Ро́боти також небезпечні

Сергій Чеберячко, професор кафедри охорони праці та цивільної безпеки НТУ «Дніпровська політехніка», д-р техн. наук

Олена Лавренюк, доцент кафедри процесів горіння та загальної хімії Львівського державного університету безпеки життєдіяльності, канд. техн. наук

Олена Яворська, професор кафедри охорони праці та цивільної безпеки НТУ «Дніпровська політехніка», канд. техн. наук

Владислав Лісовенко, здобувач другого магістерського рівня за спеціальністю 263 Цивільна безпека НТУ «Дніпровська політехніка»

Як за допомогою моделювання майбутнього в стилі Tech Noir можна навчити людину мислити ризикорієнтовно. Пропонуємо кейс з оцінки ризику небезпеки для людини від використання робототехніки.

Працівники підприємств часто не усвідомлюють рівня загроз, які можуть виникнути під час виробничої діяльності. Так, на думку більшості, виконання правил безпеки – обтяжлива, непотрібна процедура, їх порушення не завжди призводить до травмування. Крім того, однією з основних причин інцидентів, нещасних випадків та аварійних ситуацій є людська помилка, коли людина втрачає реакцію або ж її реакція на наявну небезпеку є неадекватною. Отже, постає потреба у формуванні відповідального ставлення працівника до потенційних джерел небезпек, моделі поведінки, направленої на збереження його життя та здоров'я.

Водночас працівники вже мають певні переконання, підкріплені:

- ☑ власним світоглядом, який впливає на інтерпретацію здобутої інформації;
- ☑ розумовими здібностями, які відповідають за адекватний аналіз ситуації;
- ☑ упередженістю, коли працівник намагається знайти підтвердження своїх висновків, а не розібратись у ситуації;
- ☑ стереотипністю, тобто приймається рішення за визначеним раніше шаблоном, та ін.

Значний вплив на поведінку працівника також має колективна думка, що інколи призводить до прийняття рішення без аналізу небезпечної ситуації. Такий висновок робить Виконавчий орган з охорони праці у Великобританії (HSE) у керівництві HSG 48 «*Зменшення помилок та вплив на поведінку*». У дослідженні зазначається: «якщо керівники та менеджери потурають неадекватній поведінці та не подають доброго прикладу працівникам, імовірність того, що це стане нормою у поведінці збільшується».

У СТИЛІ TECH NOIR

Змінити ситуацію можливо через організацію постійного навчання працівників та формування у них ризикоорієнтованого мислення. Однак просте викладання лекційного матеріалу не дає змоги постійно підтримувати інтерес здобувача освіти до предмету вивчення. Тому постає завдання щодо пошуку різноманітних наукових кейсів, які б викликали бажання пізнавати нове, досліджувати, розвиватись. Головне – знайти тематику, яка б була цікава для аудиторії та відповідала предметній галузі дисципліни.

Одним із таких наукових кейсів, який застосовується на заняттях з цивільної безпеки, є дослідження майбутнього в стилі **Tech Noir**.

> Стиль **Tech Noir** – гібрид наукової фантастики зі стильними голлівудськими фільмами, які прогнозують розвиток нашого суспільства. Він представляє нові технології як руйнівну та дисипативну (от лат. *dissipatio* – «рассеиваю, разрушаю») силу, що загрожує кожному аспекту людської діяльності.

Такий погляд на майбутнє відкриває **широке поле можливостей для розвитку пізнавальної сфери здобувачів та формування в них ризикоорієнтованого мислення** – основи сучасного управління ризиками. У цьому контексті **досить просто стимулювати** розвиток відповідних психічних (психомоторних) процесів, які пов'язані з інстинктом самозбереження; **формування навичок** усвідомленого ставлення до безпеки, виявлення потенційних загроз і вироблення відповідного світогляду. Виконання подібних досліджень навчає здобувати інформацію, систематизувати

та аналізувати її для прогнозування розвитку певних негативних подій та уникнення небезпек чи зменшення їх негативних наслідків.

Як приклад (*табл. 1*) **спробуємо спрогнозувати взаємодію між ро́ботами і людьми**. Уявімо місто майбутнього, де живуть андроїди, які виконують роль помічників людей. Деякі з них хочуть жити серед людей непоміченими та мати власне життя. Ставимо завдання щодо визначення ймовірних небезпек, прогнозу їх розвитку і пошуку відповіді на класичне запитання: «Що робити?». Тобто **запропонувати запобіжні заходи**. Етапи вирішення завдання потрібно підкріплювати зображеннями з відомих голлівудських фільмів, які відповідають стилю Tech Noir. Підбірку кадрів можна перетворити у відповідний колаж, що допоможе прикрасити і підсилити розповідь, обґрунтувати можливий розвиток подій і візуалізувати запобіжні заходи.

