України: 32-ї студентської науково-теоретичної конференції, 18-20 березня 2020 р., Миколаїв. – Миколаїв : МНАУ, 2020. - С. 105-108. URL:http://dspace.mnau.edu.ua/jspui/handle/123456789/7065.

5. Іваненко В. С. Історична та культурна спадщина Миколаївської області, як стратегія національної безпеки України // Розвиток територіальних громад: правові, економічні та соціальні аспекти : матеріали Міжнародної науково-практичної конференції м. Миколаїв, 23-24 червня 2021 р. Миколаїв : МНАУ, 2021. С. 97-100. URL:https://dspace.mnau.edu.ua/jspui/handle/123456789/9824.

6. Герасіменя О. А., Курепін В. М. Концепція захисту населення і території у разі загрози та виникнення надзвичайних ситуацій // Актуальні проблеми життєдіяльності людини в сучасному суспільстві : тези доповідей здобувачів вищої освіти інженерно-енергетичного факультету та інших учасників освітнього процесу за результатами тематичного «круглого столу» на інженерно-енергетичному факультеті, м. Миколаїв, 18-20 листопада 2020 р. Миколаїв : Миколаївський національний аграрний університет, 2020. С. 10-12. URL:http://dspace.mnau.edu.ua/jspui/handle/123456789/8122.

7. Курепін В. М. Реформування системи Державної служби з надзвичайних ситуацій: шляхи і способи розв'язання проблеми // Розвиток територіальних громад: правові, економічні та соціальні аспекти : матеріали міжнар. наук.-практ. конф. м. Миколаїв, 23-24 червня 2021 р. Миколаїв : МНАУ, 2021. С. 26-29. URL:https://dspace.mnau.edu.ua/jspui/handle/123456789/9818.

Науковий керівник:
Курепін В.М.,
канд.екон.наук, доцент
Миколаївський національний аграрний університет

СТАТУС СЛУЖБИ ОХОРОНИ ПРАЦІ НА МАЛИХ І СЕРЕДНІХ СІЛЬСЬКОГОСПОДАРСЬКИХ ПІДПРИЄМСТВАХ

Рибачек Є.С.,
здобувач вищої освіти, інженерно-енергетичний факультет
Миколаївський національний аграрний університет

Переважна більшість українських підприємств – це малі та середні підприємства. З міркувань економії фонду заробітної плати й мінімізації кількості керівників на таких підприємствах обов'язки служби охорони праці виконує одна штатна одиниця. Цією одиницею є інженер з охорони праці, а не керівник служби [1]. В умовах агресії та ведення бойових дій на території України малі та середні підприємства опинилися у складному економічному положенні, зниженні об'ємів продукції. За таких умов в структурі підприємства можуть відбуватися такі зміни.

Чи правильно це? Керівники й спеціалісти цієї служби відповідно за своїм посадовим становищем прирівнюються до керівників і спеціалістів основних виробничо-технічних служб підприємства та мають певні посадові обов'язки.

Чи є таке рішення помилковим, чи ні? Аналізуючи завдання й обов'язки керівників, спеціалістів технічних службовців, стає очевидним, що при їх значній схожості вони мають одну принципову відмінність.

Керівник, це професіонал, який повинен керувати, координувати й контролювати роботу персоналу [2], самостійно приймати рішення, забезпечувати дотримання вимог посадових інструкцій. Не зважаючи на те, що інженер є професіоналом, він не приймає самостійних рішень, він виконує рішення та розпорядження керівника у рамках своєї діяльності. Інженеру виконавцю не бути керівником ні за статусом, ні за нормативом [3].

Тоді хто ж керуватиме службою охорони праці на підприємстві? Роботодавець не може керувати службою охорони праці, оскільки він не має відповідної професійної підготовки, не володіє в повному обсязі знаннями щодо вимог усіх необхідних нормативно-правових актів з охорони праці.

Фахівці, які займають посаду керівника служби охорони праці на малих та середніх підприємствах повинні володіти глибокими знаннями законодавчої й нормативної бази, санітарно-гігієнічних правил, фізіології, психології, будівельних норм, організації виробництва, актів з охорони праці підприємства.

Вони мають бути кваліфікованими й професійно ерудованими [4], водночас уважними слухачами і коректними, переконливими опонентами та принциповими спеціалістами, які контролюють дотримання вимог охорони праці іншими працівникам. У процесі роботи йому доводиться постійно й тісно спілкуватися із зовсім різними людьми.

Саме фахівець, який займає посаду керівника служби охорони праці, буде виконувати роль голови комісії, у тому числі при суперечливих обставинах - розслідуванні нещасних випадків. Саме ця посада у комісії надзвичайно відповідальна і особливо обтяжлива за обсягом термінової роботи. Саме голова комісії вислуховує суперечливі зауваження до ходу розслідування від інспекторів Держпраці, начальника підрозділу або керівника підприємства, на якому він працює. Саме він тісно спілкується з потерпілим, свідками й особами, які допустили порушення вимог законодавства про охорону праці, особами бездіяльність яких призвела до нещасного випадку.

Саме йому прийдеться готуватиме проєкти наказів з питань охорони праці і самому їх виконуватиме, організовувати проходження медичних оглядів, проведення спеціального навчання робітників і навчання посадових осіб, проводитиме повторні інструктажі, переглядатиме інструкції з охорони праці тощо.

У сучасних реаліях падіння економіки в країні, керівникам малих та середніх підприємств необхідно:

- зміцнювати кадровий потенціал служби охорони праці, як служби яка допомагає керівнику підтримувати високий рівень безпеки [5];
- зробити дотримання вимог законодавства з питань охорони праці неухильними та обов'язковою умовою роботи кожного робітника підприємства, незалежно яку посаду займає цей працівник;
- неухильно дотримуватися принципів пріоритету життя й здоров'я працівників.

