

СУЧАСНІ ВИКЛИКИ ТА ШЛЯХИ ПІДВИЩЕННЯ РІВНЯ БЕЗПЕКИ В УМОВАХ ЦИФРОВІЗАЦІЇ СУСПІЛЬСТВА

Вінницький національний технічний університет

Анотація

У тезах розглянуто актуальні виклики у сфері безпеки життєдіяльності та охорони праці в умовах цифровізації суспільства. Проаналізовано трансформацію ризиків, пов'язаних із використанням сучасних інформаційно-комунікаційних технологій, віддаленої та гібридної форми праці, автоматизації виробництва. Акцентовано увагу на необхідності оновлення нормативно-правової бази, впровадження інноваційних підходів у навчальному процесі та формування культури безпеки серед студентської молоді. Обґрунтовано необхідність комплексного підходу до забезпечення безпеки, що враховує фізичні, психоемоційні та інформаційні ризики.

Ключові слова: охорона праці, цифровізація, ризики, інформаційні технології, дистанційна робота, нормативно-правова база, культура безпеки, профілактика, освіта.

Abstract

The thesis addresses the current challenges in the field of life safety and labor protection in the context of digitalization of society. The transformation of risks associated with the use of modern information and communication technologies, remote and hybrid forms of labor, and production automation is analyzed. Attention is focused on the need to update the regulatory framework, introduce innovative approaches in the educational process and form a culture of safety among students. The author substantiates the need for an integrated approach to security, taking into account physical, psycho-emotional and information risks.

Keywords: labor protection, digitalization, risks, information technology, remote work, regulatory framework, safety culture, prevention, education.

Вступ

У сучасному світі процес цифровізації охоплює практично всі сфери людської діяльності, що призводить до переосмислення концепцій безпеки життєдіяльності та охорони праці. Зміна характеру праці, зростання ролі інтелектуальної праці, використання комп'ютеризованих систем та інтернету речей (IoT) породжують нові фактори ризику, які мають бути враховані під час розробки заходів безпеки. Зокрема, стрімке впровадження автоматизованих виробничих систем вимагає перегляду традиційних підходів до ідентифікації небезпек та оцінювання професійних ризиків.

Охорона праці, яка раніше переважно орієнтувалася на фізичні небезпеки – механічні травми, вплив шкідливих речовин або температур, – нині повинна враховувати психоемоційні, когнітивні та цифрові загрози. Наприклад, тривала робота з комп'ютером, хронічний стрес, спричинений постійною взаємодією з цифровим середовищем, а також ризики інформаційного перевантаження дедалі частіше фігурують у звітах щодо професійної безпеки. Крім того, робочі місця, що повністю залежать від інформаційних систем, є вразливими до кіберзагроз, які можуть спричинити не лише збої в роботі, а й небезпеку для життя та здоров'я персоналу.

Поглиблений аналіз дозволяє зробити висновок, що цифровізація не просто модифікує окремі виробничі процеси, а докорінно змінює саму природу праці, структуру ризиків і механізми їх подолання. Якщо раніше охорона праці концентрувалася на запобіганні травмам, то сьогодні ключовим стає управління стресом, інформаційними перевантаженнями, захист від цифрових атак і дотримання етичних норм у цифровому середовищі. Це означає, що поняття «безпека життєдіяльності» потребує концептуального оновлення.

У контексті реформування освітнього процесу важливим аспектом є формування культури безпеки серед студентської молоді. У навчальних закладах вищої освіти впроваджуються інтерактивні методи викладання дисципліни «Безпека життєдіяльності та основи охорони праці», зокрема використання кейс-методів, симуляцій, віртуальних лабораторій і моделювання надзвичайних ситуацій.

Це дозволяє сформувати не лише знання, але й стійкі практичні навички реагування на потенційно небезпечні ситуації. Активне залучення студентів до ситуаційного аналізу та вирішення реальних виробничих кейсів сприяє розвитку критичного мислення та відповідального ставлення до особистої та колективної безпеки.

