Касьянова Н.В., Кравчук Н.М. Управління економічною безпекою підприємства за допомогою цифрових технологій. Адаптивне управління підприємствами в умовах неотехнологічного відтворення: Монографія. За редакцією Ареф'євої О.В. К.: ФОП Маслаков, 2020. 260 с. С. 235-244

Касьянова Н.В.
Доктор економічних наук, професор
Національний авіаційний університет, м. Київ
Кравчук Н.М.
Кандидат економічних наук, доцент
Національний авіаційний університет, м. Київ

УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА ЗА ДОПОМОГОЮ ЦИФРОВИХ ТЕХНОЛОГІЙ

Одне з найбільш актуальних питань сучасності є питання забезпечення економічної безпеки. Компанії, які є піонерами цифрової трансформації, не тільки отримують значні переваги, але й несуть підвищені ризики. Останнім часом все більше інформації, в тому числі і критично важливу для окремих людей та підприємств зберігають, обробляють і передають за допомогою автоматизованих систем обробки інформації - сукупності технічних засобів та програмного забезпечення, а також методів обробки інформації і дій персоналу, які необхідні для виконання автоматизованої обробки інформації.

Ще півтора десятиліття тому, коли цифрова економіка тільки зароджувалася, вже на той час був помітний перекіс понять в області захисту даних. Говорячи про економічну доцільність заходів щодо підтримки інформаційної безпеки, вони насамперед означають захист від вірусів і хакерів, але згідно зі звітів провідних організацій, інсайдерські заходи завдають найбільшої шкоди. Збиток від необережних та неправомірних дій співробітників у рази перевищує обсяг завданої шкоди від дій вірусів і хакерських атак, або ж спроб зловмисного безпосереднього вилучення інформації.

Свого часу дослідженням проблем забезпечення економічної безпеки підприємств займалися такі вчені, як Ареф'єва О.В., Білошкурська Н.В., Білошкурській М.В., Бланк І.А., Гавкалова Н.Л., Гічова Н.Ю., Грунін С.О., Дикий А.П., Капітула С.В., Корчевський Л.О., Кузенко Т.Б, Мішин О. Ю., Мішина С. В., Наумова Л.Г., Олєйніков Є.О., Ружицький А.В., Тамбовцев В. Л., Тимофєєв Т.В., Філіппова С.В., Чаплігіна Ю.С., Шевченко С.І., Якубець В.М. та інші.

Віддаючи належне науковій та практичній значущості праць учених, які займалися проблемою економічної безпеки підприємства, слід зазначити, що досі інформаційна складова економічної безпеки не була належним чином відображена в літературі, зокрема в можливості використання інноваційних технологій щодо забезпечення інформаційної безпеки підприємства.

Мета дослідження полягає в обґрунтуванні використання сучасних інформаційних технологій для формування потенціалу економічної безпеки підприємства.

В епоху інформаційної постіндустріальної економіки необхідністю для підприємств є забезпечення економічної безпеки для досягнення стратегічних

та тактичних цілей господарської діяльності, які досягаються шляхом виявлення реальних та прогнозування потенційних загроз, пошуку шляхів їх запобігання, пом'якшення або усунення наслідків їх впливу, аналізу сил та засобів, необхідних для забезпечення економічної безпеки.

Системний підхід до вирішення даної проблеми базується на принципі цілісності об'єкта, тобто вивченні характеристик економічної безпеки як єдиного цілого. Це пов'язано з результатом виникнення синергетичного зв'язку між окремими елементами системи. Структурні компоненти системи економічної безпеки - це суб'єкти системи, ресурси, організаційно-правова база побудови та функціонування системи економічної безпеки, механізми управління системою, механізми стратегічної взаємодії, технології, методи і засоби забезпечення економічної безпеки. Оскільки економічна безпека перебуває в площині забезпечення життєздатності підприємства, то управління економічною безпекою має включати підсистеми на всіх рівнях управління.

Забезпечення економічної безпеки пропонується розглядати захищеність науково-технічного, технологічного, виробничого, інформаційного та кадрового потенціалу підприємств від активних або пасивних економічних загроз як ендогенного, так і екзогенного характеру.

