інформації розуміється сукупність умов та факторів, що створюють потенційну або реально існуючу небезпеку, пов'язану з витоком інформації, та/або з несанкціонованим та/або ненавмисним впливом на неї [8]. Та під загрозою безпеки інформації розуміється подія чи дія, що може викликати зміну функціонування ІС пов'язані з порушенням захищеності оброблюваної у ній інформації, тобто. з негативним впливом неї. Під негативною дією розуміється порушення фізичної цілісності, логічної структури, несанкціоноване отримання, модифікація тощо [9].

Аналіз даних визначень показує, що у першому визначенні розглядається деяка сукупність чинників, тобто. фактично поняття загрози інформації поєднується з поняттям вразливостей системи захисту, типом зловмисника, його оснащенням та здібностями, системою захисту та її налаштуваннями тощо. Спільно ці чинники призводять до існування небезпек.

У другому визначенні під загрозою розуміється деяка подія, що виникає в системі і веде до деяких негативних наслідків.

Таким чином, визначення загрози інформаційної безпеки, що використовується, впливає на вибір класифікаційних ознак.

У разі, коли під загрозою розуміється сукупність факторів, що призводять до завдання шкоди інформації, як класифікаційна ознака використовується будь-який з подібних факторів, або їх сукупність. При цьому виділяються такі ознаки, як:

— джерела загроз;

— кошти, що застосовуються для реалізації загроз;

— способи, що застосовуються для реалізації загроз;

— етапи життєвого циклу, на яких відбувається реалізація загрози;

— випадковість.

У разі, коли під загрозою розуміється подія, яка веде до завдання шкоди інформації. Як класифікаційна ознака виділяються:

— вид завданих збитків (результат реалізації загрози);

— спрямованість загроз.

Також є підходи до класифікації загроз, у яких використовується відразу кілька класифікаційних параметрів. До них відносяться класифікація загроз для розподілених обчислювальних систем та системна класифікація загроз [10,11].

Враховуючи концепцію здійснення загрози, в якій поняття загрози відокремлено від поняття вразливості, основним критерієм для порівняння є визначення загрози інформаційній безпеці, що лежить в основі класифікації. Виходячи з прийнятого критерію порівняння, вибираються підходи щодо виду збитків, спрямованості загроз, загроз для розподілених обчислювальних систем і системна класифікація загроз.

На жаль, всі виявлені підходи не розглядають взаємозв'язок між загрозами, тобто. в них не знаходить відображення той факт, що реалізація загрози може призвести до реалізації інших загроз. Наприклад, загроза розкрадання жорсткого диска з даними призводить одночасно до реалізації загроз розкриття конфіденційності даних, що зберігаються на диску. У наведених класифікаціях дані загрози будуть у різних класах і поміж них не буде встановлено явного зв'язку.

Таким чином, виникає необхідність у розробці такої моделі чи класифікації загроз, яка у явному вигляді визначала б взаємозв'язки між різними загрозами.

Список джерел:

1. Грищук, Р. В. Основи кібербезпеки / Р. В. Грищук, Ю. Г. Даник // – Ж.: ЖНАЕУ, 2016. – 688 с.
2. Молодецька, К. В. Соціальні інтернет-сервіси як суб’єкт інформаційної безпеки держави / К. В. Молодецька // Information technology and security. – 2016. – Vol. 4, Iss. 1. – С. 13–20.
3. Молодецька, К. В. Технологія виявлення організаційних ознак інформаційних операцій у соціальних інтернет-сервісах / К. В. Молодецька // Проблеми інформаційних технологій. – 2016. – № 20. – С. 84– 93.
4. Молодецька-Гринчук, К. В. Виявлення інформаційних впливів у соціальних інтернет-сервісах на основі інтелектуального аналізу текстового контенту / К. В. Молодецька-Гринчук // Актуальні питання забезпечення кібербезпеки та захисту інформації. – 2017. – С. 121–122.
5. Молодецька-Гринчук, К. В. Методика виявлення маніпуляцій суспільною думкою у соціальних інтернет-сервісах / К. В. Молодецька-Гринчук // Інформаційна безпека. – 2016. – № 24. – С. 80–92.
6. Молодецька-Гринчук, К. В. Метод побудови профілів інформаційної безпеки акторів соціальних інтернет-сервісів / К. В. Молодецька-Гринчук // Інформаційна безпека. – 2017. – № 26. – С. 104–110.
7. . Hells U., Karras A., Scherer K.R. Multichannel communication of emotion: synthetic signal production // Facets of Emotion. Recent research / Ed. K.R.Scherer/ — Hillsdate, N.J. — 1988. — P. 162.
8. Council of Europe Convention on Access to Official Documents, Tromso, 2009 / / CETS № 205.
9. Cooruption, Inequality, and the Rule of Law : The Building Pocket Makes the Easy Life / By Eric M. Uslaner. — Cambridge University Press, 2008. — 360 p.].
10. Cooruption, Inequality, and the Rule of Law : The Building Pocket Makes the Easy Life / By Eric M. Uslaner. — Cambridge University Press, 2008. — 390 p.].

11. Breslin, Brigid ; Doron Ezickson ; John Kocoras (2010). «The Bribery Act 2010 raising the bar above the US Foreign Corrupt Practices Act». Company Laweyr. Sweet & Maxwell. 31 (II) . ISSN 0144-1027 C. 35.].

УДК 378:004

СУЧАСНИЙ ОСВІТНІЙ ПРОЦЕС І КІБЕРБЕЗПЕКА

Костікова М. В., доцент, канд. техн. наук, доцент кафедри інформатики та прикладної математики, Харківський національний автомобільно-дорожній університет

Анотація. В матеріалі розглянута проблематика кібербезпеки у навчальному середовищі і надані пропозиції щодо її розв'язання. Акцентовано, що найбільш значущими серед кіберзагроз для учасників навчально-виховного процесу є методи соціальної інженерії, знання яких та протидія яким можуть бути найбільш ефективними для забезпечення кібербезпеки.

Ключові слова: кібербезпека, навчальне середовище, кіберзагроза, суб'єкт освітнього процесу, соціальна інженерія.

Розвиток цифрового інформаційного суспільства все більше набуває динамічності. Швидкість розповсюдження інформації потребує постійного, пильного контролю, адже в сучасному світі з'явилось безліч нових загроз, таких як дезінформація, маніпуляція, пропаганда, фейкові новини, вірусні атаки що заполонили цифрову площину. Отже, інфосфера стає дедалі більш вразливою щодо стороннього кібернетичного впливу [1].

На сучасному етапі новітніх інформаційних технологій актуального значення набуває кібербезпека, що містить у собі міжвідомчий характер у глобалізованому світі. Адже кібербезпека є правозахисним проявом сучасного віртуального світу на тлі інноваційного розвитку інформаційних технологій в системі законного капіталу [2]. При розбудові національної системи кібербезпеки Україна враховує як кращий міжнародний досвід, так і особливості свого соціально-економічного, політичного, культурного та історичного розвитку.

На теперішній час гостро стоїть питання щодо захисту цифрової інформації, комп'ютерних мереж, операційних систем, серверів, баз даних, приватних і державних установ від несанкціонованого втручання сторонніх осіб. Тому цілком природною є необхідність створення надійної системи кібернетичної безпеки та її постійного удосконалення. Питання кібербезпеки гостро стоять з того часу, як комп'ютерна техніка перестала бути лише прерогативою великих наукових центрів. З появою та поширенням локальних і глобальних мереж змінилося розуміння кібербезпеки, відповідних трендів, проблем і задач.

Навчальне середовище є одним з наріжних каменів освіти. Внаслідок переходу до дистанційного та гібридного навчання, освітній сектор України стикнувся з великим спектром кіберзагроз. Усвідомлення цих загроз може допомогти вишам та їхнім співробітникам захистити себе та своїх студентів від цих уразливостей. В установах вищої освіти циркулюють великі обсяги персональних даних і фінансової інформації про студентів, викладачів, співробітників, а також інформації про наукові дослідження. Це робить їх привабливою ціллю для кіберзлочинців. Людський фактор, тобто помилки співробітників або студентів через необізнаність або зневажання елементарними правилами кібергігієни лежать в основі більшості успішно реалізованих кібератак.

Ознаки кіберзагроз в галузі освіти можна розділили за дев'ятьма критеріями: загрози через людський фактор, крадіжка персональних даних, загрози на пристрої IoT, програми-вимагачі або зловмисне програмне забезпечення, фінансова вигода, шпигунство, фішинг, DDoS-атаки, загрози на CMS. Знання основних загроз освітніх мереж і систем, розуміння поширених способів злому і витоків конфіденційних даних

студентів, викладачів та інших співробітників дозволить вибирати й застосовувати навчальним закладам найбільш ефективні інструменти і стратегії на всіх рівнях кіберзахисту. Кібербезпека є спільною відповідальністю для всіх, а її успіх залежить від обізнаності про мотиви та методи зловмисників, дотримання належної кібергігієни кожним та контролем за дотриманням вимог.

Крім того, у кожного суб'єкта освітнього процесу, в залежності від функції та місця в освітньому процесі, повинні бути інструкції про те, на які теми і як можна спілкуватися із сторонніми особами стосовно персональних особливостей, яку інформацію можна надавати для служби технічної підтримки, яку і як інформацію може повідомити учасник навчального процесу стороннім особам і працівникам мас-медіа. Крім того, необхідно дотримуватися наступних дев'яти типових правил протидії імовірним загрозам [3].

1. Призначені для користувача облікові дані є власністю навчального закладу. Всім співробітникам в день прийому на роботу має бути роз'яснено те, що ті логіни і паролі, які їм видали (якщо це має місце), не можна використовувати в інших цілях (на web-сайтах, для особистої пошти тощо), повідомляти іншим співробітникам, які не мають на це права або третім особам. Наприклад, співробітник на час відпустки може передати власні авторизовані дані своєму колезі для того, щоб той зміг виконати деяку роботу або подивитися певні дані в момент його відсутності. Персональні дані з результатів тестування та виконання психологічних і медичних обстежень можуть бути застосовані користувачами соціальної інженерії (метод одержання необхідного доступу до інформації, заснований на особливостях психології людей), тому потребують обережного використання.

2. Необхідно проводити вступні та регулярні навчання учнів і співробітників, спрямовані на підвищення знань з інформаційної безпеки. Проведення таких інструктажів дозволить суб'єктам освітнього процесу мати актуальні дані про існуючі методи соціальної інженерії, а також не забувати основні правила з інформаційної безпеки.

3. Обов'язковою є наявність регламентів з безпеки, а також інструкцій, до яких користувач повинен завжди мати доступ. В інструкціях повинні бути описані дії суб'єкта освітнього процесу при виникненні тієї чи іншої ситуації. Наприклад, у регламенті можна прописати, що необхідно робити і куди звертатися при спробі третьої особи запросити конфіденційну інформацію або облікові дані.

4. На комп'ютерах користувачів завжди має бути актуальне антивірусне програмне забезпечення, а також слід встановити брандмауер.

5. У корпоративної мережі навчального закладу або об'єднання закладів необхідно використовувати системи виявлення та запобігання атак. Необхідно також використовувати системи запобігання витоку конфіденційної інформації. Усе це дозволить знизити ризик виникнення фішингових атак.

6. Необхідно щонайбільше обмежити права користувача в системі. Наприклад, можна обмежити доступ до web-сайтів і заборонити використання знімних носіїв, які можуть бути використані за межами навчального закладу.

7. Необхідно бути пильним щодо джерела, яке запитує конфіденційні дані. Представники Міністерства освіти і науки навряд чи будуть телефонувати до школи, щоб дізнатися дані щодо конкретного учня або студента. Якщо людину просять ввести особисті дані – краще окремо зайти на сайт компанії, наприклад, банку. Ще краще – для уточнення інформації зателефонувати на офіційний номер установи.

8. Ніколи не слід відкривати вміст додатків або переходити за посиланням, не вивчивши всіх деталей. Часто адреса відправника містить помилки в назвах, а посилання мають неправдоподібний вигляд.

9. Критично відноситися до отриманих повідомлень: наскільки правдоподібною

може бути інформація про те, що принц з африканської країни або американський мільярдер міг залишити вам спадщину?

Рекомендується повідомляти про такі небезпеки інших членів сімей, насамперед, літніх людей, які не мають досвіду користування електронними засобами та не обізнані з питань соціальної інженерії.

Проте нові кіберзагрози потребують і нових підходів до захисту користувачів, особливо учасників освітнього процесу.

Для викладачів закладів освіти особливого значення набуває не тільки знання критеріїв надійності джерел та достовірності даних і засобів їх оцінювання, а й використання ефективних педагогічних технологій формування відповідних умінь учнів і студентів, а також засоби оцінювання рівня розвитку таких умінь. Нам потрібно знати, як захистити себе і своїх учнів від кібератак. Можливі ситуації, коли наші учні опиняться кіберзлочинцями, проте можливі й інші – в яких вони вже будуть жертвами. Молодь швидко освоює цифрові програми, деякі навіть вміють їх зламувати, однак життєвого досвіду у них все ж замало. Вони можуть бути недостатньо проникливі і мудрі, щоб розпізнати всі небезпеки онлайн-світу, з якими їм доведеться зіткнутися. Тому викладачі зобов'язані захистити своїх учнів і розповісти їм про кібербезпеку, щоб вони могли захиститися в Інтернеті.

Кібербезпека – захищеність життєво важливих інтересів громадянина і людини, суспільства та держави під час використання кіберпростору. Питання кібербезпеки у сучасному освітньому процесі є актуальним, широко обговорюється та знайшло відображення у багатьох публікаціях. Так у джерелах [4, 5] ця проблематика знайшла своє глибоке освітлення.

Інформатизація та цифровизація в наш час проникають у всі сфери діяльності держави, суспільства, бізнесу, науки, освіти та окремої людини. Тому пошук шляхів забезпечення кібербезпеки (зокрема, розробка відповідних технологій) стали важливим аспектом діяльності ІТ-сфери.

Таким чином, проблеми кібербезпеки не зводяться лише до технічних аспектів захисту інформаційних ресурсів, вони у повному обсязі мають включати такі види захисту: правові, інформаційні, технічні, організаційні та психологічні. Загрози учасникам навчально-виховного процесу з боку кіберпростору можуть бути як пасивні та активні, тому необхідно розробляти адекватні засоби захисту та життєстійкості системи «суб'єкт освітнього процесу – засоби навчання – середовище».

Список літератури

1. Доценко С. О., Лебедєва В. В. Роль і місце кібербезпеки в освітній діяльності. *Дистанційна освіта: Реалії та перспективи*: матеріали І всеукраїнської науково-практичної конференції (м. Харків, 12 грудня 2018). Харків, 2018. С. 12–15.