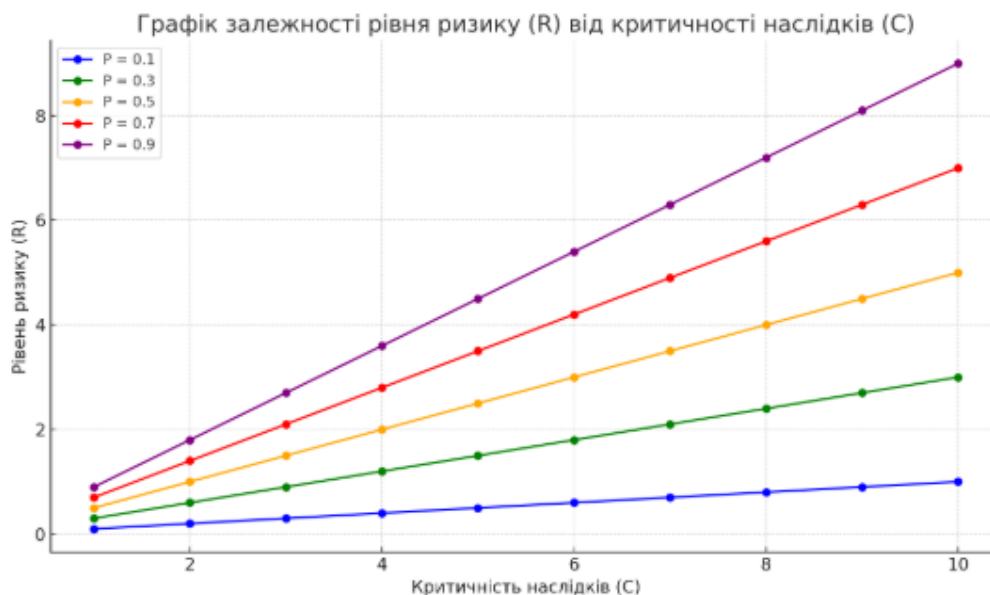
У контексті оновлення підходів до викладання безпеки життєдіяльності в ЗВО особливу роль відіграють методичні рекомендації Міністерства освіти і науки України, які наголошують на важливості адаптації змісту дисциплін до умов цифрової трансформації. У документі підкреслено необхідність міждисциплінарного поєднання безпекових знань із цифровою грамотністю та критичним мисленням, що відповідає сучасним викликам у сфері охорони праці та безпеки [5].

Одним із ключових аспектів підвищення рівня безпеки життєдіяльності в умовах цифровізації є активне застосування інноваційних технологій у навчанні та на практиці. Зокрема, цифрові рішення можуть бути ефективно використані для моніторингу та аналізу ризиків у реальному часі, що дозволяє оперативно реагувати на потенційні небезпеки. Наприклад, використання сенсорних технологій, автоматизованих систем управління безпекою та інтелектуальних алгоритмів для прогнозування можливих аварійних ситуацій може значно знизити кількість нещасних випадків та травм на виробництві. Також важливим є розвиток персоналізованих систем навчання, які адаптуються до індивідуальних потреб кожного студента чи працівника, надаючи йому необхідні знання та навички для ефективної роботи в умовах цифрової трансформації. Всі ці аспекти вимагають комплексного підходу до розробки та впровадження заходів, що забезпечують безпеку життєдіяльності в епоху цифрових змін.

З метою оцінювання цифрових ризиків у сфері безпеки життєдіяльності доцільно застосовувати кількісну модель розрахунку ризику, яка базується на класичній формулі:

$$R = P \times C$$

де R — рівень ризику, P — імовірність настання небезпечної події, а C — критичність наслідків (шкала від 1 до 10). Наприклад, у випадку кібератаки на систему управління виробництвом, яка має високу критичність (8) та середню імовірність (0,4), рівень ризику складатиме $R = 0,4 \times 8 = 3,2$, що свідчить про потребу в негайному впровадженні заходів реагування. Для наочності на рисунку 1 подано графік залежності рівня ризику від критичності наслідків при різних рівнях імовірності. Як видно з графіка, цифрові ризики навіть із низькою імовірністю можуть мати високий вплив, що вимагає комплексного моніторингу та захисту.



