– умови внутрішнього попиту: якість і розвиток обсягу попиту, відповідність тенденціям розвитку на світовому ринку;

– суміжні і сервісні галузі (галузеві кластери): джерела отримання сировини і напівфабрикатів, сфери використання сировини, обладнання, технологій;

– стратегію і структуру фірм, внутрішньогалузеву конкуренцію, стратегії, способи організації, менеджмент компаній;

– випадкові події: політичні, соціально-економічні та інші явища, які значною мірою можуть впливати на становище у країні і не можуть контролюватися керівництвом компаній, а деколи і керівництвом країни;

– загальнодержавну соціально-економічну і технічну політику.

СПИСОК ДЖЕРЕЛ:

1. Ковальська Л. Л. Методичні підходи до оцінки конкурентоспроможності регіонів держави [Електронний ресурс] / Л. Л. Ковальська // Економічні науки. Серія «Регіональна економіка» : зб. наук. праць. — Луцький національний технічний університет. — Випуск 5 (17). — Ч. 2. — Луцьк, 2008. — 360 с. — Режим доступу: [http://www.nbuv.gov.ua/Portal/Soc_Gum/En/RE/2008_5_2/index.html].
2. http://competitiveukraine.org/ua/indexes/methodology
3. http://competitiveukraine.org/ua/indexes/regions
4. http://competitiveukraine.org/ua/indexes/twelve/diagram/2013/6.html#top
5. Будкін В. Інноваційна модель розвитку національних економік // Економіка України. - № 6. – 2010, СС. 67-78.
6. Наукова та інноваційна діяльність Донецької області за 2012 рік // Статистичний збірник. - Головне управління статистики у Донецькій області. – Донецьк. - 2013. - 252 с.
7. Державна Програма активізації розвитку економіки на 2013-2014 роки (проект). - Режим доступу: [http: // http://eimg.pravda.com.ua/files/a/4/a428a25---------.pdf]
8. Войнаренко М. Концепція кластерів — шлях до відродження виробництва на регіональному рівні // Економіст. — 2009. — № 1. — С. 29—33.

ЦІЛЬОВІ АТАКИ В КОНТЕКСТІ ПРОМИСЛОВОГО ШПИГУНСТВА

Якубівська Ю.Є. к.е.н., старший викладач кафедри фінансово-економічної безпеки Тернопільського національного економічного університету (Україна)

Якубівська Ю. Є. Цільові атаки в контексті промислового шпигунства.

Наукова стаття присвячена дослідженню процесу промислового шпигунства як прихованої форми отримання конфіденційної інформації конкурентів. З цією метою розглянуто понятійний апарат зазначеного явища в системі економічної безпеки, виділено типи інсайдерських загроз, деталізовано форми промислового шпигунства. В статті розглянуто особливості застосування цільових атак в контексті промислового шпигунства, проаналізовано тенденції розвитку промислового шпигунства на світовому рівні, подано основні показники результативності цільових атак в мережі Інтернет. Визначено характер цільових атак в контексті промислового шпигунства, акцентуючи увагу на загальновизнаних в економічній літературі припущеннях про їхні особливості, автором внесено відповідні сучасному розвитку даної сфери корективи. На основі отриманих результатів сформульовано висновки про характер цільових атак, наголошено на необхідності поєднання реактивних та превентивних заходів на шляху протидії їхньому впливу на макро- та мікрорівні.

Ключові слова: промислове шпигунство, цільові атаки, програмне забезпечення, кібер-безпека, комерційна таємниця.

Якубивская Ю.Е. Целевые атаки в контексте промышленного шпионажа.