До внутрішніх загроз економічній безпеці підприємства, що лежать в сфері виробничої діяльності необхідно віднести:

- зниження виробничого потенціалу через вибуття частини статутного капіталу та його непоповнення;
- відставання техніки та технології;
- високі виробничі витрати;
- можливість шахрайства та крадіжок всередині підприємств;
- помилкові виробничі дії персоналу;
- використання персоналу підприємства як каналу отримання інформації.

До зовнішніх загроз економічній безпеці інноваційних промислових підприємств належать:

- неможливість реалізації свого товару з прибутком (втрата своєї ніші на ринку товару), що забезпечує розширення відтворення;
- зміна фінансової ситуації в країні в гіршу сторону, зниження інвестиційної активності;
- зниження вартості акцій підприємств на фондовому ринку, тобто зниження капіталізації підприємства;
- платіжна недисциплінованість серед покупців спричиняє погіршенню фінансового стану підприємства, що призводить до погіршення інвестиційної діяльності та не дозволяє підприємствам йти шляхом інноваційного розвитку;
- недобросовісна конкуренція та контрагенти;
- кримінальна конкуренція;
- промислове шпигунство;
- слабкі сторони кримінально-правової та економічної політики держави

- злочини у сфері використання комп'ютерних технологій, які порушують захищеність інформаційних систем, інформаційних ресурсів підприємства і створюють загрози інформаційної безпеки;

- складності розробки та постановки на виробництво нової продукції.

Особливої гостроти проблемі економічної безпеки підприємства в умовах цифрової економіки надають інформаційні загрози:

1) широкомасштабне впровадження інформаційних і комунікаційних технологій в усіх сферах функціонування підприємства та суспільства в цілому;

2) зростання ролі інформаційних ресурсів та їх принципова вразливість від різного роду погроз, інформаційної зброї, оскільки властивість їх безпеки не є «вродженим», емерджентним, системоутворюючим;

3) суттєва зміна в організації інформаційних і комунікаційних технологій, що характеризується мініатюризацією, швидкодією, мережевою інтеграцією. Все це забезпечує не тільки високу ефективність, а також дозволяє використовувати сучасні технології в якості інформаційної зброї;

4) зростаюча загроза зловмисних дій щодо інформаційних ресурсів, як інструменту, що забезпечує конкурентні переваги.

До порушень інформаційної безпеки підприємства відносяться:

- вихід системи з штатного режиму експлуатації в силу випадкових або навмисних дій по завантаженню інформації (перевищення розрахункового числа запитів, надмірний обсяг інформації тощо);

- порушення роботи (випадкове або навмисне) систем зв'язку, електропостачання, водо- і / або теплопостачання;

- витік та оприлюднення приватної інформації, шахрайство, поширення небезпечного контенту, вплив на особистість шляхом збору персональних даних;

- вплив на системи интернет-банкінгу, онлайн-торгівлі, геоінформаційних систем і хакерські атаки на сайти.

Найчастіше від зовнішніх загроз страждають стратегічно важливі напрямки або великі підприємства, яким можна завдати непоправної шкоди за допомогою порушення їх інформаційної безпеки, крадіжки даних або коштів. Що стосується малого та середнього бізнесу, то такі підприємства рідко потрапляють під зовнішній удар, оскільки не представляють особливого інтересу, навіть враховуючи значно слабші засоби захисту від зовнішніх загроз.

У внутрішнього же порушника, особливо в тому випадку, якщо його дії свідомі і не є помилкою, стимулів значно більше. Від банальної образи до матеріальної вигоди у разі підкупу з боку конкурентів, а можливостей при цьому значно більше, оскільки він спочатку вже є легальним користувачем мережі, має доступ, включаючи конфіденційні ресурси організації, і може використовувати корпоративні додатки та обробляти в них дані на законних підставах. Приблизно в 40% випадків зовнішнього втручання в роботу підприємства - обхід системи інформаційної безпеки не відбувається через те,

що для удару використовувалися внутрішні ресурси підприємства і зацікавлені штатні його співробітники.