2. Лісовська Ю. П. Кібербезпека: ризики та заходи: навч. посібник. Київ: Видавничий дім «Кондор», 2019. 272 с.

3. Биков В. Ю., Буров О. Ю., Дементієвська Н. П. Кібербезпека в цифровому навчальному середовищі. *Інформаційні технології і засоби навчання.* 2019. Том 70, № 2. С. 313–331. URL: https://www.researchgate.net/publication/332716122_KIBERBEZPEKA_V_CIFROVOMU_NAVCALNOMU_SEREDOVISI (дата звернення 19.09.2022).

4. Закон України № 2163-VIII «Про основні засади забезпечення кібербезпеки України» (Відомості Верховної Ради (ВВР), 2017, № 45, с. 403). URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 20.09.2022).

5. Кібербезпека. Аспект 1: соціальні мережі. *Міністерство оборони України: офіційний веб сайт.* URL: https://www.mil.gov.ua/ukbs/shhodenni-kiberzagrozi/kiberbezpeka-aspekt-1-soczialni-merezhi.html (дата звернення 20.09.2022).

УДК 656.051

НЕЙРОННІ МЕРЕЖІ ПРИ ОБРОБЦІ ЗОБРАЖЕНЬ В ІНТЕЛЕКТУАЛЬНИХ СИСТЕМАХ СПОСТЕРЕЖЕННЯ

Фастовець В.І., доцент,
Харківський національний автомобільно-дорожній університет
магістр факультету Інфокомунікацій
Харківський національний університет радіоелектроніки, Україна
Шуляков В.М. , доцент
Харківський національний університет радіоелектроніки, Україна

Анотація. *Проведений огляд нейронних мереж для вибору інтелектуальних систем відеоспостереження на їх основі.*

Ключові слова: нейронні мережі, нейрон, синапс, Згорткові нейронні мережі, рекурентні нейронні мережі, навчання нейронної мережі.

Мозок та нервова система людини складається з клітин, які називаються нейронами, і має надзвичайну складність. Унікальною здатністю нейрона є прийом, обробка і передача електрохімічних сигналів по нервовим шляхам. Від тіла нейрона до інших нейронів ідуть дендрити (деревоподібні відростки на входах нейрона). Вони приймають сигнали в точках з'єднання, які називаються синапсами.

Прийняті синапсом вхідні сигнали підводяться до тіла нейрона, де вони підсумовуються. Нейрон збуджується і посилає по спеціальному відростку, так званому аксону, сигнал іншим нейронам.

Більшість нейронних мереж складаються з формальних нейронів (рис. 1). Цей примітивний обчислювальний пристрій (або його модель), що має кілька входів і один вихід, і є основним обчислювальним елементом нейромережі.

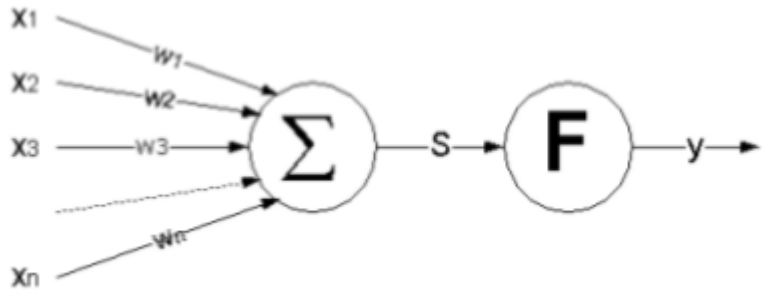


Рис. 1 Формальний нейрон.

Тут x1..xn - значення, що надходять на входи (синапси) нейрона,
w1..wn - ваги синапсів (можуть бути як гальмуючі, так і підсилюючі),
S - зважена сума вхідних сигналів.
$S = \sum_{i=1}^{n} W_i X_i - T = (W, T) - T = |W| * |X| * cos \propto -T$,
де T - поріг нейрона,
F - функція активації нейрона, що перетворює зважену суму в вихідний сигнал,
α - кут між векторами (вхідним вектором і вектором ваг).

Штучна нейронна мережа складається з набору пов'язаних формальних нейронів і здатна виконувати логічні операції і перетворення, реалізовані дискретними пристроями з кінцевої пам'яттю. Формальний нейрон моделює деякі властивості біологічного нейрона. Нейрони в природних нейронних мережах набагато складніші. Мозок може мати квантову структуру, а процес мислення може бути заснований на

квантових ефектах. Мозок людини містить 10 трильйонів нейронів, пов'язаних між собою більше ніж 1000 синапсами. Зв'язки між нейронами розвиваються і модифікуються протягом усього життя, тобто свій інтелектуальний досвід людина отримує в процесі навчання. Все це свідчить про перспективність розвитку штучних нейронних мереж.

Кожна нейронна мережа включає перший вхідний шар нейронів. Цей шар не виконує обчислень та перетворень, він приймає вхідні сигнали та розподіляє їх по іншим нейронам.

За структурою нейронні мережі розподіляються на такі типи:

1) Одношарова нейронна мережа. Сигнали з вхідного шару направляються на вихідний шар, який, перетворює сигнал і відразу видає відповідь. Вхідні нейрони є об'єднаними з основним шаром за допомогою синапсів з різними вагами для забезпечення якості зв'язків.

2) Багатошарова нейронна мережа. Тут, крім вихідного та вхідного шарів, є ще проміжні шари. Число цих шарів залежить від ступеня складності нейронної мережі. Вона вже більше нагадує структуру біологічної нейронної мережі. В процесі обробки даних кожен проміжний шар — це проміжний етап, на якому здійснюється обробка та розподіл інформації.

Нейронні мережі також можна класифікувати за напрямом розподілу інформації по синапсам між нейронами:

1) Нейромережі прямого поширення, або односпрямовані. У таких мережах сигнал переміщається від вхідного шару до вихідного. Сьогодні розробки односпрчиованих нейромереж широко поширені і успішно вирішують завдання розпізнавання образів, кластеризації і прогнозування.

2) Рекурентні нейронні мережі (Recurrent Neural Network, RNN) - це мережі зі зворотніми зв'язками.. Сигнал може рухатися і у прямому, і у зворотному напрямку. Результат виходу здатний повертатись на вхід. Вихід нейрона визначається ваговими характеристиками та вхідними сигналами, та може доповнюватись попередніми виходами, які знову повернулися на вхід. Цим нейромережам властива функція короткочасної пам'яті.

3) Радіально-базисні функції.

4) Картки, що самоорганізуються.

Але це далеко не всі варіанти класифікації та види нейронних мереж. Також їх розподіляють:

1) Залежно від типів нейронів: однорідні та гібридні.

2) За типом вхідної інформації: аналогові, двійкові та образні.

3) За характером налаштування синапсів: з фіксованими та динамічними зв'язками.

За характером навчання і формування зв'язків нейронні мережі можуть бути наступних видів:

– Навчання з учителем. Заздалегідь відомі еталонні значення реультатів, зв'язки налаштовуються в процесі навчання.

– Самонавчання (навчання без вчителя). Еталонні значення результатів невідомі, мережа в процесі навчання повинна організувати вхідні образи на основі їх подібності.

– Фіксований зв'язок. Визначаються характером розв'язуваної задачі.

Також можна класифікувати нейронні мережі, як:

– Нейронні мережі прямого поширення (Feed Forward Neural Networks, FFNN).

– Згорткові нейронні мережі (Convolutional neural network, CNN).

– Рекурентні нейронні мережі (Recurrent Neural Network, RNN).

Для розпізнавання відео- і аудіо-потоку зазвичай використовують рекурентні мережі, а для розпізнавання образів згорткові мережі (наприклад, LeNet-5 у Франції та неокогнітрон у Японії).

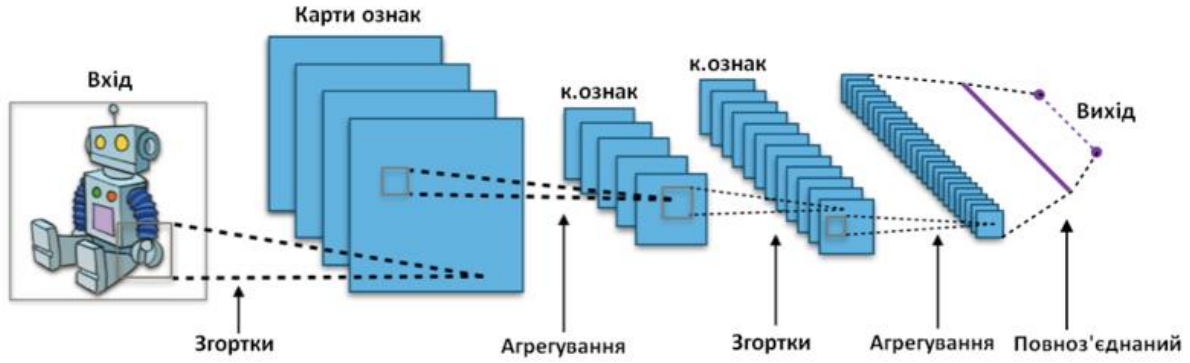


Рис 2. Типова архітектура загорткової нейронної мережі

У звичайному перцептроні, який представляє собою повнозв'язну нейронну мережу, кожен нейрон пов'язаний з усіма нейронами попереднього шару, причому кожний зв'язок має свій персональний ваговий коефіцієнт. У згортковій нейронної мережі в операції згортки використовується лише обмежена матриця ваг невеликого розміру, яку також називають ядром згортки. Її інтерпретують як графічне кодування якої-небудь ознаки, наприклад, наявність похилої лінії під певним кутом. Наступний шар, що вийшов в результаті операції згортки такою матрицею ваг, показує наявність даної ознаки в оброблюваному шарі і її координати, формуючи так звану карту ознак (англ. Feature map). Звісно, в згортковій нейроннії мережі набір ваг не один, а ціла гама, що кодує елементи зображення (наприклад, лінії і дуги під різними кутами). При цьому ядра згортки не закладаються заздалегідь, а шляхом навчання мережі класичним методом зворотного поширення помилки формуються самостійно. Прохід кожним набором ваг формує свій власний примірник карти ознак, при цьому на одному шарі формується багато незалежних карт ознак, що робить нейронну мережу багатоканальною.

Згорткова нейронна мережа складається з шарів входу та виходу, а також із спецалізованих прихованих шарів, які складаються зі згорткових шарів, агрегувальних шарів, повноз’єднаних шарів та шарів нормалізації.

Згортковий шар (convolutional layer) застосовує до входу операцію згортки, передаючи результат до наступного шару:

$$Z^l = h^{l-1} * W^l,$$

де Z^l – постсинаптичний рівень збудження нейронів l-го шару нейромережі,
h^{l-1} – активаційний рівень нейронів (l–1)-го шару нейромережі,
W^l – налагоджуваний параметр l-го шару нейромережі,
* – дискретний оператор згортки.

Параметри шару складаються з набору ядер, або фільтрів для навчання, які мають досить вузьке рецептивне поле, але простягаються на всю глибину вхідної ємності. При прямому проходженні кожен фільтр обчислює скалярний добуток даних входу та фільтру, здійснює згортку за шириною та висотою вхідної ємності, і формує двовимірну карту збудження цього фільтру.

При переборі шаром матриці ваг її пересувають зазвичай не на розмір цієї матриці, а на невелику відстань. Так, наприклад, при розмірності матриці ваг 6 × 6 її зрушують на один або два нейрона (пікселя) замість шости, щоб не пропустити шукану ознаку.

Далі виконується зменшення розмірності сформованих карт ознак за допомогою операції підвибірки, або сабдискретизації (англ. Subsampling, Pooling), виконується зменшення розмірності карт ознак, що були сформовані на попередньому етапі. Далі приймається положення, що інформація про факт наявності шуканої ознаки важливіше точного знання її координат, тому з кількох сусідніх нейронів карти ознак вибирається максимальний і приймається за один нейрон ущільненої карти ознак меншої розмірності. Після цього мережа стає більш інваріантною до масштабу вхідного зображення.

Початковий шар нейромережі приймає вхідне зображення, потім сигнал проходить серію згорткових шарів, в яких чергується власне згортка і субдискретизація (пулінг). В результаті обробки на кожному наступному шарі карта ознак зменшується в розмірі, натомість збільшується кількість каналів, що означає здатність розпізнавання складних ієрархій ознак. Після проходження декількох шарів карта ознак може виродитися у вектор або скаляр, але таких карт ознак стає дуже багато. На виході згорткових шарів мережі додатково встановлюють кілька шарів повнонейронної мережі, або перцептрон, на вхід якого подаються кінцеві карти ознак.

Максимізаційне агрегування (max pooling) використовує максимальне значення з кожного з кластерів нейронів попереднього шару. Воно розділяє вхідне зображення на набір прямокутників без перекриттів, і для кожної такої підобласті виводить її максимум:

$$h_{x,y}^{l} = max_{i,j}\{h_{(x+i)(y+j)}^{l-1}\}, i = 0, \dots, s, j = 0, \dots, s,$$

де $h_{x,y}^{l}$ – рівень активації нейрона з індексами (x, y) l-го шару нейромережі.

Існує способ пулінга, званий агрегуванням областей інтересу (Region of Interest pooling, RoI pooling) – це різновид максимізаційного агрегування, в якому розмір виходу фіксовано, а прямокутник входу є параметром.

Агрегування, яке використовує усереднене значення з кожного з кластерів нейронів попереднього шару, називається усереднювальним агрегуванням (average pooling):

$$h_{x,y}^{l} = \frac{1}{s^2}\sum_{i=0}^{s}\sum_{j=0}^{s} h_{(x+i)(y+j)}^{l-1}$$

L -нормове агрегування (L^2 -norm pooling) базується на Евклідовій відстані:

$$h_{x,y}^{l} = \sqrt{\sum_{i=0}^{s}\sum_{j=0}^{s}(h_{(x+i)(y+j)}^{l-1})^{2}}$$

Шар зрізаних лінійних вузлів (Rectified Linear Units layer, ReLU) застосовує ненасичувальну передавальну функцію ReLU і посилює нелінійні властивості функції ухвалення рішення і мережі в цілому. При цьому цей шар не зачіпає рецептивних полів згорткового шару. Інші функції, такія. як насичувальний гіперболічний тангенс та сигмоїдна функція, також можуть використовувтись для посилення нелінійності.

Згладжувальний шар (flatten layer) згортає просторові розмірності входу в розмірність каналу.

Повноз’єднаний шар (fully connected layer) забезпечує високорівневий зв’язок кожного нейрона одного шару з кожним нейроном наступного шару:

$$Z^l=W^l h^{l-1}.$$

У багатьох нейромережах завершальним є шар втрат (loss layer), який визначає, як навчання штрафує відхилення між передбаченими та справжніми мітками класів.

