УДК 656.073.8

Ю.В.Коноваленко,
Київський національний торговельно-економічний університет,
м. Київ

КОМПЛЕМЕНТАРНІСТЬ ТЕХНОЛОГІЧНИХ РІШЕНЬ ПРИ МОНІТОРИНГУ БЕЗПЕКИ КОНТЕЙНЕРНИХ ПЕРЕВЕЗЕНЬ

У статті порушується питання комплементарності доступних у даний час на ринку технологічних рішень при моніторингу безпеки контейнерних перевезень. За умови зростання обсягів контейнерних вантажних перевезень та їх зручності, а також існування загроз безпеки перевезень проблема убезпечення вантажу набуває нової актуальності. В результаті дослідження рішень пропонуються їх поєднання для різних рівнів автоматизації системи моніторингу безпеки перевезень.

В статье поднимается вопрос комплементарности доступных в данный момент на рынке технологических решений при мониторинге безопасности контейнерных перевозок. При росте объемов контейнерных грузоперевозок и их удобства, а также существовании угроз безопасности перевозок проблема сохранности груза приобретает новую актуальность. В результате исследования решений предлагаются их сочетания для различных уровней автоматизации системы мониторинга безопасности перевозок.

The article looks in into the question of complementariness of technological solutions currently available on market for monitoring of security of container shipments. Under condition of growing volumes of container shipments and their convenience as well as existence of shipments security threats, the issue of securing cargo gains new topicality. In the course of research into the solutions their compatibility for different levels of automation of shipments security monitoring system is put forward.

Ключові слова: контейнерні перевезення, безпеки перевезень, управління ризиком, транспортний ризик, несанкціоноване проникнення.

Діяльності підприємства притаманна безмежна кількість ризиків як внутрішніх, так і зовнішніх, якість управління якими визначатиме рівень прибутковості суб'єкта господарювання, його конкурентну позицію. Детальне вивчення ризику надає змогу прийняття більш поінформованих управлінських рішень та визначення слабких місць у бізнес-процесах підприємства, які вимагають реконфігурації, як в плані послідовності виконуваних процедур, так і відповідальних осіб.

Донедавна дещо ігнорований вид ризику, а саме транспортний, а точніше управління ним надає змогу розкрити прихований потенціал оптимізації та убезпечення перевізницької діяльності і збільшити прибутковість підприємства. Авторське дослідження діяльності 46 українських торговельних підприємств демонструє доцільність прийняття даного виду ризику до уваги.

Так, наприклад, 86,67% опитаних менеджерів зазначених підприємств зазначили, що відповідними працівниками на їхніх підприємствах витрачається на управління транспортним ризиком всього лиш до 10% робочого часу; значення від 10% до 30% часу було зазначено 11,11% опитаних і лише 2,22% менеджерів вказали, що на підприємстві витрачається від 30% до 50% робочого часу на таку процедуру. При цьому, частка витрат, спричинених проявом транспортного ризику у 2011 р., склала в прибутку підприємств до 25%, а в загальних витратах – до 5%.

Крім цього, хоча й по галузі чи загалом дані щодо втрат від прояву транспортного ризику відсутні навіть у країнах із зразковим статистичним обліком, такі установи та організації, як FreightWatch, CargoNet, Chubb Insurance та Supply Chain Information Sharing and Analysis Center (SC-ISAC) при використанні схожих

методик збору та реєстрації даних лише для випадків викрадення вантажу при перевезенні наводять дані в межах від 8 до 30 млрд. дол. США за рік для США [1, с. 3-4]. А за даними бази Alphaliner близько 10 тис. контейнерів втрачаються при перевезенні морським транспортом, що складає 0,77% річного обороту контейнерів, або у грошовому виразі – 1,16 млрд. дол. США (і це без врахування збитків від пошкодження контейнерів, часткового чи повного викрадення або пошкодження вантажу в контейнері, контейнерних перевезень іншими видами транспорту) [2]. Враховуючи зручність контейнерних вантажних перевезень та їх постійно зростаючу роль, проблема прояву транспортного ризику, зокрема в розрізі контейнерних перевезень, при здійсненні вантажних перевезень є досить актуальною та вимагає дослідження.

Невпинний розвиток технологій та нових господарських рішень у вигляді програмних продуктів розширює можливості підприємства в плані реалізації дій у власних бізнес-процесах, які до цього були неможливими (визначення місця перебування контейнера під час транспортування з точністю до кількох десятків чи сотень метрів) чи досить затратними (система відеоспостереження із модулем GSM для передачі відеосигналу власникові вантажу чи його уповноваженому представникові). Попри наявність значної кількості та різноманіття технологічних рішень на ринку, дослідниками до цього приділялося недостатньо уваги можливості поєднання таких технологій, їх особливостям при таких поєднаннях та можливим синергетичним ефектам для забезпечення більш надійних контейнерних перевезень. Наприклад, використання виключно сенсорів шоку на контейнері може виявитися не досить надійним без поєднання їх із GSM- чи GPS-пристроями передачі даних, які нададуть можливість визначення місця неправильного поводження з контейнером та, як результат, відповідальної сторони.

