

Список джерел:

1. Держстат України. Економічна статистика. Електронний ресурс. Режим доступу http://www.ukrstat.gov.ua/operativ/menu/menu_u/size.htm.
2. Стеценко С.П., Сорокіна Л.В., Ізмайлова К.В. Фінансовий аналіз та економічна діагностика. Навчальний посібник. Київ: КНУБА. 2019 – 160 с.
3. Беленкова О.Ю. Вплив економічної кризи на фінансовий стан підприємств виду діяльності «будівництво» / О.Ю. Беленкова // Будівельне виробництво. Міжвідомчий науково-технічний збірник – 2010. - Вип. 52.- С.16 - 20.
4. Ізмайлова К.В., Беленкова О.Ю., Моголівець А.А. Сутність економічних циклів та їх вплив на фінансову стійкість будівництва// Наукові праці НДФІ. 2019. № 2. С. 138-15.

УДК 346.548, 004.056

Росинський А. В.,
аспірант кафедри економіки будівництва
Київський національний університет будівництва і архітектури

КІБЕРЗЛОЧИННІСТЬ ЯК ВИКЛИК ЕКОНОМІЧНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА В УМОВАХ ФОРСОВАНОЇ ЦИФРОВІЗАЦІЇ

Міжнародний досвід показує, що поряд з низкою переваг, форсована цифровізація має великий вплив на зростання кіберзлочинності. Це вимагає забезпечення відповідного рівня цифрової безпеки як у розрізі всієї країни, так і у розрізі кожного окремого підприємства. Чим більш діджиталізованим стає підприємство, тим гострішим стає питання його цифрової безпеки, адже кіберзлочини чи хакерські атаки матимуть підвищені ризики не тільки локального масштабу, в розрізі окремого підприємства, але й глобального, у розрізі людських життів чи екологічних катастроф.

Підприємства доволі часто не звертають увагу на загальну картину даної проблеми через нестачу знань і досвіду у цій сфері та, якщо і користуються підходами щодо забезпечення кібербезпеки, то частіше за все такими, що не відповідають викликам сучасності.

Із неспинним збільшенням кількості цифрових технологій у бізнес-процесах підприємства зростає важливість визначення рівня кібербезпеки в розрізі оцінки загального рівня економічної безпеки компанії. І, якщо раніше кібербезпека у структурі економічної безпеки підприємства розглядалася суто як частина інформаційної безпеки, то зараз поняття кібербезпеки підприємства виходить на новий рівень, адже має на меті не лише захист інформації, а й захист іміджу та репутації, збереження довіри споживачів та клієнтів, фізичну та фінансову безпеку, не говорячи вже про збереження ринкових переваг та протидію проявам нечесної конкуренції.

Зважаючи на це, на перший план виходить необхідність у кібернавчанні персоналу, адже доволі популярними серед кіберзлочинців є і залишаються методи соціальної інженерії, що базуються на низькій цифровій грамотності робітників, які і є слабкою ланкою у будь-якій, навіть розвинутій системі кібербезпеки підприємства.

Одночасно з цим виникає всеохоплююча проблема щодо дефіциту спеціалістів у сфері кібербезпеки, адже й досі традиційно більша частина уваги при навчанні персоналу приділяється промисловій безпеці та охороні праці, практично не торкаючись інформаційної і абсолютно ігноруючи цифрову безпеку. Починаючи навчання персоналу щодо кібербезпеки, звичайно, потрібно зважати на низьку первинну підготовку робітників і необхідність навіть у базовому цифровому навчанні.

Мабуть, найбільшою вразливістю, якою користуються кіберзлочинці, є застаріле програмне і антивірусне забезпечення. Багато підприємств, особливо тих, що не пов'язані зі сферою ІТ, не бачать необхідності у оновленні програмного забезпечення і використовують застарілі операційні системи, чим створюють додаткові ризики з точки зору кібербезпеки всього підприємства, адже є очевидним, що застарілі системи не можуть враховувати і протидіяти сучасним викликам і загрозам, не кажучи вже про неможливість інсталивати у них всі необхідні оновлення безпеки. Підхід керівництва підприємств за принципом «Не треба змінювати, поки працює» є архаїзмом і блокує розвиток компанії, адже створює великі ризики не тільки з точки зору кібербезпеки, а й у розрізі загальної економічної безпеки підприємства.