На жаль, великі зусилля витрачаються саме на захист від зовнішніх загроз і на це є кілька причин. Будувати систему захисту від зовнішнього ворога досить просто. Це добре відомий шлях, засоби захисту від загроз в більшості випадків схожі, а деталі вимагають лише адаптивності до певної ситуації. Крім того, побудова системи захисту від зовнішніх загроз безпосередньо не впливає на працездатність підприємства.

Захист же від внутрішніх загроз набагато складніший та вимагає великих зусиль, а також витрат. Він полягає у забезпеченні безпеки самих додатків та грамотному адмініструванні, яке означає, що співробітників компанії мають чіткі привілеї щодо доступу до інформаційних ресурсів підприємства. Рішення проблеми інформаційної безпеки вимагає, з одного боку, високоорганізованого кадрового забезпечення, створення системи підготовки фахівців, що володіють відповідними знаннями та навичками забезпечення інформаційної безпеки підприємства. З іншого боку, економічна безпека неможлива без використання інноваційних технологій, однією з яких є блокчейн.

Блокчейн - це тип захищеної бази даних, яка підтримує список записів, що постійно розширюється. Кожен із записів або блоків бере посилання на попередні блоки. Це само по собі робить їх стійкими до модифікацій з боку зовнішніх джерел. Аналіз блокчейн-системи дозволяє виділити основні властивості блокчейна: наявність бази даних; використання шифрованих методів ідентифікації користувачів; розподіл між користувачами; вільна реєстрація та подальший вільний доступ до функціоналу; захищений механізм консенсусу.

Технологія блокчейн забезпечує наскрізну конфіденційність та шифрування, забезпечуючи зручність для користувачів. Фундаментом безпеки блокчейну служить децентралізована система, яка зарекомендувала себе краще, ніж централізована, яка вразлива для атак. Блокчейн може допомогти в боротьбі з кібератаками та завдяки своїй природі розповсюдження та тиражування, консенсусу учасників і використання останніх досягнень в криптографії. Безпека технології блокчейн базується на ряді принципів.

1. Однорангові з'єднання дозволяють користувачам взаємодіяти один з одним на рівних умовах. Крім того, у кожного вузла є копія розподіленої книги. Велика кількість вузлів забезпечує стійкість блокчейну навіть тоді, коли деякі з них недоступні. І якщо деякі комп'ютери заражені шкідливими програмами, правильний блокчейн буде як і раніше доступний через інших учасників мережі, які можуть легко виявити поведінку, яка відхиляється від норми.

2. Розподілений консенсус вимагає згоди між більшістю вузлів, чого важко досягти. Однак такий підхід дозволяє блокчейн-технології підтвердити єдину версію правди, не вимагаючи центрального авторитету. Порушення механізму консенсусу можливо лише в тому випадку, якщо хакери

використовують 51% обчислювальної потужності блокчейну. Щоб підробити запис довелося б зламати не менше 50% + 1 комп'ютери, з'єднаних в мережу. Все це робить хакерську атаку складною та занадто витратною. Тому блокчейн вважається дуже надійним способом зберігання даних.

3. Шифрування - використовується для захисту даних та забезпечення безпеки інформації під час її руху по мережі. Блокчейн є результатом багаторічних глобальних досліджень та розробок у галузі безпеки та криптографії, що робить його потенційно ефективним інструментом захисту конфіденційної інформації та підвищення економічної безпеки.

Крім того, технологія блокчейн дозволяє створювати нові бізнес-моделі та забезпечувати підвищення рівня ефективності. У сфері фінансових послуг блокчейн дозволяє виконувати операції автоматично та з більшою ефективністю. На виробництві дає можливість постачальникам відстежувати окремі деталі від надходження сировини до доставки готової продукції споживачеві. Блокчейн підвищує ефективність, зменшує потребу в контролі, скорочує кількість посередників та оптимізує якість перевірок.