ОДИН ІЗ ВАРІАНТІВ ВИКОНАННЯ ЗАВДАННЯ

Незважаючи на значні переваги використання ро́ботів, є низка небезпек та проблем, які потенційно можуть нашкодити людям. До найбільших потрібно віднести:

- ☑ можливі проблеми з аутентифікацією людини чи навіть завдання фізичної шкоди через різноманітні збої програмного забезпечення, випадкові помилки, проникнення вірусів, фізичне втручання, кібератаки, підробки ключів доступу та ін.;
- ☑ інформацію, яку постійно накопичують ро́боти про своїх власників, можуть викрасти зловмисники;
- ☑ можливий неконтрольований обмін даними між самими ро́ботами.

У *таблиці 1* вибірково наведено небезпеки, які підкріплені відповідними кадрами з фільмів, можливі загрози для людини в результаті створення відповідних умов і надано рекомендації щодо їх усунення.

У *таблицях 2–4* вказано **принцип оцінки ризику матричним методом,** який потрібно застосовувати для вирішення цього завдання.

Під час розробки цього кейсу використано **теорію множинного інтелекту Говарда Гарднера**, що базується на твердженні про наявність різних видів інтелекту: лінгвістичного, логіко-математичного, музичного, тілесно-кінестетичного, просторового, міжособистісного, внутрішньоособистісного, натуралістичного, екзистенційного (*рис. 1*). Суть теорії в тому, що для підвищення результативності навчання потрібно застосовувати різні стратегії, які враховують пізнавальні відмінності слухачів. Схожої думки дотримується **професор Роб Лонг**, який будує свої заняття з урахуванням індивідуальних відмінностей слухачів для підвищення розуміння поставлених завдань.

Таблиця 1

Приклад виконання кейсу з оцінки ризиків під час взаємодії людини і ро́бота

№	Небезпеки	Небезпечна подія	Наслідки небезпечної події	Початковий ризик			Запобіжні заходи	Кінцевий ризик		
				Ймовірність	Важкість	Ризик		Ймовірність	Важкість	Ризик
1	Недоліки аутентифікації 	Конструктивні недоліки, недосконалість, недостатня надійність засобів виробництва	Тяжка травма, інвалідність або смерть 	C	III	H	Багатофакторна Аутентифікації 	F	III	П
2	Фізична небезпека 	Дія рухомих і таких, що обертаються, деталей обладнання, машин і механізмів	Тяжка травма, інвалідність або смерть 	C	III	H	Фізичний захист, захисні екрани тощо 	F	III	П
3	Викрадення даних 	Використання даних проти власника	Емоційний стрес 	D	V	ПП	Шифрування, захист від спуфінгу*, фільтрація, 	F	V	П
4	Пошкодження програмного забезпечення 	Незадовільне функціонування пристроїв, аварійна ситуація	Емоційний стрес, вивід з ладу обладнання 	D	V	ПП	Резервне копіювання / навчання користувача 	F	V	П

* спуфінг (от англ. spoofing) – кібератака, у межах якої шахрай видає себе за певне надійне джерело.

Таблиця 2

Рівні ризику

Група ризику	Позначення	Визначення рівнів ризику	Колір	Оцінка рівня ризику
I	КН	Катастрофічний		IA, IB, IIA
II	В	Високий		IC, ID, IE, IIB, IIC, IID, III A, IIIB, IIIC, IVA, IVB
III	З	Значний		IF, IIE, IIF, IIID, IIIE, IID, IVC, IVD, VA, VB, VC, VIA, VIB
IV	Н	Низький		IIIF, IVF, IIIF, VF, VIF, VIIF, IVE, IIIE, VE, VIE, VIIE, VD, VID, VIID, VIC, VIIC, VIIB, VIIA

