Юзікова Н.С.

доктор юридичних наук, доцент, професор кафедри адміністративного і кримінального права Дніпровського національного університету імені Олеся Гончара

Yusikova N.S.

Doctor of Law, Associate Professor, Professor of the Department of Administrative and Criminal Law of Dniprovsky National University named after Oles Gonchar

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СИСТЕМІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

Актуальність кримінологічних досліджень факторів, що детермінують злочинність, загострюють криміногенну ситуацію, і відповідно пошук інноваційних ефективних заходів запобігання новим проявам злочинності у контексті сучасних глобалізаційних процесів, потужних кібератак набуває першочергового значення. Небезпека, руйнівні наслідки соціального, особистісного та техногенного характеру, які спричиняє злочинність вимагають сучасних специфічних заходів реагування та протидії.

Кризова ситуація, в якій опинилася держава, негативно впливає на зміну суспільних цінностей, розшарування населення за рівнем доходів, призводить до дисфункціональності соціальних інститутів та моральної дезорієнтації частини суспільства.

Екологічні катастрофи, загрози терористичної, екстремістської діяльності та радикалізації терористичного руху, кіберзлочинність негативно відзеркаліються на функціонуванні об'єктів критичної інфраструктури держави, а відповідно на рівні безпеки суспільства. Це, у свою чергу, потребує особливої уваги з боку держави до своєчасного виявлення ризиків, загроз і забезпечення невідкладного реагування на них, а також формування належної системи захисту критичної інфраструктури, що ґрунтується на відповідному інформаційному полі, має належне правове та технічне забезпечення.

Чим більше інформації у арсеналі правоохоронних органів та наукової спільноти, тим краще розуміння природи небезпеки, вчасного визначення загроз і ризиків та більше можливостей для особливих заходів системи захисту критичної інфраструктури в Україні та світі.

Залучення України до міжнародного обміну інформацією щодо критичних інфраструктур є прийнятним для української превентивної діяльності. Це сприятиме своєчасному розпізнанню загроз, які з'явилася у зв'язку із стрімким розвитком технологій, активною міграцією та ризиками окремих радикально налаштованих громадян, терористичних груп та угрупувань.

Підґрунтя ефективного захисту критичних інфраструктур, відповідно до Директиви «Про європейські критичні інфраструктури та заходи по їх захисту» від 08.12.2008 року, становить розробка загальних методик ідентифікації та класифікації ризиків, загроз та уразливих місць у активах інфраструктури. Крім того їх захист потребує взаємодії, координації і співробітництва на національному рівні та на рівні держав-членів ЄС [1]. Принципи запровадження Європейської програми захисту критичної інфраструктури охоплюють: субсидіарність, взаємодоповнення, конфіденційність, співробітництво, пропорційність, поетапний підхід [2] Крім того, Європейська Комісія рекомендувала країнам ЄС вжити низку заходів спрямованих на захист критичної інфраструктури, більшість з яких знайшли відображення у Концепції створення державної системи захисту критичної інфраструктури, схваленій розпорядженням Кабінету Міністрів України від 6.12.2017р.

Аналізуючи правове забезпечення захисту критичної інфраструктури європейських країн Д.Бірюков зазначає, що на сьогодні концепція захисту критичної інфраструктури імплементована як в загальноєвропейському законодавстві, так і в національних законодавствах окремих країн – членів ЄС. Загальноєвропейською критичною інфраструктурою вважається та, що має транскордонне, в межах ЄС, значення [3]. При цьому, автор слушно зауважує, що Україна за своїм географічним розташуванням є частиною енергетичного та транспортного панєвропейського простору та відповідно пов'язана із європейською критичною інфраструктурою, що відкриває можливості для співпраці у сфері захисту критичної інфраструктури між вповноваженими органами влади України та країн ЄС.

Відповідно до постанови Кабінету Міністрів «Про затвердження порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» від 23.08.2016р. під критичною інфраструктурою розуміється сукупність об'єктів інфраструктури держави, які є найбільш важливими для економіки та промисловості, функціонування суспільства та безпеки населення і виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону,

природне середовище, призвести до значних фінансових збитків та людських жертв.

