УДК 681.3

В.О. ЯЩЕНКО*

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ В УМОВАХ ЗРОСТАЮЧОГО МІЖНАРОДНОГО І ДЕРЖАВНОГО ТЕРОРИЗМУ

*Інститут проблем математичних машин і систем НАН України, м. Київ, Україна

Анотація. *У роботі представлений короткий огляд інформаційних технологій і систем забезпечення безпеки життєдіяльності в умовах зростаючого міжнародного і державного тероризму. Розглянуто деякі питання безпеки життєдіяльності як науки про захист людини від негативних впливів. Захист населення від терористичних дій як одна з основних задач, що включає засоби запобігання спробам, навчання, профілактичний огляд, охорону, знешкодження, системи контролю і розвідки для виявлення намірів терористів, штучний інтелект. На штучний інтелект покладаються особливі надії в боротьбі з терористами і терористичними організаціями. Такі системи вимагають обробки великих масивів інформації. Вивченню великих обсягів даних перешкоджає людський фактор, так як для обробки інформації використовуються фахівці. У зв'язку з цим особливу затребуваність набувають технології, пов'язані з автоматичною інтелектуальною обробкою великих масивів. Для забезпечення безпеки життєдіяльності населення країни необхідно на основі існуючих комп'ютерних систем і принципово нових систем, що базуються на технології штучного інтелекту, створювати бази даних і знань, розподілені по всій країні і об'єднані в одну потужну інтелектуальну базу інформаційного забезпечення безпеки держави і її населення. Така інтелектуальна база інформаційного забезпечення безпеки держави і її населення повинна володіти сильним штучним інтелектом, надшвидкодіючим. Основою, двигуном такої бази, інтелектуальним оброблювачем інформації може виступати система, створена на основі проекту «Думаючий комп'ютер або електронний мозок для роботів та інтелектуальних систем». У роботі коротко розглянуті цілі і завдання розробки проекту, технологічна основа проекту і її переваги.*

Ключові слова: *інформаційні технології, безпека життєдіяльності, тероризм, штучний інтелект.*

Аннотация. *В работе представлен краткий обзор информационных технологий и систем обеспечения безопасности жизнедеятельности в условиях возрастающего международного и государственного терроризма. Рассмотрены некоторые вопросы безопасности жизнедеятельности как науки о защите человека от негативных воздействий. Защита населения от террористических воздействий как одна из основных задач, которая включает меры предосторожности, обучение, профилактический осмотр, охрану, обезвреживание, системы контроля и разведки для выявления намерений террористов, искусственный интеллект. На искусственный интеллект возлагаются особые надежды в борьбе с террористами и террористическими организациями. Такие системы требуют обработки больших массивов информации. Изучению больших объемов данных препятствует человеческий фактор, так как для обработки информации используются специалисты. В связи с этим особую востребованность приобретают технологии, связанные с автоматической интеллектуальной обработкой больших массивов. Для обеспечения безопасности жизнедеятельности населения страны необходимо на основе существующих компьютерных систем и принципиально новых систем, базирующихся на технологии искусственного интеллекта, создавать базы данных и знаний, распределенные по всей стране и объединенные в одну мощную интеллектуальную базу информационного обеспечения безопасности государства и его населения. Такая интеллектуальная база информационного обеспечения безопасности государства и его населения должна обладать сильным искусственным интеллектом, сверхбыстродействием. Основой, двигателем такой базы, интеллектуальным обработчиком информации может выступать система, созданная на основе проекта «Думающий компьютер или электронный мозг для роботов и интеллекту-*

ISSN 1028-9763. Математичні машини і системи, 2019, № 2

альных систем». В работе кратко рассмотрены цели и задачи разработки проекта, технологическая основа проекта и ее преимущества.
Ключевые слова: *информационные технологии, безопасность жизнедеятельности, терроризм, искусственный интеллект.*

Abstract. *The paper presents a brief overview of information technologies and life safety systems in the context of increasing international and state terrorism. Considered: some issues of life safety – as a science about protecting a person from negative impacts; Protection of the population from terrorist influences as one of the main tasks which includes precautionary measures, training, preventive inspection, protection, neutralization; Control and intelligence systems to identify the intentions of terrorists; Artificial Intelligence. Special hopes are placed on artificial intelligence in the anti-terrorism effort and terrorist organizations. Such systems require processing of large amounts of information. The study of large amounts of data is hampered by the human factor, since experts use information processing. In this regard, technologies related to the automatic intelligent processing of large arrays are becoming particularly relevant. To ensure the safety of life of the population, it is necessary on the basis of existing computer systems and fundamentally new systems based on artificial intelligence technology to create databases and knowledge distributed throughout the country and combined into one powerful intellectual base of information security of the state and its people. Such an intellectual base of information security of the state and its population should have a strong artificial intelligence, super-fast action. The basis, the engine of such a base, an intellectual information processor can be a system created on the basis of the project «Thinking computer or electronic brain for robots and intelligent systems». The paper briefly discusses the goals and objectives of the project, the technological basis of the project and its benefits.*
Keywords: *information technology, life safety, terrorism, artificial intelligence.*

1. Вступ

Двадцять перше століття – століття інформаційних технологій. У сучасному світі інформаційні технології стали частиною життя кожної людини. Якщо на зорі комп'ютеризації комп'ютери використовувалися тільки для обчислення математичних розрахунків, то вже сьогодні вони використовуються повсюди.

Розвиток ЕОМ налічує 5 поколінь: 1-е покоління (початок 50-х рр.), елементна база – електронні лампи. ЕОМ відрізнялися малою швидкодією, низькою надійністю, великим споживанням енергії, великими габаритами; 2-е покоління (кінець 50-х рр.), елементна база – напівпровідникові елементи. Всі технічні характеристики, в порівнянні з попереднім поколінням, значно покращилися; 3-е покоління (початок 60-х рр.), елементна база – інтегральні схеми. Збільшення продуктивності, підвищення їх надійності, зниження габаритів ЕОМ; 4-е покоління (з середини 70-х рр.), елементна база – мікропроцесори, великі інтегральні схеми. Покращилися технічні характеристики. Масовий випуск персональних комп'ютерів. Напрями розвитку: потужні багатопроцесорні обчислювальні системи з високою продуктивністю, створення дешевих мікро-ЕОМ; 5-е покоління (з середини 80-х рр.). Почалася розробка інтелектуальних комп'ютерів, яка триває досі. В даний час активно розробляються системи штучного інтелекту, робототехніка, відбулося впровадження інтернету в усі сфери життя людини, повсюдне застосування комп'ютерних інформаційних технологій.

