розпорядчі методи в системі управління охороною праці займають важливу питому вагу та є базовими у діяльності управлінського персоналу різного рівня підпорядкування.

Список використаних джерел:

1. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР // *Вдомості Верховної Ради України*. — 1996. — № 30. — Ст. 141.
2. Закон України «Про охорону праці» від 21.11.2002 р.
3. Г. Г. Гогіташвілі. Системи управління охороною праці. Навчальний посібник. Львів: Афіша, 2002. 320 с.
4. В. А. Батлук, Б. О. Білінський, В. В. Ковалишин, О. Л. Мірус. Основи охорони праці в підрозділах МНС України. Навчальний посібник. Львів: Афіша, 2011. 505с.
5. Мірус О. Л., Марич В. М., Білінський Б. О. Удосконалення системи управління охорони праці на підприємствах лісового господарства на основі ДСТУ OHSAS 18001:2010. Збірник наукових праць Всеукраїнської науково–практичної конференції викладачів та фахівців–практиків «Охорона праці: освіта і практика» та XI Всеукраїнської науково-практичної конференції курсантів, студентів, аспірантів та ад'юнктів «Проблеми та перспективи розвитку охорони праці» . Львів – 2021. – С. 45-47.
6. Мірус О. Л., Пятова А. В., Марич В. М. Принципи державної політики у системі управління охороною праці. Матеріали IV Всеукраїнської науково–практичної конференції викладачів та фахівців–практиків «Охорона праці: освіта і практика» та XIV Всеукраїнської науково-практичної конференції курсантів, студентів, аспірантів та ад'юнктів «Проблеми та перспективи розвитку охорони праці». Львів – 2024. – С. 45-51.

УДК 658.8

ІНТЕГРАЦІЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПРОМИСЛОВОСТІ: СУЧАСНІ ТЕНДЕНЦІЇ ЗАХОДІВ БЕЗПЕКИ

Курепін В.М., *доцент кафедри методики професійного навчання, канд. екон. наук, доцент*
Миколаївський національний аграрний університет

На тлі стрімкого впровадження штучного інтелекту та цифровізації організацій у різних сферах глобальний ландшафт кіберзагроз продовжує змінюватися. Такі зміни вимагають кваліфікованих фахівців [1, с. 66]. Але реалії сьогодення показують тенденцію дефіциту кваліфікованих фахівців у цій сфері. Аналітики-дослідники, що спеціалізується на ринках інформаційних технологій

окреслили шість ключових трендів у сфері кібербезпеки, які вплинуть на розвиток галузі. Розглянемо їх:

1. Генеративний штучний інтелект. Традиційно зусилля щодо забезпечення безпеки зосереджені насамперед на захисті структурованої інформації, такої як бази даних.

Однак розвиток генеративного штучного інтелекту призводить до трансформації цього підходу та усунення фокусу на захист неструктурованих даних - тексту, зображень та відеоматеріалів. На цьому фоні багато об'єктів господарювання повністю переглянули свої інвестиційні стратегії в галузі штучного інтелекту, що значно впливає на процес навчання великих мовних моделей.

У перспективі, впровадження генеративного штучного інтелекту дозволить мінімізувати кількість інцидентів безпеки з вини співробітників. Крім того, генеративний штучний інтелект значно підвищить ефективність моніторингу ІТ-інфраструктури з метою виявлення підозрілої активності. Оскільки генеративний штучний інтелект дає можливість перекладати результати аналізу природною мовою, співробітники з меншими технічними навичками можуть працювати більш продуктивно. Це може змінити підхід підприємств до найму та навчання фахівців у відповідній сфері [2, с. 225].

Штучний інтелект допомагає виявляти потенційні ризики: невідомі пристрої та хмарні програми, застарілі операційні системи або незахищені конфіденційні дані. Генеративний штучний інтелект може отримати інформацію з кількох джерел для створення простих для розуміння звітів, якими фахівці з безпеки можуть швидко поділитися з іншими співробітниками в організації.

2. Управління ідентифікаційними даними машин. Зростання застосування генеративного штучного інтелекту, хмарних сервісів, призвело до широкого використання облікових записів та ідентифікаційних даних машин, таких як різні фізичні пристрої та робочі навантаження. Для їх захисту застосовують спеціальні ключі, цифрові сертифікати тощо [3, с. 143]. У такій ситуації керівники об'єктів господарювання змушені розробляти стратегії щодо впровадження надійної ідентифікації та керування доступом до машин для захисту від кібератак.

3. Зміна підходу до використання штучного інтелекту. Об'єкти господарювання стикаються зі змішаним ефектом від реалізації проєктів у галузі штучного інтелекту, що змушує їх переглядати пріоритети. На цьому тлі підприємства, організації фокусують зусилля на вужчих варіантах використання штучного інтелекту, які дають вимірний результат і швидше виправдовують інвестиції.

4. Оптимізація технологій кібербезпеки. Великі та малі підприємства використовують у середньому більш як 45 інструментів кібербезпеки (статистика) [4, с. 147]. За наявності біля п'яти тисяч постачальників у сфері інформаційної безпеки керівники об'єктів господарювання стікаються з оптимізацією наборів програмного забезпечення для створення більш ефективних платформ захисту.

