4. European Commission (EC). Europe 2020: A Strategy for Smart, Sustainable and Inclusive Growth. Communication from the Commission; Publications Office of the European Union: Luxemburg, 2010. URL: https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52010DC2020&from=EN.
5. Fedulova L. Inclusive Innovations in the System of Socio-Economic Development. *Economy: the realities of time. Scientific journal*. 2016. № 3 (25). Pp. 56-65. URL: http://economics.opu.ua/files/archive/2016/n3.html.
6. George G., McGahan A., Prabhu J. Innovation for Inclusive Growth: Towards a Theoretical Framework and a Research Agenda. *Journal of Management Studies*, 2012. Vol. 49 (4). Pp. 661-683.
7. Lagarde K. Towards the Inclusive Future. *The World in 2019. The Economist*. 2019. 75 p.
8. The Inclusive Development Index 2018. URL: https://www.weforum.org/reports/theinclusive-development-index-2018.
9. Weizsäcker E., Wijkman A. Come On! Capitalism, Short-termism, Population and the Destruction of the Planet. *Report to the Club of Rome*. New York: Springer-Verlag, 2018.

ГРЕБЕНЮК Андрій Миколайович,
завідувач кафедри економічної та інформаційної безпеки Навчально-наукового інституту права та підготовки фахівців для підрозділів Національної поліції Дніпропетровського державного університет внутрішніх справ, кандидат технічних наук

ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВІЙСЬКОВОГО СТАНУ

Зараз по всьому світові спостерігається зростання інформаційних загроз, і ця тенденція пов’язана з розвитком інформаційних технологій та їх інтеграції з технологіями штучного інтелекту. Спостерігається зростання загроз інформаційної безпеки та впливу на функціонування як національних, так і транснаціональних структур підприємств. Великі компанії все частіше розглядають кібербезпеку як загрозу №1 – і це не без причин. На теперішній час при військовій агресії нашого сусіда бойові дії ведуться в повітрі, на землі, на морі і в кіберпросторі. Що посилило загрози з боку хакерів, через зловмисні дії, такі як атаки програм-вимагачів, знищення даних, розкрадання та крадіжки інтелектуальної власності, виведення з ладу комунікаційних ресурсів та багато іншого [1].

В теперішній складний час для нашої країни та для багатьох компаній які євакуювалися або зазнали величезних фінансових і людських втрат не готові стримувати цю зростаючу загрозу. Деякі керівники вважають, що в компанії найкращій захист інформаційної безпеки. Але з огляду на те,

що підвищена загроза навряд чи зменшиться найближчим часом, багатьом компаніям потрібно переорієнтуватися на те, щоб забезпечити максимальний захист від кіберзагроз.

Інциденти кібербезпеки, в нашій країні, були численними як до, так і під час вторгнення, включаючи розподілені атаки на відмову в обслуговуванні, зловмисне програмне забезпечення, що стирає дані, і пошкодження веб-сайтів.

При цьому дуже складно спрогнозувати великим компаніям з відкіля може виникнути інформаційна загроза навіть як що вони достатньо виділяють коштів на забезпечення своєї інформаційної безпеки. Адже вони зазвичай мають тисячі постачальників. І ось ці постачальники як що в них недостатньо відпрацьований захист від кіберзлочинців, можуть створити загрозу й затримати ланцюжки поставок, якщо кібератака залишить їх нездатними працювати, і вони також можуть поширювати ті самі проблеми своїм клієнтам.

Але не тільки приватні чи державні компанії під загрозою, а й прості користувачі. Тому що інформаційні технології тісно ввійшли в наше життя і перш за все імпульсом масового переходу й використання соціальних мереж та потужних платформ дистанційного навчання та саморозвитку, послугували карантинні заходи які були введені в багатьох державах світу в зв'язку з пандемією COVID-19. В свою чергу попит та збільшення користувачів сприяло розвитку інструментарію на цих платформах. Також з'явилися потужні мобільні пристрої які постійно під'єднані до мережі інтернет, через мобільний інтернет, через мережу відкритих Wi-Fi точок. Це і доступ до відкритих сайтів новин, і банківські додатки де ми отримуємо доступ до фінансових рахунків, перевіряємо робочу електронну пошту та спілкуємося з сім'єю та друзями [2].