Сучасний етап світового розвитку характеризується тим, що власне інформація та засоби інформатизації безпосередньо впливають на економічний, соціальний і духовний розвиток як окремих держав, так і світової спільноти в цілому. Це свідчить про те, що в сучасних умовах інформація і управління нею стають підставою і головним інструментом досягнення цілей у новому світоустрою. В Окінавській хартії глобального інформаційного суспільства продекларовано, що інформаційно-телекомунікаційні технології стали одними з найбільш важливих факторів, що впливають на формування суспільства XXI століття.

Поряд з очевидними благами світова інформаційно-технологічна революція створила принципово нові потенційні загрози життєдіяльності як окремих суспільств, держав і

їхніх громадян, так і світової спільноти в цілому. Найбільшою мірою це стосується тероризму, мутація якого, на думку фахівців, найбільшою мірою відбувається саме в інформаційній сфері. Швидкий розвиток нових технологій істотно розширив можливості терористичних організацій з маніпулювання свідомістю населення при підготовці і проведенні терористичних акцій.

Спостережуване останнім часом посилення впливу інформаційних технологій практично на всі сфери життєдіяльності людства ставить завдання інформаційної протидії в розряд основних завдань забезпечення безпеки життєдіяльності та, зокрема, боротьби з тероризмом.

Мета статті – зробити огляд інформаційних технологій і систем забезпечення безпеки життєдіяльності в умовах зростаючого міжнародного і державного тероризму.

2. Безпека життєдіяльності

Безпека життєдіяльності – наука про захист людини в техносфері від негативних впливів антропогенного і природного походження та досягнення комфортних умов життєдіяльності.

Ця наука вирішує такий ряд завдань:

• ідентифікація небезпек – процес виявлення небезпек і встановлення їх характеристик;

• захист від небезпек на основі зіставлення витрат на забезпечення безпеки і вигод від реалізації цих заходів;

• ліквідація можливого, залишкового, наддопустимого ризику.

Основна мета безпеки життєдіяльності як науки – захист людини в техносфері від негативних небезпек антропогенного і природного походження. Визначати найбільш ймовірні зони дії цих небезпек, попереджати і ліквідувати їх. Техногенні небезпеки прогнозовані і у людства досить засобів і способів захисту від них. Однак використання інформаційних технологій нового покоління дозволяє практично повністю усунути вплив шкідливих техногенних факторів. Антропогенні небезпеки обумовлені недостатньою увагою людини до проблем безпеки і схильністю людини до ризику. Вплив антропогенних небезпек може бути зведено до мінімуму за рахунок використання інформаційних процесів у навчанні населення та персоналу небезпечних виробництв основам безпеки життєдіяльності [1].

Безпека життєдіяльності розглядає:

• безпеку в побутовому середовищі – це всю сума факторів, що впливають на людину в побуті. Реакцію організму на побутові чинники вивчають такі розділи науки, як комунальна гігієна, гігієна харчування, гігієна дітей та підлітків;

• безпеку в виробничому середовищі – це сукупність факторів, що впливають на людину у процесі трудової діяльності;

• безпеку у природному середовищі – це одна з галузей екології. Екологія вивчає закономірності взаємодії організмів із навколишнім середовищем [2].

Останнім часом значну загрозу життєдіяльності представляє міжнародний і внутрішньодержавний тероризм. Відповідно, тут необхідно додати безпеку життєдіяльності при тероризмі.

У світовій практиці цей вид загрози безпеки життєдіяльності розглядається як найнебезпечніший злочин. Тероризм поділяють на політичний, націоналістичний, релігійний, корисливий і безадресний.

Політичний тероризм має на меті завоювання політичної влади у країні. Відомо два типи такого тероризму. Лівий тероризм, що виникає в результаті соціального конфлікту, коли різко погіршується економічне становище держави та населення. Правий тероризм

виражає прагнення певної частини суспільства до встановлення реакційного тоталітарного режиму.

Націоналістичний тероризм організовується і проводиться етнічними угрупованнями, які прагнуть домогтися незалежності від держави або забезпечити перевагу своєї нації над іншими. Метою такого тероризму може бути також захист територіальної цілісності або збереження свого етносу.

Релігійний тероризм здійснюється зазвичай для того, щоб затвердити свою релігію як головну.

Корисливий тероризм має на меті неправомірне отримання фінансових коштів шляхом захоплення заручників. Іноді терористи разом з фінансовими висувають і політичні вимоги.

Безадресний (психологічний) тероризм зазвичай не мотивований. Психічна агресія при цьому є практично єдиною причиною вчинення терористичного акту і носить демонстративний характер [3].

2.1. Захист населення від терористичних дій

Захист населення від терористичних дій – одна з основних задач, яка включає засоби запобігання спробам, навчання, інформаційне забезпечення, роз'яснювальну роботу, профілактичний огляд, охорону, знешкодження.

У даний час вплив технологій інформаційно-психологічного впливу на суспільство в цілому, на маси людей і на окрему людину безперервно зростає. Йдеться про можливі деформації системи масового інформування та поширення дезінформації, що ведуть до потенційних порушень суспільної стабільності, про нанесення шкоди здоров'ю та життю громадян, внаслідок пропаганди або агітації, що збуджують соціальну, расову, національну чи релігійну ненависть і ворожнечу, про діяльність тоталітарних сект, що пропагують насильство і жорстокість. Окремі види інформаційно-психологічного впливу, звернені до населення, здатні серйозно порушити нормальне функціонування і життєдіяльність державних структур і громадських організацій [4].

Для боротьби з сучасним тероризмом необхідно створити широкий діапазон технологій і засобів. Одним із важливих напрямів протидії тероризму є розробка і вдосконалення інформаційних технологій.

3. Інформаційні технології

Інформаційні технології все більше проникають в усі сфери нашого життя. Вони грають важливу роль в управлінні атомними електростанціями, гідровузлами, енергомережами, системами контролю і забезпечення безпеки польотів, фінансовими інститутами всіх видів (біржа, страховий бізнес і т.п.).