Критична інфраструктура США - це основа, на якій базуються економіка, безпека і здоров'я країни. Критична інфраструктура підтримує американський спосіб життя і зміцнює національну конкурентоспроможність. Інфраструктура зберігає здорову економіку, утримуючи мільйони працюючих і підтримуючи й розвиваючи інноваційні технології сприяє поліпшенню добробуту американців. Інфраструктура країни складається з 16 секторів. Найбільш важливими є об'єкти, що стосуються сфери водопостачання, енергетики, транспорту і палива. Національна інфраструктура (Nation) також включає кібер-технологію. Департамент внутрішньої безпеки США наголошує, що значна кількість активів інфраструктури США наближається до кінця їх запланованих термінів життя. Скорочення бюджету в федеральних, державних і місцевих органах влади обмежує фінансування для інспекцій інфраструктури, технічного обслуговування, модернізації і ремонту. У деяких критично важливих секторах інфраструктури нестача робочої сили в найближчі десятиліття, ймовірно, буде заважати зусиллям, спрямованим на впровадження і підтримку критичної модернізації інфраструктури. Ризик відмови в системах транспортування, енергії, води та стічних вод, а також в секторах гребель, швидше за все, зросте протягом наступних 10 років. При цьому, забезпечення безпеки і стійкості критично важливої інфраструктури є національним пріоритетом, який вимагає планування і координації державного управління та приватного сектора на всіх рівнях. Поліпшення доріг, мостів, водних систем, електричних мереж та інших життєво важливих інфраструктурних систем вимагає інновацій, інвестицій та спільних зобов'язань [4].

Ефективний захист передбачає використання новітніх технологій та останніх інноваційних досягнень людства. До яких безперечно належить розвиток и запровадження у різні сфери штучного інтелекту. Дослідження та інтеграція зарубіжного досвіду у цій сфері є найкращою інвестицією у формування вітчизняних форм і напрямів захисту критичної інфраструктури в Україні, сприятиме своєчасному виявленню ризиків, загроз.

Штучний інтелект визначається як наука та технологія, що охоплює автоматизацію розумної поведінки та пов'язана зі створенням інтелектуальних машин, комп'ютерних програм. Метою штучного інтелекту виступає створення технічних систем, які здатні вирішувати завдання не розрахункового характеру і виконувати дії, що вимагають переробки змістовної інформації притаманної людській розумовій діяльності. Одним з важливих завдань штучного інтелекту є створенні інтелектуальних

роботів здатних автономно здійснювати операції по досягненню цілей, поставлених людиною із можливістю корективи дій.

Кібербезпека виступає базовим фактором у сучасній системі захисту критичної інфраструктури. Кібератака у травні минулого року «WannaCry» слугувала нагадуванням про небезпеку, що створюється шкідливими програмами та спричинила мільйонні збитки [5]. Захист критичної національної інфраструктури особливо важливий, оскільки вдала кібератака на об'єкти критичної інфраструктури таких галузей як енергетика, хімічна промисловість, транспорт, екологія, продовольство та інші стратегічно важливі для функціонування економіки і безпеки держави, суспільства й громади сфери, впливає на національну безпеку і оборону, природне середовище та може призвести до фінансових збитків та людських жертв. Важливо зауважити, що у сучасному світі руйнівні наслідки кіберзагроз продовжують зростати. Крім того, глобальний вплив онлайн-ресурсів, мережі Інтернет та її складових представляє зростаючий масив ризиків та уразливих місць у активах інфраструктури для кіберзлочинців, які можуть їх використовувати.

Thales AI-powered Cybels Sensor tool забезпечує сучасний захист від кібератак на об'єкти критичної інфраструктури. Cybels Sensor шляхом умонтування штучного інтелекту постійно спостерігає за будь якими джерелами атаки. Експерти лабораторії Thales фіксують новітні види шкідливих програм. При цьому архітектура програмного забезпечення Cybels Sensor виявляє загрозу та маскує цю сигнатуру, щоб кіберзлочинці не знали про викриття та виявлення вірусу, тим самим ускладнюючи злочинцю можливість обійти захист.

Агентство національної безпеки Франції вивчає систему захисту Thales, при цьому La Poste (Французька поштова служба) використовує датчик виявлення кібератак Cybels Sensor.

Cybels Sensor загружений поведінковими алгоритмами, які здатні відмічати будь-яку активність, що штучний інтелект вважає ненормальною. Також він здатний аналізувати кожен файл, що проходить крізь мережу, досліджуючи і виявляючи можливі загрози, шкідливі програми та інші аномалії.

Створення кібербезпечного простору для захисту критичної інфраструктури охоплює: з одного боку, інформацію про особу від якої може бути кіберзагроза, з іншого, знання про різні форми небезпеки, що проявляються у шпіонських програмах, вірусах, троянських програмах, фільтрації, розкритті даних тощо.

Інформація щодо профілю, мотивації, стратегії злочинців дає можливість розрізняти рівень загрози об'єкти посягання, а відповідно обирати форму і ступінь захисту. Розрізняють декілька типів осіб, що здійснюють кібератаку: групи активістів-анонімів, які здійснюють атаки на компанії з політичних ідеологічних або соціальних мотивів; молодь, яку приваблює можливість самоствердження шляхом втручання та проникнення у систему захисту підприємств, установ; кібер-терористи, які посягають на стратегічні об'єкти, компрометуючи владу, порушуючи безпеку у державі та переслідуючи інші цілі; кібер-злочинці, які викрадають або вимагають гроші, шукають шляхи незаконного збагачення; цілеспрямовані найманці (кібер-пірати), які здійснюють вторгнення, створюючи загрозу та фінансуються з метою викрадення інформації або дестабілізації ситуації [6].

