- after receiving the negative test result, the probability that we will receive an unsuitable message $P(D_2|T_2) = P(D_2, T_2)/P(T_2) = 0,8928$;

- the probability that after receiving the negative test result, we will get a suitable message (error of type I) is $P(D_1|T_2) = P(D_1, T_2)/P(T_2) = 0.1071$.

According to the results of the research, the following conclusions were drawn:

- the accumulation of test results and their inclusion in a tables based on Bayesian methods positively affects on the accuracy of obtaining the appropriate probabilities;

- different probabilities characterize the sign on which spam testing is performed. At large values of type I and II errors it is possible to draw a conclusion regarding the quality of the test is low. So the sign could be excluded from the list of signs;

- changes in testing technology can affect the results of obtaining the appropriate probabilities. When changing the testing technology it is necessary to reject the outdated values of statistical data;

- accumulating new data and rejecting outdated, processing data using Bayesian methods, evaluating data — we can assume that this is a described model of DSS with artificial intelligence that carries out artificial intelligence machine learning on the signs of spam.

Keywords: Bayesian methods; machine learning; artificial intelligence; decision support systems; spam.

УДК 658.5+681.51

Ю. І. КАТКОВ, канд. техн. наук, доцент;
М. В. ХОМЕНКО,
Державний університет телекомунікацій, Київ

ЗАГРОЗИ ВІД ІНТЕЛЕКТУАЛЬНИХ ІНФОРМАЦІЙНИХ СИСТЕМ ПОШУКУ ДЛЯ КРИТИЧНИХ ІНФРАСТРУКТУР

Розглянуто питання прояву уразливості елементів інтелектуальної інформаційної системи пошуку інформації. Інтелектуальна інформаційна система пошуку інформації розглядається як складова частина критичної інфраструктури системи управління в складній організаційній системі. Критична інфраструктура — це система, в якій відмова (повністю або частково) уразливого елемента може спричинити ланцюжок відмов у складній організаційній системі взаємопов'язаних інших елементів і тому значно впливає на безпеку і добробут у різних сферах забезпечення основних людських потреб. У XXI столітті критичні інфраструктури стають все більш залежними від нового виду загроз — упровадження сучасних технологій на основі штучного інтелекту. Грунтуючись на цих технологіях, створюються інтелектуальні системи, від яких залежить основна функціональність критичної інфраструктури. Виникає питання: чи можна довіряти інтелектуальним системам автоматично приймати рішення, якщо в них є уразливі елементи і присутній людський фактор? Тому залежність критичних інфраструктур від інтелектуальних систем проявляється не тільки в тому, які технології на основі штучного інтелекту використовуються, а й у тому, яка організація управління прийнята самими інфраструктурами. Аналіз залежності критичних інфраструктур від загроз є складною обчислювальною проблемою. У цьому дослідженні подано опис проблеми прояву уразливості елементів інтелектуальної інформаційної системи пошуку інформації, яка входить до складу інфраструктури системи управління складної організаційної системи. Метою цієї статті є виявлення уразливих елементів інтелектуальних інформаційних систем пошуку, а також визначення їх наслідків для забезпечення безпеки і стабільності інфраструктури та окреслення заходів щодо захисту.

Ключові слова: інтелектуальна інформаційна система пошуку інформації; критична інфраструктура; вразливі елементи.

ВСТУП

У сучасному світі мережу Інтернет використовують як довідковий інструмент. Досить згадати сленгові слова «прогугліть питання». Засобом отримання інформації слугують пошукові системи, наприклад Google, Bing, Yahoo!, Baidu, Yandex та ін., які є невід'ємною частиною інтернету. Пошук інформації виконують інформаційно-пошукові системи із застосуванням технологій штучного інтелекту (ШІ), які сьогодні мають назву ***інтелектуальні інформаційні системі пошуку***.

Інтелектуальна інформаційна система пошуку (ІІСП) — це один із видів автоматизованих інформаційних систем, заснованих на знаннях. ІІСП є комплексом програмних, лінгвістичних і логіко-математичних засобів для підтримання діяльності людини і пошуку інформації у режимі розширеного діалогу на природній мові з використанням технологій ШІ. Результатом упровадження ІІСП є пошук і аналіз інформації, відкритої в публічному інформаційному просторі; виявлення згадок (натяків, непрямих доказів та ін.) заданих об'єктів спостережень (персони, організації, факти, події); здатність обробляти великі обсяги даних і отримувати необхідну релевантну інформацію; створення різних інтерактивних звітів потрібної тематики, з можливістю приведення їх до необхідних стандартизованих форм звітів потрібних типів, наприклад аналіз активності джерел із досліджуваних тем, аналіз популярності персон (організації) та ін.