Інфраструктура інформаційних технологій об'єднує всі інформаційні технології та ресурси, включає системи зв'язку, інформаційні центри, мережі та бази даних, супутникову (космічну), радіо- і телекомунікаційні системи. Кожна з них відіграє специфічну роль у житті держави і, відповідно, має різну вразливість щодо терористичних дій.

Таким чином, інформаційні технології складають сутність управління всіма критичними елементами інфраструктури сучасної цивілізації. Ці елементи інфраструктури уразливі з урахуванням можливості терористичних дій на комп'ютерні та телекомунікаційні мережі державного і навіть глобального масштабу.

Взаємовідносини інформаційних технологій і тероризму є подвійними. З одного боку, інформаційні технології істотно розширюють можливості для протиправних дій терористів. З іншого боку, сучасні інформаційні технології в раціональному поєднанні з традиційними методами є ефективним засобом боротьби з самим тероризмом [3].

Аналіз існуючих джерел показав, що на сьогодні в антитерористичній діяльності реально використовуються інформаційні технології, такі як дактилоскопія, обробка телефонних розмов (наприклад, розпізнавання ключових слів у потоці мовлення), розпізнавання (ідентифікація) підозрюваних осіб, створення та обробка інформації в базах даних і деякі інші [5].

Для боротьби з тероризмом використовуються технології збору даних, їх аналізу і технології прийняття рішень.

Технології збору даних в основному видаються технологіями реалізації сенсорів, сенсорних мереж і злиття інформації з безлічі різних джерел. До технологій аналізу даних і прийняття рішень (або аналітичних технологій) відносяться технології взаємодії осіб, що приймають рішення; вибору і обґрунтування рішень, аналізу текстів; розпізнавання і аналізу образів; прогнозуючого моделювання; обробка природної мови. За допомогою цих технологій можна створювати моделі зразків діяльності терористів, витягувати об'єкти і зв'язки між ними з великих масивів даних, співпрацювати, робити висновки і спільно використовувати інформацію, висувати гіпотези і перевіряти можливі дії терористів і стратегії протидії, вести пошук і використовувати велику кількість різних мультимедійних даних, багатомовної мови і тексту, здійснювати вибір можливих рішень і передбачуваних стратегій антитерористичних дій.

Технології вибору і обґрунтування рішень, а також підтримки взаємодії осіб, що приймають рішення, дозволяють вирішувати завдання на основі оптимізаційних методів прийняття рішення і методів, заснованих на знаннях і логічному висновку; обмінюватися інформацією і кооперуватися особам, які приймають рішення; маніпулювати елементами уявлення можливих або очікуваних дій терористів; перетворювати вхідні дані, що надійшли від різних джерел, в ситуативну інформацію і ситуативну інформацію в операційні знання.

Технології візуалізації забезпечують графічне представлення інформації, що аналізується в вигляді різних карт і зображень місцевості, діаграм, схем дій, а також допомагають аналітикам відображати і виділяти необхідну інформацію, дозволяють візуально представляти приховані неочевидні образи, зв'язок та аномалії при обробці величезних масивів даних.

Технології обробки відеоінформації забезпечують аналіз, виявлення, попередню обробку (на основі зменшення шуму, збільшення масштабу, поліпшення колірної гами і контрасту) і витяг необхідних відомостей з відеоінформації, дозволяючи відслідковувати підозрілі і небезпечні дії людей.

Технології підтримки семантичної узгодженості термінології дозволяють забезпечувати спільне узгоджене розуміння значення слів і фраз у конкретному контексті.

Технології інтелектуального пошуку здійснюють пошук серед безлічі географічно розподілених багатомовних різнотипних сховищ інформаційних ресурсів. Можуть використовувати різні критерії пошуку: по повному або частковому збігу окремих слів і фраз, за ступенем релевантності, за семантичною подобою. Забезпечують пошук будь-яких типів документів і даних, розміщених на web- і файл-серверах, в базах даних, системах управління документами та ін.

Технології природної мови забезпечують обробку мови і текстів на різних мовах.

Технології розпізнавання і аналізу образів призначені для виявлення підозрілих об'єктів, суб'єктів і процесів, включаючи людей, місця їх перебування, які події відбуваються з ними, а також для подальшого визначення, чи присутні інші взаємопов'язані об'єкти, суб'єкти і процеси з метою відокремити ситуації, що вимагають подальшого дослідження, від більшості інших ситуацій.

Технології прогнозують моделювання можливих подій, дозволяють висувати гіпотези про можливі майбутні дії, пропонувати і перевіряти способи протидії, а також прогно-

зувати можливі наслідки передбачуваних сценаріїв дій, базуючись на наявному досвіді експертів, минулих подій і прецедентах [3].

Технології маніпулювання даними та фільтрації інформації з безлічі різних джерел забезпечують збір, індексування, збереження, пошук, витяг, інтеграцію, аналіз, агрегування, відображення і поширення інформації. Вони надають можливість одночасного пошуку великої кількості джерел інформації, сортування і категоризації різних елементів інформації відповідно до релевантності запитів, реалізують представлення різних аспектів, релевантних запиту, поряд з можливістю візуалізації семантичних зв'язків, що відносяться до різних елементів інформації.

Технології моніторингу подій та оповіщення дозволяють відстежувати події і оповіщати посадових осіб операторів у реальному часі про виявлення підозрілих і критичних подій. При виявленні відповідної події виконується автоматичне оповіщення, яке може бути представлено як у вигляді простих дій, так і більш складних [3].

Біометричні технології пов'язані з вимірюванням, у тому числі з дистанційним, і обробкою інформації про фізіологічні та поведінкові характеристики людини для її ідентифікації або виявлення психофізіологічного стану і можливих намірів. У біометрії вивчаються можливості використання таких характеристик, як відбитки пальців, геометрія рук, відбитки долоні, будова кровоносних судин, термографія особи, форма обличчя у дво- і тривимірних вимірах, голос, хода, райдужна оболонка ока і т.д. [5].

4. Бази даних і знань на основі використання інформаційних технологій

Для вирішення завдань безпеки життєдіяльності слід передбачити створення бази даних, а також бази знань на основі використання інформаційних технологій.

Інформаційні технології в забезпеченні безпеки життєдіяльності представляють системно організовану послідовність операцій, які виконуються з інформацією, з використанням засобів і методів автоматизації.

Типовими операціями є елементарні дії з інформацією, починаючи від збору і реєстрації даних і закінчуючи процесом вироблення управлінського рішення.