Так, наприклад, хоча І.Зуді, С.Кумером та Е.Ленер виділяються убезпечуючі заходи (в тому числі і технологій), які можуть підвищити рівень безпеки контейнера та його вмісту при перевезенні, не приділяється увагу доцільності поєднання кількох видів технологій [3, с.153-167]. Такі науковці, як Е.Госвамі [4], Я.Пул [5], Т.Кенні та В.Кестер [6, с.1-22], Й.Лі та Р.Мутарасан [6, с.161-180], Т.Кенні [6, с.181-191, 307-320], А.Чу [6, с.457-480], Ф.Торнтон та К.Лантем [7], Р.Вонт [8], К.Світ [9] та М.Едгертон [10] хоча і займалися дослідженням окремих видів технологій чи рішень та їх особливостями при застосуванні до убезпечення вантажних контейнерних перевезень, проте не приділяли уваги можливості та необхідності поєднання рішень задля забезпечення більш повного охоплення всіх кроків.

Проте система безпеки перевезень на кожному підприємстві має бути переважно індивідуально сконфігурованою залежно від виду вантажу, який перевозиться, обсягів перевезень, бюджету, який передбачається на організацію та підтримання системи безпеки, інших індивідуальних факторів. Розмаїття потреб та вимог, що висуваються підприємствами із перевізницькою функцією до убезпечення вантажоперевезень, визначає окремі технології для використання та їх поєднання. Тому, на думку автора, важливим виступає розгляд питання

можливості та доцільності поєднання окремих технологічних рішень з метою підвищення рівня безпеки вантажних контейнерних перевезень.

У даній статті автором ставиться завдання розгляду основних технологій в сфері убезпечення вантажних контейнерних перевезень, дослідження їх основних функцій та можливості поєднання із іншими рішеннями. Залежно від вимог підприємства (повна чи часткова автоматизація моніторингу безпеки контейнерних перевезень) автором планується розглянути випадок необхідності втручання людини в процес моніторингу для забезпечення комплементарності технологій та випадок відсутності такої потреби.

Для дослідження були обрані окремі види технологічних рішень для забезпечення моніторингу безпеки контейнерних перевезень (наприклад, система безпеки Zoner-Relayer на основі технології RFID) та збірні види рішень, що передбачають можливість модифікації продуцентом специфікації кінцевого продукту, проте без суттєвої зміни властивостей чи функцій пристрою (технології) (наприклад, хімічні, біологічні чи теплові сенсори, GPS- та GSM-пристрої для передачі даних). Технології, що були обрані для конфігурації системи безпеки контейнерних перевезень, включають такі, які на даний момент досить поширені та доступні, а можливість застосування не ускладнюється необхідністю вивчення нових технологій (технології прості у використанні) та включають:

1) GPS-пристрої для передачі даних (представлені всіма варіаціями пристроїв системи глобального позиціонування, які забезпечують отримання інформації про місцезнаходження об’єкта, до якого прилаштований пристрій такого класу; не включають пристрої-гібриди a-GPS чи інші пристрої, які використовують інші частоти чи мережі для отримання даних про місцезнаходження пристрою);

2) GSM-пристрої для передачі даних (всі пристрої глобальної системи мобільних комунікацій частот 1800, 1900 і 900 MHz та інтерфейсу TDMA, які з певною попередньо визначеною частотою чи на запит користувача визначають місце розташування даного пристрою та передають його до серверу користувача; не включають пристроїв-гібридів, які поєднують антени для GPS та GSM);

3) RFID-пломби (поєднують у собі властивості звичайної пломби та RFID-тегу, що забезпечує реєстрацію в реальному часі (активну чи пасивну) спроби проникнення до контейнеру; при цьому необхідною є наявність RFID-зчитувача);

4) RFID-наклейки на вантажі (на відміну від попередньої технології, RFID-теги прикріплюються до вантажу безпосередньо, а RFID-зчитувачем, у випадку спроби викрадення вантажу, буде реєструватися переміщення вантажу зі звичного його місця);

5) систему безпеки Zoner-Relayer на основі RFID (дія системи полягає у під'єднанні RFID-тегів (zoners) до всіх стінок контейнера окрім дверей; на двері вмонтовується RFID-зчитувач (relayer), який постійно комунікує із тегами; RFID-теги реєструють проникнення до контейнера збоку, а RFID-зчитувач передає цю інформацію до серверу, за чим слідкує власник вантажу чи його уповноважений представник);