У [1] показано, що інформаційно-інтелектуальні системі розглядаються як частина критичної інфраструктури (КІ) (*Critical Infrastructure* — CI) системи управління в складній організаційній системі (СОС). ІІСП є однією з видів інформаційно-інтелектуальної системи. Особливості КІ розглянуто в [2–4], де показано, що будь-яка СОС має уразливі об'єкти (критичні елементи, *Critical Elements* — CE).

Уразливий об'єкт — це слабка ланка в системі, яка нездатна протистояти шкідливим впливам (загрозам), дія яких порушує технологію управління. Якщо цей об'єкт посідає важливе місце в системі, то його пошкодження (втрата) може призвести до катастрофічних наслідків. Розрізняють людську, технічну та інформаційну уразливість. Людська уразливість виникає внаслідок психологічних впливів. Технічна — це результат виникнення несправності в механізмах управління системою. Інформаційна уразливість є наслідком непередбачуваного впливу інформації на процес прийняття рішень. Загроза і уразливий об'єкт — це передумови виникнення критичного стану інфраструктури. Уразливість в інформаційній системі є подією, за якої компрометується один або кілька аспектів безпеки інформації (доступність, конфіденційність, цілісність і достовірність). Наявність уразливого об'єкта створює слабку ланку, що може призвести до порушення безпеки інформації. Природно, що вплив загрози на технологію управління може спричинити критичний стан як її складових, так і всієї СОС [2–3].

У XXI столітті критичні інфраструктури стають все більш залежними від нового виду загроз — упровадження сучасних інформаційних технологій на основі ШІ. Сьогодні на основі технологій ШІ створюються різноманітні інтелектуальні системи (ІС), у нашому випадку це ІІСП, від яких залежить функціональність КІ [4; 5]. Залежність КІ від ІІСП проявляється не тільки в тому, які технології на основі ШІ використовуються, а й у тому, які наслідки можуть дати уразливі елементи ІІСП. Тому виникає питання: чи можна довіряти ІІСП автоматично приймати рішення, яку інформацію зібрати, які висновки робити, якщо в них є уразливі елементи і присутній людський фактор? Звідси мета цієї статті — проаналізувати механізм впливу інтелектуальних технологій на уразливі елементи ІІСП для розуміння значимості цих загроз, а також визначити наслідки для забезпечення безпеки інфраструктури СОС і окреслити заходи щодо захисту.

Постановка проблеми. Відомо, що ІІСП розглядаються як інструмент допомоги особам, що приймають рішення і яким потрібна актуальна інформації для прийняття рішень, наприклад політикам, маркетологам, різного роду аналітикам і управлінцям. Ці системи на основі ключових слів приймають рішення щодо вибору і підбору інформації, яка може бути використана для прийняття рішення під час управління СОС. ІІСП входить до складу КІ будь-якої СОС і тому може створити умови небезпеки для організації, в якій вона працює. Небезпека у тому, що у будь-якої ІІСП обов'язково є уразливі елементи. Небезпека виникає двояко.

По-перше, якщо якийсь уразливий елемент перестає працювати внаслідок помилки (збою) у роботі, наприклад помилки індексації в засобі фіксування і збору інформації; або збою засобу передавання відповідних даних та повідомлень; або відмови засобу збереження інформації; або помилки засобу аналізу, обробки і подання інформації, то це призведе до втрати певного обсягу актуальних нових даних. Тоді ІІСП буде формувати відповіді на основі вже не актуальних даних. А це може призвести до помилки під час прийняття рішення.

По-друге, існує проблема релевантності оцінювання інформації для клієнта. Дійсно, метрика такого оцінювання в більшості випадків є суб'єктивною: що становить інтерес для одного клієнта, може бути абсолютно неважливим для іншого. Унаслідок технічних або програмних помилок, з одного боку, та проблеми релевантності оцінювання інформації, з другого, породжується проблема довіри до ІІСП.

Звідси виникає завдання визначити уразливі елементи ІІСП на основі аналізу їх функціонування в СОС відносно потенційно можливих загроз. Об'єкт дослідження — ІІСП. Предмет дослідження — теоретичні, методичні та практичні аспекти критичності функціонування ІІСП (виявлення уразливих елементів).

Аналіз останніх досліджень і публікацій. Сьогодні вже накопичено значний теоретичний і практичний матеріал із різних аспектів розвитку ІІСП, наприклад, у [6] розкрито питання, присвячені розвитку, упровадженню, використанню інтелектуальних інформаційних технологій та систем у різних сферах життєдіяльності суспільства. У [2] показано, що в СОС завжди існує критичний елемент, вплив на який з боку небезпеки може призвести до критичного стану всю систему. У [3] висвітлено роль і місце інформаційної інфраструктури під час виникнення явища критичності в СОС. У [7] розглянуто критичні технології та їхній вплив на систему. Але в зазначених джерелах відсутні дослідження аспектів критичності функціонування ІІСП. Таким чином, аналіз вітчизняної та зарубіжної літератури за темою дослідження аспектів критичності функціонування ІІСП дозволяє дійти висновку про недостатність науково

обґрунтованих подань і висновків про особливості функціонування таких систем. Ця недостатня розробленість і вивченість проблеми довіри до ІІСП свідчить про актуальність та своєчасність теми.