Отже, в умовах економічної кризи, райдужної перспективи переходу на режим неповного робочого тижня, оптимізації та скорочення чисельності працівників, керівникам підприємств необхідно дбати про якісний склад спеціалістів служби охорони праці, змінити ставлення до охорони праці й оплаті праці її фахівців, підвищити реальний статус служби охорони праці.

Бібліографічний список

1. Іваненко В. С. Державна політика щодо кадрового забезпечення агропромислового комплексу: пріоритети та напрями // Актуальні проблеми, пріоритетні напрямки та стратегії розвитку України : тези доповідей III міжнародної наук.-практ. онлайн-конференції, м. Київ, 13 жовтня 2021 року / редкол. О.С. Волошкіна та ін. Київ : ІТТА, 2021. С. 1076-1081. URL:https://dspace.mnau.edu.ua/jspui/handle/123456789/10108.

2. Курепін В.М. Управління розвитком кадрового потенціалу підприємств аграрного профілю // Сучасні тенденції розвитку фінансових та інноваційно-інвестиційних процесів в Україні : матеріали IV Міжнародної науково-практичної конференції 12 березня 2021 року : збірник наукових праць [Електронний ресурс]. – Вінниця: ВНТУ, 2021., -С. 730-733. URL:http://dspace.mnau.edu.ua/jspui/handle/123456789/8907.

3. Основи охорони праці. Модуль № 1. «Правові та організаційні основи охорони праці». Тема № 3. «Державне управління, нагляд і громадський контроль за охороною праці. Організація охорони праці на підприємствах АПК» : конспект лекцій / уклад. В. М. Курепін. – Миколаїв : МНАУ, 2021. – 29 с. URL:https://dspace.mnau.edu.ua/jspui/handle/123456789/9867.

4. Іваненко В. С., Курепін В. М. Фактори дотримання кадрової безпеки підприємств аграрного профілю // Наукові та освітні трансформації в сучасному світі : матеріали Всеукраїнської міждисциплінарної науково-практичної конференції, м. Чернігів, 15 липня 2021р. – Чернігів : Науково-освітній інноваційний центр суспільних трансформацій, 2021. С. 91-93. URL:https://dspace.mnau.edu.ua/jspui/handle/123456789/9848.

5. Курепін В.М., Грушковська І.М. Перспективи розвитку сільськогосподарських підприємств в залежності від показників, пов’язаних з умовами праці. *MOTROL*. 2012. Vol.14. №.4. 28-31. URL:http://hdl.handle.net/123456789/1180.

Науковий керівник:
Курепін В.М.,
канд.екон.наук, доцент
Миколаївський національний аграрний університет

ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Рагуліна Анастасія, здобувач вищої освіти
спеціальність 071 Облік і оподаткування
Миколаївський національний аграрний університет

Проблеми забезпечення кібербезпеки виникли у зв'язку з бурхливим розвитком мережі Інтернет. Запроваджений як дослідницький інструмент для науковців, Інтернет поступово перетворився на головну інфраструктуру світової інформаційної спільноти. Зі збільшенням кількості користувачів, пристроїв і програм на сучасному підприємстві в поєднанні зі збільшенням потоку даних, значна частина яких є конфіденційними, важливість кібербезпеки продовжує зростати. Збільшення кількості зловмисників і методів атак ще більше ускладнюють проблему.

Кіберзахист, також відомий як цифрова безпека, – це практика захисту цифрової інформації, пристроїв і активів. Це стосується особистих відомостей, облікових записів, файлів, фотографій і навіть ваших грошей [1]. Ефективна кібербезпека вимагає постійних зусиль, які охоплюють не лише безпеку додатків, тестування на проникнення та управління інцидентами, але й поведінку співробітників, ризики третіх сторін і багато інших потенційних уразливостей. Кібербезпеці постійно загрожують хакери, втрата даних, конфіденційність, управління ризиками та зміна стратегій.

Типи кіберзагроз включають: шкідливе програмне забезпечення — це форма шкідливого програмного забезпечення, за допомогою якого будь-який файл або програма може завдати шкоди користувачеві комп'ютера. Сюди входять віруси, трояни та шпигунське програмне забезпечення. Програми-вимагачі — ще один тип шкідливих програм. Він включає в себе зловмисника, який блокує системні файли комп'ютера жертви — як правило, за допомогою шифрування — і вимагає платити за їх розшифрування та розблокування. Атаки соціальної інженерії – це атака, яка базується на взаємодії людини, щоб обманом змусити користувачів порушити процедури безпеки, щоб отримати конфіденційну інформацію, яка зазвичай захищена. Фішинг — це форма соціальної інженерії, за якої надсилаються шахрайські електронні чи текстові повідомлення, схожі на повідомлення з відомих джерел. Часто випадкові атаки, ці повідомлення спрямовані на викрадення конфіденційних даних, таких як дані кредитної картки або дані для входу. Внутрішні загрози — це порушення безпеки або збитки, спричинені людьми — наприклад, працівниками, підрядниками чи клієнтами. Внутрішні загрози можуть бути зловмисними або недбалими [2].

Надійна стратегія кібербезпеки може забезпечити надійний захист від зловмисних атак, призначених для доступу, зміни, видалення, знищення або виманювання систем і конфіденційних даних організації або користувача. Кібербезпека також відіграє важливу роль у запобіганні атакам, які мають на меті вимкнути або порушити роботу системи чи пристрою [3].

Створення ефективної стратегії інформаційної безпеки вимагає застосування різноманітних інструментів і технологій. Більшість стратегій використовують певну комбінацію методів. Методи, завдяки яким можна