Основними рисами згорткових нейромереж є:

1) Просторова організація, тобто згорткові шари мають нейрони, впорядковані у трьох вимірах: ширина, висота та глибина; нейрони всередині шару з'єднані лише з невеликою областю попереднього шару, яка називається рецептивним полем.

2) Для формування архітектури ЗНМ складають різні типи шарів, як локально-, так і повноз'єднані.

3) Для кожного рецептивного поля шару використовується один і той же банк ваг, або фільтр. Кожен фільтр повторюється на всьому зоровому полі, а повторні вузли використовують спільну параметризацію (вектор ваг та упередженості) й формують карту ознак. Це означає, що всі нейрони в заданому згортковому шарі реагують на одну й ту ж саму ознаку в межах свого рецептивного поля. Повторювання вузлів таким чином дозволяє ознакам бути виявленими незалежно від їхнього положення в зоровому полі, забезпечуючи таким чином властивість інваріантності відносно зсуву.

4) У шарах об'єднання карти ознак поділяються на прямокутні підрегіони, а ознаки кожного прямокутника зменшуються до одного значення, (середнього або максимального). Спільне використання ваг різко зменшує кількість вільних параметрів, на яких вчиться мережа. Це зменшує обсяг необхідної пам'яті та поліпшує продуктивність згорткової нейромережі.

5) Навчання згорткових нейромереж найчастіше здійснюють шляхом використання техніки зворотного поширення помилки.Для навчання глибинної мережі необхідні великий набір даних та великі обчислювальні потужності.

Досить швидко та ефективно можуть ідентифікувати та обробляти дані зображення згорткові нейронні мережі. Експерти Facebook AI Research (FAIR) створили глибокого навчання під назвою Mask R-CNN. Для кожного об'єкта, який присутній на зображенні, вона може створити піксельну маску. Ця архітектура є розширеною версією архітектури виявлення об'єктів Faster R-CNN.

FAST R-CNN використовує координати рамки та клас об'єкта в якості двох частин даних для кожного об'єкта на зображенні. Mask R-CNN надає додатковий поділ та виводить маску об'єкта після виконання сегментації. Спочатку ConvNet, до якої передається вхідне зображення, генерує карту об'єктів для зображення. Потім до карт об'єктів система застосовує мережу регіональних ознак (RPN) і генерує їх з оцінками об'єктивності. До ознак застосовується шар об'єднання для приведення їх до одного розміру. На останньому етапі система передає ознаки повнозв'язному шару для класифікації та генерує вихід з обмежуючими контурами для кожного об'єкта[1].

Література

1. Субботін С. О. Нейронні мережі : теорія та практика: навч. посіб. / С. О. Субботін. – Житомир : Вид. О. О. Євенок, 2020. – 184 с.

УДК 004.49

ЗВ'ЯЗОК КІБЕРАТАК ІЗ НАЗЕМНИМИ БОЙОВИМИ ДІЯМИ

Товкун Юлія Ігорівна
студентка VI курсу факультету Інфокомунікацій
Харківський національний університет радіоелектроніки, Україна
Добринін Ігор Станіславович
кандидат технічних наук, доцент, доцент кафедри інфокомунікаційної інженерії імені В.В. Поповського
Харківський національний університет радіоелектроніки, Україна

Анотація. На тлі військового вторгнення в Україну кібератаки та операції були націлені на критично важливу інфраструктуру та цивільні об'єкти.

Нанесення ударів по об'єктах критичної інфраструктури викликає особливу стурбованість, оскільки ця інфраструктура необхідна для виживання цивільного населення. Кібератаки на інфраструктуру, таку як енергетика, водопостачання, охорона здоров'я, фінансові установи, транспорт і послуги зв'язку, можуть мати руйнівні наслідки для цивільного населення.

Крім ризиків для критичної інфраструктури та цивільних об'єктів, кібератаки сіють недовіру й обмежують доступ до достовірної інформації або поширюють неправдиву інформацію.

Ключові слова: кібератака, Wiper, бойові дії, атака, хакер, безпека.

Незадовго до вторгнення в Україну в лютому компанія Microsoft повідомила про 237 кібератак, у яких брали участь шість державних груп, пов'язаних із Росією. З них близько 40 було класифіковано як "руйнівні" атаки, спрямовані на зниження можливостей цілі [1].

У звіті показано кілька великих російських кібератак, які передували фізичним нападам на об'єкти в Україні.

У середині січня потужної хакерської атаки зазнали держсайти, а також портал "Дія", що зберігає персональні дані мільйонів українців: адреси, телефони, е-мейли тощо. У залишеному повідомленні хакери писали: "Уся інформація про вас стала публічною, бійтеся і чекайте гіршого". Влада запевняла, що особисті дані викрадені не були. Але пізніше з'явилися відомості про те, що 2 млн записів із "Дія" продають в інтернеті за $15 000.

Найпотужніша DDoS-атака в довоєнній історії України почалася 15 лютого, коли вивели з ладу десятки сайтів банків і держструктур. Вона не припинялася до самого передодня війни.

1 березня за кібератакою на українську телекомпанію з руйнівним витоком даних послідував ракетний удар по одній з її телевеж.

2 березня дані було вкрадено в організації з ядерної безпеки під час захоплення наземними військами військ атомних електростанцій у країні.

11 березня держоргани міста Дніпро зазнали цілеспрямованої атаки, трохи згодом, цього самого дня було завдано перших ударів по урядових будівлях Дніпра.

На початку наступу на місто Маріуполь було здійснено масштабну розсилку електронною поштою з дезінформацією, надходили листи від людини, яка видавала себе за жителя міста і стверджувала, що уряд збирається кинути його населення [1].

Також видно, що кібератаки на Україну з боку Росії перед вторгненням розпочалася ще на початку 2021 року, коли пов'язані з Росією хакери досліджували організації всередині України, щоб визначити мету подальших атак.

Кібератаки з використанням шкідливого програмного забезпечення типу Wiper почалися на початку 2022 року, коли дипломатичні зусилля зазнали невдачі і можливість війни стала більш імовірною. Найбільша хвиля російських кібератак такого роду припала на період безпосередньо перед і після початку вторгнення: з 23 лютого по 2 березня.

Кібератака, спрямована на Viasat, яка тимчасово вимкнула модеми KA-SAT 24 лютого 2022 року, того самого дня, коли російські збройні сили вторглися в Україну, була наслідком шкідливого ПЗ Wiper.

Висновки було отримано наступного дня після того, як американська телекомунікаційна компанія повідомила, що вона стала ціллю багатогранної та навмисної кібератаки на свою мережу KA-SAT, пов'язавши її з "вторгненням у наземну мережу зловмисника, який використовував неправильну конфігурацію у пристрої VPN", для отримання віддаленого доступу до довіреного сегмента управління мережі KA-SAT [2].

Отримавши доступ, зловмисник віддав "деструктивні команди" десяткам тисяч модемів, що належать службі супутникового широкосмугового зв'язку, які "переписали ключові дані у флеш-пам'яті модемів, зробивши модеми нездатними отримати доступ до мережі, але не назавжди".

Другою версією є IsaacWiper. IsaacWiper знаходиться або в Windows DLL, або в EXE без підпису Authenticode [3].

Для зразків DLL ім'я в каталозі експорту PE - Cleaner.dll , і він має єдиний експорт _Start@4.

За допомогою VirusTotal вийшло дізнатися, що IsaacWiper у %programdata% і C:\Windows\System32 міг перебувати під такими іменами:

- **clean.exe;**
- **cl.exe;**
- **cl64.dll;**
- **cld.dll;**
- **cll.dll.**

IsaacWiper починає з перерахування фізичних дисків і викликає DeviceIoControl, щоб отримати їхні номери пристроїв. Потім він стирає перші 0x10000 байт кожного диска, використовуючи генератор псевдовипадкових чисел Mersenne Twister. Генератор заповнюється з використанням значення GetTickCount [2].

Потім він перераховує логічні диски і рекурсивно стирає кожен файл кожного диска випадковими байтами, також згенерованими PRNG Mersenne Twister. Він рекурсивно стирає файли в одному потоці, а це означає, що стирання великого диска займе багато часу.

25 лютого 2022 року зловмисники скинули нову версію IsaacWiper з журналами налагодження . Це може вказувати на те, що зловмисники не змогли стерти деякі з цільових машин і додали повідомлення журналу, щоб зрозуміти, що відбувається.

Третя версія Wiper – CaddyWiper була виявлен а в Україні 14 березня 2022 р. під час розгортання в мережі банку. Він був розгорнутий через об'єкт групової політики, що вказує на те, що зловмисники заздалегідь мали контроль над мережею цілі. Wiper стирає призначені для користувача дані та інформацію про розділи з підключених дисків, роблячи систему непрацездатною і такою, що не підлягає відновленню [4].

На відміну від програм-вимагачів, мета розгортання вайпера не фінансова, його єдина мета – знищити все, що можна. В умовах триваючої війни між Росією та Україною кіберзлочинці використовуватимуть такі можливості, щоб отримати вигоду з конфлікту.

Список джерел:

1. Special Report: Ukraine - An overview of Russia's cyberattack activity in Ukraine [Електронний ресурс] – Режим доступу до ресурсу: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.
2. A Modem Wiper Rains Down on Europe [Електронний ресурс] – Режим доступу до ресурсу: https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/.
3. IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine [Електронний ресурс] – Режим доступу до ресурсу: https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/.
4. CaddyWiper: More destructive wiper malware strikes Ukraine [Електронний ресурс] – Режим доступу до ресурсу: https://www.zdnet.com/article/caddywiper-more-destructive-wiper-malware-strikes-ukrainian-targets/.

УДК 004.056

АКТУАЛЬНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Плєхова Г. А., доцент, канд. техн. наук, доцент кафедри інформатики та прикладної математики, Харківський національний автомобільно-дорожній університет,
Костікова М. В., доцент, канд. техн. наук, доцент кафедри інформатики та прикладної математики, Харківський національний автомобільно-дорожній університет

Анотація. Досліджені проблеми інформаційної безпеки та захисту інформаційних систем від навмисного чи випадкового втручання. Висвітлюються актуальні проблеми розвитку системи інформаційної безпеки. Інформаційна безпека має першорядне значення у зв'язку із значним поширенням атак, яким постійно піддаються як окремі мережі підприємств, так і національні мережі в цілому.

Ключові слова: інформаційні системи, інформаційна безпека, небезпека, Lorenz, захист інформації.

Широке поширення обчислювальної техніки як засобу обробки інформації призвело до інформатизації суспільства та появі принципово нових, інформаційних технологій. Поява будь-яких нових технологій зазвичай має як негативні, так і позитивні сторони. Тому багато прикладів. Атомні та хімічні технології, вирішуючи проблеми енергетики та виробництва нових матеріалів, породили екологічні проблеми. Інтенсивний розвиток транспорту забезпечує зручну і швидку доставку людей, матеріалів, сировини і товарів у необхідних напрямах, а й матеріальні збитки і жертви при транспортних катастрофах зросли. Інформаційні технології також не є винятком з цього правила, і тому слід завчасно подбати про безпеку при використанні та розробці таких технологій.

Від ступеня безпеки інформаційних технологій сьогодні залежить добробут, а часом життя багатьох людей. Така плата за ускладнення та поширення автоматизованих систем обробки інформації.

Інформаційні технології все більш наполегливо проникають в усі сфери людської діяльності. У сучасному суспільстві важливою проблемою є захист інформації, яка перетворилася на ринку в предмет купівлі-продажу. У зв'язку з цим зараз широко обговорюється інформаційна безпека. Завдання кожної організації створити таку систему захисту, яка була б стійка до втручання сторонніх осіб. Це передбачає безпеку мереж та всієї інфраструктури, захист програмного забезпечення та баз даних, регулярний аудит інформаційних систем. На цю тему видано чимало наукових статей та методичних посібників.

Так у підручнику [1] розглянуті концептуальні засади інформаційної безпеки, національні інтереси в інформаційній сфері, стратегія розвитку та формування єдиного інформаційного простору України, загрози безпеці держави та її громадянам в інформаційній сфері, технології інформаційно-психологічного та інформаційного впливу й захисту від цих впливів, система забезпечення інформаційної безпеки України, особливості функціонування та функції її суб'єктів.

Проблема інформаційної безпеки має давнє походження і стала особливо значущою у наш час, коли використання інформаційно-телекомунікаційних технологій відбувається вже практично у всіх житті суспільства. Розгляду питань інформаційної безпеки приділяють величезну увагу як вітчизняні, так і закордонні дослідники.

Доктор Вільям Столінгс зробив унікальний внесок у розуміння широкого спектру технічних розробок у галузі комп'ютерної безпеки, комп'ютерних мереж та

комп'ютерної архітектури. У [2] пропонується вичерпне та уніфіковане пояснення кращих практик та стандартів, які є перевіреними та узгодженими методами реалізації кібербезпеки.

Перед розгортанням нових технологій у виробничому середовищі необхідно розглянути їх аспекти безпеки. Програмно-визначені мережі (*SDN*) та віртуалізація мережевих функцій (*NFV*) – це дві нові технології, які використовуються, наприклад, для підвищення керованості, безпеки та гнучкості корпоративних/виробничих/хмарних *IT*-середовищ. У [3] представлений аналіз безпеки кількох програмно-визначуваних мереж (*SDN*) та додатків віртуалізації мережевих функцій (*NFV*) з використанням середовища моделювання загроз *Microsoft STRIDE*.

Проблема інформаційної безпеки в останні роки стала дуже актуальною і розглядається як одне із пріоритетних державних завдань.

Метою роботи є визначення напрямів удосконалення забезпечення інформаційної безпеки у взаємозв'язку з інформаційною діяльністю, з огляду на реальні й потенційні загрози, а також ключових інструментів її забезпечення.

Для досягнення поставленої мети необхідно визначити актуальні проблеми розвитку системи інформаційної безпеки.

Комп'ютерні мережі характерні тим, що проти них роблять так звані віддалені атаки. Порушник може перебувати за тисячі кілометрів від об'єкта, що атакується, при цьому нападу може зазнавати не тільки конкретний комп'ютер, але й інформація, що передається по мережевих каналах зв'язку.

Формування режиму інформаційної безпеки – комплексна проблема. Заходи щодо її вирішення можна поділити на п'ять рівнів:

1. Законодавчий (нормативні акти, закони, стандарти тощо).

2. Морально-етичний (різні стилі поведінки співробітників або цілої організації).

3. Адміністративний (дії загального характеру, що вживаються керівництвом організації).

4. Фізичний (електро та електронно-механічні, механічні перешкоди на можливих шляхах проникнення потенційних порушників).