Для протидії цим численним та швидкоплинним загрозам експерти з кібербезпеки Thales надають зацікавленим підприємствам, установам, агентствам з безпеки у оборонній, енергетичній, морській, фінансовій та інших сферах консалдінгові послуги й рішення, що адаптовані до конкретної ситуації загрози, ризику чи уразливих місць. Фахівці з кібернетики Thales здійснюють аналіз профіля об'єкту захисту підприємств з метою виявлення потенційних шляхів атак, засобів розповсюдження, виявлення кола можливих агресорів. Здійснюється моніторинг, виявлення та реагування для відповідної матриці загроз щодо кожного підприємства. Зміст стратегії захисту критичної інфраструктури охоплюється наступним: навіть самі темні провулки можна зробити безпечними, якщо знати де сяє світло.

1. *Council Directive 2008/114/EC «On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection». – [Електронний ресурс]. – Режим доступу : http:// eur-lex.europa.eu/*
2. *Communication from the commission on a European Programme for Critical Infrastructure Protection // Commission of the European Communities (COM/2006/786 final) 786. – [Електронний ресурс]. – Режим доступу : http://eur-lex.europa.eu/*
3. *Бірюков Д. Концепція захисту критичної інфраструктури як елемент загальноєвропейської безпекової політики // Наукові записки. Випуск – 6(68). [Електронний ресурс]. – Режим доступу: - http://www.ipiend. gov.ua/uploads/nz/nz_68/birukov_kontseptsia.pdf*

4. *Critical Infrastructure DHS 2025 Strategic Risk Assessment. [Електронний ресурс]. – Режим доступу: https://publicintelligence.net/dhs-ocia-critical-infrastructure-2025/*
5. *Leveraging artificial intelligence to maximize critical infrastructure cybersecurity. [Електронний ресурс]. – Режим доступу: https://www.thalesgroup.com/en/worldwide/security/magazine/leveraging-artificial-intelligence-maximize-critical-infrastructure*
6. *Threat intelligence: forewarned is forearmed. [Електронний ресурс] . – Режим доступу: https://www.thalesgroup.com/en/worldwide/security/magazine/threat-intelligence-forewarned-forearmed*

Юзікова Н.С. Перспективи використання штучного інтелекту у системі захисту критичної інфраструктури в Україні

Кризова ситуація, в якій опинилася держава, негативно впливає на зміну суспільних цінностей, розшарування населення за рівнем доходів, призводить до дисфункціональності соціальних інститутів та моральної дезорієнтації частини суспільства.

Екологічні катастрофи, загрози терористичної, екстремістської діяльності та радикалізації терористичного руху, кіберзлочинність негативно відзеркалюються на функціонуванні об'єктів критичної інфраструктури держави, а відповідно на рівні безпеки суспільства. Це, у свою чергу, потребує особливої уваги з боку держави до своєчасного виявлення ризиків, загроз і забезпечення невідкладного реагування на них, а також формування належної системи захисту критичної інфраструктури, що ґрунтується на відповідному інформаційному полі, має належне правове та технічне забезпечення.

Чим більше інформації у арсеналі правоохоронних органів та наукової спільноти, тим краще розуміння природи небезпеки, вчасного визначення загроз і ризиків та більше можливостей для особливих заходів системи захисту критичної інфраструктури в Україні та світі.

Ключові слова: штучний інтелект, захист критичної інфраструктури

Yusikova N.S. Perspectives of using artificial intelligence in critical infrastructure protection system in Ukraine

The crisis situation in which the state was, negatively affects the change of social values, the stratification of the population by income, leads to dysfunctionality of social institutions and moral disorientation of a part of society.

Environmental disasters, threats of terrorist activity, extremist activity and the radicalization of the terrorist movement, cybercrime are negatively reflected in the functioning of critical infrastructure objects of the state, and accordingly, at the level of social security. This, in turn, requires the state to pay particular attention to timely detection of risks, threats and emergency response, as well as appropriate legal and technical support for the establishment of a proper critical infrastructure protection system based on the relevant information field.

The more information in the arsenal of law enforcement and the scientific community, the better understanding of the nature of danger, the timely identification of threats and risks, and more opportunities for special measures of the critical infrastructure protection system in Ukraine and in the world.

Key words: artificial intelligence, protection of critical infrastructure