Засоби і методи автоматизації включають техніку, програми, способи і підходи до організації інформаційних систем і технологій. Інформаційні технології, пов’язані з забезпеченням безпеки життєдіяльності, розрізняються складом, призначенням, ступенем автоматизації, надійністю, об’ємом вирішуваних завдань. Забезпечення безпечних умов життєдіяльності на сучасному етапі передбачає використання інформаційних технологій для управління джерелами і причинами виникнення небезпек, прогнозування та оцінки їх впливу у просторі і часі, захисту людини і навколишнього природного середовища від небезпек техногенного характеру. Управління безпекою техносфери на базі моніторингу небезпек та застосування найбільш ефективних заходів і засобів захисту дозволяє використовувати інформаційні системи і технології в усіх областях діяльності людини.

4.1. Інформаційна безпека

Інформаційна безпека – захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, які могли б зашкодити власникам або користувачам інформації і підтримуючої інфраструктури.

Здійснення системи захисту інформації в сучасних технологіях безпеки життєдіяльності породжує комплекс проблем. У комплексі система захисту інформації повинна вирішувати ряд завдань: забезпечення конфіденційності інформації на всіх рівнях управління безпекою; захист від спотворення; сегментування і забезпечення індивідуальності політики безпеки для різних сегментів системи; аутентифікацію користувачів та ін.

Відомості, що надходять з різних підрозділів, повинні зберігатися і оброблятися в єдиній системі просторової бази. Це дозволить контролювати ситуацію, організовувати взаємодію різних служб усіх держав, а також приймати рішення і проводити заходи щодо забезпечення безпеки.

5. Системи і види безпеки життєдіяльності

В основі будь-яких систем безпеки знаходиться особиста і колективна (громадська) безпека людини, яка входить в область локальної безпеки життєдіяльності і складає базовий сенс поняття «безпека життєдіяльності», що визначається як безпечна взаємодія людини з середовищем існування або ефективна захищеність прийнятних умов життя людини в середовищі проживання, його життєвих інтересів і самого існування від перевищення допустимого рівня впливу негативних факторів (небезпек, загроз) соціального, техногенного або природного характеру.

5.1. Системи особистої і колективної безпеки людини

Системи особистої і колективної (суспільної) безпеки людини включають в себе такі основні види безпеки життєдіяльності:

• безпеку здоров'я, під якою розуміють соматичну (тілесну) норму стану людини, самовідчуття нормального, звичного функціонування всіх систем власного організму з урахуванням природних вікових змін;

• психологічну безпеку, яка передбачає внутрішню врівноваженість людини, адекватність його реакцій на зовнішні впливи, відповідність поведінки людини встановленим, загальноприйнятим у житті громади нормам моралі і моральності;

• соціальну безпеку, до якої відноситься необхідність усілякої підтримки найбільш вразливих у соціальному відношенні категорій населення (пенсіонерів, інвалідів, багатодітних сімей, сиріт) і яка визначає рівень моральності самого людського суспільства;

• антикримінальну безпеку, актуальну практично для кожної людини, що виявилася жертвою шахрайства, крадіжки, грабежу, а також більш тяжких злочинів проти особистості та суспільства;

• антинаркотичну безпеку, що стала в останні роки однією з важливих умов виживання значної частини молодого покоління, підданого дії алкогольної або наркотичної залежності;

• техногенну (виробничу, побутову) безпеку, пов'язану з інтенсивним зростанням різноманітності в сучасному світі техногенних загроз і небезпек (електромагнітних випромінювань, вибухів, механічних і термічних впливів, радіації, токсичних речовин і т.д.);

• транспортну безпеку, обумовлену зростаючим числом жертв автомобільних аварій, льотних пригод, катастроф на морі і залізницях;

• протипожежну безпеку, що вимагає найпильнішої уваги у зв'язку з застарілістю електромереж значної частини старого житлового фонду країни, браком фінансових коштів на їх планову заміну, збільшенням поверховості новобудов, підвищенням потужності побутових електроприладів;

• природну та екологічну безпеку, для здійснення якої людина змушена, з одного боку, боротися з погрозами природного характеру (такими, як сходження снігових лавин, повені, цунамі, урагани, землетруси, виверження вулканів), а з іншого боку, захищати саму природу під час екологічних, природоохоронних заходів від хижацького винищення рідкісних видів тварин і рослин, вирубки і підпалів лісових масивів, браконьєрського вилову риби і морських тварин, отруєння водних ресурсів відходами підприємств, руйнування шару атмосфери, забруднення ближнього космосу;

• біологічну безпеку, яка передбачає захист людини від бактеріологічних і вірусних інфекцій, грибкових і паразитних захворювань, отруйних комах, змій, грибів, рослин;

• фінансову безпеку, під якою розуміється захищеність коштів кожної окремої людини і всього населення країни від будь-якого роду фінансових загроз і небезпек;

• безпеку підприємництва, що передбачає активну захищеність самих людей, зайнятих бізнесом (від спроб їх захоплення в заручники, вбивства), підприємств (від нанесення їм матеріального або фінансового збитку), службової інформації (від її розголошення), що випускається (від її розкрадання, руйнування, дискредитації);

• інші види безпеки людини і суспільства [6].

5.2. Система державної (національної) безпеки

До складу системи державної (національної) безпеки входять такі основні види:

• безпека конституційного ладу держави, що передбачає активну захищеність законодавчо встановленого суспільного устрою країни і стабільність усієї законодавчо прийнятої системи державної влади;

• безпека державних органів влади і управління, яка передбачає активну і всебічну захищеність вищих посадових осіб країни, можливість нормального виконання ними своїх конституційно встановлених функцій, а також охорону місць розташування органів влади;

• безпека цілісності і суверенітету країни, що є необхідною умовою політичної і економічної стабільності будь-якої держави на внутрішньо-і зовнішньополітичній арені;

• антитерористична безпека, що представляє собою систему заходів ефективної захищеності життєво важливих інтересів і самого існування всіх структурних рівнів об’єктів безпеки від руйнівних сил тероризму і хаосу в будь-яких формах їх мотивації і прояви;

• безпека національної економіки, що передбачає активну захищеність держави від спадів у діяльності міжнародної економічної системи, збалансованість експортно-імпортних і товарно-сировинних потоків, стійкість проведеної фінансової політики і всієї банківської системи, реалізацію національних інтересів на міжнародній арені;

• інформаційна безпека, яка представляє собою комплекс заходів із захисту інформаційних потоків і баз даних «закритої» (тобто з грифом секретності) інформації державного або відомчого значення від несанкціонованого доступу, викрадення, розголошення або пошкодження комп’ютерними «вірусами»;

• безпека національної культури, пов'язана зі збереженням, підтриманням і захистом національних особливостей і реліквій народів країни від руйнування, агресивного впливу або експансії з боку інших держав;

• демографічна безпека, що передбачає сталість або зростання населення країни, збільшення тривалості життя людей;

• інші види державної (національної) безпеки [6];

• у цей список доцільно додати корупційну безпеку, що представляє собою комплекс заходів по боротьбі з корупцією на державному рівні.