Одним з ефективних способів оцінки професійних ризиків у цифрову епоху є застосування кількісної моделі, яка базується на розрахунку рівня ризику (R) як добутку імовірності виникнення небезпечної події (P) та критичності її наслідків (C), тобто $R = P \times C$. Такий підхід дозволяє формалізувати процес оцінювання ризиків, зробити його об'єктивним і відтворюваним. На графіку, що до-

повнює цю модель, зображено залежність рівня ризику від критичності наслідків при фіксованих значеннях імовірності (наприклад, $P = 0.1, 0.5, 0.9$). Криві зростають лінійно, демонструючи, як навіть помірна імовірність у поєднанні з високою критичністю може призводити до суттєвих загроз. Це дозволяє візуально ідентифікувати найбільш критичні сценарії (з високими R), які потребують першочергових заходів реагування. Така модель широко застосовується в системах управління ризиками на підприємствах, у сфері кібербезпеки та при розробці політик охорони праці в умовах цифровізації, де загрози часто мають складну, динамічну природу.

Умови цифрової трансформації вимагають від суспільства системного, а не фрагментарного підходу до безпеки. Сьогодні недостатньо лише оновити окремі інструкції чи впровадити нові технології – потрібно синхронізувати дії всіх зацікавлених сторін: освітніх закладів, роботодавців, державних органів і працівників. Це забезпечить стале функціонування безпекової інфраструктури на тлі постійних технологічних змін.

У зв'язку з активною цифровізацією соціальних і виробничих процесів, важливу роль у забезпеченні безпеки життєдіяльності відіграє інтеграція інформаційних технологій у системи моніторингу та управління ризиками. Використання таких технологій, як штучний інтелект, великий аналіз даних (Big Data) і машинне навчання, дозволяє значно покращити процес оцінки та прогнозування небезпек. Такі інструменти допомагають автоматично виявляти потенційно небезпечні ситуації на ранніх етапах та здійснювати ефективний контроль за умовами праці в реальному часі. Однак, крім технологічних інновацій, важливим є й адаптаційний процес, який включає зміни в організаційних структурах і процедурах на всіх рівнях — від навчальних закладів до виробничих підприємств. Зокрема, необхідно розвивати навички роботи з новими цифровими системами як серед студентів, так і серед вже працюючих спеціалістів, щоб забезпечити їх здатність ефективно застосовувати ці технології для забезпечення безпеки [3], [4].

Сучасна цифрова економіка породжує нові типи ризиків, зокрема у сфері зберігання персональних даних, цифрового тиску на працівників, кібербезпеки та соціальної ізоляції. Як зазначає Портной Є. В., цифрова трансформація потребує не лише технологічного переозброєння підприємств, але й усвідомленого управління ризиками цифрового середовища, включно з людським чинником [6]. Це ще раз доводить, що питання безпеки життєдіяльності повинне розглядатися в тісному зв'язку з економічною безпекою працівників та підприємств.

Актуальною є також потреба перегляду нормативно-правових документів у сфері охорони праці. Багато положень ще не враховують специфіку віддаленої праці, гібридного формату робочого процесу та роботи з високими інтелектуальними навантаженнями. Зокрема, вимоги до організації безпечного робочого простору вдома, використання сертифікованих засобів захисту даних та психологічна підтримка персоналу — всі ці питання мають бути інтегровані у систему управління охороною праці.

Не менш важливою є роль профілактики — як на рівні організації, так і особистого самоконтролю. Забезпечення ергономічного середовища, дотримання режиму праці та відпочинку, застосування психологічної підтримки та регулярне підвищення обізнаності працівників щодо нових ризиків є ключовими напрямками превентивної роботи. Відповідно до сучасних рекомендацій, інтегровані моделі безпеки мають включати фізичну, інформаційну, психоемоційну та соціальну компоненти.

Окремої уваги заслуговують тенденції інноваційного розвитку підприємств у цифрову епоху, де безпека праці стає елементом загальної стратегії сталого розвитку. Як показує аналіз досліджень у сфері управління інноваціями, компанії, які інвестують у безпечні цифрові середовища для працівників, мають вищий рівень лояльності персоналу та ефективності роботи. Це демонструє, що цифровізація не повинна зводитися лише до автоматизації, а має супроводжуватися створенням безпечного й підтримувального робочого середовища.

Одним з головних викликів майбутнього є баланс між швидкістю цифрових інновацій та здатністю людей адаптуватися до нових ризиків. Якщо цифрові системи розвиваються експоненційно, то зміна мислення, поведінки та нормативної бази відбувається значно повільніше. Саме тому важливо вже зараз формувати культуру безпеки цифрової доби, яка поєднує технічну компетентність з етикою відповідальності.