ОСНОВНА ЧАСТИНА

Особливості побудови ІІСП

Відомо, що функціонування ІІСП засновано на *технологіях аналізу індексування інформації про документи* та *семантичного пошуку* і *хешуванні* [8].

Технології аналізу індексування інформації про документи базуються на ***індексуванні інформації***, що означає присвоєння документу набору ключових слів або кодів, які вказують зміст документа і використовуються як засіб прискорення операції його пошуку. У процесі індексування здійснюється переклад змісту документів із природної мови на штучну інформаційно-пошукову мову (ІПМ), у результаті чого створюється пошуковий образ документа і пошуковий образ запиту. За допомогою цього перекладу відбувається згортання інформації, що знаходиться в документі, і перетворення її на ІПМ у вигляді індексу, рубрики, коду або дескриптора, ключового слова [10].

Функціями індексування вважаються: закріплення логічної структури класифікації даних; створення зв'язку між адресою розміщення даних у таблицях баз даних, рубриками, відділами на книжкових полицях при систематичній розстановці; запис результатів систематизації в бібліографічних записах, у самих виданнях тощо [11]. Типову систему комплексного індексування в інтернеті зображено на рисунку [12].

Система комплексного індексування в мережі Інтернет

Основною перевагою використання індексування є значне прискорення процесу вибірки або вилучення даних. Відомі види індексування [12]:

- контрольоване (*controlled indexing*), яке контролюється машинними словниками системи;
- вільне (*free indexing*) — координатне індексування тексту документа ключовими словами, які вибираються безпосередньо із самого тексту чи долучаються в пошуковому образі документа (ПОД) без використання будь-якого нормативного словника;
- надлишкове (*redundant indexing*) — доповнення ПОД лексичними одиницями ІПМ, пов'язаними парадигматичними відношеннями з лексичними одиницями початкового ПОД, зокрема індексами інших рівнів при використанні системи багаторівневої індексації;
- верхньорівневе, або висхідне (*pedigree indexing*) — різновид надлишкового індексування, яке характеризується тим, що ПОД доповнюється лексичними одиницями (верхніми індексами) тезауруса, які стоять на вищому щаблі ієрархії, ніж ті, що використовувались у формуванні початкового ПОД;
- одноаспектне (*single indexing*) — уводить у ПОД лексичні одиниці, які характеризують тематичний зміст документа;
- багатоаспектне (*multiple-aspect indexing*) — метод індексування, при якому в ПОД входять лексичні одиниці, що характеризують кілька тематичних аспектів змісту опрацьованого документа, та інші види індексування.

Відповідно до [8–12] індексування в ІІСП дає змогу:

- обробляти значні обсяги інформації;
- задовольняти велику кількість запитів різного рівня складності;
- надавати розподілений доступ до всіх документів організації в одному вікні;
- здійснювати одночасний пошук документів у всіх підімкнених до неї інформаційних системах;
- бути застосоване для якісного аналізу ринку (конкурентів, попиту і пропозиції, відгуків споживачів, моди і тенденції), а також середовища, в якому існує компанія;
- аналізувати неструктуровані дані, різного роду текстів веб-сторінок.

Недоліком індексних схем є уповільнення процесу відновлення даних, оскільки при кожному додаванні нового запису в індексований файл потрібно також додати новий індекс в індексний файл. Індексний файл (*index file*) — це файл, в якому зберігається інформація індексу. Він є файлом особливого типу, в якому кожний запис складається з двох значень: даних і покажчика номера запису. Термін «індекс» тісно пов'язаний із поняттям «ключ». Таким чином, індексний файл

є критичним елементом, оскільки його втрата або некерована зміна створює помилку в пошуку інформації.

Семантичний пошук — це технологія пошуку інформації, заснована на використанні контекстного (смислового) значення запитуваних фраз, замість словникових значень окремих слів або виразів при пошуковому запиті. Головним недоліком семантичного пошуку порівняно з технологією індексування є той факт, що алгоритми обробки змісту текстів залежать від особливостей конкретної аналізованої природної мови, тобто потрібне створення спеціальних алгоритмів для різних природних мов. При цьому для кожної природної мови має бути враховано її синтаксичні та семантичні особливості, відносини між словами та ін. Це пов'язано з парадоксами мов. Наприклад, у російській мові є такий парадокс: «тарелка *стоит* на столе, а вилка *лежит* на столе, но тарелка *лежит* в сковороде, а сковорода *стоит* на столе». В українській мові «тарілка *стоїть* на столі, а виделка *лежить* на столі, але тарілка *лежить* у пательні, а пательня *стоїть* на столі». В англійській мові «a plate *is on* a table, a fork *is on* the table, the plate *is in* the skillet, the skillet *is on* the table». Як бачимо, однакові за функціональним призначенням кухонні предмети в слов'янських мовах можуть стояти і лежати на столі одночасно, а в англійській мові «is on/in» просто вказує, що предмет є. Звідси алгоритми семантичного пошуку в різних мовах різні. Приклад показує, що реалізація підходів семантичного пошуку в багатомовних системах є дуже складною. Тому алгоритм контекстного (смислового) значення запитуваних фраз є критичним елементом через імовірність виникнення помилки в розумінні.