5. Програми безпечної поведінки та культури інформаційної безпеки. Фахівці-дослідники зазначають, що все більше керівників об'єктів господарювання усвідомлюють важливість безпекових заходів щодо зниження ризиків кібербезпеки. Некоректні дії співробітників можуть призводити до серйозних інформаційно-безпекових-інцидентів [5, с. 6]. У результаті спостерігається стратегічний зсув у бік впровадження безпеки в організаційну культуру, як структурних підрозділів, так і об'єкту господарювання в цілому.

6. Боротьба з вигорянням у сфері кібербезпеки. Інформаційно-безпекові - фахівці можуть стикатися з тривалим стресом на робочому місці, що пов'язано з ландшафтом загроз, що постійно змінюється, новими нормативно-правовими вимогами, обмеженими повноваженнями і недостатніми ресурсами. Це призводить до зниження працездатності, погіршення якості, помилок і зазвичай закінчується відходом із компанії.

Отже, успішні приклади інтеграції та автоматизації у промисловому виробництві свідчать про те, що сучасні ІТ-технології відіграють ключову роль у підвищенні ефективності виробництва, покращенні якості продукції та оптимізації бізнес-процесів, якісно вирішують безпекові проблеми.

ІТ-технології дозволяють об'єктам господарювання збільшити продуктивність, оптимізувати управління виробництвом, забезпечити безпеку даних виробничих процесів.

Список використаних джерел:

1. Курепін В. М. Іваненко В. С. Застосування цифрових технологій у сільському господарстві для досягнення цілей сталого розвитку. Modern Economics. 2024. № 47(2024). С. 62-69. DOI: https://doi.org/10.31521/modecon.V47(2024)-09.

2. Іваненко В. С., Курепін В. М. Подолання кризових явищ у аграрній сфері за допомогою технології доповненої реальності // Урожайність та якість продукції рослинництва за сучасних технологій вирощування: матеріали міжнар. наук.-практ. інтернет-конф., присв. 90-річчю з дня народження професора Г. П. Жемели (м. Полтава, 30 верес. 2023 р.). Полтава: ПДАУ, 2023. С. 224-226. URL: https://dspace.mnau.edu.ua/jspui/handle/123456789/15512.

3. Іваненко В. С. Інновації у сфері безпеки: захист різних сфер діяльності місцевих громад. Розвиток територіальних громад: правові, економічні та соціальні аспекти: матеріали IV міжнар. наук.-практ. конф., (м. Миколаїв, 9 грудня 2024 р. Миколаїв: МНАУ, 2024. С. 141-144. URL: https://dspace.mnau.edu.ua/jspui/handle/123456789/20102.

4. Лотарєва Д. В. Сучасні інформаційні технології у системі управління. Екологічні та соціальні аспекти розвитку економіки в умовах євроінтеграції: матеріали X Всеукраїнської науково-практичної конференції (м. Миколаїв, 23-25 жовтня 2024 р.). Миколаїв: МНАУ, 2024. С. 146-148. URL: https://dspace.mnau.edu.ua/jspui/handle/123456789/18921.

5. Кузнецова В. А. Сучасні підходи, стратегія та тактика до управління ризиками на підприємстві. OSHAgro – 2024: матеріали III Міжнародної науково-практичної конференції (м. Київ, 30 вересня 2024 року). Київ: МОН України, Національний університет біоресурсів і природокористування України, Науково-виробничий журнал «Охорона праці», Європейське співтовариство з охорони, 2024. С. 5-7. URL: https://dspace.mnau.edu.ua/jspui/handle/123456789/18903.

УДК: 330.131

ОЦІНКА РИЗИКІВ ТА ПЛАНУВАННЯ РОБІТ З ОХОРОНИ ПРАЦІ

Курепін В.М., *доцент кафедри методики професійного навчання, канд. екон. наук, доцент*
Миколаївський національний аграрний університет

Ефективне управління охороною праці на будь-якому підприємстві повинно ґрунтуватися на виявленні та оцінюванні наявних ризиків. У свою чергу оцінка ризиків є наріжним каменем планування заходів з охорони праці на об'єктах господарювання. Метою охорони праці є підвищення безпеки праці та планомірне покращення умов на робочих місцях. Робота з охорони праці створює рамки, в яких можна збудувати всю цю діяльність.

Роботодавець у своїй діяльності повинен враховувати плани роботи з охорони праці [3, с. 98] у яких відображаються заходи щодо організації та вдосконалення заходів безпеки на робочих місцях. Подібний план, це відображення загальної політики підприємства у галузі безпеки, чи детальний та конкретний план роботи. За допомогою оцінки ризиків визначаються потреби розвитку охорони праці [2, с. 52]. У план роботи повинні бути включені дієві на практиці заходи, які здатні усунити недоліки, ставитися конкретні цілі та заходи для здійснення вимог забезпечення безпеки та збереження здоров'я.