5. Апаратно-програмний (система заходів спрямованих на безпеку організації та зменшення вірогідності та шкоди від загроз) має відповідати наступним принципам: захист тим ефективніший, чим простіше користувачеві з ним працювати; вартість засобів захисту має бути меншою, ніж розміри можливої шкоди; можливість відключення в екстрених випадках.

Фахівці, які працюють в сфері адміністратора з кібербезпеки повинні розуміти свої дії у разі атак на систему та алгоритм дій при відповідних атаках. Адміністратор захисту системи не повинен підлягати контролю системи. Тобто він не може бути серед тих, кого ця система контролюватиме. Система захисту має надавати докази коректності своєї роботи. Особи, які здійснюють інформаційну безпеку системи несуть особисту відповідальність.

При захисті об'єктів потрібно систему розділяти на групи. Таким чином ми можемо захистити частину системи при проникненні та порушенні захисту в якоїсь її частині.

Коли ми будуємо надійну систему з надійним захистом то вона має бути повністю протестована та узгоджена. Більш гнучким та ефективним захист стає, якщо він може мати параметри які допускають зміну параметрів при необхідності зі сторони менеджера з кібербезпеки. Крім того потрібно враховувати в системи захисту що при використанні системи користувачі будуть робить помилки при користуванням системою.

Таким чином найбільш критичні та важливі рішення мають прийматися людиною. Існування механізмів захисту має бути приховано від користувачів, робота яких перебуває під контролем.

Незважаючи на те, що сучасні ОС для персональних комп'ютерів, мають власні підсистеми захисту, актуальність створення додаткових засобів захисту зберігається. Справа в тому, що більшість систем не спроможні захистити дані, що перебувають за їх межами, наприклад, при мережевому інформаційному обміні.

Апаратно-програмні засоби захисту можна розбити на п'ять груп:

1. Системи ідентифікації (розпізнавання) та аутентифікації (перевірки справжності) користувачів.
2. Системи шифрування дискових даних.
3. Системи шифрування даних, що передаються мережами.
4. Системи аутентифікації електронних даних.
5. Управління криптографічними ключами.

Системи ідентифікації та аутентифікації користувачів – ці функції системи дозволяють обмежити доступ користувачів які випадково або незаконно питаються проникнути в комп'ютерну систему. Користувачам які мають доступ в систему, потрібно підтвердити його особистість, перевірити її справжність і потім надати чи не надати користувачеві можливість роботи з системою.

При побудові цих систем виникає проблема якості ідентифікації користувачів та вибору інформації для здійснення процедури ідентифікації та аутентифікації. Для цього формують такі типи: секретна інформація, яку має користувач (секретний ключ, пароль, персональний ідентифікатор тощо), користувач повинен запам'ятати цю інформацію або для неї можуть бути застосовані спеціальні засоби зберігання; фізіологічні параметри людини (малюнок райдужної оболонки ока, відбитки пальців тощо) або особливості поведінки (особливості роботи на клавіатурі тощо).

Системи, засновані на першому типі інформації, вважаються традиційними. Системи які використовують фізіологічні параметри людини – біометричні системи. Зараз є тенденція випереджаючого розвитку біометричних систем ідентифікації.

Системи шифрування дискових даних існують для того, щоб зробити інформацію марною для противника, використовується сукупність методів перетворення даних, звана криптографією (від грец. kryptos – прихований і grapho – пишу). Системи шифрування можуть здійснювати криптографічні перетворення даних тільки на рівні файлів або на рівні дисків. До програм першого типу можна віднести архіватори типу *RAR* та *ARJ*, які дозволяють використовувати криптографічні методи захисту архівних файлів. Прикладом систем другого типу може бути програма шифрування *Diskreet*, що входить до складу популярного програмного пакета *Norton Utilities, Best Crypt*. Крім того системи шифрування дискових даних можливо розпізнати за методом їх функціонування. За способом функціонування системи шифрування дискових даних ділять на два класи: системи «прозорого» шифрування; системи, що спеціально викликаються для здійснення шифрування на диск, що захищається, а система захисту в процесі запису виконує його шифрування [4]. Коли використовуються системи прозорого шифрування то в таких системах криптографічні перетворення йдуть в режимі реального часу. Користувач непомітно для себе перетворює інформацію в криптографічні шифри и таким чином здійснюється шифрування «на льоту». Наведемо приклад, користувач підготував документ в текстовому редакторі. Далі він записує документ на диск, що захищається, а система захисту в процесі запису виконує його шифрування. [4]

Системи другого класу зазвичай є утиліти. При шифруванні утиліти їх необхідно спеціально викликати для виконання шифрування. Архіватори є прикладом таких утиліт із вбудованими засобами парольного захисту.

Більшість систем, які пропонують встановити пароль на документ, не шифрують інформацію, а тільки забезпечують запит пароля при доступі до документа. До таких систем належить *MS Office*, 1С та багато інших.

Розрізняють два основні способи шифрування даних, що передаються мережами: канальне шифрування та кінцеве (абонентське) шифрування.

У разі канального шифрування захищається вся інформація, що передається каналом зв'язку, включаючи службову. Цей спосіб шифрування дозволяє (маючи вбудовану процедуру шифрування на канальному рівні) використовувати апаратні засоби що в свою чергу робить систему більш продуктивній [4]. Однак цей підхід має і суттєві недоліки:

- Шифрування службових даних ускладнює механізм маршрутизації мережевих пакетів та вимагає розшифрування даних у пристроях проміжної комунікації (ретранслятор, шлюзи и тощо).

- Шифрування службової інформації може призвести до появи статистичних закономірностей у шифрованих даних, що впливає на надійність захисту. Крім того вона накладає обмеження на використання криптографічних алгоритмів.

- Абонентське шифрування дозволяє зробити дані конфіденційними коли вони передаються між двома абонентами. І тут захищається лише зміст повідомлень, вся службова інформація залишається відкритою. Головним недоліком є можливість з можливість аналізувати інформацію об абонентах. Такої інформації може бути інформація про обсяг даних, що передаються, яку структуру мають повідомлення та інформацію об абонентах.

Системи аутентифікації електронних даних використовують при обміні даними мережами, тут виникає проблема автентифікації автора документа і самого документа, тобто. встановлення автентичності автора. Важливо також зробити та перевірити відсутність змін в отриманому документі. Здійснення автентифікації даних робиться з застосуванням коду автентифікації повідомлення (імітівставки) або електронного підпису.

Імітівставка виробляється з відкритих даних за допомогою секретного ключа. Це спеціальне шифрування з використанням до якого додається секретного ключа та передається каналом зв'язку в кінці зашифрованих даних. Імітівставка перевіряється одержувачем за допомогою секретного ключа шляхом повторення процедури, виконаної раніше відправником, над отриманими відкритими даними.

Електронний цифровий підпис є відносно невеликою кількістю додаткової аутентифікуючої інформації, що передається разом з текстом, що підписується. Відправник формує цифровий підпис, використовуючи секретний ключ відправника. Отримувач перевіряє підпис, використовуючи відкритий ключ відправника.

Таким чином, для реалізації імітівставки використовуються принципи симетричного шифрування, а для реалізації електронного підпису – асиметричного шифрування.

Засоби управління криптографічними ключами це безпека будь-якої криптосистеми визначається криптографічними ключами. У разі ненадійного керування ключами зловмисник може заволодіти ключами та отримати повний доступ до всієї інформації в системі чи мережі.

Розрізняють такі види функцій управління ключами: генерація, зберігання та розподіл ключів.

Способи генерації ключів для симетричних та асиметричних криптосистем різні. Розглянемо генерації ключів симетричних криптосистем. В таких системах використовуються апаратні та програмні засоби генерації випадкових чисел. Генерація ключів для асиметричних криптосистем більш складна, оскільки ключі повинні мати певні математичні властивості.

Функція зберігання передбачає організацію безпечного зберігання, обліку та видалення ключової інформації. Для забезпечення безпечного зберігання ключів застосовують їхнє шифрування за допомогою інших ключів. Такий підхід призводить до

концепції ієрархії ключів. У ієрархію ключів зазвичай входить головний (тобто майстер-ключ). Майстер-ключ використовують для шифрування ключів та як ключ шифрування даних. Генерація та зберігання майстер-ключа є критичним питанням криптозахисту. [5]

Розподіл - найвідповідальніший процес у керуванні ключами. Цей процес повинен гарантувати скритність ключів, що розподіляються, а також бути оперативним і точним. Між користувачами мережі ключі розподіляються двома способами: за допомогою прямого обміну сеансовими ключами; використовуючи один або кілька центрів розподілу ключів. [5]

Нова операція з викупу, відома як атакувальна система *Lorenz*, націлена на організації в усьому світі за допомогою індивідуальних атак, які вимагають сотні тисяч доларів викупу. Програма-вимагач *Lorenz* почала діяти у квітні 2021 року і з тих пір накопичила зростаючий список жертв, чиї вкрадені дані були опубліковані на сайті витоку даних. Шифратор *Lorenz* є таким же, як і попередня операція, відома як *ThunderCrypt*. Як і інші атаки програмного забезпечення, *Lorenz* порушує мережу та поширюється на інші пристрої, доки вони не отримують доступ до облікових даних адміністратора домену *Windows*. Поширюючись по всій системі, програма-вимагач збиратимуть не зашифровані файли із серверів жертв, які вони завантажують на віддалені сервери під їхнім контролем. Ці вкрадені дані потім публікуються на спеціальному сайті для витоку даних, щоб тиснути на жертв, щоб вони заплатили викуп або продали дані. На сайті витоку даних *Lorenz* перераховано дванадцять жертв, дані оприлюднені для десяти з них. Коли команда *Lorenz* публікує дані, вона робить трохи інакше, ніж інші групи. Щоб змусити жертв сплатити викуп, *Lorenz* спочатку надає дані для продажу іншим суб'єктам загроз або можливим конкурентам. Минає час, вони починають випускати захищені паролем *RAR*-архіви, що містять дані жертви. Зрештою, якщо викуп не сплачується, а дані не купуються, *Lorenz* випускає пароль для архівів витоку даних, щоб вони були загальнодоступними ля всіх, хто завантажує файли. Іншою цікавою характеристикою, якої немає на інших сайтах витоку даних, є те, що *Lorenz* продає доступ до внутрішньої мережі жертви разом з даними. Для деяких суб'єктів загроз доступ до мереж може бути більш цінним, ніж самі дані.

Зі зразків програм-вимагачів *Lorenz*, учасники загроз налаштовують виконуваний файл шкідливого програмного забезпечення для конкретної організації, на яку вони націлені.

В одному зі зразків, наданих *BleepingComputer*, програма-вимагач видасть такі команди, щоб запустити файл під назвою ScreenCon.exe з того, що, здається, є контролером домену локальної мережі.

Під час шифрування файлів програма-вимагач використовує шифрування *AES* і вбудований ключ *RSA* для шифрування ключа шифрування. Для кожного зашифрованого файлу до імені файлу буде додано розширення *.Lorenz.sz*40. Наприклад, файл з іменем 1.*doc* буде зашифрований і перейменований на 1.*doc.Lorenz.sz*40.

На відміну від інших програм-вимагачів, орієнтованих на підприємства, зразок Lorenz, не вбиває процеси або не закриває служби Windows перед шифруванням.

Кожна папка про викуп на комп'ютері буде записуватися під назвою *HELP_SECURITY_EVENT.html,* яка містить інформацію про те, що сталося з файлами жертви. Вона також міститиме посилання на сайт витоку даних *Lorenz* і посилання на унікальний платіжний сайт *Tor*, де жертва може побачити свій запит на викуп. Кожна жертва має спеціальний платіжний сайт Tor, який містить вимогу викупу в біткойнах і форму чату, в якому жертви можуть домовитися зі зловмисниками. Зі записів про викуп, які бачив *BleepingComputer*, вимоги *Lorenz* про викуп варіюються від 500 000 до 700 000 доларів. Попередні версії програм-вимагачів включали вимоги викупу на мільйон доларів, але неясно, чи були вони пов'язані з тією ж операцією.

Зараз програму-вимагач аналізують на наявність слабких місць, і

BleepingComputer не радить жертвам платити викуп, поки не буде визначено, чи може безкоштовний дешифратор відновити файли безкоштовно. Вже створений дешифратор, який надає можливість частково відновити вкрадені дані.

Таким чином, інформація – це ресурс. Втрата конфіденційної інформації завдає моральної чи матеріальної шкоди. Умови, що сприяють неправомірному оволодінню конфіденційною інформацією, зводяться до її розголошення, витоку та несанкціонованого доступу до її джерел. У сучасних умовах безпека інформаційних ресурсів може бути забезпечена лише комплексним системним захистом інформації. Комплексна система захисту має бути: безперервною, плановою, цілеспрямованою, конкретною, активною, надійною. Система захисту має спиратися на систему видів власного забезпечення, здатного реалізувати її функціонування у повсякденних умовах, у критичних ситуаціях. Різноманітність умов, що сприяють неправомірному оволодінню конфіденційною інформацією, викликає необхідність використання не менш різноманітних способів, сил та засобів для забезпечення інформаційної безпеки.

Способи забезпечення інформаційної безпеки мають бути орієнтовані на запобіжний характер дій, що спрямовуються на завчасні заходи запобігання можливим загрозам комерційним секретам. Забезпечення інформаційної безпеки досягається організаційними, технічними та організаційно-технічними заходами, кожне з яких забезпечується специфічними силами, заходами та засобами, що мають відповідні характеристики.

Список літератури

1. Остроухов В.В., Присяжнюк М.М., Фармагей О.І., Чеховська М.М. та ін. Інформаційна безпека: підручник. Київ: Видавництво Ліра-К, 2021. 412 с.

2. Stallings W. Effective Cybersecurity: A Guide to Using Best Practices and Standards. Addison-Wesley, 2019. 800 p.

3. Sagare A.A., Khondoker R. Security Analysis of SDN Routing Applications. In: Khondoker, R. (eds) SDN and NFV Security. Lecture Notes in Networks and Systems, vol. 30. Cham: Springer, 2018. pp. 1-17. DOI: https://doi.org/10.1007/978-3-319-71761-6_1.

4. Канали втрати конфіденційної інформації. *Канали втрати конфіденційної інформації – Канали витоку інформації sites.google.com.* URL: https://sites.google.com/site/kanalivitokuinformaciie/klasifikacia-kanaliv-vitoku-informaciie/kanali-vtrati-konfidencijnoie-informaciie (дата звернення 21.10.2022).

5. Апаратно-програмні засоби захисту інформації. *Апаратно-програмні засоби захисту інформації – Студопедія studopedia.com.ua.* URL: https://studopedia.com.ua/1_221082_aparatno-programni-zasobi-zahistu-informatsii.html (дата звернення 21.10.2022).