Необхідно впроваджувати нові та більш глобальні і ефективні методи боротьби з кіберзлочинністю. Це вдосконалення контрактних умов, оновлення офіційної політики щодо вимог постачальників до кібербезпеки, уточнення того, які постачальники є найважливішими для бізнесу, а також впровадження засобів контролю ризиків і заходів із зменшення ризиків, таких як жорсткіший доступ третіх сторін до систем компанії.

Успішна боротьба з цією сферою ризику вимагає:

- ідентифікувати та класифікувати постачальників на основі ризику кібербезпеки та ймовірного впливу (як прямого, так і пов'язаного з ланцюгом поставок);
- оцінювати постачальників та партнерів як під час їхнього першого вибору, так і на постійній основі – за допомогою власних команд або за допомогою зовнішньої служби оцінки ризиків нового типу;
- знизити ризик до прийнятного рівня за допомогою таких заходів, як неформальне переконання, умови контракту, додаткові засоби контролю та диверсифікація ланцюга постачання для підвищення безперервності.

Це складно зробити надійно та в масштабі, тому багато компаній у кінцевому підсумку живуть із високим, але невизначеним рівнем ризику кібербезпеки [3].

Зусилля та інвестиції, необхідні для того, щоб переконати постачальників покращити свою кібербезпеку, також можуть призвести до більш широких переваг.

І вже зараз потрібно створювати такі системи захисту які виходять за межі сьогоднішнього типового підходу, за яким більшість компаній просто виділяють певний відсоток доходу чи ІТ-бюджету на безпеку, не оцінюючи своїх справжніх потреб. Ефективна кібербезпека вимагає постійних зусиль, які охоплюють не лише безпеку додатків, тестування на проникнення та управління інцидентами, але й поведінку співробітників, ризики третіх сторін і багато інших потенційних уразливостей.

Список використаних джерел:

1. Рибальченко Л. В., Гребенюк А. М. Основи управління інформаційною безпекою: навч. посібник. 2020, 144 с.
2. Дикий А. П., Наумчук К. М., Тростенюк Т. М. Аналіз сучасних загроз інформаційній безпеці держави. *Економічний простір*, 2021. Вип. 176. С. 155-158.
3. Rybalchenko L., Ryzhkov E. Ensuring enterprise economic security *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs*. 2019. Special Issue № 1 (102). Pp. 268-271.

РИБАЛЬЧЕНКО Людмила Володимирівна,
завідувач кафедри інформаційних технологій
Дніпропетровського державного
університету внутрішніх справ,
кандидат економічних наук, доцент

СУЧАСНИЙ СТАН ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ

Забезпечення стійкого та надійного соціального й економічного розвитку країни, підвищення рівня життя кожного громадянина, створення заходів для протидії будь-яким внутрішнім і зовнішнім загрозам є важливим для суверенної та незалежної держави, якою є Україна на сучасному рівні стану її економіки.

Економічна безпека містить декілька основних її складових, які визначають стан забезпечення економічної безпеки країни та вказують на ті фактори, які можуть негативно впливати на її суверенітет, незалежність та можливі загрози.

Актуальність даного питання визвана ситуація, що відбувається в нашій країні через повномасштабне вторгнення російської агресії на території України. Вирішення загроз національної безпеки впливають на подальшу долю та добробут населення країни, становлення національної незалежності, повагу до своєї держави, соціально-економічний розвиток та розвиток системи міжнародної економічної взаємозалежності.

Саме забезпечення системи економічної безпеки виступає необхідною умовою для стійкого та стабільного соціально-економічного розвитку держави