ПРОМИСЛОВЕ ШПИГУНСТВО З БОКУ КИТАЮ ЯК ЗАГРОЗА ДЛЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ

Автор: доц..каф.ФЕБІВ, к.е.н. Якубівська Ю.Є.

Промислове шпигунство є активним методом збору інтелектуальних і конфіденційних даних неетичним або незаконним методами з метою отримання переваги на ринку в недобросовісній конкуренції. Китайські компанії станом на сьогодні не мають жодних організаційно-правових методів, які б стримували чи забороняли промислове шпигунство. Відтак акти промислового шпигунства можуть бути трактовані як прояв недобросовісної конкуренції. Основна філософія промислового шпигунства полягає у тому, навіщо витрачати роки і мільйони етапів на дослідження і розробки, на формування клієнтської бази, якщо виникає спокуса дати хабар співробітнику в команді конкурента, прослухати телефони, або шпигувати за їхніми офісами і т.д.

За даними Американського товариства з промислової безпеки (ASIS), випадки промислового шпигунства в американському бізнесі зросли більш ніж на 260 відсотків з 1985 року [1]. Промислове шпигунство в Китаї розглядається як прийнятний спосіб ведення бізнесу без наявності законодавства, яке б регулювало його. Очевидно, що на сучасній бізнес-арені інформація є більш цінним об’єктом, ніж будь-коли. Кожна організація є вразливою перед загрозою крадіжки інформації. Зацікавлена в отриманні інформації особа-шпигун найчастіше входить до колективу підприємства, а близько 85% злочинів із застосування активних методів промислового шпигунства скоюються співробітниками. Система безпеки підприємства може бути ефективно захищеною назовні, щоб тримати аутсайдерів, але водночас мало захищеною, щоб запобігти інсайдерам, котрі експортують секрети підприємства чи компанії.

У зв'язку з цим підприємствам необхідно змінити спосіб формування системи безпеки. Вони повинні визначити свої цінні інформаційні ресурси, і цільову групу осіб-конкурентів, які можуть бути зацікавлені в них. Крім того, маючи безпосередній доступ до інформації компанії, недобросовісні програмісти можуть бути підкуплені конкурентами, а це в свою чергу надасть їм доступ до комп'ютерного забезпечення компанії, щоб посадити вірус «троянського коня» в корпоративну комп'ютерну систему, і при цьому будувати «чорний хід», уможливлюючи повторний доступ до даних компанії. Судовий процес, однак, не завжди є ефективним методом боротьби з промисловим шпигунством, оскільки компанія повинна зловити шпигуна і вдатися до застосування цивільної або кримінальної відповідальності. Водночас характер вкраденої конфіденційної інформації, звичайно оприлюднено в ході судового процесу, який є наслідком правових норм. В результаті, щоб домогтися справедливості, потерпілий повинен буде оприлюднювати ту ж саму інформацію, яку він намагається захистити, що робить вартість конфіденційної інформації набагато нижчою. Тому завдання боротьби з промисловим шпигунством на підприємстві полягає в тому, щоб захистити конфіденційну інформацію таким чином, що шпигун не зміг отримати її.

У 2015 році Комісія з питань крадіжок американської інтелектуальної власності оголосила свої висновки про загрозу, що виходить від промислового шпигунства для американської промисловості, головним чином в сфері кібербезпеки, і запропонувала кроки щодо їх удосконалення. Повна доповідь Комісії під головуванням адмірала у відставці Денніса Блера і колишнього посла США в Китаї Джона Хантсмена [2] безумовно підкреслює масштаби проблеми, оцінюючи, що щорічні втрати від крадіжки інтелектуальної власності сягають 300 млрд. дол.. США, а це, у свою чергу, призводить до втрати мільйонів робочих місць в економіці США. У доповіді також прямо обвинувачується Китай в якості основного джерела вищезазначених крадіжок, чия частка становить 50-80 % світового промислового шпигунства та крадіжок конфіденційної інформації в цілому. Національні цілі промислової політики

Китаю заохочують до розкрадання інтелектуальної власності, і велика кількість китайців в бізнес і урядових організаціях займаються цією практикою.

Комісія запропонувала деякі цінні пропозиції, як підсумовують Д. Блер і Дж. Хантсмен в провідній американській газеті «The Washington Post»: «заборонити та вилучити з обігу товари, які містять вкрадену інтелектуальну власність на ринку США; обмежити використання фінансової системи США іноземними компаніям, які неодноразово викрадали інтелектуальну власність; активно застосовувати охорону та захист права інтелектуальної власності як основні критерії для інвестицій в США в рамках програм Комітету з іноземних інвестицій в США (CFIUS), а також для іноземних компаній, які котируються на фондових біржах США [3].

Отже, ефективним кроком на шляху боротьби з промисловим шпигунством з боку Китаю є законодавче закріплення норм, які б дозволяли використовувати методи контратаки в кіберсфері у випадках, якщо Китай відкрито займається викраденням інтелектуальної власності. Такі напади є незаконними сьогодні, як і будь-який злом, але якби вони була узаконені, це б підвищило вартість скоєння замахів на інтелектуальну власність саме для замовників, а це б потенційно стримувало їх від проведення цих заходів.

Література:

1. How Criminals Made $18 Million By Holding Our Data Hostage [Electronic resourse] / American Society for Industrial Security (ASIS). – 2016. – Access: https://sm.asisonline.org/Pages/Held-Hostage.aspx

2. The Report of the Commission on the Theft of American Intellectual Property [Electronic resourse] / The IP Commission. – 2013. – Access: http://www.ipcommission.org/report/ip_commission_report_052213.pdf

3. Blair D., Huntsman J. Protect U.S. Intellectual Property Rights [Electronic resourse] / The Washington Post. – 2013. – Access: https://www.washingtonpost.com/opinions/dennis-blair-and-jon-huntsman-protect-us-intellectual-property-rights/2013/05/21/b002e10e-c185-11e2-8bd8-2788030e6b44_story.html