УДК 005.254

АНАЛІЗ ВИМОГ МІЖНАРОДНИХ СТАНДАРТІВ ЩОДО ЗДІЙСНЕННЯ АУДИТУ СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Клочкова Діана Юріївна
студентка VI курсу факультету Інфокомунікацій
Харківський національний університет радіоелектроніки, Україна
Добринін Ігор Станіславович
кандидат технічних наук, доцент, доцент кафедри інфокомунікаційної інженерії імені В.В. Поповського
Харківський національний університет радіоелектроніки, Україна

Анотація. У статті проаналізовані вимоги до проведення аудитів системи менеджменту інформаційної безпеки згідно серії стандартів ISO/IEC 270xx та ISO 19011:2018. Автор робить висновок про вимоги які спрямовані на забезпечення достатнього рівня інформаційної безпеки системи менедженту. На підставі проведеного аналізу визначено головні вимоги до аудитів у сучасних умовах.

Ключові слова: система менеджменту інформаційної безпеки (СМІБ), аудит, внутрішній аудит, організація, аудитор.

Актуальність теми. Міжнародний стандарт інформаційної безпеки ISO/IEC 27001, який увібрав у себе найкращі практики з організації управління інформаційною безпекою та найкращі методи протидії ризикам. Впровадження даного стандарту в національну систему інформаційної безпеки допоможе державі в максимально швидких строках реагувати на різного роду загрози в інформаційному середовищі. Дотримання саме цього стандарту – великий крок до визнання перед світовим товариством а також покращує економічні показники країни. Виходячи з цього, тема роботи є актуальною на сьогодні.

Метою роботи є проведення аналізу вимог стандартів ISO/IEC 270xx та ISO 19011:2018 щодо проведення аудиту інформаційної безпеки.

Виклад основного матеріалу. Аудит - систематичний, незалежний та задокументований процес отримання об’єктивних доказів та їх об’єктивного оцінювання, щоб визначити ступінь дотримання критеріїв аудиту.

Головна мета аудиту інформаційної безпеки - проведення оцінки рівня безпеки інформаційної системи підприємства для управління ним загалом з урахуванням перспектив його розвитку.

Основною метою діяльності організацій є забезпечення необхідного та достатнього рівня ІБ, який є безперервним процесом, та ефективний захист якого неможливий без комплексу організаційних заходів.

Організація повинна оцінювати результативність інформаційної безпеки та ефективність системи управління інформаційною безпекою. Організація повинна зберігати відповідну задокументовану інформацію як доказ результатів моніторингу та вимірювань.

Організація повинна проводити внутрішні аудити через заплановані інтервали часу для забезпечення того, що інформація чи система управління інформаційною безпекою: відповідають: власним вимогам організації для її системи управління інформаційною безпекою; та вимогам цього стандарту; ефективно впроваджена та підтримується.

Аудитор повинен перевірити внутрішні аудити СМІБ організації, використовуючи програми та плани аудитів СМІБ, звіти про результати аудиту, плани

дій тощо. Аудитори повинні визначити, наскільки внутрішні аудити СМІБ підтверджують відповідність СМІБ вимогам, визначеним в ISO/IEC 27001, правовим та договірним вимогам, а також іншим вимогам та вимогам СМІБ організації, встановленим внаслідок процесу оцінки ризику.

Організація має бути здатна отримувати максимальну користь із використання доступних ресурсів під час проведення внутрішніх аудитів СМІБ. Організація має встановити процес використання результатів минулих аудитів під час планування майбутніх внутрішніх аудитів СМІБ.

Аудитор СМІБ має бути спроможним сформувати висновок, чи реалізувала організація ефективну програму внутрішнього аудиту СМІБ. Аудитор СМІБ має бути також здатний сформувати висновок, чи справді результати внутрішніх аудитів СМІБ забезпечують адекватні свідчення використання компонентів для вдосконалення процесів СМІБ.

Вище керівництво повинно переглядати систему управління інформаційною безпекою організації через заплановані проміжки часу для гарантування її постійної придатності, адекватності й ефективності. Вихідні дані перегляду з боку керівництва повинні включати рішення стосовно можливостей постійного вдосконалення та будь-яких потреб внесення змін до системи управління інформаційною безпекою. Організація повинна зберігати документовану інформацію як доказ результатів переглядів з боку керівництва.

Процес перевірки, що проводиться керівництвом, не повинен бути заходом, що здійснюється виключно для задоволення вимог стандарту та аудиторів; він має бути інтегральною частиною процесу управління бізнесом організації. Загальна перевірка, що проводиться керівництвом, являє собою складний процес, що здійснюється на різних рівнях організації. Перевірка завжди має бути двостороннім процесом, що виробляється вищим керівництвом за участю всіх рівнів організації.

Аудитори повинні також розглянути, як структуровано керівництво організації та як у цій структурі використовується процес перевірки, що проводиться керівництвом. Записи перевірки, що проводиться керівництвом, необхідні, але їх формат не специфікований. Найпоширенішим видом записів є протоколи нарад, але прийнятними видами записів можуть бути також електронні записи, статистичні діаграми, презентації тощо. буд. не потрібні. Процес перевірки, що проводиться керівництвом, може також включати елементи планування СМІБ, де розглядаються зміни процесів і систем. У цьому випадку аудитори повинні перевірити, чи враховуються такі моменти: - чи оцінюються запропоновані зміни до реалізації; - чи розглядаються питання, пов'язані зі СМІБ, під час підготовки стратегічних планів; - ідентифікуються чи необхідні заходи та засоби контролю та управління до реалізації змін, наприклад, до початку аутсорсингу процесу.

Аудит ІБ повинен проводиться відповідно до вимог стандартів серії ISO/IEC 270xx та ISO 19011:2018.

Треба розробити програму аудиту, яка може охоплювати аудити стосовно одного чи кількох стандартів на системи управління чи стосовно інших вимог, що їх проводять окремо чи в поєднанні (комбінований аудит). Особа, яка керує програмою аудиту, має забезпечити збереження цілісності аудиту, а також унеможливлення надмірного впливу на аудит.

Пріоритет аудиту треба віддавати розподіленню ресурсів та методам так, щоб аудит стосувався питань системи управління з вищим рівнем притаманного ризику та нижчим рівнем дієвості. Для керування програмою аудиту треба призначати компетентних осіб. У програмі аудиту треба подати інформацію та визначити ресурси, які дають змогу результативно й ефективно виконувати аудит у визначені строки. Треба, щоб інформація охоплювала: цілі програми аудиту; ризики та можливості, пов’язані з

програмою аудиту, та дії щодо них; сферу (обсяг, межі, місця розташування) кожного аудиту в межах програми аудиту; графік (кількість/тривалість/періодичність) аудитів; види аудитів, такі як внутрішні чи зовнішні; критерії аудиту; методи аудиту, що їх застосовуватимуть; критерії формування групи аудиторів; перелік відповідної задокументованої інформації.

Частини цієї інформації може не бути в наявності до завершення більш докладного планування аудиту

Потрібно визначити та оцінити ризики та можливості, пов'язані з середовищем функціювання об'єкта аудиту, які можуть стосуватися програми аудиту та можуть вплинути на досягнення її цілей. Особа, яка керує програмою аудиту, має визначити та описати замовнику аудиту ризики та можливості, що їх вона розглядає під час розроблення програми аудиту, а також вимоги щодо ресурсів з тим, щоб їх можна було належно врахувати.

В організації повинні бути визначені ролі та обов'язки осіб. Особі, яка керує програмою аудиту, треба мати необхідну компетентність для результативного та ефективного керування програмою та пов'язаними з нею ризиками та можливостями, а також зовнішніми та внутрішніми чинниками. Особа, яка керує програмою аудиту, має призначити членів групи аудиту, зокрема керівника групи та будь-яких технічних експертів, потрібних для проведення конкретного аудиту та покласти відповідальність за проведення окремого аудиту на керівника групи аудиту.

Повинно бути забезпечене керування результатами виконання програми аудиту та ведення протоколів за програмою аудиту та керування ними.

Особа, яка керує програмою аудиту, має проводити моніторинг програми аудиту. Та разом з замовником аудиту мають проаналізувати програму аудиту, щоб оцінити чи було досягнено її цілей. Досвід, набутий з аналізування програми аудиту, треба використовувати як вхідні дані до процесу поліпшення програми.

Сімейство стандартів ISO/IEC 270xx спрямовані забезпечення достатнього рівня інформаційної безпеки систем менеджменту. Розглянемо докладно вимоги стандартів ISO/IEC 270xx. Стандарт ISO/IEC 27006-2008, заснований на ISO/IEC 17021-2008, задає специфічні вимоги до ряду аспектів, таких як:

1. Вимоги до ресурсів: до компетентності керівництва та персоналу, до персоналу, що бере участь у діяльності з сертифікації, до залучення окремих зовнішніх аудиторів або зовнішніх технічних експертів;

2. Вимоги до інформації: до загальнодоступної інформації, до документів із сертифікації, до посилання на сертифікацію та використання маркування;

3. Вимоги до процесу: до загальних вимог, до початкового аудиту та сертифікації, до діяльності з нагляду, до повторної сертифікації, до спеціальних аудитів, до призупинення, скасування або скорочення сфери дії сертифікації, до апеляцій, до скарг, до документів заявників та клієнтів.

Аудит інформаційної безпеки є основним інструментом контролю за станом захищеності системи менеджменту. Він може виконуватися як у сукупності із загальним аудитом, так і у вигляді самостійного проекту та є невід'ємною частиною забезпечення безпеки інформації.

Висновки. На підставі отриманих результатів можна зробити висновки про те, що сімейство стандартів ISO/IEC 270xx з проведення аудиту інформаційної безпеки спрямовано на забезпечення достатнього рівня інформаційної безпеки СМІБ, підвищує ефективність і забезпечує надійний захист конфіденційних даних. Запропоновані стандартами вимоги до проведення аудиту інформаційної безпеки допомагають забезпечити контроль за якістю виконання плану проведення аудиторської перевірки та регулюють відносини між організаціями та аудиторськими організаціями. При проведенні аудиту СМІБ важливо дотримуватись усіх принципів, описаних у стандарті

ISO 19011 та у серії стандартів ISO/IEC 270xx. Функція аудиту в організації повинна бути незалежною від області, що перевіряється, для отримання об'єктивних результатів.

Список джерел:

1. ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги»
2. ДСТУ ISO/IEC 27006:2015 «Інформаційні технології. Методи захисту. Вимоги до органів, які надають послуги з аудиту і сертифікації систем управління інформаційною безпекою».
3. ДСТУ ISO/IEC 27007:2014 «Інформаційні технології. Методи забезпечення безпеки. Керівництво для аудиту систем менеджменту інформаційної безпеки» .
4. ДСТУ ISO 19011:2019 «Настанови щодо проведення аудитів системи управління».

УДК 004.056.53: 654.9

МОЖЛИВОСТІ ІНТЕГРОВАНИХ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ

Семеренська Вікторія Владиславівна
студентка VI курсу факультету Інфокомунікацій
Харківський національний університет радіоелектроніки, Україна
Пшеничних Сергій Васильович
кандидат технічних наук, старший науковий співробітник, доцент кафедри інфокомунікаційної інженерії імені В.В. Поповського
Харківський національний університет радіоелектроніки, Україна

Анотація. Можливості сучасної аналітики дають змогу системам відеоспостереження вийти за рамки охоронних функцій і стати ефективним інструментом реагування на події в розвитку, скорочення втрат і збитків, і навіть запобігання потенційно небезпечним ситуаціям. Алгоритми і технології аналізу відео розвиваються і вдосконалюються стрімко, що дає змогу найкращим системам працювати в мінливих зовнішніх умовах, майже не реагувати на перешкоди, враховувати безліч критеріїв, класифікувати об'єкти за цілою низкою ознак, мінімізувати кількість хибних спрацьовувань. спрацьовувань. [1]

Ключові слова: Системи відеоспостереження, інтегрована система безпеки, відеоаналітика, сигналізація.

Забезпечення безпеки різних об'єктів потребує комплексу заходів, спрямованих на попередження, припинення та усунення загрози або небезпечної ситуації. Комплекс заходів має ґрунтуватися на принципах системного підходу до діяльності із забезпечення безпеки як на етапах організації, підготовки, проектування, так і в процесі експлуатації, а також включати сукупність організаційних і технічних заходів - систему комплексної безпеки.

Взаємодія систем відеоспостереження та інших систем безпеки дає більше, ніж сума їх функціональних можливостей. За рахунок прозорого обміну даними і командами досягається синергія – система стає більш інтелектуальною – вона може реагувати на зовнішні впливи самостійно, без оператора. Програмне забезпечення може взяти на себе всі рутинні завдання, а оператор матиме змогу реагувати тільки на події. Нижче наведені основні завдання системи відеоспостереження в складі комплексної системи безпеки.

1. Верифікація подій. Для систем сигналізації існує проблема "хибних" спрацьовувань, викликаних перешкодами в системі і не пов'язаних з реальними тривожними подіями: пожежею або появою порушника. Реагування на хибні тривоги витрачає ресурси служби безпеки. Система відеоспостереження дозволяє оператору підтвердити або спростувати (верифікувати) причину спрацювання систем охоронної та пожежної сигналізації (ОПС). Для систем контролю управління доступуом (СКУД) відеоспостереження дозволяє значно підвищити ефективність контролю доступу: при зчитуванні картки доступу співробітника інтегрована система може надати оператору онлайн потік з відеокамери, прив'язаної до даної точки доступу, і вивести на екран фотографію співробітника, якому повинна належати пред'явлена картка доступу (так звана "фотоверифікація"). [2]

2. Сценарії управління. Інтегрована система безпеки передбачає використання сценаріїв управління, коли події з однієї системи спричиняють реакцію іншої. Система відеоспостереження може бути джерелом подій для запуску реакцій інших систем: наприклад, розпізнавання реєстраційного номера автомобіля з "білого" списку може запустити сценарій відкриття доступу з боку СКУД. З іншого боку, сама система

відеоспостереження може управлятися іншими системами: наприклад, подія від системи охоронної сигналізації периметра може запустити сценарій перемикання високошвидкісної PTZ-камери в задане положення і виведення зображення з цієї камери на монітор сигналізації оператора. [2]

3. Ситуаційна відеоаналітика як джерело подій. В останні роки відеоаналітика (алгоритмічний або нейромережевий аналіз відеоданих з камер відеоспостереження) стала однією зі звичних опцій відеокамер. Існує безліч функцій відеоаналітики різного ступеня складності:

- перетин лінії розмежування (Tripwire);
- контроль зони / вторгнення в зону (Intrusion);
- об'єкт покинутий / відсутній (Abandoned / Missing);
- розпізнавання осіб (Face Detection);
- автоматичне стеження;
- автоматичне стеження за допомогою високошвидкісної поворотної PTZ-камери;
- розпізнавання осіб;
- розпізнавання номерних знаків;
- виявлення гучних звуків (крик, постріл і т.д.);
- міжкамерне стеження (відстеження об'єкта від однієї відеокамери до іншої).[3]

Для підвищення ефективності системи безпеки системи відеоспостереження можуть бути інтегровані наступним чином.