У підсумку слід зазначити, що питання безпеки життєдіяльності в умовах цифровізації є міждис-

циплінарним та потребує комплексного підходу. Лише тісна взаємодія між науковцями, законодавцями, викладачами та роботодавцями дозволить адаптувати наявні системи безпеки до сучасних реалій та забезпечити ефективний захист життя і здоров'я людини в усіх сферах її діяльності.

Висновки

У даному дослідженні було розглянуто ключові виклики та перспективні шляхи підвищення рівня безпеки життєдіяльності в умовах цифровізації суспільства. Показано, що активне впровадження інформаційних технологій, автоматизованих систем управління та дистанційних форматів праці створює не лише нові можливості, але й численні ризики для здоров'я та безпеки людей. Зміни у характері професійної діяльності зумовлюють потребу у перегляді традиційних підходів до охорони праці та формування культури безпеки, особливо серед молоді. Також було підкреслено важливість оновлення нормативно-правової бази, адаптації освітніх методик до цифрових умов, розвитку профілактичних заходів та інтеграції психоемоційних і інформаційних аспектів у систему управління ризиками.

Отже, забезпечення безпеки життєдіяльності у цифрову епоху має ґрунтуватися на міждисциплінарному підході, що об'єднує зусилля фахівців з технічних, соціальних, медичних і педагогічних галузей. Тільки завдяки такій співпраці можливо сформувати ефективну, адаптивну та сталу систему безпеки, здатну відповідати на сучасні виклики та запобігати потенційним загрозам у цифровому середовищі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Томчук М.А., Крещенко М. Г., Малініч І. П. «ІТ-безпека у телекомунікаційних системах в епоху штучного інтелекту» в Матеріали конференції «LII Науково-технічна конференція факультету інформаційних технологій та комп'ютерної інженерії (2023)» Вінниця, 2023. [Електронний ресурс]. Режим доступу: <https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2023/paper/view/18871>.
2. Гутарук М. І., Кравченко А. П. Сучасні підходи до формування культури безпеки студентської молоді // Техногенно-екологічна безпека. – 2021. – № 2(18). – С. 89–94.
3. Білокінь І. В. Інтеграція інформаційно-комунікаційних технологій у безпеку життєдіяльності та навчання математики через хмарні ресурси у школі [Електронний ресурс] / І. В. Білокінь. – 2024. – Режим доступу: <http://dspace.pnpu.edu.ua/handle/123456789/25987>
4. Богачук Р. С., Томчук М.А. «Психоемоційне вигорання фахівців іт-сфери як чинник професійної небезпеки» в Матеріали конференції «LIV Всеукраїнська науково-технічна конференція факультету інформаційних технологій та комп'ютерної інженерії (2025)» Вінниця, 2025. [Електронний ресурс]. Режим доступу: <https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2025/paper/view/24154>
5. Томчук М. А. «Вдосконалення процедури тестового контролю у закладах вищої освіти» в Матеріали «Використання інноваційних технологій в процесі підготовки фахівців - 2018» Вінниця, 2018. [Електронний ресурс]. Режим доступу: <https://conferences.vntu.edu.ua/index.php/itpf/2018/paper/view/5787>
6. Цифрова економіка та економічна безпека // Портной Є. В. – [Електронний ресурс]. – Режим доступу: <https://repository.sspu.edu.ua/bitstreams/049352f1-0356-479e-ace7-31fd4a47579e/download>

Іщенко Олексій Русланович – студент групи ІСТ-22Б, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, Вінниця, e-mail: oleksiy26032005@gmail.com

Томчук Микола Антонович – кандидат технічних наук, доцент кафедри безпеки життєдіяльності та педагогіки безпеки, Вінницький національний технічний університет, Вінниця, e-mail: tomchuk@vntu.edu.ua

Ishchenko O. R. – Department of Automation and intelligent information technologies, Vinnytsia National Technical University, Vinnytsia, e-mail: oleksiy26032005@gmail.com

Tomchuk M. A. – candidate of Technical Sciences, Associate Professor of Life Safety and safety pedagogy, Vinnytsia National Technical University, Vinnytsia, e-mail: tomchuk@vntu.edu.ua