Корупція на державному рівні є одним із найсерйозніших чинників державної безпеки. Інформаційні технології, що застосовуються в системах корупційної безпеки, використовують безліч різних підходів, включаючи методи штучного інтелекту.

Цікавий приклад використання штучного інтелекту в боротьбі з корупцією в Китаї. Як пише газета South China Morning Post (SCMP), дослідники з Академії наук КНР спільно із представниками контролюючих органів Компартії Китаю розробили високотехнологічний проект Zero Trust, призначений для виявлення корупціонерів серед чиновників за допомогою аналізу відомостей про них із 150 різних баз даних. Система може відстежувати доходи чиновників та їхніх родичів, підозрілі транзакції, великі покупки та інші деталі, які вказують на те, що той чи інший службовець живе невідповідно до своїх достатків. З часу запуску в 2012 році проект допоміг виявити більше 8 тис. чиновників, замішаних у розтра-

тах, корупції і кумівстві. Через кілька років після початку роботи системи все більше відомств стали відмовлятися від її використання, посилаючись на «дискомфорт», який вона завдає. В даний час подальша доля Zero Trust невідома. Ймовірність її повноцінного запуску на всій території Китаю невелика, хоча дослідники все ще розраховують на впровадження антикорупційної системи [7].

У сфері боротьби з тероризмом зарубіжні експерти особливу увагу приділяють штучному інтелекту. Все питання в тому, що найбільшу небезпеку становлять особи, які за своїми зовнішніми ознаками ніде не виявлялися, в поле зору спецслужб не потрапляли, однак здатні здійснити теракт.

У даний час в ЄС і США ведуться дослідження і розробляються програми з вивчення психолого-поведінкових причин тероризму. Результати досліджень планується використовувати як основу для побудови систем штучного інтелекту, які могли б за зовнішніми поведінковими ознаками виявляти суб'єктів, потенційно небезпечних для суспільства. Розробники припускають, що подібні системи зможуть прогнозувати можливу небажану поведінку людей, виробляти і вживати запобіжних заходів. У разі, якщо коефіцієнт благонадійності суб'єкта буде нижче встановленого рівня, «інтелект» зможе відключати людину від зв'язку, блокувати її банківські рахунки, проїзні квитки і т.д.

6. Автоматизована інформаційна система забезпечення безпеки життєдіяльності

У сучасних умовах загрози техногенного, природного, криміногенного і терористичного характеру досі становлять реальну небезпеку для населення регіонів і розвитку держави в цілому. З метою захисту від цих загроз створюються автоматизовані інформаційні системи забезпечення безпеки життєдіяльності.

Як приклад розглянемо одну з автоматизованих інформаційних систем забезпечення безпеки життєдіяльності великого мегаполісу [8].

Завдання забезпечення безпеки життєдіяльності, як правило, вирішуються в умовах жорсткого дефіциту часу. Обмеженість тимчасових і матеріально-технічних ресурсів і можливостей людини при великих масштабах і швидкості розвитку надзвичайних ситуацій впливає на адекватність і достовірність інформації, використовуваної при прийнятті рішень, а також на оперативність прийняття цих рішень. Ці аспекти зумовлюють необхідність використання для вирішення завдань безпеки сучасних технологій автоматизованого збору, обробки, аналізу і візуалізації інформації. Таким чином, заходом, спрямованим на підвищення ефективності забезпечення безпеки життєдіяльності, є впровадження у процеси управління новітніх інформаційних і телекомунікаційних технологій.

6.1. Структурна схема процесу автоматизації інформаційної системи забезпечення безпеки життєдіяльності в мегаполісі

Структурна схема процесу автоматизації інформаційної системи забезпечення безпеки життєдіяльності (рис. 1).

Процеси інформаційної підтримки прийняття рішень показані на рис. 2.

Керуючим об'єктом є сукупність виконавчих органів державної влади, територіальних органів федеральних органів виконавчої влади та органів місцевого самоврядування, керівництво підприємств, установ та їх структурних підрозділів, чергові та диспетчерські служби. Під об'єктами управління розуміється сукупність контрольованих об'єктів, де можуть виступати населення, всі значущі об'єкти інфраструктури, навколишнього середовища, господарської та економічної діяльності, а також сили і засоби, задіяні в забезпеченні безпеки життєдіяльності.

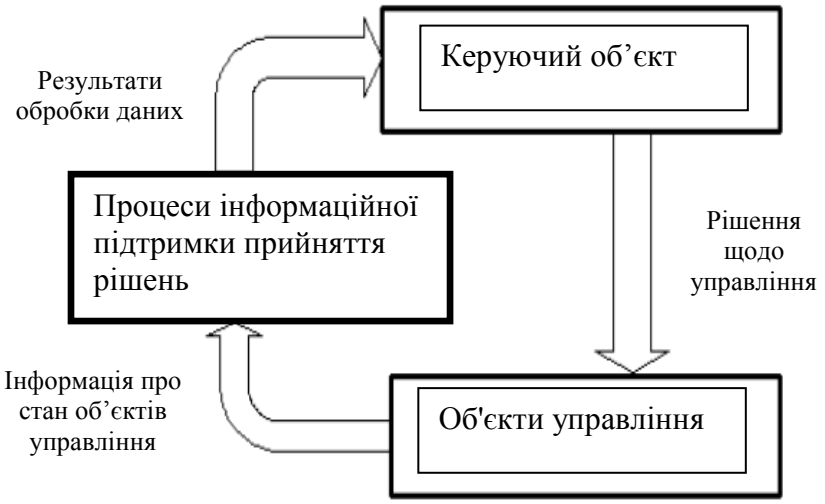


Рисунок 1 – Структурна схема процесу автоматизації інформаційної системи забезпечення безпеки життєдіяльності

Рисунок 2 – Процеси інформаційної підтримки прийняття рішень

Вихідною інформацією, необхідною для прийняття управлінських рішень у сфері забезпечення безпеки життєдіяльності мегаполісу, є:

- достовірні дані про поточний стан (місцезнаходження) об’єктів управління;
- критичні значення параметрів, що характеризують стан об’єктів управління;
- архівні дані про об’єкти управління;

• прогнозна інформація про тенденції та перспективи змін стану об’єктів і процесів, отримана за результатами опрацювання архівних даних із використанням математичних моделей;

• еталонні дані інформаційних систем (карти, кадастри, регістри, реєстри і т.д.);

• дані інших інформаційних систем.

