надає нові можливості для управління інфраструктурою, забезпечуючи контроль за станом пристроїв у реальному часі. Загалом управління ІТ-проєктами в умовах цифровізації вимагає від менеджерів гнучкості, інноваційного підходу та готовності до постійного навчання. Цифрові технології надають нові інструменти для підвищення ефективності, але водночас створюють нові виклики, які необхідно долати для досягнення успіху.

СПИСОК ВИКОРИСТАНИХ ПОСИЛАНЬ

1. Schwaber K., Sutherland J. The scrum guide. 2020. 13 p.
2. Карпенко А. В., Карпенко Н. М. Формування проєктної команди у кластерних організаціях. *Домінанти розвитку HR-інжинірингу, економіки і бізнесу у XXI столітті в умовах перманентної трансформації національної і світової економік:* матеріали II Міжнародної науково-практичної конференції, присвяченої 60-річчю Хмельницького національного університету (17–18 листопада 2022 р., м. Хмельницький). Хмельницький: Хмельницький національний університет, 2022. С. 296–299.
3. Cockburn A., Highsmith J. Agile software development: The people factor. Computer. 2001. Vol. 34, iss. 11. P. 131–133.

ЗАХИЩЕНІСТЬ ПЕРСОНАЛЬНИХ ДАНИХ ФІЗИЧНИХ ОСІБ ЯК ФАКТОР НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Климанський В. І.
Державний торговельно-економічний університет, Київ (Україна)
e-mail: v.klymanskyy@knute.edu.ua

Захист персональних даних клієнтів став викликом для бізнесу в умовах війни, адже компанії зіштовхуються з постійними кібератаками з боку держави-агресора, спрямованими на викрадення інформації про клієнтів.

Однією з найбільших кіберзагроз для населення залишається фішинг, за допомогою якого злочинці можуть отримати несанкціонований до персональних даних, як-от контактні дані, банківські рахунки та інша чутлива інформація.

Згідно з даними сервісу opendatabot, кожен дев’ятий опитаний українець ставав жертвою шахраїв від початку повномасштабного вторгнення. За результатами опитування було виявлено, що 11 % українців стали жертвою шахраїв від початку повномасштабного вторгнення. На частку купівля / продажу товару в інтернеті припадає 52,7 % усіх шахрайств, а на шахрайські посилання ще 18,6 %. Ще 12 % припадає на злами приватних соціальних мереж [1]. Для порівняння, за вісім місяців 2023 року в Україні було відкрито майже 60 тисяч проваджень про шахрайство за ст. 190 ККУ. Це більше, ніж загалом за два попередні 2 роки: так, у 2021 році було відкрито 23,8 тисяч проваджень, а у 2022 році – 32 тисячі [2].

Одним із прикладів ІТ-ініціативи на рівні держави є платформа «Дія», яка стала одним з основних засобів доступу до державних послуг. Використовуючи систему «Дія», громадяни можуть отримувати різноманітні сервіси, що значно

скорочує потребу у фізичному контакті з урядовими установами, що особливо актуально під час війни. Це знижує ризики атак на фізичну інфраструктуру, але водночас може сприяти підвищенню ризиків національного суверенітету в інформаційному просторі. Ще до початку повномасштабного вторгнення РФ в Україну портал «Дія» було неодноразово атаковано хакерами, і хоча офіційні особи заявляють, що особисті дані не були втрачені, багато українців підозрювали саме нещодавню атаку на сервер причиною витоку персональних даних [3].

Отже, система надання послуг не може бути на 100 % захищена і гарантувати абсолютну захищеність персональних даних. Це доводить, до саме під час великих соціальних зрушень та загроз, зокрема війни, зростають кіберризики, і питання кібербезпеки наразі є як ніколи актуальним. А отже, кібербезпека актуальна для електронної комерції та інших онлайн-майданчиків надання послуг.

Забезпечення безпеки платіжної інформації стає пріоритетом для банків, платіжних систем та інтернет-магазинів. Для боротьби з такими загрозами компанії впроваджують сучасні системи кіберзахисту, зокрема автоматизовані системи відстеження аномалій, біометричні методи автентифікації та блокчейн-рішення для підвищення безпеки транзакцій [4].

Найбільші онлайн-постачальники цифрових продуктів для створення власних інтернет-магазинів, як-от Shopify, головними кіберзагрозами для діяльності електронної комерції визначають DDoS-атаки, витоки персональних даних, платіжне шахрайство, шкідливе програмне забезпечення, яке може бути встановлене несанкціоновано, та програми-вимагачі, загрози злому доступу до адміністративних налаштувань вебсайтів та основного коду тощо [5]. І це ще не весь список потенційних загроз, із якими може зіткнутися вебсайт електронної комерції.

