6. Вільна, нерегульована вартість страхового товару.

7. Забезпечення страховим компаніям доступу до перестрахування за кордоном та часткової державної підтримки для великих виплат [4].

До речі, військове страхування в Британії згодом було переформатовано у національне страхування, яке охоплювало всі види ризиків та допомоги, а також забезпечувало безкоштовне медичне обслуговування, зробивши величезний внесок у сучасну систему соціального захисту британських громадян.

Закликаючи іноземний капітал прийти в Україну з інвестиціями або фінансувати роботи з відновлення інфраструктури, ми повинні усвідомлювати, що їхні стандарти бізнесу вимагають, щоб усі етапи будівництва чи реконструкції були застраховані від багатьох ризиків, у тому числі й військових.

Список використаних джерел:

1. Бурбель Л. Шість головних викликів, з якими зустрівся страховий ринок упродовж шести місяців війни. Interfax – Україна інформаційне агентство. URL: https://interfax.com.ua/news/blog/856594.html.

2. Дерев'янко А. Страхування воєнних ризиків − досвід України та інших країн. Commercial Property. URL: https://commercialproperty.ua/interview/strakhuvannya-voennikh-rizikiv-dosvid-ukraini-ta-inshikh-krain/.

3. Зубко Г. Страхування в умовах воєнної економіки та повоєнного відновлення на основі британського досвіду. Українська правда. URL: https://www.epravda.com.ua/columns/2023/03/9/697856/.

4. Міжнародний історичний досвід повоєнної реконструкції економіки: уроки для України : матеріали міжнародної науково-практичної конференції (Київ, 27 квітня 2023 р.) / ДУ «Ін-т екон. та прогнозув. НАН України», Інститут вищої освіти НАПН України. – Електрон.дані. – К., 2023. – 125 с.

БЕЗПЕКА ЦИФРОВИХ СИСТЕМ, ЯК ЗАСІБ ЗАБЕЗПЕЧЕННЯ ЕФЕКТИВНОЇ РОБОТИ ТРАНСПОРТНОЇ СФЕРИ

Масан В. В., *аспірант, Український державний університет залізничного транспорту, м. Харків*

Ефективне функціонування економіки стало залежним від цифрового середовища. При цьому все більше зростає число невизначеностей, властивих цифровому простору. Цифрові загрози стали масштабнішими, що найчастіше призводить до значних фінансових, репутаційних та часових витрат [1]. Напрями, пов'язані з цифровими технологіями, так чи інакше позначені у планах розвитку більшості держав, які прагнуть вирішувати соціально-економічні проблеми і знижувати ризики цифровізації шляхом розробки та реалізації стратегій безпеки в цифровий простір.

Безпека цифрових систем є актуальною проблемою для економіки та суспільства загалом і одним із ключових та «наскрізних» напрямів управління цифровізацією, що вимагає адекватних заходів захисту всіх учасників.

У багатьох країнах стратегія цифрової безпеки приймається як цілісний документ, пов'язаний із забезпеченням національної безпеки. При цьому всі знають, що масштаби загроз і ризики виходять за межі окремих держав і стають світовими. Усвідомлення цього факту сприяло створенню рядом країн спеціалізованих організацій для координації мережевої та інформаційної безпеки на національному та міжнародному рівні. Типовими цілями стратегій із забезпечення безпеки у цифровому просторі є [2]:

- виявлення кібератак і реагування на них;
- запобігання загрозам, підтримці та розробці надійних продуктів і послуг для державних структур і суб'єктів економічної діяльності;
- підтримка державних установ та операторів інфраструктури;
- сприяння розвитку освіти в галузі цифрових технологій.

Крім того, у більшості країн створено національні програми захисту інфраструктури, які визначають технічні та функціональні критерії для цифрових технологій та сприяють ідентифікації щодо потенційно вразливих елементів, зокрема транспорту, на основі розробки правил та процедур забезпечення доступу до них. Наприклад, деякими країнам були створені комп'ютерні групи реагування на надзвичайні ситуації для більш ефективного обміну інформацією та розвитку співробітництва з організаціями приватного сектору, а також для координації цифрової взаємодії між країнами. Загальновизнаними вважаються необхідність подальшого міжнародного співробітництва, реалізація конкретних оперативних ініціатив у сфері міжнародної та регіональної безпеки в цифровому середовищі, а також інші форми двостороннього та багатостороннього сприяння [3].

