Матеріали XIV міжнародної науково-практичної конференції
«Сучасні проблеми менеджменту»

СВІТОВИЙ ДОСВІД УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ЕКОНОМІЧНИХ СУБ'ЄКТІВ

Скоробогатова Н.Є., *к.е.н., доц.*
кафедри міжнародної економіки
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»

В умовах масштабної інформатизації суспільства все більшої актуальності набуває проблема формування ефективної системи кібербезпеки, як економічних суб'єктів, так і повсякденних користувачів інформаційних технологій [1]. Питання забезпечення кібербезпеки виходить далеко за межі певної країни, набуваючи рівня однієї з глобальних проблем людства. Зокрема, зростання кількості кібератак на державні ресурси та загальне збільшення кіберзлочинів обумовлює необхідність впорядкування даної проблеми на міжнародному рівні.

Питання розробки ефективної системи кіберзахисту та управління кібербезпекою обговорюються Організацією Об'єднаних Націй, Міжнародним союзом електрозв'язку, Радою Європи тощо [2]. На даний час дієвим міжнародним правовим документом є «Конвенція про кіберзлочинність» [2].

Її підписали 30 країн, однак далеко не всі ратифікували. Одна з причин відмов від ратифікації – те, що згідно з положеннями Конвенції, будь-яка зі сторін має право без згоди отримувати доступ до комп'ютерних даних, розташованих на території іншої сторони, що ставить під сумнів принцип суверенності держав. У той же час провідні країни світу та міжнародні організації із забезпечення кібербезпеки ініціюють можливість визнання кібератаки, як акту агресії та відповідно реагувати.

Положеннями «Стратегічної концепції оборони та безпеки членів Організації Північноатлантичного договору» від 19 листопада 2010 року зазначається, що «кібератаки стають дедалі частішими, організованими та більш збитковими для державних установ, підприємств, економіки і, можливо, також транспортної и електричної мереж та інших об'єктів критичної інфраструктури; вони можуть досягти критичного рівня, який загрожує національному та євроатлантичному процвітанню, безпеці и стабільності…» [3].

Опрацювання аналітичної інформації свідчить про те, що більшість країн-членів ЄС започаткували робочі групи для вирішення питань захисту критичної інфраструктури. Водночас,

майже половина державних установ, зосереджених на діяльності щодо захисту критичної інфраструктури, підпорядковуються Міністерству внутрішніх справ або подібній установі сектору безпеки країни ЄС. Лише у двох краї□нах Європи є державні установи, які заи□маються винятково питаннями захисту критичної інфраструктури (Велика Британія – CPNI, Іспанія – CNPIC) [5]. У більшості країн центральна установа зосереджується на загальній координації діяльності щодо захисту критичної інфраструктури, а окремі міністерства відповідають за питання певної галузі. Зокрема, на центральну установу покладаються завдання міжнародного співробітництва, організації роботи міжвідомчих робочих груп, формування державної політики тощо. Проте у Норвегії центральна установа виконує ще и□ контрольну функцію щодо ефективності заходів захисту критичної інфраструктури у кожному окремому міністерстві [4].

Досвід США, Великої Британії, Ізраїлю, Німеччини свідчить про створення системи кібербезпеки з єдиним координуючим органом, який здатен за короткий проміжок часу акумулювати сили та засоби різних державних і недержавних органів для протидії та неи□тралізації□ кібератак. Таким чином, можна зазначити, що у краї□нах із високим рівнем інформатизації питання захисту критичної інфраструктури від кіберзагроз є складовою загальнодержавної системи кібернетичної безпеки.

За даними дослідження Booz & Company (Italia) S.r.l. [5], жоден уряд краї□ни-члена ЄС не надає приватним установам фінансову допомогу для компенсації витрат, пов’язаних із приведенням і□х діяльності у відповідність із державними програмами захисту критичної інфраструктури. Натомість, більша частина державної фінансової допомоги, призначена для управління під час надзвичаи□них ситуацій та забезпечення безпеки, залишається у розпорядженні урядових установ, які займаються цими питаннями.

Оскільки державні органи, які координують діяльність щодо захисту критичної інфраструктури, переважно входять до функціональних структур управління вищого рівня, то ним надається перевага при фінансуванні заходів загальнодержавного значення. Водночас приватний сектор має забезпечувати кібербезпеку свого бізнесу та безперервність діяльності за рахунок власних джерел або запозичень. Слід відзначити, що дана модель фінансування має певні недоліки. Фінансове забезпечення власних кваліфікованих фахівців з даного питання та наявність матеріально-технічної бази не завжди є можливими для приватних підприємств через обмеженість обігових коштів.

Інформаційні технології передбачають постійну комунікацію економічних суб'єктів, що потребує відповідних технічних потужностей та засобів зв'язку. Тому вважаємо доцільним при розробці системи кіберзахисту економічного суб'єкту використовувати принцип системності та комплексний підхід, що дозволить врахувати вагомість певного об'єкту та наявність фінансових ресурсів.

Список літератури

1. Новікова А. П. Аналіз розвитку світового та українського ринку ІТ-послуг / А. П. Новікова, Н. Є. Скоробогатова // Інвестиції: практика та досвід. – 2018. - № 3. – С. 52 – 56.

2. Дубов Д. В. Сучасні тенденції забезпечення кібербезпеки на міжнародному рівні [Електронний ресурс] / Дмитро Володимирович Дубов. – 2011. – Режим доступу до ресурсу: http://sp.niss.gov.ua/content/articles/files/1-1441958808.pdf.

3. Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation / NATO. Official site [Електроннии ресурс]. – Режим доступу до ресурс : http://www.nato.int/lis-bon2010/strategic-concept-2010-eng.pdf

4. Кондратьев А. Современные тенденции в исследовании критической инфраструктуры в зарубежных странах / А. Кондратьев // Зарубежное военное обозрение. — 2012. — № 1. — С. 19–30.

5. Study: stock-taking of existing critical infrastructure protection activities : final report JLS/2007/D1/037 // Booz & Company (Italia) S.r.l.; European Commission. – 2009. – 492 p.

УПРАВЛІННЯ КОНФЛІКТАМИ В ОРГАНІЗАЦІЇ

Скрипник К.О., *студентка.*
Науковий керівник: к.е.н., доцент Онопрієнко О.Д.
Національнийавіаційнийуніверситет, м. Київ

Конфлікти, на природу яких існують різні погляди, виникають у процесі взаємодії та спілкування індивідів між собою.

У повсякденному уявленні конфлікт – це щось негативне та агресивне, таке, що викликає загрози і чого слід одразу уникати або негайно вирішувати, як тільки він виникає. Представники ранніх наукових шкіл управління вважали, що конфлікт є ознакою поганого управління. Е. Дюркгейм, Т.Парсонс, Е. Мейо наголошували, що конфлікт є певним відхиленням, "хворобою" людських стосунків.