Потєхін Б.Д., Буланіков Є.В.
студенти,
Національна академія Служби безпеки України

ПРОМИСЛОВЕ ШПИГУНСТВО ЯК ГОЛОВНА ЗАГРОЗА ВИРОБНИЧОГО СЕКТОРУ

З огляду на важливість промислового шпигунства в економічній реальності, в особливості виробничого сектору. Метою даної тези є теоретичний аналіз поведінки компаній при отриманні інформації від своїх конкурентів, щоб краще її зрозуміти і побачити, які можуть бути наслідки, так як, хоча промислове шпигунство є дуже поширеною практикою, лише деякі теоретичні роботи намагалися його проаналізувати. Точніше, наша мета – теоретично проаналізувати вплив промислового шпигунства на стратегічну поведінку компаній виробничого сектору в контексті стримування входу за допомогою інструментів теорії ігор. Крадіжки комерційних таємниць та інтелектуальної власності корпорацій, такі як власні виробничі процеси, формули, рецепти та розробки товарів, відбуваються десятиліттями.

Дана тематика є важливим аспектом виробництво та фармацевтичної і хімічної промисловості.

Федеральне бюро розслідувань визначає промисловий шпигунство як «приватне або приватне підприємництво, спонсорство або координація розвідувальної діяльності, що проводиться з метою підвищення їх переваг на ринку» [3, с. 48]. Незважаючи на те, що це визначення може означати, що промисловий шпигунство більш-менш збігається з діловою чи конкурентною розвідкою, Джон Ф Квін пояснює суттєву різницю між ними – тоді як бізнес-розвідка, як правило, перебуває під приватним спонсорством із використанням «відкритої» методології, шпигунство може бути або урядом, або приватним спонсором, і підпільно [1, с. 47].

Власну інформацію можуть викрасти працівники, що мають доступ до баз даних бізнесу та компанії, хакери, що проникають на сервер компанії, або спонсоровані групи грабіжників. Поки компанії можуть втратити життєво важливу ділову інформацію через залишення співробітників роботи, шпигунство відбувається, коли працівник навмисно шукає дані, викрадає їх, копіює та продає за гроші або для власного підрозділу, коли він має намір виготовити подібний предмет.

Шпигунство конкурентів передбачає шпигунство діяльності інших підприємств та незаконний збір секретної інформації, щоб вони могли керувати своїм бізнесом, приймаючи відповідні стратегії, і залишатися на рівні, якщо не випереджати конкуренцію на ринку. Зацікавлені сторонні особи та конкуренти застосовують багато методів, включаючи підкуп, детективи, що шпигують через тіньові агентства, пошук сміття, яке також називають «дайвером у сміттєвих контейнерах», шахрайство, щоб обдурити робітників через «соціальну інженерію», або навіть викрити лазівки та слабкі місця в житті працівників та шантажувати їх за збір інформації.

Проблема з тим, щоб знайти інсайдера для крадіжки комерційної таємниці, полягає в тому, що для цього потрібен час і гроші. Крадіжка або незаконне отримання інтелектуальної власності та економічної інформації, особливо конкурентами та іноземними урядами, загрожує розвитку та виробництву товарів, отриманих на основі такої інформації, а також призводить до втрати прибутку, частки ринку та, можливо, самого бізнесу, а отже може призвести до ослаблення економічної могутності своєї країни [1]. У сучасному інформаційному діловому середовищі бізнес, як правило, серйозно відповідає на загрозу і прагнучи здобути владу, зберегти контроль, збільшити частку ринку та перемогти конкуренцію, країни та бізнес підтримують шпигунство, розглядаючи його випадково та беручи участь у шпигунстві, використовуючи інформацію та технології як озброєння ділової та економічної війни [4, с. 184].

У наші дні існує підхід, який набагато простіше і дешевше для злочинця: кібер-шпіонаж. У багатьох випадках йдеться про такі країни, як Китай, чий уряд визначив кілька галузей як «стратегічні». Підприємства отримують урядові «дані розвідки» (тобто, вкрадені ІС), що дозволяє їм покращити свою конкурентоспроможність та скоротити час, витрачений на НДДКР.