Сьогодні ця технологія не тільки має велике коло користувачів, а й встигла себе зарекомендувати на державному рівні. Один із прикладів – Естонія, яка є лідером у впровадженні електронних державних послуг на основі блокчейну. Грузія була однією з перших, яка перевела весь земельний кадастр країни на блокчейн, що дозволило підвищити прозорість прав власності на землю, зменшити частоту випадків шахрайства та значно заощадити час і витрати на реєстрацію.

Industry 4.0 викликала розвиток нових технологій з Blockchain. Ця технологія гарантує, що кіберфізичні системи, складові інтелектуального виробництва, можуть безпечно та автономно замовляти необхідні запасні частини, точно визначити майбутні збої в ланцюзі поставок до того, як вони відбудуться, та оптимізувати свої виробничі процеси для зменшення споживання енергії та інших переваг. В управлінні промисловими процесами дані стають одним з найбільш важливих активів без необхідності будь-яких зовнішніх сертифікуючих агентів і, таким чином, сприяють довірі між споживачами та партнерами. В даний час існують механізми для гарантії того, що транзакції автентифікуються в мережі (авторизованих) учасників з розподіленими базами даних, що дозволяє створювати механізми співпраці між різними виробництвами.

Виділимо основні особливості використання блокчейну з метою економічної безпеки підприємства:

1. Децентралізований характер - типовий клієнт-сервер поставляється з деякими основними питаннями. Часто сервер є вразливим, а служби брандмауера недостатньо сильні, щоб стримувати хакерів. Це звичайна мережева структура багатьох підприємств і навіть витрати на протоколи безпеки не в змозі зупинити хакерів. Саме тут в гру вступає децентралізація

блокчейну, яка для підприємств пропонує піринговy мережеву систему, тому немає центрального органу для саботажу системи обліку. Більш того, тепер контроль буде в руках користувача.

2. Незмінна структура - незмінність робить леджерну систему брандмауером. В цьому випадку, якщо блок додається в Книгу один раз, ніхто не зможе його поміняти або змінити. Однак в деяких випадках підприємства можуть пред'являти і інші вимоги. Але в більшості випадків жодна людина не може змінити леджер та отримати більше привілеїв.

3. Більша прозорість – вся інформація в системі леджера відкрита для перегляду користувачами в мережі. Але блокчейн також може запропонувати процес аутентифікації та рівень доступу для захисту певної конфіденційної інформації для підприємств. Незважаючи на це, рівень прозорості величезний, тому користувачі можуть бачити, що роблять інші користувачі, хоча їх особистість може залишатися прихованою. Таким чином, можна побачити тільки публічну адресу людини.

4. Дешева вартість - розробка свого власного блокчейну є достатньо дорогою, але є можливість використовувати готові рішення. Таким чином, можна скоротити витрати розробників або навіть мережевих менеджерів, а корпоративне блокчейн-рішення поставляється з управлінням мережею. Це функція, яку багато підприємств можуть використовувати для оновлення своєї внутрішньої мережі.

5. Швидкий результат - підприємства мають справу з досить великим обсягом трансакцій щодня. Багато платформи здатні конкурувати за транзакцію протягом 20 секунд. Це значно швидший результат у порівнянні з банками, операції яких займають від трьох до шести днів.

6. Основною і головною особливістю блокчейну є використання алгоритмів математичного обчислення, і виключення людського фактору при прийнятті рішення у системі.

Технологія Blockchain може виступати інтелектуальною платформою економічної безпеки підприємства та пропонує цілий ряд можливостей - операції з блокчейнамі забезпечують більш високий рівень автоматизації, знижують витрати та прискорюють процеси, що в результаті призводить до більшої гнучкості і швидкості реакції системи.

При використанні блокчейн-технологій для побудови моделі економічної безпеки підприємства необхідно:

- враховувати тріаду (ризик – агроза - небезпека) в процесі забезпечення безпеки, а також постановку і чітке виконання всього алгоритму;

- чітко визначити мету, завдання, функції, принципи економічної безпеки підприємства;

- визначення та використання групи показників (індикаторів), що визначають економічну безпеку підприємства;

- встановлення порогових та граничних значень, при яких економічна безпека переходить в стан небезпечний;
- вибір механізму забезпечення економічної безпеки;
- моніторинг в on-line режимі основних показників та прийняття коригувальних дій.