Хешуванням, або ***хеш-індексуванням*** називається технологія швидкого прямого доступу до інформації, що зберігає записи на основі заданого значення деякого поля, при цьому зовсім не обов'язково, щоб поле було ключовим. Хешування дає змогу не зважати на необхідність підтримувати і переглядати індекси. Хешування відрізняється від індексування тим, що у файлі може бути будь-яка кількість індексів, але тільки одне хеш-поле, в якому записана ***унікальна хеш-функція***, котра звужує діапазон до оптимальної величини. Сьогодні це використовується для створення криптовалют, наприклад біткойнів.

Основні особливості технології хешування:

• кожний запис у базі даних розміщується за адресою, яка обчислюється за допомогою спеціальної хеш-функції на основі значення деякого хеш-поля, а обчислена адреса називається хеш-адресою;

• для збереження запису в базі даних спочатку обчислюється хеш-адреса нового запису, після чого Диспетчер файлів робить запис за обчисленою адресою;

• для вилучення потрібного запису за заданим значенням хеш-поля в базі даних спочатку обчислюється хеш-адреса, а потім Диспетчер файлів надсилає запит на отримання запису за обчисленою адресою.

Отже, критичним елементом для хешування є хеш-функція, оскільки зі збільшенням розміру збереженого файла кількість збігів адрес збільшується, що призводить до значного збільшення часу на пошук інформації у наборах конфліктуючих записів. Цього можна уникнути, якщо реорганізувати файл, тобто завантажити даний файл з використанням нової хеш-функції, розширивши хешування. Але при використанні хешування, яке розширюється, необхідно, аби всі значення хеш-поля були унікальні, а цього можна досягти тільки за умови, що хеш-поле є ключовим.

Таким чином, у технологіях ІІСП є критичні елементи, які спонукають більш детально розглянути побудову ІІСП і знайти критичні елементи.

Типова архітектура побудови ІІСП

Архітектура побудови ІІСП складається з таких основних компонентів:

♦ модуль управління — управління процесом руху даних по системі;

♦ модуль збору даних — збір вихідних документів із мережі Інтернет;

♦ модуль лексичного аналізу — лексичний розбір документів, зібраних модулем збору інформації;

♦ модуль аналізу та подання інформації, генерації звітів на основі даних, що зберігаються в основній схемі [11–12].

Технологія пошуку дозволяє відстежувати події і факти, пов'язані з цільовими об'єктами, за допомогою методів прогнозування, наприклад, результатів політичних заходів, реакції населення на реформи, наявність зв'язку між компаніями і/або персонами тощо. При цьому технологія пошуку сумісна і підтримує різноманітні самостійні інші інформаційні технології, такі, скажімо, як Oracle Database або Oracle RDBMS (система управління базами даних), ClaraBridge (аналіз відповідей клієнтів), Sentiment analysis (аналіз тональності). Наприклад, при використанні аналітичного інструменту Sentiment analysis є можливість оцінювати емоційне забарвлення публікацій («позитив», «негатив»), а потім аналізувати думки і ставлення авторів до цільових об'єктів. Це дає змогу опрацьовувати величезні масиви інформації і виробляти потрібну аналітику, обробити які вручну неможливо в принципі.

При побудові ІІСП застосовуються такі технології інтелектуальних систем: експертна системи (ЕС), інтерактивні банери (web + ЕС), запитально-

відповідна система (деяких джерел «системи спілкування») або інтелектуальні пошукові системи (наприклад, система Старт). Технологія «віртуальні співрозмовники» може бути додатком (для зручності користування). На основі цих технологій ІІСП виконують такі завдання [6; 8; 9].

• ***Інтерпретація даних*** — це процес визначення змісту даних, результати якого мають бути погодженими і коректними. Уразливим є сам результат, він залежіть від алгоритму інтерпретації.

• ***Діагностика*** — це процес співвідношення об'єкта з деяким класом об'єктів і виявлення несправності в деякій системі. Несправність — це відхилення від норми. Важливою специфікою є тут необхідність розуміння функціональної структури («анатомії») діагностуючої системи. Уразливим є розуміння анатомії, яке залежіть від критерію вибору алгоритму співвідношення об'єкта з деяким класом об'єктів.