1. Інтеграція датчиків. Інтеграція різних датчиків підвищує ефективність систем відеоспостереження і знижує відсоток помилкових спрацьовувань, так як дозволяє всебічно аналізувати ситуацію на об'єкті.

2. Інтеграція з аудіо. Аудіоаналітика, завжди або за тривогою, дає додаткову інформацію про ситуацію на об'єкті.

3. Інтеграція хімічних датчиків. Хімічні датчики можуть виявляти витоки газу, наркотиків, аерозольних фарб, забруднення навколишнього середовища та інші фактори. Такі датчики дають можливість запобігти аварійній ситуації на етапі, коли вона ще не стала критичною, і, відповідно, не відображається на відео.

4. Датчики підрахунку відвідувачів. Датчики підрахунку відвідувачів особливо популярні для торгових точок як ефективний інструмент бізнес-аналітики. Крім того, датчики проходу в приміщенні або на певній ділянці, дозволяють реалізовувати функції управління, прискорюючи або сповільнюючи рух ескалаторів, контролювати двері та інш. Однак камера спостереження з функцією відеоаналітики менш точна в цьому плані, оскільки може пропустити відвідувачів або ідентифікувати їх повторно. [1]

Встановлення відеокамер та сигналізації стає необхідністю для бізнесу. Це може запобігти нещасному випадку або пояснити його причину після того, як він стався.

Інтеграція обладнання для передачі тривожних сигналів в ІОД допомагає уніфікувати завдання і забезпечити швидке реагування.

Переваги інтегрованих систем безпеки відчутні на великих і середніх об'єктах. Застосування інтегрованих систем безпеки дає змогу під час організації системи захисту великих об'єктів досягати високої надійності роботи всього комплексу, реалізувати складні алгоритми взаємодії обладнання, максимально унеможливити вплив людського фактора й ефективно використовувати виділені ресурси. [1]

Список джерел:

1. Рижова В. А. Інтелектуальні системи відеоспостереження / В. А. Рижова, С. М. Яришев, В. В. Коротаєв., 2021

2. Магауенов Р.Г. Системи охоронної сигналізації: основи теорії і принципи побудови. Навчальний посібник для вузів. 2-вид. М.: Гаряча лінія – Телеком, 2004

3. AXIS Object Analytics [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://www.axis.com/products/axis-object-analytics.

УДК: 005.7:519.8

ВИЗНАЧЕННЯ ШЛЯХІВ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ МОДЕЛЮВАННЯ ПОТЕНЦІЙНОГО КОНФЛІКТУ З ВИКОРИСТАННЯМ ТЕОРІЇ ІГОР

Фукс Максимілліан Андрійович
студент V курсу факультету Інфокомунікацій
Харківський національний університет радіоелектроніки, Україна

Анотація. У статті висвітлюється можливість застосування математичного апарату теорії ігор, а саме пропозиція розгляду конфлікту між керівником відділу IT-безпеки та зловмисником за допомогою біматричних ігор як кращий варіант для визначення оптимальної стратегії захисту інформації.

Ключові слова: біматрична гра, зловмисник, система менеджменту інформаційної безпеки, стратегія, теорія ігор.

Прийняття системи менеджменту інформаційної безпеки (СМІБ) є стратегічним рішенням організації, на проектування та впровадження якої впливають як потреби, так і цілі, розмір, структура, вимоги для безпеки, наявні організаційні процеси у цій організації. СМІБ засновується на підході бізнес-ризику та направлена на створення, реалізацію, експлуатацію, моніторинг, аналіз, підтримку та підвищення ефективності інформаційної безпеки (ІБ). У межах СМІБ розглядають структуру системи, політики, дії щодо планування, обов'язки, практики, процедури, процеси та ресурси організації [1].

Загалом інформаційна безпека може трактуватися як стан захищеності інформаційної середи як від внутрішніх так і від зовнішніх загроз, які спроможні завдати шкоди інтересам особистості, компанії, держави, тощо. Таким чином, захист інформації направлений на забезпечення стану безпеки інформації, яка забезпечується за допомогою її захисту. Інформаційна безпека як механізм захисту забезпечує наступні елементи.

1) Конфіденційність – властивість інформації бути захищеною від несанкціонованого розкриття.

2) Цілісність – властивість інформації бути захищеною від несанкціонованого змінення. При цьому фізична цілісність забезпечує незмінність саме фізичного стану інформації, а логічна – правильність виконання процесів, повноту та її несуперечність.

3) Доступність – властивість інформації бути доступною за певний час авторизованому користувачеві.

Впроваджена СМІБ якраз і забезпечує збереження вищезазначених властивостей за допомогою розгортання процесу управління ризиками, а впроваджені механізми захисту інформації й направлені на підвищення та забезпечення необхідних рівнів моделі Confidentiality, Integrity and Availability (CIA).

СМІБ представляє певну схему, на основі якої є можливість обговорювати, планувати, визначати, відслідковувати проблеми безпеки компанії. Основою СМІБ може слугувати певний стандарт, який забезпечуватиме повноту та узгодженість. Звичайно, компанія сама може змінювати стандарт відповідно до власних потреб для створення найкращої відповідності СМІБ та можливих потреб з урахуванням специфіки бізнесу. Або взяти за основу декілька найпопулярніших і розробити власні внутрішні нормативні документи, політики, процедури, стандарти, інструкції.

Політика – документ, що містить визначені цілі, завдання та шляхи їх досягнення. Важливим є те, що під політикою інформаційної безпеки найчастіше мається на увазі

високорівневий документ, направлений на забезпечення якісного керування ІБ згідно з наявними вимогами бізнеса, клієнтів чи законодавчої бази. Задокументована політика у обов'язковому порядку затверджується керівництвом та доноситься усім співробітникам організації та можливим зовнішнім сторонам, якщо такі є. Окрім розроблених внутрішніх нормативних документів організації, СМІБ може включати в себе умови угод та договорів з третіми сторонами.

Існує велика кількість підходів, на основі яких компанія може розгорнути власну СМІБ, наприклад, стандарти International Organization for Standardization (ISO) та Federal Information Processing Standard (FISP), публікації The National Institute of Standards and Technology (NIST), серія стандартів 8500.x міністерства оборони США, Security Technical Implementation Guide (STIG), документи The European Union Agency for Cybersecurity (ENISA), нормативно-правові акти банку, тощо.

Яскравим прикладом може слугувати лист [2] департаменту інформатизації банкам України, у якому зазначалися питання та можливості забезпечення безпеки інформаційних ресурсів банківської системі України з додаванням вимог із захисту інформації, зумовлених конкретними потребами сфери банківської діяльності і правовими вимогами, які вже висунуто в нормативних документах Національного банку України (НБУ). Прикладом є Постанова №95 від 28.09.2017 Правління НБУ «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України», мета якої є підвищення рівня захисту інформаційних систем банків. Постанова НБУ №95 засновується на міжнародному стандарті ISO/IEC 27001:2013 та містить вимоги щодо інформаційної безпеки банку [3].

Іншим прикладом може слугувати методика IT-Grundschutz [4], що описує створення СМІБ і яка розроблена німецьким федеральним відомством з інформаційної безпеки BSI. Насправді стандарт ISO/IEC 27001:2013 містить дуже мало, а то й взагалі не має інструкції щодо застосування та впровадження зазначених у ньому вимог – усе описано доволі абстрактно. Можна зробити припущення, що саме через це німецька команда експертів створила методологію IT-Grundschutz, що містить близько 1500 ясно викладених інструкцій як створити систему керування ІБ. Вимоги зібрані у модулі, що застосовуються до процесів, обладнання, приміщень, додатків, тощо. Вони визначають як ведення необхідної документації, так і застосування засобів захисту інформації й інше.

Ціле сімейство ISO/IEC 27000 включає в себе міжнародні стандарти, що визначають вимоги до СМІБ, управління ризиками, метрикою, вимірами та керівництвом щодо її впровадження. Стандарт ISO/IEC 27003:2017 визначає методологію побудови СМІБ з урахуванням вимог, що зазначені у ISO/IEC 27001:2013. Розгортання СМІБ на основі зазначених у цьому стандарті вимог спирається на модель планування-дія-перевірка-покращення PDCA [5].

Процес визначення прийнятного ризику та вибір оптимальних стратегій для використання CISO – нелегка задача, адже навіть у вищезазначених методологіях відображена лише необхідність розгортання та впровадження засобів захисту інформації, але не представлені рекомендації щодо того, як саме провести оптимізацію вибору, тобто немає ясності яким чином потрібно виконувати зазначені у стандартах вимоги. Зазвичай, на цьому етапі впровадження СМІБ CISO чи навіть ціла команда відповідальних покладаються лише на власний досвід та намагаються якимось недетермінованим чином обрати необхідні засоби захисту. Більш того, працювати вони вимушені при доволі обмеженому фінансуванні, а тому необхідно поєднувати виділені фінансові можливості, потрібні методи захисту і принцип розумної достатності для отримання у результаті ефективної та якісної СМІБ.

Проблемі визначення ефективності проведених інвестицій у кібербезпеку загалом присвячено доволі багато літератури, публікацій та певних методів. Наприклад,

метод аналізу ієрархій Томаса Сааті, теорія корисності чи навіть математичний апарат теорії ігор.

Теорія ігор розглядає взаємовідносини між учасниками, які мають різні чи навіть протилежні мотиви. Використання теоретико-ігрового підходу для моделювання процесу боротьби за реалізацію власних інтересів між CISO та зловмисником є резонним, адже вони обидва є раціональними, розумними і некооперативними, та мають на меті максимізацію власних функцій виграшу шляхом застосування певних стратегії. Тактика кожного з гравців детермінується ходами іншого. Зокрема, коли зловмисник прагне провести атаку на актив, йому обов'язково необхідно проаналізувати можливі контрзаходи впроваджені до системи CISO, і навпаки, для обрання необхідного засобу захисту системи CISO необхідно розглянути можливі атаки на таку систему.

Найчастіше для моделювання використовують найпростішу гру – з нульовою сумою. У антагоністичній грі некооперативні гравці мають повністю протилежні виграші [6]. Але у цьому випадку, насправді, робиться припущення, що втрати організації дорівнюють виграшу зловмисника, що і є грубим спрощенням усієї гри. Для уникнення подальших проблем та некоректних результатів наявна можливість застосування дещо іншого типу ігор, а саме біматричних ігор.

Отже, гра між CISO та зловмисником може бути охарактеризована наступим чином:

- за кількістю учасників: 2 гравці;
- за кількістю стратегій: гра є кінцевою;
- за взаєминами між гравцями: безкоаліційна;
- за властивостями функцій виграшу: гра з ненульовою сумою.

Конкретизація завдання та аналіз характеристик розгортаємої математичної моделі допомагає сконцентруватися на неантагоністичних іграх двох учасників з кінцевим числом стратегій, а саме на біматричних іграх. Ігри такого роду повністю протилежні іграм з нульовою сумою, де один з гравців перемагає за рахунок програшу іншого, а тому розгляд поставленого завдання саме у розрізі біматричних ігор надає можливість приділити увагу не тільки виграшу CISO, а й зловмисника, тим самим описавши функції виграшу для кожної конфліктуючої сторони окремими матрицями.

Можливість використання біматричних ігор у моделюванні взаємодії CISO та зловмисника не суперечить наявним публікаціям та методологіям і може використовуватися як альтернатива, що потребує більше вхідних даних, адже вона розглядає як інтереси CISO, так і зловмисника, а тим самим спроможна представити більш точний результат на основі більшої інформації з обох сторін.

Список джерел:

1. Дорофеев А. Менеджмент информационной безопасности: основные концепции / А. Дорофеев, А. Марков. // Вопросы кибербезопасности. – 2014. – С. 67–73.
2. Національний банк України. Лист 03.03.2011 №24-112/365 Банкам України [Електронний ресурс] / Національний банк України // Департамент інформатизації. – 2011. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/ v0365500-11#Text.
3. Постанова № 95 Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України [Електронний ресурс] // Правління Національного банку України. – 2017. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/v0095500-17#Text.
4. BSI-Standard 200-2. // IT-Grundschutz Methodology. – 2017. – №1. – С. 131.
5. Міжнародний стандарт ISO/IEC 27001. – 2013. – №2. – С. 1–34.
6. Колобашкина Л. В. Основы теории игр / Л. В. Колобашкина., 2011. – 199 с.

ОБГРУНТУВАННЯ УПРАВЛІНСЬКИХ РІШЕНЬ ПРИ РОЗРОБЦІ ТА ВПРОВАДЖЕННІ СИСТЕМ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МЕТОДОМ АНАЛІЗУ ІЄРАРХІЙ

Фастовець В.І., доцент,
Харківський національний автомобільно-дорожній університет
магістр факультету Інфокомунікацій
Харківський національний університет радіоелектроніки, Україна

Анотація: *розглянуто метод аналізу ієрархій, який використовується при обґрунтуванні управлінських рішень при розробці та впровадженні систем менеджменту інформаційної безпеки та наведено приклад.*

Ключові слова: *метод аналізу ієрархій, управлінські рішення, системи менеджменту інформаційної безпеки.*

Розвиток комп'ютерних технологій і їх використання в багатьох сферах економіки є на сьогодні одним з головних факторів її ефективності. Проте прогрес в інформаційно-технічній сфері створив і потенційні загрози у вигляді розроблення нових та удосконалення вже відомих методів наукового шпигунства, котрі дозволяють швидко знаходити в комп'ютері необхідні відомості.

Крім того, у зв'язку з бурхливим розвитком локальних і глобальних обчислювальних мереж удосконалюються і методи розвідки (комерційного шпигунства), спрямовані на перехоплення інформації, що обробляється, передається, зберігається у локальних мережах. Відповідно, швидко удосконалюються і методи протидії розвідці.

Необхідно зазначити, що увійти у локальну мережу будь-якої організації можна лише при некваліфікованому налагодженні всіх елементів локальної мережі (кожного окремого комп'ютера) адміністратором системи. Не випадково останнім часом бурхливо розвиваються методи перехоплення інформації за допомогою каналів побічного електромагнітного випромінення і наведень (ПЕМВН) елементів комп'ютерних мереж.