Суттєвою особливістю автоматизованих інформаційних систем забезпечення безпеки життєдіяльності є складна ієрархічна структура керуючого об'єкта, окремі елементи якого взаємодіють між собою як у ході повсякденної діяльності, так і при ліквідації надзвичайної ситуації.

6.2. Структура автоматизованої інформаційної системи забезпечення безпеки життєдіяльності

Автоматизована інформаційна система забезпечення безпеки життєдіяльності являє собою сукупність локальних вузлів (ЛВ), є пунктами концентрації інформації, об’єднаних одним спеціального виду ЛВ, які реалізують ретрансляцію інформаційних потоків і є центром управління доступом (ЦУД).

ЛВ являють собою інформаційні системи, групи інформаційних систем, окремі компоненти систем (база даних, клієнт-додаток, сервер-додаток) або групи компонентів. Користувачі системи (посадові особи, служби, спеціалізовані центри) відповідно до прав доступу отримують інформацію від найближчого ЛВ або через ЦУД від будь-якого іншого ЛВ. Засобами ЛВ забезпечується єдиний призначений для користувача інтерфейс. ЦУД забезпечує єдині маршрутизацію, авторизацію і аутентифікацію на основі збереження в ньому інформації про користувачів і джерел.

Структура автоматизованої інформаційної системи забезпечення безпеки життєдіяльності представлена на рис. 3.

Схема логічної організації інформаційної взаємодії представлена на рис. 4.

Основним фактором, що визначає склад елементів системи забезпечення безпеки життєдіяльності та їх взаємозв’язок, є необхідна функціональність системи.

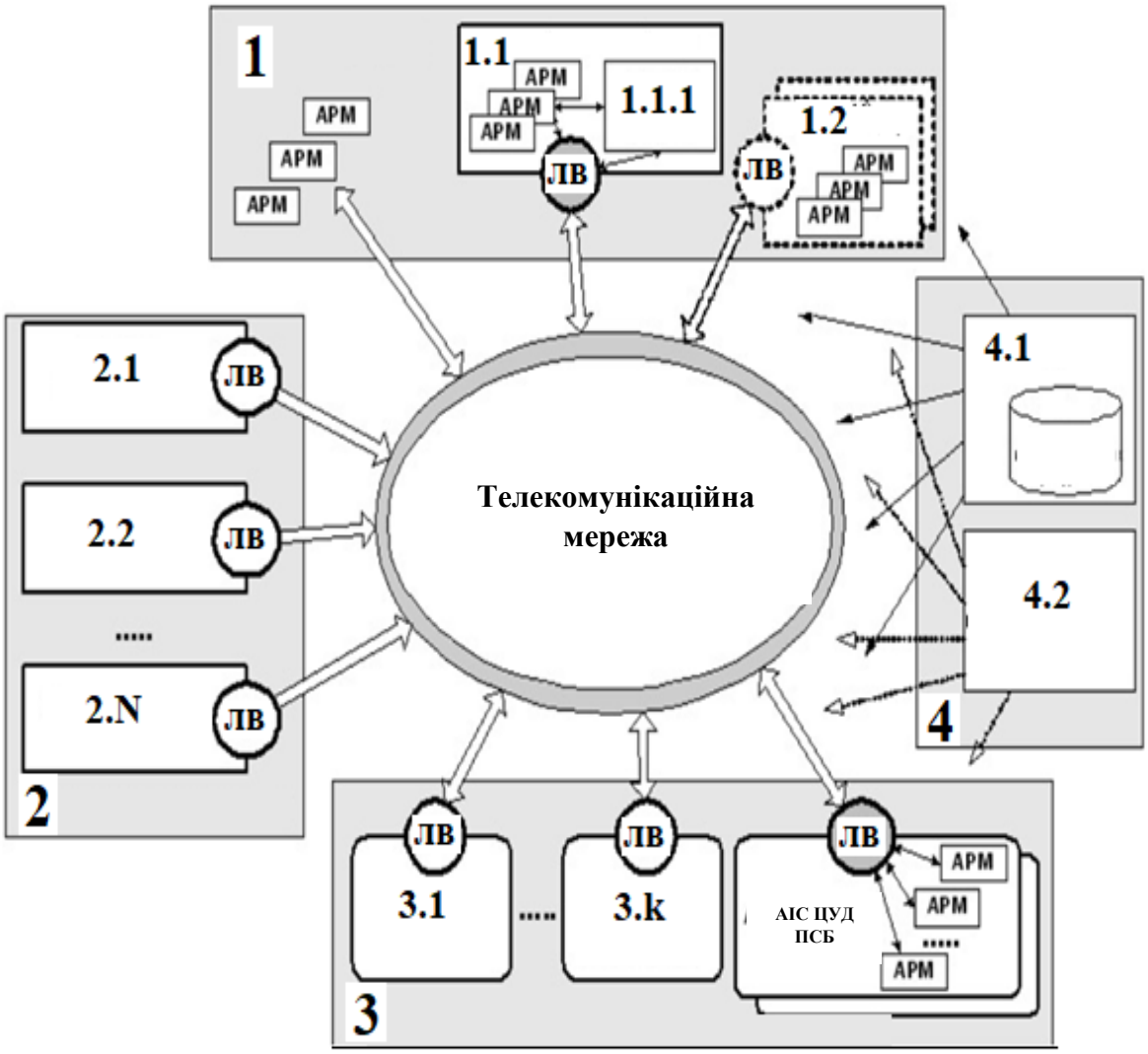
Відповідно до переліку необхідних функцій, які забезпечують систему життєдіяльності для вирішення завдань щодо забезпечення безпеки життєдіяльності, входять такі функціональні елементи:

1. Сукупність функціональних систем, які є для системи забезпечення безпеки життєдіяльності первинними джерелами інформації: системи, що забезпечують моніторинг об'єктів і процесів (датчикову систему, системи дистанційного зондування, системи відеоспостереження і т.д.); системи прийому інформації від населення, системи екстреного зв'язку; інформаційні системи, в тому числі ті, що містять еталонні дані (кадастри, регістри, реєстри, довідники, класифікатори тощо).