Модель взаємодії між учасниками виробництва на основі блокчейну прискорює процеси, оскільки проведення контролю математичними та криптографічними алгоритмами скоротить час виконання всіх операцій та зменшить кількість необхідних документів. Використання блокчейн-платформ може бути набагато ефективнішим при використанні таких технологій, як смарт-контракти та Інтернет речей.

Смарт-контракти представляють собою комп'ютерні програми, які виконують операцію залежно від дій іншого об'єкта без втручання людини. Для підприємства важливо, що смарт-контракти можуть стежити за виконанням умов виробництва, транспортування, зберігання та використання товарів і комплектуючих в ланцюзі постачань. При складанні звичайної угоди, юристи прагнуть зменшити всі можливі ризики невиконання зобов'язань однієї зі сторін, тоді як розумні контракти роблять все автоматично. Смарт-контракт не можна не виконати або виконати неналежним чином, оскільки за всім стежать математичні алгоритми.

Таким чином, немає потреби обговорювати ризики, і роботу з їх мінімізації візьме на себе нейтральний рахунок. Покупець зараховує на нього гроші, а смарт-контракт переводить їх на рахунок продавця тільки після прибуття вантажу або виконання іншої умови. Крім того, процес реалізації смарт-контракту відкрито для всіх учасників блокчейну, в тому числі і податкових органів. Інтернет речей дає можливість контролювати весь ланцюг поставок, не тільки від точки відправлення до точки призначення, але і відстежувати стан продукту. Розподілений реєстр, в даному випадку, виконує функцію інформаційного інтегратора, куди відомості надходять як від учасників, так і від сенсорного і бездротового обладнання Інтернету речей. В якості такого можуть бути встановлені датчики, камери, показники температури і вологості, GPS-навігатори та інші мобільні системи, які безпосередньо передають інформацію про стан продукту, цілісність, температурний режим, маршрут його слідування, місцезнаходження на складі та інші обставини.

Ще одним важливим завданням захисту інформації, що зачіпає, блокчейн-рішення є забезпечення довіри користувачів. Усі транзакції між усіма сторонами в такій мережі дезінтегровані та децентралізовані на глобальному рівні.

Порівняння технології блокчейну та традиційних технологій зберігання даних в виробничих системах представлено у таблиці 1.

Таким чином, використання блокчейн-технологій на підприємстві вирішує проблеми, які характерні для традиційних систем баз даних, забезпечує безпечний простір для зберігання всієї інформації. Оскільки дані децентралізовані, плавне функціонування системи не залежить від будь-якого конкретного постачальника хмарних послуг. Так, як в ланцюжку блоків технологія не дозволяє змінювати дані після їх запису, вони не можуть бути змінені власниками для особистих цілей. Математичне моделювання підтверджує частину отриманих висновків, зокрема, що стосуються достовірності одержуваної інформації та її захищеності. Блокчейн як технологія поки перебуває на стадії становлення. Але навіть в такому вигляді розподілені реєстри здатні принести користь бізнесу, зробивши його операції швидшими, прозорішими та надійнішими.

Зараз перед власниками компаній стоїть завдання органічного інтегрувати блокчейн у уже функціонуючі системи, щоб поліпшити їх та адаптувати їх до сучасної реальності цифрової епохи. Технологія блокчейну на підприємстві може бути впроваджена в поточну інформаційну систему, наприклад «1С», як окрема підсистема, яка може бути підключена до будь-якої з функціональних підсистем з мінімальними витратами праці. Найбільші труднощі полягають в тому, як обробити десятки мільйонів записів блокчейн в прийнятний час для формування звіту в інформаційній системі. Подальші дослідження повинні бути спрямовані на систематизацію показників моніторингу економічної безпеки на рівні господарюючого суб'єкта в on-line режимі, розробку та впровадження пілотних проектів по використанню інтернет речей і блокчейну, їх інституційного забезпечення, їх вплив на прибуток підприємства.