Тож як ви могли знати, якщо кібер-шпигуни вже порушили вашу мережу ОТ та вкрали конфіденційні дані історіків та логіку сходів у ПЛК, з яких вони можуть зробити висновки про таємниці дизайну та інші корпоративні ІС? Як щодо сторонніх постачальників, які підключаються безпосередньо до вашої мережі ОТ через ноутбуки або USB-накопичувачі, минаючи традиційні захисні пристрої по периметру, такі як міжмережеві стіни та пристрої IDS / IPS? В порівнянні з більш звичними кіберзлочинами, такими як крадіжка ІПІ, «крадіжки в кіберзахисті ІР значною мірою залишаються в тіні». Це тому, що, на

відміну від організацій роздрібної торгівлі та фінансових послуг, яким законодавство покладено обов'язки повідомляти про порушення даних про споживачів, промислові організації не зобов’язані повідомляти про крадіжки IP та інші вторгнення IC.

Однак ознайомтеся з цими трьома даними із звіту про розслідування порушень даних Verizon за 2017 рік (DBIR):

1. Виробництво – галузь № 1, націлена на кібершпіонаж.

2. Кібершпіонаж на сьогодні є найбільш переважаючим вектором нападу у виробничому секторі.

3. Комерційна таємниця – це № 1 тип даних, порушений у виробничих компаніях.

Хоча правові заходи та законодавство, які направляють сильні повідомлення проти шпигунства, можуть бути ефективними у запобіганні його виникненню, роль та відповідальність корпорацій є вирішальними. Незважаючи на те, що компанії несерйозно підходять до шпигунства, мало дискусій щодо того, що компанії повинні ефективно захищатись від «злодіїв інформації», як інсайдерів, так і тих, хто розв’язується сторонніми людьми, які намагаються отримати секрети всіма можливими способами. Заходи, які можуть допомогти компаніям запобігти шпигунству, включають:

– проведення опитування щодо виявлення потенційних зон ризику;

– розробка політики безпеки без великих ризиків для безпеки;

– часто оцінюйте політику та процедури безпеки та змінюйте, якщо це необхідно;

– виділення інформації, яка не повинна потрапляти в руки конкурента;

– виконання угод про нерозголошення інформації для працівників, продавців та підрядників;

– захист комп’ютерних систем та мереж шляхом встановлення відповідних засобів захисту інформаційних систем;

– моніторинг використання електронної пошти та Інтернету [2, с. 49].

Хоча вищезазначені методи можуть бути корисними для захисту від шпигунства, головним для контролю за промисловим шпигунством є підвищення рівня обізнаності та навчання працівників, оскільки одним з основних пунктів вразливості є шпигунська діяльність людей, що належать до однієї організації. «Програми підвищення обізнаності та навчання можуть допомогти інформувати працівників про політику інформаційної безпеки їх організації, підвищувати їхню ризиковість та

потенційні втрати та навчати їх використанню практик та технологій безпеки» [3, с. 382]. Вкладаючи кошти в процедури безпеки та навчання, корпорації можуть навчати працівників у галузі персоналу, кіберпростору та фізичної безпеки; їх також можна поінформувати про свої обов'язки щодо інформаційної безпеки організації.

Зростання значення інформації про комерційну таємницю на світовому та внутрішньому ринку та можливості революції в галузі інформаційних технологій призвели до значного зростання шпигунської діяльності в останні роки, особливо проти США, яка є найбільш домінуючою економічною державою у світі.

Список використаних джерел:

1. Boni W. & Kovacich G.L. (2000) *Netspionage: The Global Threat to Information*. MA: Butterworth- Heinemann.

2. Crock S. (1997) «Business Spies: The New Enemy Within?» Book Review: War By Other Means» Economic Espionage in America By John J. Fialka. *Business Week.* Available at: http://www.businessweek.com/1997/06/b351325.htm

3. Denning D.E. (1998) *Information Warfare and Security*. MA: Addison-Wesley.

4. Jones A., Kovacich G.L. & Luzvick P.G. (2002) *Global Information Warfare: How Businesses, Governments and others Achieve Objectives and At.*