Таблиця 3

Критерії оцінки професійних ризиків

Категорія ризику	Ставлення до рівня ризику	Дії щодо керування рівнем ризику
IA, IB, IIA	**Категорично неприйнятний (КН)** (відмова від ризику)	Роботу виконувати заборонено без зміни в умовах та розробки і впровадження заходів щодо зниження ризиків Першочергово мають бути виконанні запобіжні та захисні заходи для унеможливлення реалізації небезпеки в небезпечну подію та/або зниження наслідків небезпечної події. Встановлюється контроль за забороною проведення робіт.
IC, ID, IE, IIB, IIC, IID, III A, IIIB, IIIC, IVA, IVB	**Неприйнятний (Н)** (зниження ризику)	Роботу виконувати дозволено (постійно або тимчасово), але із впровадженням у часі змін в умовах роботи запобіжних та захисних заходів для унеможливлення реалізації небезпеки або зниження наслідків небезпечної події. Мають бути розроблені і впровадженні відповідні організаційно-технічні заходи.
IF, IIE, IIF, IIID, IIIE, IID, IVC, IVD, VA, VB, VC, VIA, VIB	**Прийнятний з перевіркою (ПП)** (прийняття ризику з контролем)	Роботу дозволено виконувати, але потрібен постійний контроль за небезпекою та виконанням запобвжних та захисних заходів (дій), щодо унеможливлення або зниження ризику до прийнятного рівня та аналіз змін стану небезпеки в часі та просторі.
IIIF, IVF, IIIF, VF, VIF, VIIF, IVE, IIIE, VE, VIE, VIIE, VD, VID, VIID, VIC, VIIC, VIIB, VIIA	**Прийнятний (П)** (прийняття ризику без контролю)	Не потребує вживати запобіжних та захисних заходів (дій) для унеможливлення або зниження ризику.

Згідно із запропонованою методикою навчальну групу потрібно розділити на декілька підгруп, зважаючи на домінуючі здібності, які попередньо встановлює психологічне тестування. Наприклад, **підгрупа 1** – *художники*; **підгрупа 2** – *письменники*; **підгрупа 3** – *математики*; **підгрупа 4** – *практики*. Кожна підгрупа отримує робочий лист із завданнями.

Так, математики повинні вирішувати математичні завдання (обрахувати ймовірність виникнення небезпечної ситуації згідно із статистичними даними). Письменники описують небезпеки, які оточують працівників, і можливі наслідки (травми) з урахуванням частоти їх настання. Художники розроблюють схеми (ескізи) небезпечних ситуацій з можливими варіантами їх розвитку. Практики проводять оцінку ризиків на робочому місці. Після всі обмінюються своїми напрацюваннями для створення загальної стратегії захисту (*рис. 2*).

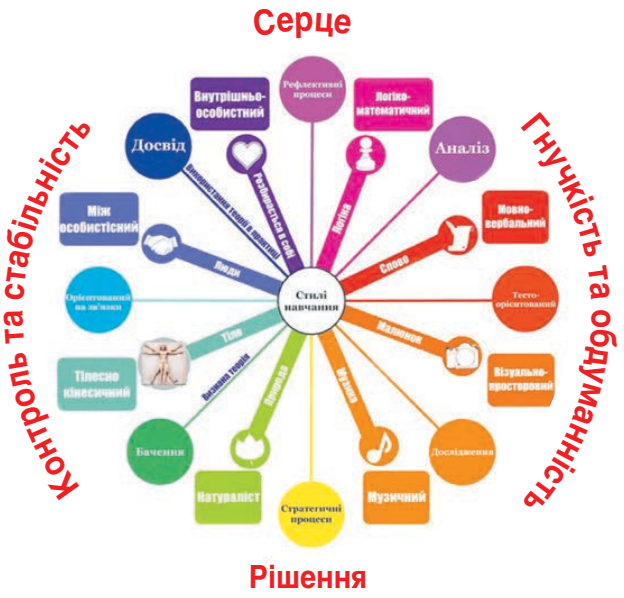

Рис. 1. Стилі навчання на основі теорії множинного інтелекту Говарда Гарднера*

* Про один із стилей навчання читайте в статті групи науковців «Смартнавчання в охороні праці» у журналі № 7/2021.

Таблиця 4

Матриця оцінки професійних ризиків

Ступінь тяжкості наслідків захворювання		Позначення ступеня тяжкості	ЙМОВІРНІСТЬ					
Критерії категорії ступеня тяжкості інциденту			Назва критерію ймовірності (частоти захворювання)					
			Високоймовірний	Імовірний	Рідкий	Малоймовірний	Практично неможливий	Неможливий
			Критерії ймовірності (частоти хронічних захворювань)					
			Небезпечна подія відбувається часто протягом розгляданого строку	Відбувається кілька разів протягом строку	Відбувається принаймні один раз протягом строку	Малоймовірно, але може відбутися протягом строку	Надзвичайно малоймовірно, що подія відбудеться протягом строку	Імовірність близька до нуля
			Позначення ймовірності (частоти інциденту)					
			A	B	C	D	E	F
КАТЕГОРІЯ ТЯЖКОСТІ НАСЛІДКІВ ЗАХВОРЮВАННЯ	Групова загибель людей	I	КН	КН	Н	Н	Н	ПП
	Загибель однієї людини, групові тяжкі травми, групові тяжкі професійні захворювання	II	КН	Н	Н	Н	ПП	ПП
	Тяжкі травми в однієї людини, травми середньої тяжкості у групи людей	III	Н	Н	Н	ПП	ПП	П
	Травми середньої тяжкості в однієї людини, легкі травми у групи людей,	IV	Н	Н	ПП	ПП	ПП	П
	Травма легкого ступеня тяжкості в однієї людини, незначні ушкодження у групи людей	V	ПП	ПП	ПП	ПП	П	П
	Незначні ушкодження в однієї людини, незначне нездужання в однієї людини, майже відсутня, низька шкода системі	VI	ПП	ПП	ПП	П	П	П
	Немає шкоди, травми, професійного захворювання, не завдано шкоди системі	VII	ПП	ПП	П	П	П	П