• ***Моніторинг*** — це неперервна інтерпретація даних у реальному масштабі часу і сигналізація про вихід тих або інших параметрів за допустимі межі. Уразливим є «пропуск» тривожної ситуації та інверсне завдання «помилкового» спрацьовування, оскільки складність цих проблем полягає в розмитості симптомів тривожних ситуацій і необхідності обліку тимчасового контексту.

• ***Проектування*** — це підготовка специфікацій на створення «об'єктів» із заздалегідь визначеними властивостями. Під специфікацією розуміється весь набір необхідних документів — креслення, пояснювальна записка та ін. Уразливим є здобуття чіткого структурного опису знань про об'єкт і проблема «сліду». Для організації ефективного проектування і ще більшою мірою його передумов необхідно формувати не лише самі проектні рішення, а й мотиви їхнього прийняття. Тому в завданнях проектування тісно поєднано два основні процеси, виконувані в рамках відповідної ЕС: процес виведення рішення і процес пояснення.

• ***Прогнозування*** — це передбачення наслідків деяких подій або явищ на підставі аналізу наявних даних. Прогнозовані системи логічно виводять імовірні наслідки із заданих ситуацій. Уразливою є параметрична динамічна модель, в якій значення параметрів «підганяються» під задану ситуацію, а висновки, що випливають із цієї моделі, дають підставу для прогнозів з імовірними оцінками.

• ***Планування*** — це визначення планів дій стосовно об'єктів, здатних виконувати деякі функції. Уразливими є моделі поведінки реальних об'єктів для логічного виведення наслідків планованої діяльності.

• ***Навчання*** — це використання комп'ютера для навчання деякої дисципліни або предмету. Уразливим є діагностування помилок при вивченні якої-небудь дисципліни за допомогою ЕОМ і підказка правильного рішення. Проблема в тому, що ЕОМ акумулюють знання про гіпотетичного «учня» і його характерні помилки, а потім у роботі вони діагностують дошкульні місця в знаннях реальних учнів для відшукання відповідних засобів щодо їх усунення.

• ***Керування*** — це функція організованої системи, що підтримує певний режим діяльності. Уразливим є процес управління поведінкою складних систем відповідно до заданих специфікацій. Тут присутній людський фактор.

• ***Підтримка прийняття рішень*** — це сукупність процедур, що забезпечує особу, яка приймає рішення, необхідною інформацією і рекомендаціями, полегшуючи процес ухвалення рішення. Уразливим є процес відбору і формування потрібної альтернативи серед безлічі пропозицій при ухваленні відповідальних рішень.

Із цього переліку завдань ІІСП у загальному випадку бачимо, що вони засновані на знаннях. Ці завдання виконують системи, які можна поділити або на системи, що вирішують завдання аналізу, або на системи, які вирішують завдання синтезу. Основна відмінність завдань аналізу від завдань синтезу полягає в тому, що якщо в завданнях аналізу безліч рішень може бути перерахована і включена в систему, то в завданнях синтезу безліч рішень потенційно не обмежена і складається з вирішень компонент або проблем. Завданнями аналізу є інтерпретація даних, діагностика, підтримка ухвалення рішення. До завдань синтезу належать проектування, планування, управління, а також комбіновані — вчення, моніторинг, прогнозування.

Таким чином, процеси виконання завдань є уразливими для загроз, які можуть пошкодити вихідну інформацію, необхідну для виконання цих завдань.

Типова схема функціонування ІІСП

Функціонування ІІСП можна описати як постійне прийняття рішень на основі аналізу поточних ситуацій для досягнення певної мети. Можна виокремити етапи, які утворюють типову схему функціонування ІІСП [8].

1. Безпосереднє сприйняття зовнішньої ситуації — результатом є формування первинного опису ситуації.

2. Зіставлення первинного опису зі знаннями системи і поповнення цього опису — результатом є формування вторинного опису ситуації в термінах знань системи.

3. Планування цілеспрямованих дій та прийняття рішень, тобто аналіз можливих дій та їхніх наслідків і вибір тієї дії, яка найкраще узгоджується з метою системи — результатом є рішення,

яке формується деякою внутрішньою мовою (свідомо або підсвідомо).

4. Зворотна інтерпретація прийнятого рішення — результатом є формування робочого алгоритму для здійснення реакції системи.

5. Реалізація реакції системи — результатом є зміна зовнішньої ситуації і внутрішнього стану системи та ін.

Не слід вважати, що вказані етапи є повністю розділеними у тому розумінні, що наступний етап починається тільки після того, як повністю закінчиться попередній. Навпаки, для інтелектуального функціонування системи характерним є взаємне проникнення цих етапів. Отже, у типову схему функціонування ІІСП закладено уразливість у вигляді черговості виконання етапів, оскільки, наприклад, будь-яке рішення може прийматися вже на етапі безпосереднього сприйняття ситуації. Насамперед це рішення про те, на які зовнішні показники слід звертати увагу, а на які не обов'язково. Зовнішніх показників багато, тому їхнє сприйняття має бути вибірковим.