2. Розрахунково-аналітичні системи, що забезпечують обробку інформації за заданими алгоритмами.

3. Система управління доступом, що забезпечує централізоване призначення прав користувача щодо використання інформаційних ресурсів системи безпеки життєдіяльності.

4. Система забезпечення інформаційної безпеки, що виконує вимоги нормативних і законодавчих актів в області захисту конфіденційної інформації при її автоматизованій обробці і передачі по каналах зв’язку [8].



1. Користувачі ресурсів.
2. Джерела, ресурси, інформація.
3. Відомчі та територіальні системи забезпечення безпеки.
4. Центр управління доступом.
1.1. Міський ситуаційний центр.
1.2. Районний ситуаційний центр.
1.1.1. Розрахунково аналітична система.
2.1. Системи моніторингу.
2.2. Системи екстреного зв'язку.
2.N. Інформаційні системи.
3.1. – 3.К. Локальна система безпеки.
4.1. База інформаційних ресурсів.
4.2. Система забезпечення інформаційної безпеки.
АРМ – 4 автоматизоване робоче місце.
АІС ЦУД ПСБ – автоматизована інформаційна система центру управління доступом поліції суспільної безпеки.

Рисунок 3 – Структура автоматизованої інформаційної системи забезпечення безпеки життєдіяльності

Рисунок 4 – Схема логічної організації інформаційної взаємодії

7. Інформаційні системи обміну даними

Інформаційні системи обміну даними тільки починають активно розроблятися і впроваджуватися. Це абсолютно новий напрям в області спецтехнологій боротьби з тероризмом. Ідея таких технологій полягає в тому, що сама інформація без належного застосування не має цінності. У зв'язку з цим важливо не тільки зібрати, обробити, а й вчасно розподілити, передати відомості між силовими відомствами з метою прийняття оперативних рішень, швидкого реагування на терористичні загрози і припинення терактів.

8. Системи визначення вибухових речовин, контролю і моніторингу людських потоків, транспортних засобів, вантажів

Одним із найважливіших місць у боротьбі з тероризмом займають технології паспортно-візового контролю для фіксації, ідентифікації та подальшого розпізнавання метричних даних фізичних осіб (особи, відбитки пальців, форма і структура зап'ясть, сітківка ока і ін.), транспортних засобів (реєстраційні номери, габарити, вага), сканування вантажів на автотранспорті, залізниці і в морських портах.

Перспективним напрямом у цій сфері вважаємо вдосконалення технологій розпізнавання з підключенням елементів штучного інтелекту для ідентифікації та виявлення осіб у разі зміни ними своїх зовнішніх даних.

9. Штучний інтелект

Найбільші труднощі у виявленні суб'єктів тероризму становлять особи, які за своїми зовнішніми ознаками ніде не виявлялися, в поле зору спецслужб не потрапляли, однак здатні здійснити теракт. У даний час в ЄС і США існують програми з вивчення психолого-поведінкових причин тероризму. Результати досліджень планується використовувати як основу для побудови систем, які могли б за зовнішніми поведінковими ознаками (починаючи від зустрічей, розмов, перегляду радикальних сайтів, соцмереж, ігор і закінчуючи змінами фізіологічних даних – температури тіла, кольору шкіри, пульсу, дихання) виявляти суб'єктів, потенційно небезпечних для суспільства. Подібні системи зможуть прогнозувати небажану поведінку людей, виробляти і вживати запобіжних

заходів. На штучний інтелект покладаються особливі надії в боротьбі з терористами і терористичними організаціями. Якщо коефіцієнт благонадійності суб'єкта буде нижче встановленого рівня, «інтелект» зможе відключати людину від зв'язку, блокувати її банківські рахунки, проїзні квитки і т.д. До таких систем пред'являються особливо жорсткі вимоги: сильний штучний інтелект, робота в реальному часі і обробка великих масивів інформації.

10. Обробка великих масивів даних – Data Mining

В ЄС для запобігання терактам, особливо на території розвинених держав і мегаполісів, як технологічні рішення боротьби з тероризмом використовуються так звані програмно-апаратні комплекси, здатні фіксувати всі контакти абонентів, їх місце розташування, пересування і т.д. Розроблено ряд нормативно-правових актів, які в рамках боротьби з тероризмом наділяють компетентні органи країн Євросоюзу правом на встановлення контролю і моніторингу різних персональних каналів зв'язку, починаючи від мобільних телефонів, електронної пошти і закінчуючи соцмережами.

Багато експертів країн ЄС, США, Близького Сходу, Азіатсько-Тихоокеанського регіону, РФ відзначають, що основою є отримання передчасної інформації про підготовлювані акції з боку екстремістських угруповань. Для цього можуть використовуватися як розгалужені агентурні мережі правоохоронних органів і спецслужб, так і технічні засоби контролю і розвідки для виявлення намірів терористів. Важливим аспектом у цьому напрямі є встановлення контролю за індивідуальними засобами комунікації терористів, електронним листуванням, соціальними ресурсами та іншими каналами зв'язку.

Однак для контролю каналів зв'язку і обробки одержуваної інформації в більшій мірі використовуються фахівці, тобто має місце людський фактор. Це перешкоджає вивченню великих обсягів даних і, як результат, не кращим чином позначається на виявленні потенційних терористичних загроз [9].

У зв'язку з цим особливого значення набувають технології, пов'язані з автоматичною обробкою великих масивів даних з подальшим встановленням взаємозв'язків між відомостями, отриманими з різних джерел (телефонів, пошти, соцмереж, камер відеоспостереження, баз даних про персоналії, банків, податкових та ін.).