Научная статья посвящена исследованию процесса промышленного шпионажа как скрытой формы получения конфиденциальной информации о конкурентах. С этой целью рассмотрены понятийный аппарат указанного явления в системе экономической безопасности, выделены типы инсайдерских угроз, детализировано формы промышленного шпионажа. В статье рассмотрены особенности применения целевых атак в контексте промышленного шпионажа, проанализированы тенденции развития промышленного шпионажа на мировом уровне, представлены основные показатели результативности целевых атак в сети Интернет. Определен характер целевых атак в контексте промышленного шпионажа, акцентируя внимание на общепризнанных в экономической литературе предположениях об их особенностях, автором внесены соответствующие современному развитию данной сферы коррективы. На основе полученных результатов сформулированы выводы о характере целевых атак, отмечена необходимость сочетания реактивных и превентивных мер на пути противодействия их влиянию на макро- и микроуровне.

Ключевые слова: промышленный шпионаж, целевые атаки, программное обеспечение, кибер-безопасность, коммерческая тайна.

Yakubivska Y.Y. Target attacks in the context of industrial espionage.

The research paper is devoted to the processes of industrial espionage as a hidden form of receiving confidential competitors' information. For this purpose, the conceptual apparatus of this phenomenon in the system of economic security is reviewed, the types of insider threats are highlighted, forms of industrial espionage are detailed. The article is concerned with the features of target attacks in the context of industrial espionage; trends in industrial espionage on a global level are analyzed; the key performance indicators of targeted attacks on the Internet are represented. The targeted attacks character in the context of industrial espionage is determined, focusing on generally accepted in the economic literature assumptions about their characteristics; the author introduced the relevant to the modern development of this sector adjustments. Based on results the conclusion about the nature of target attacks is formulated, the necessity of reagents and preventive measures combining on ways of their influence counteracting on macro and micro levels is emphasized.

Keywords: industrial espionage, target attacks, software, cyber security, trade secrets.

Постановка проблеми. Останніми роками в контексті боротьби з промисловим шпигунством доволі часто привертають до себе увагу методи соціальної інженерії та цільових атак. Даний факт є цілком аргументованим, оскільки саме із вказаними методами асоціюється поняття промислового шпигунства загалом, як незаконного отримання відомостей, що становлять комерційну таємницю, зацікавленими у них суб'єктами. А це у свою чергу являє собою значну загрозу для системи економічної безпеки як держави, так і окремих підприємств та установ. Крім того, створення зазначених об'єктів та прав зазвичай характеризується високим рівнем вартості, якщо працювати над ними особисто. А промислове шпигунство дозволяє отримати необхідну інформацію у короткий термін із незначними затратами. Факти промислового шпигунства та цільових атак зокрема найчастіше зустрічаються у високорозвинутих країнах світу, компанії на уряди яких у 60-80-ти % страждають від незаконних посягань на об'єкти інтелектуальної власності з боку Китаю, а останнім часом і країн колишнього СССР (наприклад, Росії та України). У даному випадку маються на увазі наступні об'єкти: комерційні таємниці, ноу-хау, шоу-хау, компіляції даних, комп'ютерні програми, а також права на них у вигляді відповідних прав реєстрації, свідоцтв тощо.

Аналіз останніх досліджень та публікацій. Проблематика промислового шпигунства лежить в основі досліджень наступних вчених: Е. Браун, Л. Каганер, Р. Менделл, Х. Нашері, А. Нерсесян, Ф. Растмен та ін. Серед вітчизняних науковців, котрі зосереджують свої дослідження на даному питанні, можемо виділити Г. Андрощука, В. Бегму, З. Живко, М. Єрмошенко, С. Князєва, Т. Нагачевську та інших. На основі опрацювання джерел по даній тематиці прослідковується необхідність вивчення особливостей цільових атак в контексті

промислового шпигунства. Науковці приділяють значну увагу організаційним методам захисту від промислового шпигунства в першу чергу на макрорівні. Однак поза увагою залишаються такі аспекти як: захист від інсайдерських загроз, кіберзахист, протидія промисловому шпигунству через мережу Інтернет у країнах із низьким рівнем охорони та захисту інтелектуальної власності.