Виявлення загроз від ІІСП для критичної інфраструктури

Як було вже зазначено, ІІСП надають життєво важливі послуги в усіх сферах людської діяльності, тому отримання інформації про ці послуги необхідно. Проте сам факт використання ШІ викликає занепокоєння щодо безпеки управління КІ під час застосування ІІСП. Розглянуті раніше уразливі елементи дозволяють визначити головні причини і загрози їх критичності.

1. Автоматизація процесів управління без участі людини на основі штучного інтелекту — це і загроза, і ключове рішення для захисту. Це загроза тому, що виникають умови породження нових загроз, на основі методів управління штучним інтелектом віддаленого доступу, скажімо, відомі приклади вимагання грошей шляхом проникнення через мережу доступу в систему управління медичного закладу з метою шантажу за рахунок відімкнення медичного обладнання в операційній під час операції.

2. Залучення ШІ для створення програмного забезпечення «подвійної дії» — це загроза, оскільки відомі випадки, коли програмне забезпечення для якихось послуг може бути перепрограмовано для більш шкідливих програм, наприклад, програмне забезпечення Андроід, яке дозволяє відстежувати запити користувача в маркетингових цілях, може бути використано для отримання персональних даних.

3. Залучення штучного інтелекту для створення програмного забезпечення багаторазового застосування в різних галузях — це загроза. Досить часто в певних ситуаціях або обставинах одне і те саме рішення може бути успішно вживано, наприклад, розпізнавання особи в сучасних камерах спостереження має безліч застосувань у самих різних секторах діяльності. Однак висока ймовірність того, що деякі технології за рахунок невеликих відмінностей в алгоритмах роботи, управлінні або установці можуть призвести до катастрофічних наслідків.

4. Збільшення точок дистанційного інформаційного входу в критичні інфраструктурні системи — це загроза, оскільки збільшення кількості підімкнутих пристроїв, інструментів, обладнання і транспортних засобів, що з'єднуються один з одним за допомогою Інтернету речей (IoT) дає змогу потенційним зловмисникам легше вибирати з безлічі точок входу вхід у критичну інфраструктуру системи за допомогою найменш захищеного приладу. Наприклад, незахищені прилади IoT дають не тільки інтелектуальні «речі», а й збільшують доступність для хакерів за допомогою технологій безпроводового зв'язку для зростання кількості атак через безліч незахищених приладів.

5. Наступність, або «наслідки вчорашнього дня» — це загроза. Наступність традиційно широко поширене явище, наприклад, стандартизація політик, методів і вимог. Проте, не зважаючи на безліч переваг або зручностей, можливе перенесення помилок, зроблених багато років тому, або старих поглядів, які шкодять у реальному часі та можуть призвести до чималих наслідків у майбутньому. Наприклад, у процесорах Intel виявлено нові варіанти уразливості Spectre v1 [13]. Це приклад того, що продукти, послуги та операції, які пройшли оцінку аналітиків безпеки, розробників, адміністраторів і постачальників послуг у минулому, можуть бути уразливі за нових умов функціонування.

6. Відкритість і свобода співпраці (collaboration) у наданні всіх видів послуг на основі цифрових технологій (didgital, цифровізації) — це загроза. Міжнародні загрози, такі як кібертероризм або кібератаки, контрольовані штучним інтелектом, стають все більш поширеними і найбільш імовірними, оскільки все, що нас оточує, стає все більш цифрованим, а тому доступним для нагромадження знань.

7. Людський фактор — це загроза тому, що під час упровадження інформаційних технологій можливість прийняття людиною помилкових або алогічних (нелогічних, суперечливих) рішень у конкретних ситуаціях зростає. Пов'язано це з недостатньою компетенцією або досвідом у особи, яка приймає рішення, що зумовлено відсутністю знань про подію чи явище, а також умінь і навичок прийняття рішень за нових умов.

Звідси залежність критичних інфраструктур від ІІСП спостерігається не тільки в тому, які

технології на основі штучного інтелекту використовуються, а й у тому, як організовано управління самими інфраструктурами. Тому постає проблема довіри ІІСП автоматично приймати рішення при управлінні КІ, якщо в них є уразливі елементи і присутній людський фактор. Зважаючи на цю особливість проблеми довіри ІІСП при моделюванні впливу загроз на критичні інфраструктури, пропонується такий підхід.