В основі системи забезпечення економічної безпеки підприємства повинен бути постійно діючий в часі та просторі ефективний механізм, який активно сприймає вплив зовнішніх чинників, і тому - постійно змінюється. Його функціонування можливе лише за умови наявності та взаємодії взаємопов'язаних структурних підсистем.

Таблиця 1

Порівняння технології блокчейну та традиційної технологій зберігання даних

Характеристика	Технологія блокчейн	Традиційні технології
Володіння даними	Підтримка за допомогою криптографічних ключів та власних криптографічних алгоритмів	Центральний орган управління
Конфіденційність та безпека	Криптографічна аутентифікація	Налаштування кожного рядка на основі примусового виконання з центрального органу
Довіра	Через незмінні записи	Через центральний орган
Якість даних	Незмінний запис з автоматичним	Для складних процесів вирішення конфліктів потребує ручного

	врегулюванням конфліктів за допомогою консенсусу по транзакціях	втручання
Дійсність бази даних	Безперервний потік	Надається тільки для окремих екземплярів в часі
Поширення даних	Швидке поширення по всім мережевим нотаткам	За допомогою призначених для користувача процесів синхронізації
Надійність і доступність	Однорангова мережа для розподіленої реплікації даних по всіх вузлах	Потенційна єдина точка відмови
Збережені процедури	Розумні контракти	Недоступно
Створення транзакції	Доступно для всіх дозволених сторін	Управління через центральний орган

Нормативно-правова підсистема забезпечення економічної безпеки включає всю сукупність нормативно-правових актів, що регулюють відносини, пов'язані із забезпеченням економічної безпеки на всіх рівнях управління підприємством.

Організаційно-управлінська складова охоплює органи управління підприємством, діяльність яких спрямована на реалізацію економічної політики щодо забезпечення економічної безпеки та захист економічних інтересів підприємства від загроз внутрішнього і зовнішнього характеру.

Фінансово-економічна підсистема передбачає створення та вдосконалення форм планування, кредитування, обліку та контролю заходів, пов'язаних із забезпеченням економічної безпеки, а також фінансування пріоритетних напрямків розвитку підприємства.

Завданням науково-технічної складової системи забезпечення економічної безпеки є сприяння переходу на інноваційний шлях розвитку, впровадження ресурсозберігаючих технологій та оновлення основного капіталу підприємства.

Система забезпечення економічної безпеки включає також кадрову підсистему, яка передбачає специфічну, повторювану діяльність, яка здійснюється в процесі управління та полягає в забезпеченні підприємства необхідним контингентом людей і інформації про них; впровадження науково обґрунтованих методів відбору, розподілу, навчання, стимулювання кадрів.

У процесі діяльності, спрямованої на забезпечення економічної безпеки велике значення має об'єктивна, повна, комплексна, інформація про економічний стан підприємства та рівень реалізації його пріоритетних інтересів. Тому основними завданнями інформаційно-аналітичної складової системи забезпечення економічної безпеки є аналіз економічного стану, виявлення тенденцій розвитку, виявлення та оцінка загроз економічній безпеці на всіх рівнях.

Висновки. Підводячи підсумки, визначимо основні напрями вдосконалення потенціалу економічної безпеки промислового підприємства.

1. Удосконалення фінансового потенціалу передбачає забезпечення максимально високого рівня платоспроможності підприємства та ліквідності його оборотних коштів. Активно використовувати банківський капітал, не тільки для короткострокового поповнення оборотних коштів, а й для цілей інноваційного розвитку підприємства.

2. Інтелектуальний та кадровий потенціал - створення пріоритетних умов для докорінної модернізації навчально-лабораторної та науково-виробничої бази навчальних закладів, що забезпечують підготовку та перепідготовку фахівців підприємства.

3. Техніко-технологічний потенціал економічної безпеки передбачає оптимізацію виробничих потужностей, модернізацію виробництва, освоєння нової техніки, зростання обсягів поставок продукції на внутрішній та зовнішній ринки за рахунок конкурентних переваг по співвідношенню «ціна - якість».