Виділення невирішеної проблеми. Зважаючи на той факт, що категорія «промислового шпигунства» у вітчизняній економічній літературі ще не є достатньо вивченою, можна стверджувально говорити про актуальність дослідження за темою даної наукової статті. Необхідність євроінтеграції України потребує розробки та реалізації такої моделі захисту інтелектуальної власності від проявів промислового шпигунства, яка відповідала б принципам економічної безпеки міжнародної спільноти, сприяла розвитку процесу інтелектуалізації на фоні ефективного захисту від недобросовісної конкуренції. Загострення проблем порушення економічної безпеки викликає необхідність розвитку нових ефективних форм захисту від цільових атак, що проявляються в процесі промислового шпигунства. Світовий досвід підтверджує неминуче виникнення загроз економічній безпеці країни в контексті поширення процесу промислового шпигунства. На сьогоднішній день гостро стоїть завдання розробки єдиних механізмів захисту від інсайдерських загроз. Найчастіше жертвами промислового шпигунства стають високорозвинуті країни, котрі володіють значною кількістю цінних активів у вигляді інтелектуальної власності, підкріпленої патентами, свідоцтвам та іншими охоронними документами. Такі об'єкти характеризуються високою вартістю, а відтак викликають зацікавленість у конкурентів. Останні, використовуючи методи недобросовісної конкуренції, намагаються заволодіти ними в процесі застосування цільових атак, кібернападів, інсайдерських втручань. Отримання конфіденційної інформації у мережі Інтернет супроводжується порушенням законодавства у сфері інтелектуальної власності. На фоні зазначених процесів невирішеною залишається проблема захисту від цільових атак в контексті промислового шпигунства як на макро-, так і на мікрорівні.

Метою статті є дослідження особливостей використання цільових атак в контексті промислового шпигунства. Задля досягнення вищевказаної мети потребують вирішення наступні **завдання:**

- охарактеризувати категорію промислового шпигунства та його відмінність від конкурентної розвідки;
- охарактеризувати типи інсайдерських загроз в контексті промислового шпигунства;
- проаналізувати тенденції розвитку промислового шпигунства на світовому рівні;
- дослідити особливості використання методу «цільових атак» та проаналізувати показники його результативності в мережі Інтернет;
- сформулювати висновки про характер цільових атак в контексті промислового шпигунства та запропонувати шляхи протидії останньому на макро- та мікрорівні.

Результати дослідження. *Промислове шпигунство* являє собою приховану, найчастіше незаконну практику дослідження конкурентів з метою отримання переваги в бізнесі. Ціллю такого роду діяльності може бути незаконне отримання комерційної таємниці, наприклад, специфікації продукту або формули, інформації про бізнес-плани підприємства тощо. У багатьох випадках промислові шпигуни просто шукають будь-які дані, котрі їхня організація може використати на свою користь.

Варто наголосити, що промислове шпигунство відрізняється від конкурентної розвідки, діяльність якої зосереджена на зборі загальнодоступної інформації. Промислове шпигунство не є новим явищем. Люди завжди визначали технологію як засіб, що дозволяє отримати владу над іншими, тому вони охороняли свої таємниці ретельно. Алхіміки середньовіччя вели свої таємні кодовані зошити, що містили списки інгредієнтів і їх кількості, особливо це стосувалося синтезу золота.

Промислове шпигунство можна визначити як збір інтелектуальних і конфіденційних даних у неетичний та незаконний спосіб для того, щоб отримати перевагу на ринку в контексті недобросовісної конкуренції. Деякі південноафриканські компанії не знають про виробничу практику шпигунства. У Південній Африці не існує спеціального закону, що забороняє промислове шпигунство. Однак шпигунські дії можуть розумітися під поняттями крадіжки, порушення кордонів тощо. Основна філософія промислового шпигунства полягає в тому, щоб отримати інформацію про дослідження і розробки та розвиток клієнтської бази, на котру конкуренти витрачають роки та зусилля, полегшеним та значно швидшим методом, наприклад, підкупом співробітника в команді конкурента, використовуючи їхні телефони або помилки в системі менеджменту. За даними Американського товариства з промислової безпеки (ASIS), випадки промислового шпигунства в американському бізнесі виросли більш ніж на 260 % за останні 20 років [3]. Напротивагу цьому, промислове шпигунство в Південній Африці вважається прийнятним способом ведення бізнесу, без наявності законодавства, котре б нівелювало даний процес: була зроблена спроба використовувати різні закони кримінального характеру для протидії шпигунству, однак при факті затримання ці закони не охоплювали конкретно питання крадіжки або нелегітимного збору саме конфіденційної інформації.