Щоб повніше розкрити людські і соціальні фактори, які впливають на функціонування критичної інфраструктури, скористаємося формулюванням із роботи [14], де КІ на функціональному рівні розглянуто як комбінація інтегрованих підсистем, структурованих у взаємозалежних рівнях: • системи моніторингу та контролю; • система оперативного управління; • організаційно-соціальна система з людським фактором впливу. Людський фактор найчастіше дається взнаки у вигляді некомпетентності від нестачі інформації чи досвіду при прийнятті рішення власником або оператором критичної інфраструктури (критичного інфраструктурного елемента). Системи контролю і оперативного управління являють собою технічні компоненти критичної інфраструктури. Організаційно-соціальна система є нетехнічним компонентом критичної інфраструктури, яка відбиває людські і соціальні чинники, що впливають на продуктивність системи. Таке подання критичної інфраструктури може допомогти у визначенні стратегій розробки, підтримки і підвищення ефективності критичних інфраструктур.

Наступним кроком у вирішенні проблеми довіри ІІСП пропонується визначити механізми протидії, якщо в КІ є уразливі елементи і присутній людський фактор. Для цього скористаємося властивістю гомеостазу складних систем (саморегуляції, адаптації), тобто здатності відкритої системи зберігати сталість свого внутрішнього стану за допомогою скоординованих реакцій, спрямованих на підтримку динамічної рівноваги. Упровадження інтелектуальних технологій дає можливість уведення самонавчальних інтелектуальних систем управління складними системами. В умовах постійного функціонування система управління складної системи (у нашому випадку критичної інфраструктури) за допомогою ІІСП повинна пристосовувати (адаптувати) її до нових умов функціонування. Адаптація може виявлятися в різних формах перетворення складної системи: саморегулювання, модифікація, реформування, реорганізація [3].

У разі впливу загроз у КІ передусім постає необхідність зміни в організаційній структурі інформаційної інфраструктури, тому вживаються заходи щодо реорганізації. Можна показати, що реорганізація є попередньою формою самоорганізації інтелектуальних систем. Справді, організаційна структура складається з безлічі взаємозалежних підсистем і елементів, всі вони безпосередньо або побічно впливають на ефективність досягнення ключових результатів. При цьому локальне поліпшення чогось одного в одному з них не свідчить про підвищення загальної результативності. Ефект синергії з'являється, коли знання і зусилля кількох елементів можуть організовуватися так, що вони взаємно посилюються. Тому за умов порушених причинно-наслідкових механізмів організаційної системи завдання органів управління полягає у прийнятті такого рішення, яке забезпечить виникнення ефекту синергії, а саме: провести підбір якостей та зв'язків елементів і підсистем, який гарантуватиме прийнятні результати, коли зміна зовнішніх умов завдяки реорганізації може також бути стимулюючим або переважним впливом.

ВИСНОВКИ

1. Розглянуто проблему щодо довіри до інтелектуальних систем автоматично приймати рішення при управлінні критичними інфраструктурами, якщо в них є уразливі елементи і присутній людський фактор.

2. Сформульовано і обґрунтовано новий підхід подання інформаційної інфраструктури у вигляді складної організаційної системи, який дозволяє виокремити найважливіші небезпеки рівня «загроза» для інтелектуальних систем, що впливають на уразливі елементи критичної інформаційної інфраструктури.

3. Виявлено загрози від інтелектуальних технологій для критичних інфраструктур.

Список використаної літератури

1. ***Катков Ю. І.*** *Аналіз причин критичних ситуацій в інформаційно-інтелектуальних систем // Зв'язок. 2018. №3. С. 12–19.*

2. ***Вишнівський В. В., Катков Ю. І., Сєрих С. О.*** *Роль і місце інформаційної інфраструктури під час виникнення явища критичності організаційної системи // Зв'язок. 2017. №5. С. 51–56.*

3. ***Даник Ю. Г., Катков Ю. І., Пічугін М. Ф.*** *Національна безпека: запобігання критичним ситуаціям: монографія. Житомир, 2006. 386 с.*

4. ***Вишнівський В. В., Катков Ю. І., Сєрих С. О.*** *Оцінювання процесів реорганізації системи з критичною інфраструктурою // Зв'язок. 2017. №6. С. 20–24.*

5. ***Класифікація*** *завдань, вирішуваних інтелектуальними інформаційними системами/ Інтелектуальні інформаційні системи — основи поняття та визначення [Електронний ресурс]. URL:*

http://mirznanii.com/a/308578-2/nformatika-nformatsyn-tekhnolog-2 (Дата перегляду: 05.05.2019).

6. **Інтелектуальні** інформаційні технології та системи (реферат. огляд). Київ, 2016. 49 с. [Електронний ресурс]. URL:
http://www.nbuv.gov.ua/sites/default/files/all_files/references/201603/vtdo_ro_7.pdf (Дата перегляду: 05.05.2019).

7. **Величко О. Ф., Затинайко О. І., Скурський П. П.** Критичні технології як національний пріоритет у забезпеченні обороноздатності держави // Наука і оборона. 2011. № 4. С. 23–30.