4. Політико-правова безпека передбачає чітке дотримання законодавства в податковій, тарифній, митній, освітній та соціальній сферах. А зниження податків на промислові підприємства з боку держави дозволить відновити зростання інвестицій.

5. Забезпечення інформаційної складової економічної безпеки промислового підприємства включає в себе:

- збір та аналіз інформації, що відноситься до роботи підприємства (інформація по товарним, технологічним, трудовим, фінансовим та іншим ринкам; науково-технічна, політична інформація);
- проведення аналізу отриманої інформації (систематизація і класифікація інформації, постійна аналітична діяльність);
- прогнозування тенденцій розвитку наукового та технологічного процесів в області технологічної діяльності (фінансові прогнози, прогнози стану об'єктів виробництва та технологічного розвитку підприємства);
- оцінку рівня економічної безпеки підприємства за всіма її складовими в цілому, розробка пропозицій, направлених на підвищення її рівня;
- інші види діяльності, спрямовані на забезпечення інформаційної складової економічної безпеки підприємства (діяльність служби зі зв'язків з громадськістю, захист від недозволеного доступу до конфіденційної інформації підприємства - промислового шпигунства).

6. Екологічна безпека - дотримання норм екологічної безпеки, що дозволить не тільки мінімізувати штрафні санкції, а й активізувати процес виходу продукції підприємства на світові ринки.

7. Забезпечення силової складової економічної безпеки включає в себе вирішення наступних завдань:

- фізична безпека співробітників та керівників підприємства;

- збереження майна підприємства від негативних впливів (безпека майна, баз даних, цінностей, активів інноваційних підприємств);
- силового аспекту інформаційної безпеки;
- сприяння зовнішнього середовища бізнесу (збір та аналіз інформації про контракти підприємства на ринку, здійснення попередніх заходів з боку служби безпеки підприємства).

Таким чином, проведений аналіз показує, що будь-яке підприємство постійно піддається впливу внутрішніх та зовнішніх загроз економічній безпеці та у зв'язку з цим, проблема запобігання цих загроз та компенсацію збитку від їх дії вимагає постійного контролю. При цьому повинні досягатися основні цілі економічної безпеки - стійке і максимально ефективне функціонування промислових підприємств, створення високого потенціалу зростання і розвитку їх в майбутньому.

Список використаних джерел:

1. Алькема В.Г., Літвін Н.М., Кириченко О.С. Економічна безпека інноваційного підприємства. К.: Крок, 2015 – 320 с.

2. Ареф'єва О.В., Кузенко ТБ. Планування економічної безпеки підприємств. К.: Вид-во Європ. ун-ту. 2004. – 169с.

3. Бланк И.А. Управление финансовой безопасностью предприятия. К.: Эльга, Ника-Центр. 2004. 784 с.

4. Волошин И.П. Типы блокчейн и анализ экономических характиристик. Экономическая безопасность и качество. 2018. № 4(33). С. 65-69.

5. Гавкалова Н.Л., Чаплигіна Ю.С. Підходи щодо визначення безпеки підприємства. Економіка розвитку. 2011. № 4 (60). С. 68-71.

6. Геєць В.М., Кизим М.О., Клебанова Т.С., Черняк О.І. Моделювання економічної безпеки: держава, регіон, підприємство. Монографія. Харків. Вид-во «ІНЖЕК». 2006. 240с.

7. Козаченко Г.В., Пономарьов В.П., Ляшенко О.М. Економічна безпека підприємства: сутність та механізм забезпечення: монографія. К. Вид-во «Лібра». 2003. 280с.

8. Колесников П., Бекетова Ю., Крылов Г. Технология блокчейн. Анализ атак, стратегии защиты. LAP LAMBERT Academic Publishing. 2017. 76 p.

9. Bryk A. Blockchain: Cyber Security Pros and Cons. Режим доступу: https://www.apriorit.com/dev-blog/462-blockchain-cybersecurity-pros-cons

10. Marchesoni, E. Blockchain: Shaping Industry 4.0. 2018. Режим доступу: https://www.linkedin.com/pulse/blockchain-shaping-industry-40-eloisa-marchesoni