Бундзяк Дмитро Павлович, *магістр 1 курсу*
Коростіль Наталія Жоржівна, *к.і.н., доцент,*
доцент кафедри гуманітарних та
фундаментальних дисциплін

КІБЕРБЕЗПЕКА У СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

Кібербезпека все частіше розглядається, як стратегічна проблема держави, що комплексно зачіпає економіку країни, в тому числі щодо взаємодії національних розробників програмного забезпечення і систем управління, виробників обладнання та компонентів для забезпечення IT-інфраструктури, низька ринкова конкурентоспроможність, яких призводить до необхідності використання рішення іноземних виробників. На практиці дане явище призводить до стрімкого зростання залежності від іноземних виробників і зниження рівня інформаційного захисту, виходячи з вимушеного використання «закритого» програмного і апаратного забезпечення в усіх сегментах інфраструктури як для спеціальних державних відомств, так і цивільного сектора.

Уже найближчим часом залежність від іноземних виробників обладнання та розробників програмного забезпечення може досягти критичного рівня. Наприклад, незважаючи на створену віртуальну «залізну завісу», влада Китаю фактично визнала повну залежність і незахищеність внаслідок повсюдного використання програмної платформи для мобільних пристроїв Android (частка платформи на ринку Китаю за підсумками 2016 року - 86,4%), засновану на «відкритому» коді, але підконтрольну спеціальним службам інших країн. З точки зору економіки це явище позитивно впливає на розвиток електронної промисловості і реального сектора, що використовують «відкрите» програмне забезпечення для виробництва мобільних пристроїв, але при цьому створює реальну загрозу для національної безпеки, переводячи її під можливий контроль іноземних спецслужб.

Для того щоб національна кібербезпека могла відповідати рівню провідних економічних держав, необхідні, в тому числі, послідовні дії з боку держави, спрямовані на підвищення ефективності та розвиток системи взаємодії учасників IT-галузі.

У свою чергу підприємства розробники і виробники повинні приділяти особливу увагу питанням інформаційної безпеки в розроблюваної продукції, пред'являючи підвищені вимоги до надійності і захищеності пропонованих рішень, і тільки в крайніх випадках і при необхідності підвищення ринкової орієнтованості окремих продуктів повинні використовувати рішення іноземних вендорів і розробників програмного забезпечення. Розглянемо існуючі загрози для кібербезпеки України із врахуванням актуальних тенденцій розвитку IT-галузі в світі, зокрема, технологічні і системні проблеми кібербезпеки. Поняття кібербезпеки включає в себе безліч проблем різного типу, а також містить ще більше число рішень. Кібербезпека є областю активних досліджень і розробок в співтоваристві інформаційних технологій силами учасників з усіх частин екосистеми інформаційних та комп’ютерних технологій. Схематично поняття «кібербезпека» представлено на рис. 1.

Більшість напрямів кібербезпеки мають загальну тематику і проблеми, які вимагають комплексного підходу. Серед них аналіз трафіку, запуск шпіонських програм, віруси, фітинг, DDOS, спам, викрадення адрес та послуг тощо.

У переважній більшості випадків найбільш успішні атаки хакерів, злочинців та інших зловмисників спрямовуються на сервери і комп'ютери кінцевих користувачів, підключених до Інтернет. Серед інструментів, які використовуються для атаки

комп'ютерів – шкідливе ПЗ, троянські коні, бот-мережі, фішинг, розподілені атаки типу «відмова в обслуговуванні» (DDoS), а також атаки «людина посередині».

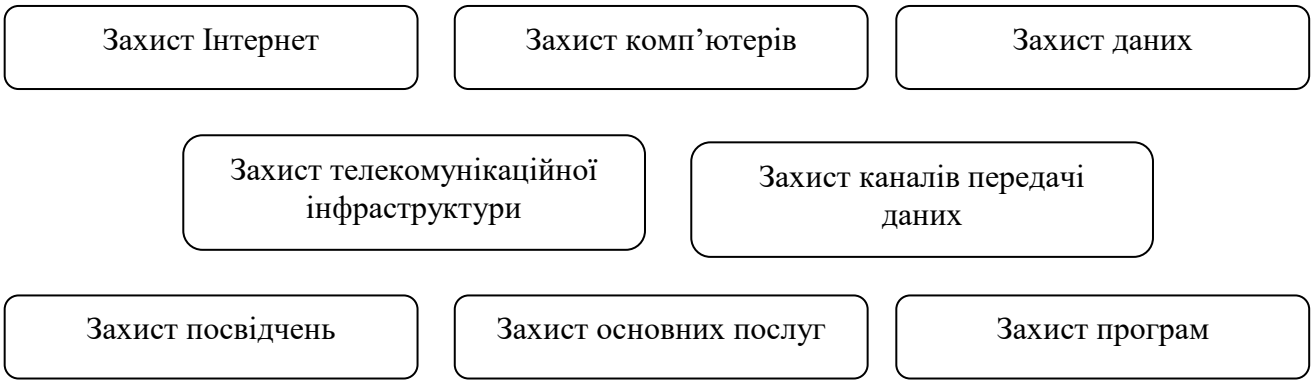

Рис. 1. Основні сфери та напрями забезпечення кібербезпеки

Забезпечення безпеки комп'ютерів - чи серверів, чи настільних комп'ютерів, чи ноутбуків, чи смартфонів - є метою роботи найрізноманітніших груп всередині IT та Інтернет-спільнот. Важливо відзначити, що переважна більшість цих компаній – іноземні розробники і виробники, що переважно домінують на вітчизняному ринку.

Проте, навіть знаходження технологічного вирішення для проблеми кібербезпеки не означає, що сама проблема зникає – просто з'являється можливість її вирішення. Наприклад, комплексне шифрування з використанням алгоритмів SSL/TLS є широко відомою технологією, яку можна використовувати в якості вирішення багатьох проблем, перерахованих вище. Однак, воно не було прийнято повсюдно. Частково це обумовлено історичними причинами і організаційною інертністю, а також технічною неграмотністю чи поганою інформованістю. Наявність добре відомих рішень добре відомих проблем має невелику цінність, якщо ці рішення не використовуються. Таким чином, питання забезпечення національної кібербезпеки залежать не тільки від технічних способів реалізації, але, що більш важливо, від наявності і реального попиту на дані рішення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *A Solution-based Examination of Local, State, and National Government Groups Combating Terrorism and Cyberterrorism. Feb2011, Vol. 21 Issue 2, p. 109-129, 21 p. [Електронний ресурс]. – Режим доступу: http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN.*
2. *Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К.: НАУ, 2013. – 432 с.*

Гончарук Валентина Олегівна, *магістр 1 курсу,*
Ляхович Галина Іванівна*, к.н.д.у., доцент,*
доцент кафедри міжнародної економіки
маркетингу і менеджменту

ЕТАПИ РОЗВИТКУ ТА СУЧАСНІ ТЕНДЕНЦІЇ ФОРМУВАННЯ ЄВРОПЕЙСЬКОГО РИНКУ ГАЗУ

Виснаження нафтових і газових родовищ посилює конкуренцію світових країн-лідерів за ресурси і змінює їх економічну і енергетичну політику. Європейські країни