Одночасно з цим, одним з наслідків форсованої цифровізації є стрімка розробка і поява нового програмного забезпечення, особливо галузевого, яке з часом буде ускладнюватися і інтегруватися з іншими сервісами, ресурсами та програмами. Збільшення рівня кіберзлочинності, як неминучий наслідок цифровізації, призводить до стрімкого збільшення кількості кібератак і, відповідно, зросту відповідальності розробників програмного забезпечення за можливі ризики та збитки внаслідок відсутності оперативного реагування на вразливість нульового дня чи фішингові атаки. Зважаючи на збільшення рівня ризиків, не є дивним, що на перший план по важливості у цьому контексті виходить показник довіри користувачів до програмного забезпечення, який стає головним у контексті впровадження цифрових технологій.

Цифровізація підприємства і його виробничих процесів неможлива без вдосконалення системи кібербезпеки, яка набуває все більшого значення при оцінці рівня економічної безпеки підприємства. В умовах цифрової трансформації економіки важливим аспектом в контексті забезпечення економічної безпеки держави стає кіберзахист критичної інфраструктури, а також політика щодо підвищення цифрової грамотності населення. Найбільше на рівень кібербезпеки підприємства впливає його здатність протистояти кіберзагрозам у режимі реального часу, саме тому пошук методів та підходів щодо протистояння кіберзлочинності має стати пріоритетним напрямком розвитку підприємств в сучасних умовах форсованої цифровізації.

Список джерел:

1. Стеценко С. П. Економічна безпека: сутність і структура / С. П. Стеценко // Інвестиції: практика та досвід. – 2013. – № 24. – С. 104-106.
2. Sorokina, L. & ets. (2017). Econometric toolkit for financial security management of construction companies. Econometric toolkit for financial security management of construction companies. K.: Kyivskyi natsionalnyi universytet budivnytstva i arkhitektury, Kryvyi Rih: Vydavets FOP Cherniavskiy D.O.

3. Боліла Н.В. Функціонально-операційна трансформація систем управління будівельним підприємством на ґрунті CALS-технологій / Н.В. Боліла // Управління розвитком складних систем. 2019. Вип. 40. С.156 -159.

УДК 346.548

Кушнерук О. Й.,
аспірант ДННУ «Академія фінансового управління», м. Київ
Короленко М. В.,
аспірант ДННУ «Академія фінансового управління», м. Київ

РОЗВИТОК МЕХАНІЗМІВ ДЕРЖАВНО-ПРИВАТНОГО ПАРТНЕРСТВА В УМОВАХ СТРУКТУРНОЇ МОДЕРНІЗАЦІЇ ЕКОНОМІКИ УКРАЇНИ

Система взаємопов'язаних і взаємодіючих інтересів суспільства завжди суперечлива. Тому кожне суспільство постає перед проблемою пошуку ефективного механізму їхнього узгодження. Єдність інтересів досягається у процесі взаємодії державного і корпоративного секторів економіки та взаємореалізації їхніх економічних інтересів.

Узгодження економічних інтересів держави та приватного капіталу передбачає управління державою економічною поведінкою власників засобів виробництва через їхній економічний інтерес за допомогою створення умов, що мотивують прийняття ними таких економічних рішень, які надавали б їхнім інтересам «фушійних» сил соціально-економічного розвитку і через те служили реалізації економічного інтересу держави як виразника загального інтересу.

Вирізняють наступні тлумачення узгодження економічних інтересів [1–2]: а) субординоване підпорядкування одних економічних інтересів іншим; б) принцип прийняття економічних рішень, відповідно до яких здійснюються постійна взаємодія та співробітництво між представниками держави та господарюючими суб'єктами для забезпечення порівнянності управлінської економічної інформації різних рівнів, несуперечності, узгодженості спільно прийнятих рішень.

В світовій практиці державно-приватне партнерство у широкому розумінні – це така система відносин держави та бізнесу, яка використовується як інструмент національного, міжнародного, регіонального, міського, муніципального, економічного і соціального розвитку. У вузькому розумінні державно-приватне партнерство – це конкретні проекти, що реалізуються спільно державними органами і приватними компаніями на об'єктах державної власності. Тому держава бере на себе ряд зобов'язань, в т.ч. і «прискорення прогресивних структурних та інституціональних змін в економіці, поліпшення інвестиційного клімату, підвищення ефективності інвестиційних процесів; стимулювання випереджувального розвитку наукоємних високотехнологічних виробництв» [3], що засвідчує про серйозне бажання та готовність до ефективної співпраці з бізнесом.

У Законі України «Про державно-приватне партнерство» державно-приватне партнерство визначене як система відносин між державними та приватними партнерами, побудована на принципах рівності партнерів і узгодженості їх інтересів, при реалізації яких можливості обох партнерів об'єднуються, з відповідним розподілом ризиків, відповідальності та отримання позитивного кінцевого результату