6) інфрачервоні сенсори руху (сенсори реєстрації наявності рухомого об’єкта в контейнері при перевезенні на основі інфрачервоних променів, що вказує на

несанкціоноване проникнення до контейнера);

7) хімічні (газові), біологічні чи теплові та оптичні сенсори (пристрої реєстрації наявності в атмосфері певного хімічного, біологічного компоненту чи варіацію температури зовнішнього середовища; при несанкціонованому відкритті дверей контейнера хімічні, біологічні та теплові (у різних поєднаннях) властивості атмосфери змінюються, що і реєструється даним видом сенсорів);

8) дверний сенсор (пристрій для визначення факту маніпуляції дверима контейнера за обходу дверних замків та пломб (зняття частин дверей із завіс, вирізання частини дверей);

9) сенсори тиску, сили та шоку (пристрої реєстрації зміни тиску на поверхню контейнера (внутрішні чи зовнішні стінки), раптового зміщення контейнеру чи його частини внаслідок завдання вмисної шкоди (спроба відкриття, псування) чи нещасного випадку (псування при перевезенні));

10) сенсори дотику (застосовуються до внутрішніх стінок контейнера, місць, які обов'язково будуть зачепленими при спробі проникнення до контейнеру (двері, нижня частина контейнеру поблизу дверей тощо) та реєструють контакт із сторонніми предметами, що можуть характеризуватися різними ступенями тиску та тривалістю контакту);

11) система відеоспостереження (система забезпечує безперервний моніторинг місць, оснащених відеокамерами);

12) електричний паркан (фізичний бар'єр, що унеможливлює несанкціоноване проникнення сторонніх осіб на територію зберігання контейнерів; пускає струм невеликої напруги при дотику до паркана, після цього спрацьовує сигналізація).

На основі функцій, виконуваних досліджуваними технологіями, автором було здійснено попарне групування рішень за можливістю компліментарності за високої автоматизації процесу моніторингу безпеки переміщення контейнера та за участю людини. В таблиці 1 наведені можливості поєднання технологій без особливого втручання людини (від працівника в даному випадку не вимагається зведення даних із кількох джерел для прийняття рішення про порушення безпеки переміщення контейнера).

Найнижчий рівень комплементарності та найвищий рівень автономності продемонстрували електричний паркан та система відеоспостереження, тоді як різноманітні сенсори виявилися досить поєднуваними із іншими рішеннями (хоча й дублювання функцій небажане через витратність; наприклад, система Zoner-Relayer та інші RFID-пристрої). GPS- та GSM-пристрої для передачі даних демонструють високий рівень поєднуваності із іншими технологіями через високу цінність даних щодо місцезнаходження (та часу) реєстрації несанкціонованого проникнення до контейнера, його пошкодження, незапланованого переміщення вантажу і т.п.

Таблиця 1

Можливість поєднання технологій за вищого рівня автоматизації процесу моніторингу безпеки

№	Назва технології	12	11	10	9	8	7	6	5	4	3	2
1	GPS-пристрої для передачі даних	--	--	+	+	+	+	+	+	+	+	--
2	GSM-пристрої для передачі даних	--	--	+	+	+	+	+	+	+	+	

3	RFID-пломби	--	--	+	+	+	+	+	+	+
4	RFID-наклейки на вантажі	--	--	+	+	+	+	+	+	
5	Система безпеки Zoner-Relayer	--	--	+	+	+	+	+		
6	Інфрачервоні сенсори руху	--	--	+	+	+	+			
7	Хімічні, біологічні чи теплові сенсори	--	--	+	+	+				
8	Дверний сенсор	--	--	+	+					
9	Сенсори тиску, сили та шоку	--	--	+						
10	Сенсори дотику	--	--							
11	Відеоспостереження	--								
12	Електричний паркан									

Умовні позначення: «–» – поєднання неможливе, «+» – поєднання можливе.

Далі в таблиці 2 показано можливості поєднання рішень при необхідності більш значної долученості працівника до процесу моніторингу (відповідальним працівником приймається рішення про порушення безпеки на основі даних із кількох джерел, що забезпечується досліджуваними технологіями; наприклад, якщо були отримані дані щодо реєстрації сенсором шоку незвичайного поводження із контейнером, проте при відеоспостереженні було помічені роботи працівниками складу з розміщення контейнерів, які могли призвести до штовхання контейнера).