Бізнесам, які оперують у сфері електронної торгівлі, варто серйозно сприймати загрозу кібершахрайства та більше ресурсів приділяти власній інтернет-безпеці і безпеці персональних даних користувачів, які можуть бути доступними бізнесу задля обробки замовлень товарів або послуг. З огляду на масштаб проблеми та загрози масових втрат персональних даних фізичних осіб, зниження рівня діяльності чи повну зупинку такої серед приватних бізнесів чи державних установ підвищення рівня кібербезпеки в умовах ведення повномасштабної війни стає критично важливим для України і напряму стосується національної безпеки країни.

Звичайно, кібербезпека державних організацій, каналів передачі інформації, зв’язку військових, фінансових та енергетичних об’єктів є критично пріоритетною в сучасних умовах. Першочергова ціль існування держави як соціального та політичного утворення полягає в забезпеченні безпечної життєдіяльності її громадян, тож втручання у кіберсферу суверенної країни і перешкоджання діяльності приватних компаній, життю і комфорту громадян варто розглядати як чергову загрозу безпеці та втручання у національні інтереси суверенної держави.

СПИСОК ВИКОРИСТАНИХ ПОСИЛАНЬ

1. Кожен дев'ятий опитаний українець ставав жертвою шахраїв від початку повномасштабного вторгнення. *Сервіс статистики opendatabot.* 09.10.2023. URL: https://opendatabot.ua/analytics/stopfraud-nbu
2. Кількість справ про шахрайство у 2023 році сягнула історичного антирекорду. *Сервіс статистики opendatabot.* 02.10.2023. URL: https://opendatabot.ua/analytics/fraud-pandemic-2
3. З «Дії» чи ні? Звідки хакери взяли персональні дані 2 млн українців. *Розслідування DOU.* 28.01.2022. URL: https://dou.ua/lenta/articles/inquiry-about-diia-data-leak/
4. Ковальчук В. П. «Захист персональних даних у бізнесі: виклики та рішення». *Журнал корпоративної безпеки.* 2023. № 3. С. 59–74.
5. How To Improve Ecommerce Security for Your Online Store. Shopify Blog. URL: https://www.shopify.com/blog/ecommerce-security

ВИЯВЛЕННЯ ТА ВІДСТЕЖЕННЯ ОБ'ЄКТІВ БПЛА У РЕАЛЬНОМУ ЧАСІ НА ОСНОВІ CNN

Колосова К. К.[1*], Січко Т. В.[2*]

[1,2]Донецький національний університет імені Василя Стуса, Вінниця (Україна)

[*]e-mail: kolosova.k@donnu.edu.ua

Тема дослідження полягає у виявленні та відстеженні об'єктів у режимі реального часу за допомогою безпілотних літальних апаратів (БПЛА) на основі згорткових нейронних мереж (CNN). Ця технологія має велике значення в різних сферах, зокрема у військовій діяльності, рятувальних операціях, сільському господарстві, захисті території, моніторингу інфраструктури та охороні навколишнього середовища.

CNN є потужним інструментом у сфері комп'ютерного зору завдяки своїй здатності автоматично виявляти та розпізнавати об'єкти у складних умовах, зокрема за змінного освітлення, різних погодних умов та руху камери. Внаслідок інтеграція CNN із дронами можна отримувати відеопотоки в режимі реального часу та обробляти їх для відстеження об'єктів, зокрема людей, транспортні засоби чи інші цілі, що робить систему надзвичайно ефективною та гнучкою [1].

Основним завданням є забезпечення високої точності та швидкості обробки даних, особливо під час роботи у складних умовах, а також оптимізація ресурсів для роботи на мобільних платформах, як-от дрони.

Виявлення та відстеження об'єктів за допомогою безпілотних літальних апаратів (БПЛА) у режимі реального часу охоплює кілька ключових викликів:

- обмежені ресурси обробки: БПЛА мають обмежені апаратні ресурси, тому вони не можуть застосовувати передові моделі CNN для швидкої обробки великих обсягів даних у реальному часі;
- нестабільність зображення: це пов'язано з тим, що БПЛА є мобільним, тому якість відеопотоку погіршується через коливання умов освітлення, погодних явищ і вібрації, що впливає на точність виявлення та відстеження об'єктів;