Перевалов Н.Ю., Курсант факультету №4
Лучик С.Д., доктор економічних наук, професор
Харківський національний університет внутрішніх справ
м. Кам'янець-Подільський, Україна

ШТУЧНИЙ ІНТЕЛЕКТ НА ЗАХИСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БІЗНЕСУ

Сьогодні кібербезпека є одним із пріоритетів у системі національної безпеки України. 14 травня 2021 року Рада національної безпеки і оборони України схвалила Стратегію кібербезпека України на 2021-2025 роки, що дозволяє фінансувати та здійснювати заходи, спрямовані на протидію кіберзлочинності. Кібербезпека є обов'язковою складовою успішного бізнесу.

Бізнес-структури сьогодні працюють з великими обсягами інформації, здійснюють обробку значної кількості клієнтських даних з використанням інформаційних та цифрових технологій. Кожна складова бізнес-процесів представляє лише окрему ланку в нескінченному ланцюзі взаємопов'язаних елементів. Сьогодні компаніям складніше ніж коли-небудь чітко визначити критичні точки у власній багатогранній інфраструктурі через яку вони взаємодіють з оточуючим світом [1].

Сьогодні компанії використовують в своїй діяльності новітні інформаційні, цифрові технології і процеси, а також застосовують нові принципи організації праці. І на тлі стрімкого розвитку сучасних комп'ютерних технологій спостерігається загальносвітова закономірна тенденція до збільшення кількості та масштабів правопорушень у кіберсфері. Атаки поступово стають все більш витонченими, а потенційні цілі, серед яких зараз більше об'єктів критичної інфраструктури на тлі загострення політичної ситуації в країні, та збитків від атак, зростають. Сьогодні в інтернеті кожні 39 секунд відбувається нова атака, яка коштує трильйони доларів щорічно. Ці атаки можуть бути надзвичайно шкідливими для бізнесу, коштуючи непомірних доларів і відновлення ресурсів [2].

Найбільшими внутрішніми загрозами для захисту інформації на підприємствах є витоки даних через співробітників або з їх вини та вразливе програмне забезпечення. Серед зовнішніх загроз бізнесу виділяють шкідливе програмне забезпечення; DDoS-атаки; фішингові атаки; проникнення у мережу; втрата пристроїв зі збереженими паролями. Боротись або попереджати такі серйозні загрози компаніям нелегко. Да й не завжди вони ставляться до проблеми кіберзахисту даних професійно та відповідально. Так, бізнес ненавчений використовувати надійне антивірусне програмне забезпечення чи спеціалізовані рішення щодо захисту від DDoS-атак, вживати надійних дій для захисту інформації та фінансових транзакцій.

Значну роль у кібербезпеці сьогодні відводять штучному інтелекту. З одного боку, компанії намагаються використовувати штучний інтелект (ШІ) різними способами для підвищення ефективності, економії часу та зменшення витрат. І саме завдяки цьому ШІ швидко стає цінним ресурсом для компаній у різних сферах діяльності.

З іншого боку, більше половини власників бізнесу використовують штучний інтелект для кібербезпеки та боротьби з шахрайством [3]. Оскільки штучний інтелект стає все більш інтегрованим у бізнес-операції, тому компаніям слід приділяти першочергову увагу кібербезпеці, управлінню, відповідності та захисту даних, щоб забезпечити успішну готовність до внутрішнього ШІ. Так, можливості, які пропонує штучний інтелект для аналізу великих обсягів даних на основі алгоритмів машинного навчання, істотно допомагають у вирішенні існуючих проблем співробітників, які перевантажені аналізом логів, запобіганням спроб злому, розслідуванням можливих випадків шахрайства і нестачі персоналу. На відміну від інструментів виявлення на основі сигнатур попереднього покоління, машинне навчання може відстежувати та записувати моделі використання мережі та надавати раннє попередження про виявлення аномальної поведінки.

Експерти з кібербезпеки рекомендують бізнес-структурам готуватися до внутрішнього розгортання штучного інтелекту і зосередитися на таких заходах кібербезпеки.

Безпека кінцевих точок: Рішення безпеки кінцевих точок, такі як антивірусне програмне забезпечення та брандмауери, можуть захистити системи та дані штучного інтелекту від несанкціонованого доступу та кіберзагроз.

Безпечний зв'язок: Захищені протоколи зв'язку, такі як шифрування SSL/TLS та віртуальні приватні мережі (VPN), можуть захистити дані під час передання між системами штучного інтелекту та іншими кінцевими точками.

Шифрування даних: Шифрування може захистити конфіденційні дані від несанкціонованого доступу, шифруючи дані в стані спокою та під час передання.

Управління вразливостями: регулярна оцінка вразливостей та тестування на проникнення може допомогти компаніям виявляти та усувати вразливості в системах і даних штучного інтелекту [4].

Не слід забувати, що широке впровадження штучного інтелекту в бізнес-структурах матиме як позитивні, так і негативні наслідки для кібербезпеки. Як власники бізнесу намагаються ефективно використовувати штучний інтелект для підвищення кіберзахисту своїх даних, так і хакери також навчаються на наявних інструментах штучного інтелекту розробці більш просунутих атак на традиційні системи безпеки і, навіть, системи, посилені штучним інтелектом. Щоб компанія була повністю готова до штучного інтелекту, потрібно комплексно підходити до питань управління, дотримання вимог і кіберзахисту інформації.

Література:

1. Кібербезпека бізнесу це не лише технічні заходи. *Legal IT Group.* URL: https://legalitgroup.com/kiberbezpeka-biznesu-tse-ne-lishe-tehnichni-zahodi/ (дата звернення: 30.11.2023).

2. Що потрібно знати бізнесу про кібербезпеку у 2023 році. *BDO Україна.* URL: https://www.bdo.ua/uk-ua/insights-2/information-materials/2023/what-businesses-need-to-know-about-cybersecurity-in-2023 (дата звернення: 01.12.2023).

3. How Businesses Are Using Artificial Intelligence In 2023. *Forbes Advisor*. URL: https://www.forbes.com/advisor/business/software/ai-in-business/ (дата звернення: 02.12.2023).

4. Чотири питання щодо кібербезпеки при впровадженні ШІ. *EBA.* https://eba.com.ua/4-pytannya-shhodo-kiberbezpeky-pry-vprovadzhenni-shi/ (дата звернення: 04.12.2023).

Перевозчикова А. А., здобувачка другого (магістерського) рівня вищої освіти
Київський національний університет ім. Т. Шевченка,
м. Київ, Україна

ДИВЕРСИФІКАЦІЯ ЯК ІНСТРУМЕНТ ПОДОЛАННЯ НАСЛІДКІВ ВІЙНИ

За сучасних умов підприємства, незалежно від галузі та масштабів діяльності, постійно стикаються з різними ризиками. Вони можуть бути пов'язані з економічними, політичними, соціальними та іншими факторами. Але особливо бізнес найбільш вразливий в період війни. Загальними причинами цього можна вважати макроекономічну нестабільність, зниження рівня купівельної спроможності населення, втрату ланцюжків постачання великої кількості товарів, дефіцит та зростання цін на паливно-мастильні матеріали тощо [4, с. 86]. За результатами опитування Європейської Бізнес Асоціації серед представників малого та середнього бізнесу втрати для бізнесу, спричинені війною, безперервно зростають, і лише 6% підприємців не зазнали негативних наслідків цієї кризи. Безпосередньо внаслідок