Таблиця 2

Можливість поєднання технологій за умови більшої залученості працівника до процесу моніторингу безпеки

№	Назва технології	12	11	10	9	8	7	6	5	4	3	2
1	GPS-пристрої для передачі даних	--	--	+	+	+	+	+	+	+	+	*
2	GSM-пристрої для передачі даних	--	--	+	+	+	+	+	+	+	+	
3	RFID-пломби	--	**É**	±	±	±	±	±	--	+		
4	RFID-наклейки на вантажі	--	**É**	±	±	±	±	±	--			
5	Система безпеки Zoner-Relayer	--	**É**	±	±	±	±	±				
6	Інфрачервоні сенсори руху	--	**É**	±	±	±	±					
7	Хімічні, біологічні чи теплові сенсори	--	**É**	±	±	±						
8	Дверний сенсор	--	**É**	±	±							
9	Сенсори тиску, сили та шоку	--	**É**	±								
10	Сенсори дотику	--	**É**									
11	Відеоспостереження	+										
12	Електричний паркан											

*Умовні позначення: «–» – поєднання неможливе; «+» – поєднання можливе; «±» – за більшої залученості людини бажаний вибір однієї із технологій, що певним чином дублює функції інших рішень (наприклад, сенсор дотику та дверний сенсор); «**É**» – забезпечення рішенням 11 додатковою інформацією працівника у випадку позитивної реєстрації порушення технологіями 3-10; «*» – можливе поєднання за можливого поганого сигналу GSM-пристрою.*

Дані таблиці 2 свідчать про більшу кількість можливих варіацій поєднання технологій через участь людини у прийнятті остаточного рішення щодо наявності порушення безпеки перевезення. Проте і в даному випадку електричний паркан продемонстрував найменшу міру комплементарності через виконувані ним функції, тоді як система відеоспостереження за нових умов починає виступати джерелом додаткової інформації для забезпечення прийняття рішення.

Слід зауважити, що у наведених таблицях зазначається лише попарне поєднання технологій без припущення тієї можливості, що, наприклад, рішення «А» при вдалому поєднанні із рішенням «Б» та при вдалому поєднанні рішення «Б» із технологією «В», рішення «А» не може поєднуватися із технологією «В», якщо це прямо не зазначено в таблиці. В даному випадку рішення «Б» виступає

спільним елементом системи безпеки, що згруповує за собою можливість (необхідність) паралельного застосування рішень «А» та «В», поєднання яких би, за умови відсутності рішення «Б», не мало би ніякої користі чи було би невиправданим.

Здійснене дослідження надало можливість прослідкувати доцільність поєднання доступних технологічних рішень для забезпечення функціонування системи моніторингу безпеки контейнерних перевезень. Оскільки наявність такої системи передбачає, в цілях підвищення її ефективності та оптимальності, відсутність дублювання окремих функцій моніторингу та реєстрації порушень, доповнюваність окремих рішень для забезпечення цілісності та уникнення можливості незареєстрованого несанкціонованого проникнення до контейнеру при перевезенні, результати, отримані при написанні даної статті, уможливлюють побудову системи безпеки за уникнення повторюваності функцій технологічних рішень. Подальші дослідження в даному напрямку мають спрямовуватися на розробку гібридних технологічних комплексів з метою більш високої кастомізації для задоволення потреб підприємства. Має при цьому включатися можливість поєднання технологій різних учасників ланцюга постачань (відправник чи отримувач вантажу, найманий перевізник, експедитор тощо) для мінімізації витрат на встановлення та підтримку функціонування системи моніторингу безпеки контейнерних перевезень.

Список використаних джерел:

1. Dan Burges. Cargo Theft, Loss Prevention, and Supply Chain Management / Dan Burges. — Butterworth-Heinemann, 2012. — 392 pages.
2. Офіційний сайт всесвітньої довідкової бази лайнерних перевезень "Альфалайнер" (Alphaliner). — [Електронний ресурс] — Режим доступу : http://www.alphaliner.com
3. Michael Essig. Supply Chain Safety Management: Security and Robustness in Logistics (Lecture Notes in Logistics) / Michael Essig, Michael Hülsmann, Eva-Maria Kern, Stephan Klein-Schmeink. — Springer, 2012. — 383 pages.
4. Subrata Goswami. Indoor location technologies / Subrata Goswami. — Springer New York, 2013. — 123 pages.
5. Ian Poole. Cellular Communications Explained: From Basics to 3G / Ian Poole. — Newnes, 2006. — 216 pages.
6. Jon S. Wilson. Sensor Technology Handbook / Jon S. Wilson. — Newnes, 2004. — 704 pages.
7. Frank Thornton. RFID Security / Frank Thornton, Chris Lanthem. — Syngress, 2005. — 448 pages.
8. Roy Want. An Introduction to RFID technology / Roy Want // IEEE Pervasive Computing. — January-March, 2006. — Vol. 5. — No. 1. — PP. 25—33.
9. Kathleen M. Sweet. Transportation and Cargo Security: Threats and Solutions / Kathleen M. Sweet. — Prentice Hall, 2005. — 416 pages.
10. Michael Edgerton. A Practitioner's Guide to Effective Maritime and Port Security / Michael Edgerton. — Wiley, 2013. — 296 pages.