Забезпечення інформаційної безпеки в корпоративних, міжкорпоративних, локальних обчислювальних та інших автоматизованих системах зараз набуває особливої актуальності. За даними статистики, основним джерелом загрози безпеці корпоративної мережі, як і раніше, залишаються саме легальні користувачі. Відтік або втрата конфіденційної інформації та вихід з ладу обладнання може статися внаслідок: незумисних помилок користувача; умисних шкідливих дій користувача; таємного введення в систему програм-закладок з вірусами «троянський кінь», «черв'як» тощо.

Значна кількість важливої інформації зберігається не лише на серверах, а й на робочих станціях (комп'ютерах) користувача. Ці дані можуть бути легко втрачені або розголошені, якщо не вживати відповідних заходів. За допомогою списків управління доступом (ACL) можна обмежити доступ до комп'ютера як для окремого, так і для групи користувачів. Наприклад, один з користувачів зможе читати зміст файлу, інший – вносити до нього зміни, а всі інші взагалі позбавлені доступу до файлу. Це необхідно, коли на одному комп'ютері працює кілька користувачів або в мережі підприємства не встановлено обмежень на їх реєстрацію і будь-який користувач, який має фізичний доступ до комп'ютера, може зареєструватися на ньому.

Найбезпечнішою з усіх можливих загроз при підключені до глобальної мережі Internet є злам мережі з хуліганських мотивів. В разі під'єднання комп'ютерних мереж державних установ, підприємств, науково-дослідних інститутів та організацій до глобальної мережі Інтернет слід очікувати, окрім хуліганських зламів мережі і

кваліфікованого проникнення до ресурсів корпоративної мережі. Протидіяти цьому дуже складно. Тому мережу Інтернет необхідно ізолювати від внутрішніх важливих ресурсів, де зосереджені конфіденційні дані, дані для обмеженого користування і доступу. В мережах, у яких не використовується інформація з обмеженим доступом, для ізоляції, як правило, досить використати фільтруючий маршрутизатор, що виконує роль брандмауера, тобто шлюзу, який обмежує доступ до інформаційних ресурсів внутрішньої мережі підприємства.

Достатній захист від проникнення з глобальної мережі можна забезпечити за допомогою міжмережевих екранів. Проте найповніша безпека гарантується лише фізичною ізоляцією локальної мережі від мережі Інтернет.

Мета роботи: розглянути метод аналізу ієрархій, який використовується при обґрунтуванні управлінських рішень при розробці та впровадженні систем менеджменту інформаційної безпеки та навести приклад.

Метод аналізу ієрархій (MAI) — це структурований метод організації та аналізу складних рішень, заснований на математиці та психології [1,2]. Він був розроблений в 1970-х роках Томасом Л. Сааті, і з тих пір він широко вивчався та вдосконалювався. Він представляє точний підхід для кількісної оцінки ваги критеріїв прийняття рішень. Для оцінки відносної величини факторів за допомогою парних порівнянь використовується досвід окремих експертів.

Опишемо коротко метод. Нехай:

A1 ... An – множина з n елементів;

W1…Wn – співвідносяться наступним чином:

Таблиця 1 – Розрахунок відносної сили критеріїв

	A_1	…	A_n
A_1	1	…	W_1/W_n
…	…	1	A_n
A_n	W_n/W_1	…	1

Оцінка заповненої матриці порівнянь проводиться у разі формулам (табл. 2) для обчислення вектора пріоритетів.

Таблиця 2 – Оцінка пріоритетів

	A_1	…		A_n		
A_1	1	…		W_1/W_n	$X_1=(1*(W_1/W_2)*…*(W_1/W_n))^{1/n}$	ВАГА(A_1) $=X_1/СУМА(X_i)$
…	…	1		A_n	…	…
A_n	W_n/W_1	…		1	$X_n=((W_n/W_1) *…*(W_n/W_{n-1}) *1)^{1/n}$	ВАГА(A_n)= $=X_n/СУМА(X_i)$
					СУМА(X_i)	

Наступний крок: обчислення індексу узгодженості (ІУ), що дає інформацію про рівень порушення узгодженості.

$$ІУ= (L_{max} – 1) / (n – 1)$$

де

$$L_{max} = \sum_{i=1}^{n} S_i \cdot W_i ,$$

S_i – сума пріоритетів у стовпці,

W_i – вага, записана у рядку.

Далі потрібно розділити отриманий індекс на параметр із спеціальної матриці випадкових індексів (ВІ) (табл. 3), яка була отримана експериментально.

Таблиця 3 – Випадкові індекси

Розмір матриці	1	2	3	4	5	6	7	8	9	10
Випадкова узгодженість	0	0	0,58	0,9	1,12	1,24	1,32	1,41	1,45	1,49

Обчислюється відношення узгодженості (ВУ), як відношення ІУ та випадкового індексу ВІ для матриці:

$$ВУ = ІУ/ВІ.$$

Величина ВУ має бути близько 10% або менше, щоб бути прийнятною. У деяких випадках ВУ допускається до 20%, але не більше, інакше необхідна додаткова перевірка суджень, здійснених раніше.

Вирішимо задачу вибору копіювального апарату з використанням методу аналізу ієрархій.

Нехай на ринку є копіювальні апарати, закодуємо їх номерами N1, N2, N3, N4.

Задамо критерії оцінки та систему кодування:

А1 – Вартість апарату;

А2 – Підтримка копіювання документів формату А3 (так/ні – 0/1);

А3 – Швидкість копіювання (низька/середня/висока – 0/1/2);

А4 – Розмір (малий/середній/великий – 0/1/2);

Придумаємо чисельну систему порівняння якісних критеріїв.

Таблиця 4 – Параметри вибраних копіювальних апаратів та оцінка різниці для порівняння

Параметри Апарати	A1	A2	A3	A4
N1	200	0	0	0
N2	200	0	1	0
N3	500	1	1	1
N4	800	1	2	2
	Різниця-параметр	Різниця - параметр	Різниця - параметр	Різниця - параметр
	0 – 1 100 – 3 400 – 5 700 – 7 900 – 9	0 – 1 1 – 3	0 – 1 1 – 3 2 – 5	0 – 1 1 – 3 2 – 5

Таблиця 5 – Оціка приоритетів

	A1	A2	A3	A4	Добуток	Корінь	Вага	Si*Wi
A1	1	6	7	4	168	3,60	0,58	0,91
A2	1/6	1	4	3	2	1,19	0,19	1,45
A3	1/7	1/4	1	1/3	0,01	0,33	0,05	0,80
A4	1/4	1/3	3	1	0,25	0,71	0,11	0,95
Суми	1,56	7,58	15,00	8,33		5,83		4,11

ИС=0,04
ОС=0,04

A1							
	N1	N2	N3	N4	Произведение	Корень	Значение
N1	1	1	4	6	24	2,21	0,36
N2	1	1	4	6	24	2,21	0,36
N3	1/4	1/4	1	4	0,25	0,71	0,11
N4	1/6	1/6	1/4	1	0,01	0,29	0,05
Суммы	2,42	2,42	9,25	17,00		5,42	

Рисунок 1– Результат обчислень А1

A2							
	N1	N2	N3	N4	Произведение	Корень	Значение
N1	1	1	3	3	9	1,73	0,28
N2	1	1	3	3	9	1,73	0,28
N3	1/3	1/3	1	1	0,11	0,58	0,09
N4	1/3	1/3	1	1	0,11	0,58	0,09
Суммы	2,67	2,67	8,00	8,00		4,62	

Рисунок 2 – Результат обчислень А2

A3							
	N1	N2	N3	N4	Произведение	Корень	Значение
N1	1	3	3	5	45	2,59	0,42
N2	1/3	1	1	3	1	1,00	0,16
N3	1/3	1	1	3	1,00	1,00	0,16
N4	1/5	1/3	1/3	1	0,02	0,39	0,06
Суммы	1,87	5,33	5,33	12,00		4,98	

Рисунок 3 – Результат обчислень А3

A4							
	N1	N2	N3	N4	Произведение	Корень	Значение
N1	1	1	3	5	15	1,97	0,32
N2	1	1	3	5	15	1,97	0,32
N3	1/3	1/3	1	3	0,33	0,76	0,12
N4	1/5	1/5	1/3	1	0,01	0,34	0,05
Суммы	2,53	2,53	7,33	14,00		5,04	

Рисунок 4 – Результат обчислень А4

Наводимо зведені оцінки за критеріями. Для отримання результатів необхідно для кожного апарату підсумувати нормалізовані критерії, помножені на свої ваги.

	A1	A2	A3	A4	
	0,91	1,53	1,16	0,81	**результат**
N1	0,36	0,28	0,42	0,32	**1,49**
N2	0,36	0,28	0,16	0,32	**1,19**
N3	0,11	0,09	0,16	0,12	**0,53**
N4	0,05	0,09	0,06	0,05	**0,30**

Рисунок 5 – Зведені результати

У результаті отримуємо, що потрібно вибрати копіювальний апарат N1. Наступний за перевагою апарат N2.

У статті розглянутий метод аналізу ієрархій, який використовується при обґрунтуванні управлінських рішень при розробці та впровадженні систем менеджменту інформаційної безпеки та вирішено задачу вибору копіювального апарату.

Література

1. Волошин О.Ф, Мащенко С.О. Моделі та методи прийняття рішень: нвч. посібник для студ. вищ. навч. закл. – К.: Видавничополіграфічний центр «Київський університет», 2010. – 336 с.

2. Зайченко Ю.П. Дослідження операцій. Підручник. Сьоме видання, перероблене та доповнене. – К.: Видавничий Дім «Слово», 2006. – 816 с.

УДК 615.47

РОЗРОБКА КОНФОКАЛЬНОГО ЛАЗЕРНОГО СКАНУЮЧОГО МІКРОСКОПУ НА БАЗІ DVD ПРИВОДА

студент 3-го курсу **Лебединський О.Е.**
Науковий керівник – к.т.н., **Носова Я.В.**
Харківський національний університет радіоелектроніки, каф. БМІ,
м. Харків, Україна

Анотація. Дана робота присвячена опису принципів роботи лазерного скануючого мікроскопа та побудові його прототипу з використанням DVD приводів. Розглянуто структуру прототипу мікроскопа та програми для його роботи.

Ключові слова: КЛСМ, мікроскоп, скануючий, Arduino, DVD.

Сучасний процес долсідження біологічних зразків містить у собі декілька загальних кроків, одним з яких є отримання збільшеного, переважно цифрового зображення. Для отримання якісного результату, необхідна відповідна апаратура, що буде відповідати вимогам певного дослідження. Зокрема, таким приладом може бути конфокальний лазерний скануючий мікроскоп (КЛСМ). Але вплив катодних променів високої енергії на зразки з металевим покриттям у вакуумній камері громіздкого та дорогого приладу – не єдиний спосіб отримати необхідні зображення [1-2].

КЛСМ – це спеціальний світловий мікроскоп, який використовує сфокусований лазерний промінь для сканування зразка з подальшим реконструюванням тривимірних структур з наборів зображень, отриманих на різних глибинах. Сканування лазера вздовж зразка здійснюється шляхом руху лазера в напрямку *x* і *y*. Зображення складається шляхом комбінування виміряних світлових точок. КЛСМ часто використовуються в поєднанні з флуоресцентними маркерами для вивчення властивостей біологічних зразків [3].

Роздільна здатність такого мікроскопу визначається кількістю можливих вимірювань, зроблених у напрямку *x*, і кількістю ліній у напрямку *y*. Максимальна роздільна здатність обмежена числовою апертурою лінзи об'єктива системи та довжиною хвилі лазера, як і у звичайних оптичних мікроскопах. Оскільки роздільна здатність DVD – рідера повинна бути достатньо висока для читання інформації на диску (рис 1) [4], то можна зробити висновок, що головка із блоком лінз і її сервоприводи можуть бути використані для побудови КЛСМ.

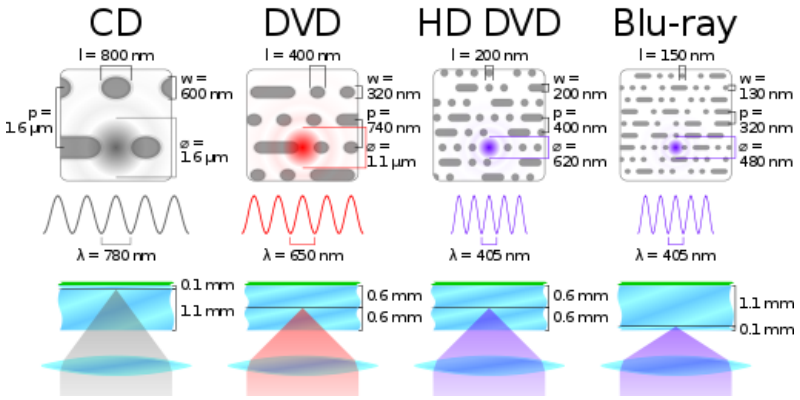


Рисунок 1 – Роздільна здатність різних типів головок диск – рідерів

Прототип установки використовує дві голівки. Одна випромінює лазер і сканує в напрямку *x*. Друга голівка захоплювача несе зразок і рухається в напрямку *y*. Сигнал

фіксується простим фотодіодом. Сервоприводами, що рухають голівки, а також струмом, що подається на лазер керує Arduino Micro з електронним приводом на печатній платі (рис. 2), а зображення відтворюються в програмі Processing [5-6]. Processing надсилає налаштування на мікроскоп, а у відповідь отримує данні для зчитування зображення рядок за рядком. Можна встановити такі параметри: тип лазера (інфрачервоний, ультрафіолетовий, червоний і тд.); потужність лазера; стартова позиція; роздільна здатність сканування; колірна схема і яскравість [3].