У провідних світових країнах, як і раніше, пріоритетне заохочення подальшого розвитку інфраструктури широкосмугової мережі, оскільки доступність даного виду зв'язку вважається рушійною силою інновацій, зростання робочих місць у цифровій економіці. Це означає, що високоякісна інфраструктура повинна бути доступна для широкого загалу потенційних користувачів, щоб забезпечити розвиток таких сфер діяльності, як охорона здоров'я, освіта, фінанси, транспорт. За останні кілька років були розроблені та впроваджені національні плани (як складові стратегій) щодо розвитку широкосмугового доступу, що передбачають розширення мереж та їх модернізацію для забезпечення більш високих швидкостей передачі даних для конкретних соціальних та економічних груп населення. Заходи щодо здійснення подібних стратегій варіюються від створення базової комунікаційної інфраструктури до розробки складних цифрових систем в тому числі й на транспорті.

Таким чином, широкомасштабне вирішення проблем економічної безпеки транспорту у цифровому суспільстві дозволить забезпечити цілеспрямоване формування процесу економічного зростання та підвищення економічного добробуту всього суспільства.

Список використаних джерел:

1. Економічні ризики: методи вимірювання та управління: навчальний посібник / Скопенко Н.С., Федулова І.В., Мазник Л.В., Кириченко О.М., Удворгелі Л.І.; за заг. ред. Скопенко Н.С. К. : НУХТ, 2021. 344 с.

2. Толстова А.В., Хоменко К.В. Методика оцінювання рівня економічної безпеки підприємства. *Вісник економіки транспорту та промисловості*. 2018. № 63. С. 187-195.

3. Каличева Н. Є. Підходи до управління конкурентними перевагами підприємств залізничного транспорту. *Причорноморські економічні студії*. 2017. Вип. 21. С. 86-91.

ОРГАНІЗАЦІЯ ВНУТРІШНЬОГО АУДИТУ ЗАПАСІВ В СИСТЕМІ УПРАВЛІННЯ СУБ'ЄКТА ГОСПОДАРЮВАННЯ В УМОВАХ ВОЄННОГО СТАНУ

Мізік Ю. І., *канд. екон. наук, доцент,* ***Юнг Р. В.,*** *магістр, Харківський національний університет міського господарства імені О. М. Бекетова*

Військова агресія росії проти України викликала масштабні руйнування виробничого капіталу та інфраструктури, принесла людські жертви та соціальні втрати. Війна призвела до скорочення робочих місць і доходів, зменшення купівельної спроможності і обсягів накопичених активів. У 2022 році національна економіка втратила 29,2% реального ВВП, що майже третина від довоєнного рівня [1].

Внутрішній аудит завжди був на передовій захисту інтересів інвесторів і спільноти в широкому бізнесовому розумінні. Безумовно, війна в Україні накладає суттєві обмеження на функціонування внутрішнього аудиту, адже на перший план вийшли питання фізичної безпеки працівників. Утім, багато в чому досвід роботи під час пандемії став у пригоді.

Організація ефективного аудиту в умовах воєнного стану потребує передовсім якісної інформаційної бази для його виконання щодо суб'єкта господарської діяльності. Інформаційна база містить інформацію, тобто відомості, отримані аудитором із різних джерел, які корисні й потрібні для прийняття управлінських рішень і формування судження аудитора про об'єкт аудиту. Організація і формування джерел надходження своєчасної, обґрунтованої та оперативної інформації, необхідної для виконання аудитором своїх функціональних обов'язків являє собою інформаційне забезпечення аудиторського процесу. Завданням інформаційного забезпечення є інформування учасників аудиторського процесу щодо стану, якості функціонування об'єктів перевірки та відповідності діяльності підприємств нормативно-правовим актам та законодавству. Це засвідчує вагому роль інформаційного забезпечення у виконанні аудиту.

Об'єктами внутрішнього аудиту виробничих запасів є:

1) кількісне та якісне приймання запасів від постачальників, а також при внутрішньому переміщенні в міжцеховому напрямку, між матеріально відповідальними особами, складами та виробництвом;

2) умови зберігання запасів і закріплення матеріальної відповідальності;