11. Проект «Думаючий комп'ютер або електронний мозок для роботів та інтелектуальних систем»

Очевидно, що для забезпечення безпеки життєдіяльності населення країни, та й, власне, державної безпеки необхідно на основі існуючих комп'ютерних систем і принципово нових систем, що базуються на технології штучного інтелекту, створювати бази даних і знань, розподілених по всій країні і об'єднаних в одну потужну інтелектуальну базу інформаційного забезпечення безпеки держави і її населення. Така інтелектуальна база інформаційного забезпечення безпеки держави і його населення повинна володіти високим штучним інтелектом, надшвидкодіючим, одночасно обробляти величезні масиви різної інформації, приймати рішення в реальному часі. Основним двигуном такої бази може виступати система, створена на основі проекту «Думаючий комп'ютер або електронний мозок для роботів та інтелектуальних систем».

11.1. Технологічна основа проекту

Нова технологія, новий тип нейромережі – багатозв'язна, багатовимірна, рецепторно-ефекторна нейроподібна зростаюча мережа, що функціонує за аналогією з мозком людини. Від подібних технологій вона відрізняється нетрадиційною не фон-нейманівською

архітектурою системи, що забезпечує масовий паралелізм. Ця структура здійснює одночасне сприйняття, аналіз, синтез, запам'ятовування, класифікацію та узагальнення інформації, представленої у різних вимірах (наприклад, візуальному, звуковому, тактильному та ін. у реальному часі). В результаті аналізу інформації нейроподібна структура виробляє керуючі сигнали на виконавчі механізми. Отже, формуються умовні рефлекси і складні адаптивні механізми поведінки системи з нейроподібною структурою в навколишньому середовищі.

11.2. Переваги технології

Високий інтелект. Система вирішує поставлені завдання за допомогою навчання або самонавчання. Відсутність програмування – система навчається користувачем або самонавчається. Масовий паралелізм, сприйняття, накопичення та обробка надвеликих обсягів інформації: швидкодія системи за рахунок одночасного виконання операцій по всьому об'єму активної структури. Відносна швидкість збільшується зі збільшенням обсягу оброблюваної інформації. Малі габарити і енергоспоживання. Стійкість і надійність.

11.3. Цілі і завдання

При реалізації проекту переслідуються такі цілі.

Короткострокова мета (перший етап). Протягом 10-ти місяців на базі програмно-апаратних моделей системи розпізнавання об'єктів, системи спілкування «Dialog» і віртуального робота «Vitrom» розробити прототип «Електронного мозку».

Довгострокова мета (другий етап). На базі прототипу «Електронний мозок» протягом 1–1,5 року організувати промислове виробництво електронного мозку для роботів.

Більш детально питання реалізації проекту опубліковані в різних наукових журналах [10–13].

12. Висновок

У житті людини постійно присутні і діють природні, техногенні і антропогенні небезпеки. Повністю усунути постійно діючі, природні небезпеки до теперішнього часу не вдавалося, але використання сучасних засобів інформаційного забезпечення дозволяє визначати найбільш імовірні зони дії цих небезпек, попереджати їх і ліквідувати з мінімальними матеріальними і людськими втратами.

Техногенні небезпеки прогнозовані і у людства досить засобів і способів захисту від них. Використання інформаційних технологій нового покоління дозволяє практично повністю усунути вплив шкідливих техногенних факторів, а вплив техногенних травмонебезпечних факторів обмежений допустимим ризиком за рахунок вдосконалення джерел небезпек і застосування засобів захисту.

Очевидно, що для забезпечення безпеки життєдіяльності населення країни, та й, власне, державної безпеки необхідно на основі існуючих комп'ютерних систем і принципово нових систем, що базуються на технології високого штучного інтелекту, створювати бази даних і знань, розподілених по всій країні і об'єднаних в одну потужну інтелектуальну базу інформаційного забезпечення безпеки держави і його населення.

Таким чином, аналіз існуючої практики та тенденцій розвитку інформаційної протидії тероризму свідчить про різні підходи до запобігання і нейтралізації загроз тероризму. Ефективне вирішення цього завдання вимагає координації зусиль, що базуються на загальнодоступному обміні інформацією, про досягнення в області інформаційної безпеки як окремих держав, так і світової спільноти в цілому.

СПИСОК ДЖЕРЕЛ

1. Ступко К.О., Мироненко О.Е., Голева А.И. Информационные технологии в сфере безопасности жизнедеятельности. URL: http://www.xn----9sbb.su/pr_90.html.
2. Содержание дисциплины «БЖД», ее цели и задачи. URL: http://bgdstud.ru/bilety-i-otvety-po-ekzamenu-bzhd/393-soderzhanie-discipliny-bzhd-ee-celi-i-zadachi.html.
3. Использование информационных технологий в антитеррористических целях. URL: http://www.honestnet.ru/terrorizm/ispolzovanie-informatsionnyh-tehnologiy-v-antiterroristicheskih-tselyah.html.
4. Основы противодействия терроризму: учеб. пособие для студ. высш. учеб. заведений / ред. Я.Д. Вишнякова. М.: Издательский центр «Академия», 2006. 240 с.
5. Котенко И.В., Юсупов Р.М. Информационные технологии для борьбы с терроризмом. *Защита информации. INCIDE*. 2009. № 2. С. 74–79.
6. Системы и виды безопасности жизнедеятельности. URL: https://studme.org/1417012028515/bzhd/sistemy_vidy_bezopasnosti_zhiznedeyatelnosti.
7. В Китае отказались от искусственного интеллекта для поиска коррупционеров. URL: https://www.yaplakal.com/forum3/topic1907329.html.
8. Автоматизированная информационная система обеспечения безопасности жизнедеятельности. URL: https://works.doklad.ru/view/XhmzmRRpqyI.html.
9. Технологии для борьбы с терроризмом. URL: https://tech.onliner.by/2015/11/22/antiterrorizm.
10. Ященко В.А. От многомерных рецепторно-эффекторных нейроподобных растущих сетей к электронному мозгу роботов. *Математичні машини і системи*. 2013. № 4. С. 14–19.
11. Yashchenko V. Artificial intelligence theory. *Science and Information Conference*, London, UK, August 27-29, 2014. London, UK, 2014. P. 473–480.
12. Yashchenko V. Multidimensional neural-like growing networks – a new type of neural networks. *International Journal of Advanced Computer Science and Applications*, (IJACSA). 2015. Vol. 6, N 4. P. 48–55.
13. Ященко В.А. Некоторые проблемные вопросы разработки искусственного мозга. *Математичні машини і системи*. 2018. № 4. С. 19–31.

Стаття надійшла до редакції 11.02.2019