8. **Типова** схема функціонування інтелектуальної системи [Електронний ресурс]. URL:
https://megapredmet.ru/1-80951.html (Дата перегляду: 05.05.2019).

9. **Власова Г. В.** Індексування як процес аналітико-синтетичної переробки інформації: навч. посіб. Київ, 2006. С. 172.

10. **Сукиасян Э. Р.** Школа индексирования: практ. пособие. Москва, 2005. 143 с.

11. **Кушнаренко Н. Н.** Документоведение: уч. 7-е изд., стер. Київ, 2006. 459 с.

12. **Координатне** (посткоординатне) індексування в електронному просторі як ефективний засіб створення пошукового образу документа [Електронний ресурс]. URL:
https://www.libr.dp.ua/text/vkp_2012_1_6.pdf (Дата перегляду: 05.05.2019).

13. **Процесори** Intel не отримали захист від Spectre і Meltdown [Електронний ресурс]. URL:
https://news.finance.ua/ua/news/-/436454/protsesory-intel-ne-otrymaly-zahyst-vid-spectre-i-meltdown (Дата перегляду: 05.05.2019).

14. **Лапин Н. И., Коржева Э. М., Наумова Н. Ф.** Теория и практика социального планирования. Москва, 1975. 245 с.

Рецензент: доктор техн. наук, професор **В. В. Вишнівський**, Державний університет телекомунікацій, Київ.

Ю. И. Катков, М. В. Хоменко

УГРОЗЫ ОТ ИНТЕЛЛЕКТУАЛЬНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ ПОИСКА ДЛЯ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Рассмотрены вопросы проявления уязвимости элементов интеллектуальной информационной системы поиска информации. Интеллектуальная информационная система поиска информации рассматривается как составная часть критической инфраструктуры системы управления в сложной организационной системе. Критическая инфраструктура — это система, в которой отказ (полностью или частично) уязвимого элемента может вызвать цепочку отказов в сложной организационной системе взаимосвязанных других элементов и поэтому значительно влияет на безопасность и благосостояния в различных сферах обеспечения основных человеческих потребностей. В XXI веке критические инфраструктуры становятся все более зависимыми от нового вида угроз — внедрение современных технологий на основе искусственного интеллекта. На основе этих технологий создаются интеллектуальные системы, от которых зависит основная функциональность критической инфраструктуры. Возникает вопрос: можно ли доверять интеллектуальным системам автоматически принимать решения, если в них есть уязвимые элементы и присутствует человеческий фактор? Поэтому зависимость критических инфраструктур от интеллектуальных систем проявляется не только в том, какие технологии на основе искусственного интеллекта используются, но и в том, какая организация управления принята самыми инфраструктурами. Анализ зависимости критических инфраструктур от угроз является сложной вычислительной проблемой. В этом исследовании представлено описание проблемы проявления уязвимости элементов интеллектуальной информационной системы поиска информации, которая входит в состав инфраструктуры системы управления сложной организационной системы. Цель этой статьи — выявить уязвимые элементы интеллектуальных информационных систем поиска, а также определить их последствия для обеспечения безопасности и стабильности инфраструктуры и наметить меры по защите.

Ключевые слова: интеллектуальная информационная система поиска информации; критическая инфраструктура; уязвимые элементы.

Yu. I. Katkov, M. V. Khomenko

THREATS FROM INTELLIGENT INFORMATION SEARCH SYSTEMS FOR CRITICAL INFRASTRUCTURES

The article deals with issues of manifestation of the vulnerability of elements of the intellectual information system of information seeking. Intellectual information search information system is considered as an integral part of the critical infrastructure of a management system in a complex organizational system. Critical infrastructure is a system in which a failure (totally or partially) of a vulnerable element can cause a failure chain in a complex organizational system of interconnected other elements and therefore significantly affects security and well-being in various areas of basic human needs. In the twenty-first century, critical infrastructures are becoming increasingly dependent on new types of threats — the introduction of modern technologies based on artificial intelligence. Based on these technologies, intelligent systems are created, on which the critical functionality of the critical infrastructure depends. The question arises: can I trust the intelligent systems, automatically make decisions if they have vulnerable elements and the human factor is present? Therefore, the dependence of critical infrastructures on intellectual systems is manifested not only in the technology used on the basis of artificial intelligence, but also in the management organization adopted by the infrastructures itself. An analysis of the dependence of critical infrastructures on threats is a complex computational problem. This research presents the description of the problem of vulnerability of the elements of the intelligent information search information system, which is part of the infrastructure of the management system of a complex organizational system. The purpose of this article is to identify vulnerable elements of intelligent search information systems, as well as to determine their implications for security and stability of the infrastructure and to identify protective measures.

Keywords: Intellectual information system of information retrieval; critical infrastructure; vulnerable elements.