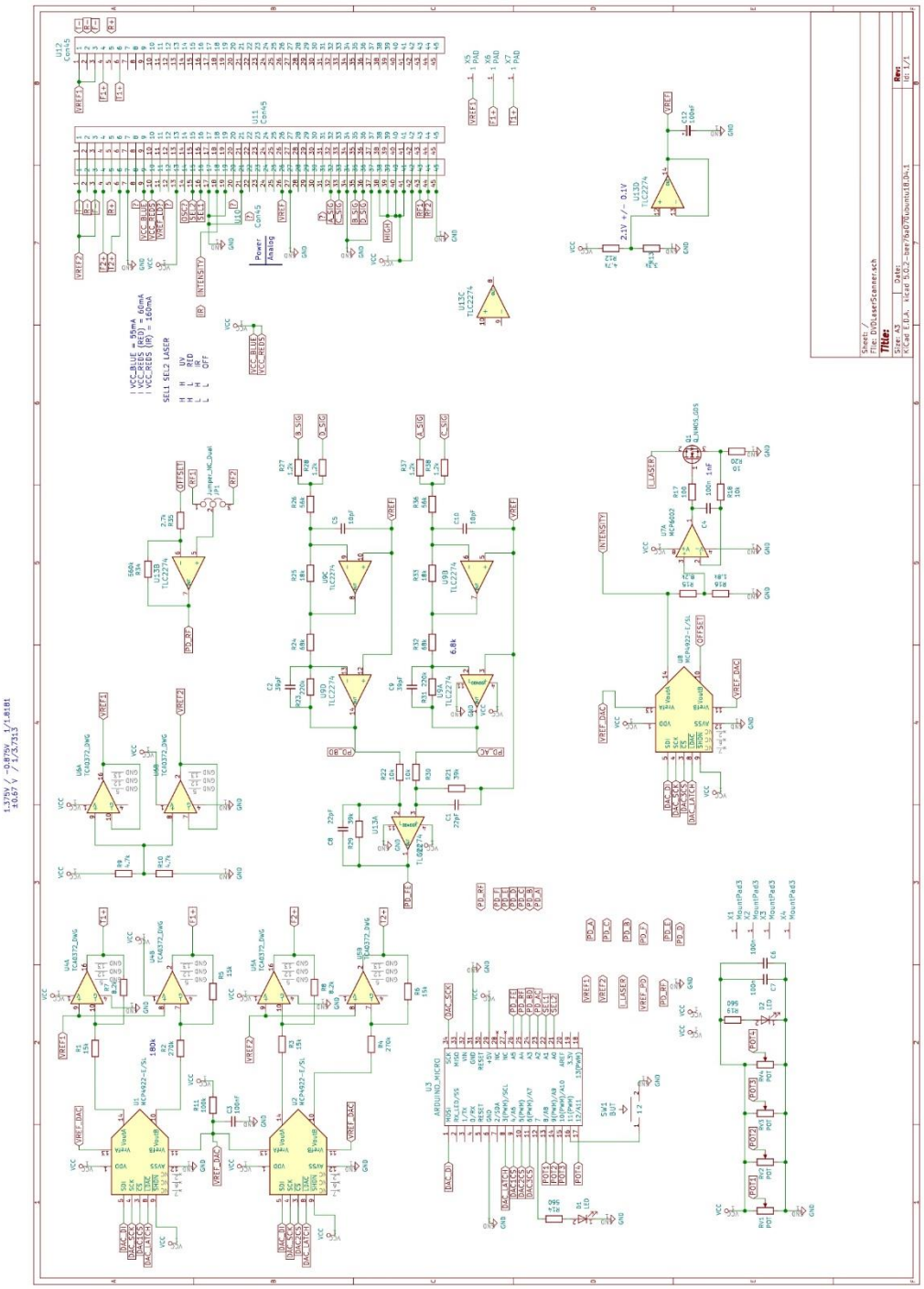


Рисунок 2 – Схема КЛСМ

Використовуючи прототип зібраний за схемою і запрограмований відповідним програмним забезпеченням можна отримати монохромні зображення з досить високою роздільною здатністю для показу, наприклад, клітин дріжжів (рис. 3) [3].

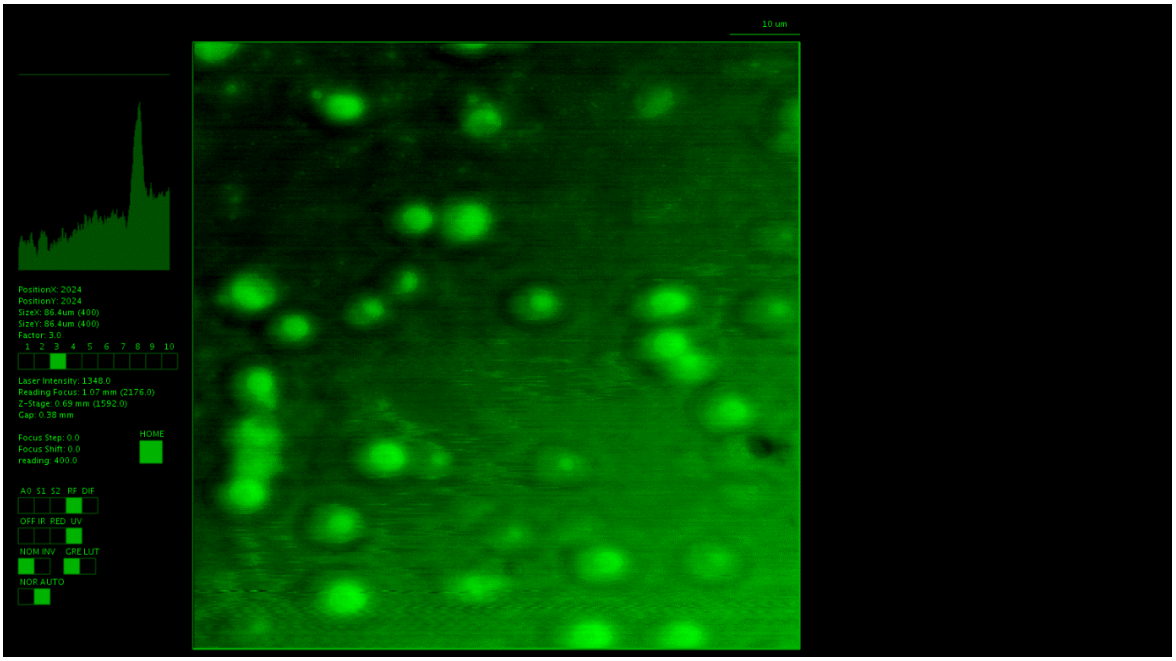


Рисунок 3 – Зображення клітин дріжжів за допомогою КЛСМ

Обґрунтовано корисність розробки КЛСМ за використанням DVD приводів, що дозволить науковцям чи студентам з невеликим бюджетом побудувати мікроскоп, здатний отримувати цифрові зображення з досить високою роздільною здатністю. Розроблено структурну схему прототипу КЛСМ на основі DVD приводів. Перспективою роботи є подальше удосконалення коду програми керування приводом та розробка відповідної вакуумної камери для покращення умов отримання зображення.

Список використаних джерел:

1. Аврунин О. Г. Опыт разработки биомедицинской системы цифровой микроскопии / О. Г. Аврунин // Прикладная радиоэлектроника. – 2009. – Т.8. – № 1. – С. 46-52.

2. Опыт разработки автоматизированных систем для проведения гистологических исследований / О. Г.Аврунин, С. Ю. Масловский, Т. В. Носова, В. В. Семенец // Сб. науч. трудов. конференции «Актуальные проблемы биомединженерии». – 2008. – Т. 4. – С. 91–93.

3. Gaudenz, U. (2017, 9 вересня). DVD laser scanner microscope. gaudi.ch - open culutre technology. http://www.gaudi.ch/GaudiLabs/?page_id=652

4. Cmglee. (2022, 6 червня). Comparison CD DVD HDDVD bd.svg - wikimedia commons. Wikimedia Commons. https://commons.wikimedia.org/wiki/File:Comparison_CD_DVD_HDDVD_BD.svg

5. Cook, J. (2021, 3 лютого). DIY laser scanning microscope. Hackster.io. https://www.hackster.io/news/diy-laser-scanning-microscope-ccf2294a0c49.

6. Gaudi Labs. (2020, 17 жовтня). OpenLaserScanningMicroscope. GitHub. https://github.com/GaudiLabs/OpenLaserScanningMicroscope/tree/master/PCB/DVDLaserScannerII

УДК 004.8

РОЗРОБКА ІНТЕЛЕКТУАЛЬНОЇ ІНФОРМАЦІЙНО-УПРАВЛЯЮЧОЇ СИСТЕМИ ДЛЯ БЕЗПІЛОТНОГО ТРАНСПОРТНОГО ЗАСОБУ З БЛОКОМ ВІРТУАЛЬНОЇ РЕАЛЬНОСТІ

Кулакова Людмила Євгеніївна
асистент кафедри комп'ютерних технологій і мехатроніки
Харківський національний автомобільно-дорожній університет, Україна
Іващенко Микита Олександрович
студент V курсу Механічного факультету
Харківський національний автомобільно-дорожній університет, Україна
Гулага Яна Сергіївна
студентка VI курсу механічного факультету
Харківський національний автомобільно-дорожній університет, Україна
Ідріссі Семлалі Яссін
студент VI курсу механічного факультету
Харківський національний автомобільно-дорожній університет, Україна

Анотація. У статі наведено огляд концепції інтелектуальної інформаційно-управляючої системи для безпілотного транспортного засобу з блоком віртуальної реальності. Наведено приклад використання технології віртуальної реальності у автомобілях.

Ключові слова: інтелектуальна система, інформаційно-управляюча система, безпілотний транспортний засіб, віртуальна реальність.

Інформаційно-управляючі системи набувають все більшої популярності. Їх широке використання у технічних системах обумовлено тим, що вони дозволяють підвищити енергоефективність технічної системи, а саме точність, швидкодію і т.п. Розглянемо використання інформаційно-управляючих систем для безпілотних транспортних засобів. Інформаційно-управляючі системи для безпілотних транспортних засобів побудовані за класичною схемою. Це по-перше, частина, що збирає інформацію (наприклад, лідар, радар, відеокамера і т.д.). По-друге, частина, що обробляє інформацію і видає управляючі дії на виконавчі органи (зазвичай це блок управління). По-третє, частина, що виконує управляючі дії – виконавчі органи (енергетична установка, гальма і т.п.). Для того, щоб ще підвищити енергоефективність технічної системи зараз широко використовують системи зі штучним інтелектом, які насамперед за рахунок навчання досягають більш високих показників енергоефективності системи ніж звичайні системи. Зазвичай використовують для навчання методи еволюційного моделювання, які засновані на принципах біологічної еволюції. Еволюційні алгоритми – це методи, які розв'язують проблеми за допомогою ітерацій. Вони вимагають впровадження передових обчислювальних технологій. Під час створення еволюційного алгоритму існує кілька проблем, таких як попередня обробка даних і визначення швидкості конвергенції. Розгляд цих проблем допомагає створити ефективний еволюційний алгоритм, який дає результати, що відповідають очікуванням [1-6].

В останні роки дуже популярна технологія глибокого навчання. Глибоке навчання можна використовувати для досягнення оптимальних результатів у багатьох сферах, включаючи комп'ютерне зір, обробку природної мови та робототехніку. Існує багато різних типів алгоритмів глибокого навчання, таких як згорткові нейронні мережі, рекурентні нейронні мережі та автокодери. Нові технології та структури постійно розробляються в області глибокого навчання [4].

Багато автовиробників і технологічних компаній активно розробляють безпілотні автомобілі. Це може призвести до того, що в найближчі кілька років або десятиліть моделі повсякденної мобільності суттєво зміняться, оскільки в безпілотних автомобілях все знаходиться в салоні, люди будуть пасажирами, а водії будуть мати вільний час.

Holoride – стартап, який працює з Audi та Porsche, оголосив про початок випуску своїх гарнітур віртуальної реальності у Німеччині. Трохи згодом процес поширеться на США, Канаду та Азію, включаючи Китай (рис. 1,2) [7,8].

Рис. 1. Гарнітури віртуальної реальності для моделей Audi A4, A5, A6, A7, A8, Q5, Q7, Q8, e-tron, e-tron Sportback та e-tron GT

У комплект входить гарнітура HTC Vive Flow, яка окремо продається на ринку. Якщо власник вже має Vive Flow, то за 50 євро можна докупити спеціальний контролер. Однак це не всі витрати, пов'язані з наявністю віртуальної реальності в Audi [7].

Holoride – це послуга з передплати, які стають все більш поширеними в сучасному світі, незалежно від того, подобається нам це чи ні. Комплект поставляється безкоштовно на 12 місяців, але після цього коштує 20 євро на місяць (або 180 євро на рік). За ці гроші ви отримуєте дві оригінальні гри для пристрою, які можуть використовувати власне програмне забезпечення замість платформи HTC, встановленої за замовчуванням [7].

Особливість платформи Holoride – миттєва синхронізація картинки у VR-окулярах з рухами автомобіля. Дані з бортових систем обробляються реальному часі, що дає різним органам почуттів посилати у мозок конфліктуючі сигнали. Так, при повороті машини бічні перевантаження будуть точно відповідати тому, що пасажири бачать в окулярах віртуальної реальності – у Holoride це називають Elastic Content, тобто контентом, який реагує і на дії людини, і на рухи автомобіля [9].

Рис. 2. Гарнітура віртуальної реальності Holoride

Список джерел:

1. Greengard S. Virtual Reality. Cambridge: MIT Press Essential, 2019. – 240 p.

2. Goyal D., Balamurugan S., Senthilnathan K., Annapoorani I., Israr M. Cyber-Physical Systems and Industry 4.0. Practical Applications and Security Management. CRC Press by Apple Academic Press, 2022. – 290 p.

3. Bodyanskiy Y., Zaychenko Y., Boiko O., Hamidov G., Zelikman A. Structure Optimization and Investigations of the Hybrid GMDH-Neo-fuzzy Neural Networks in Forecasting Problems. System Analysis & Intelligent Computing, Springer, 2022, Vol.1022. – PP. 209-228.

4. Müller A. Introduction to Machine Learning with Python / A. Müller, S. Guido / O'Reilly Media, 2017. – 392 p.

5. Uspensky B., Avramov K., Nikonov O. Nonlinear modes of piecewise linear systems forced vibrations close to superharmonic resonances. Proceedings of the Institution of Mechanical Engineers, Part C: Journal of Mechanical Engineering Science, 2019, Vol.233, Issue 23-24. – PP. 7489-7497.

6. В.П. Волков и др., Интеллектуальные и телематические технологии на транспорте. Шымкент: Изд-во ЮКГУ им. М. Ауэзова, 2016. – 504 с.

7. Віртуальна реальність в автомобілях Audi – Режим доступу: https://avtosota.com/21105-virtualna-realnist-v-avtomobilyah-audi-koshtuvatyme-blyzko-700-yevro.html

8. Would You Use VR in a Car? Audi's Spin-Off Holoride Wants You To – Режим доступу: https://www.gizmodo.com.au/2022/11/audi-holoride-car-vr/

9. Віртуальна реальність в автомобілях Audi – Режим доступу: https://theroad.in.ua/v-avtomobiliakh-audi-z-iavylys-vr-ihry/

Матеріали

Всеукраїнської науково-практичної
Internet-конференції
«МОДЕЛЮВАННЯ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В НАУЦІ, ТЕХНІЦІ, КІБЕРБЕЗПЕЦІ ТА ОСВІТІ»

15-16 листопада 2022 року
м. Харків, Україна

Відповідальний за випуск *В.І. Фастовець*

В авторській редакції