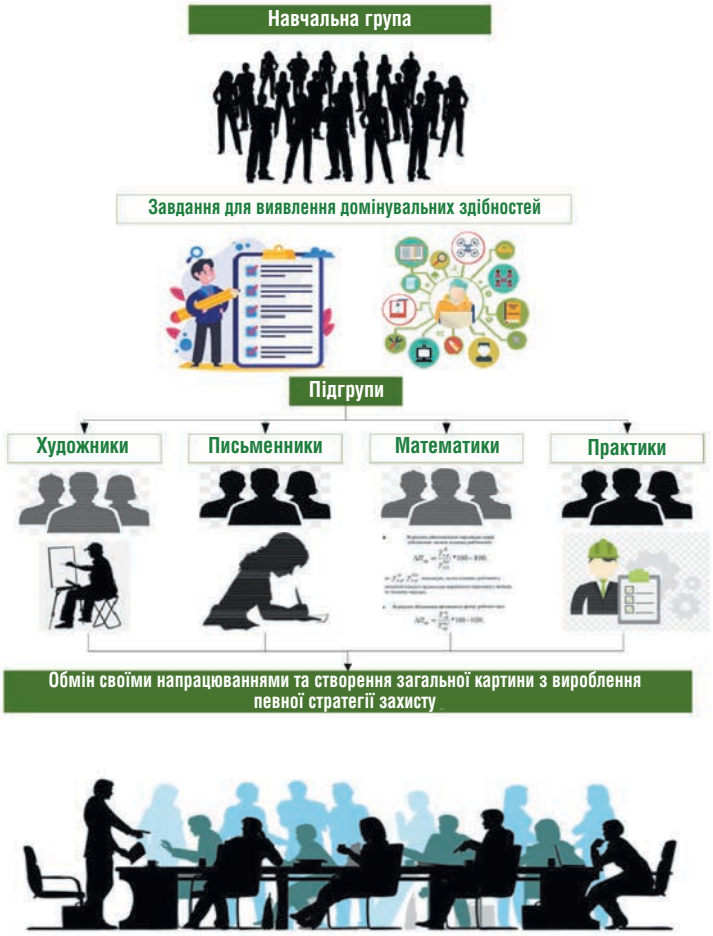

Рис. 2. Схема навчального процесу згідно з теорією множинного інтелекту

Висновок 1. Нещасні випадки переважно настають унаслідок хибної оцінки ситуації, несприйняття реальної загрози через переоцінювання своїх можливостей. Чим більший розрив між сприйняттям загрози та її реальністю, тим менше шансів уникнути небезпеки. Важливе значення має психологічний стан і настрій працівника, які можуть змінюватися протягом робочого часу через певні взаємини в колективі, особисті обставини, самопочуття, занепокоєння та ін. Звідси витікає потреба у формуванні партнерських відносин – дослухатись один до одного і підтримувати один одного, підсилюючи слабкі сторони своїх колег.

Для запобігання нещасних випадків і забезпечення ефективної роботи системи управління охороною праці на підприємствах важливо сформувати у фахівців усвідомлене ставлення до питання безпеки праці. Встановлено, що для формування безпекових компетенцій потрібно стимулювати розвиток відповідних психічних (психомоторних) процесів у працівників за рахунок набуття ситуаційної обізнаності, що передбачає усвідомлене ставлення працівника до безпеки на робочому місці, розвиток навичок для виявлення потенційних небезпек та пошук і обґрунтування подальших дій.

Висновок 2. За роботизованими системами майбутнє. Вони швидко знаходять свою нішу у різних виробничих сферах, особливо у критичній інфраструктурі. Однак ро́боти представляють декілька серйозних небезпек, які розглянуто під час вирішення поставленого завдання. Ці небезпеки можуть значно вплинути на працездатність інфраструктури, що переросте від економічних втрат до людських. Тому розглянуті небезпеки та спроби віднайти запобіжні заходи вже нині формують відповідне бачення у здобувачів освіти щодо експлуатації ро́ботів, основою якого є захист від будь-яких можливих кібервпливів.

* Про базову методологію управління ризиками в системах менеджменту читайте в статті Віталія Цопи в № 1/2018 (с. 18).