В сучасному світі рівень промислового шпигунства процвітає і включає найрізноманітніші методи: від використання випадкових співробітників, що працюють в якості таємних агентів, хакерів, найманих команд грабіжників до треш-зборів, вивчення сміттєвих контейнерів, підслуховування тощо. Промисловий шпигун може являти собою внутрішню загрозу, виступаючи у якості фізичної особи, котра отримала роботу в компанії з метою нелегітимного шпигунства, або незадоволеного співробітника, який торгує інформацію в корисливих цілях або з метою помсти керівництву чи інших корисливих мотивів. Шпигуни можуть також проникнути в довіру співробітників в якості формування соціальної політики підприємства та за допомогою методів психологічного впливу отримувати необхідну їм конфіденційну інформацію. Для великих підприємств поширеними є випадки, коли промислові шпигуни фізично порушують встановлені керівництвом норми поведінки: переглядаючи корзини для сміття або копіюючи файли або жорсткі диски комп'ютерів, що залишені без нагляду.

Корпоративне та промислове шпигунство є реальною загрозою, котра може вплинути на будь-який тип бізнесу - від невеликих до передових компаній у міжнародному списку Fortune.

Виділяють чотири *типи інсайдерських загроз* в контексті промислового шпигунства :

- хабарництво - конкурент або агент розвідки (найнятий конкурентом) звертається до співробітника цільової компанії із пропозицією та стимулюванням до витоку конфіденційних даних, мотивуючи їх готівкою або іншим методом матеріального та нематеріального стимулюванням;
- група змови - виникає у випадку, коли декілька співробітників, групуючись разом, використовують свої колективні знання і привілеї, щоб отримати доступ до конфіденційної інформації компанії;
- соціальна інженерія - становить собою систему маніпуляцій мережевими адміністраторами та IT-персоналом, а також інсайдерами або аутсайдерами, які мають доступ до конфіденційної інформації ком-панії;
- управлінські привілеї - нелегітимні дії в контексті порушення принципу конфіденційності інформації на підприємстві співробітниками, які використовують свої управлінські повноваження для доступу до службової або конфіденційної інформації та подальшого незаконного її розголошення.

Все частіше останніми роками відбувається вторгнення через корпоративну мережу у формі так званих «цільових атак». Як правило, цілеспрямований напад проводиться з метою отримання початкового доступу до мережі, що згодом переростає у постійну загрозу у формі крадіжки даних. Широко застосовуються стільникові телефони, котрі залишаються в залі для запису і передачі інформації заінтересованим суб'єктам, здійснюючи моніторинг конфіденційної зустрічі віддалено. Більшість стільникових телефонів мають камери і записуючі пристрої. Є дуже багато програм, які можна встановити на смартфони сьогодні, щоб отримати доступ до бази даних самого телефону. Особливо небезпечною є робота пристрою у незахищеній мережі Wi-fi. Але записуючі пристрої можуть бути розміщені не тільки в мобільних телефонах. Серед ексклюзивних прикладів можна виділити: цифрові пристрої запису у чорнильній ручці, окуляри з вмонтованим носієм запису та USB палички. Ці пристрої мають можливість запису сотні годин, і вони не прослідковуються на конкретній частоті, саме тому їх майже неможливо виловити.

Ще одним з напрямків, що становлять загрозу для підприємства, є порушення у сфері кібер-безпеки. Мережеві адміністратори не мають належних протоколів безпеки на підприємстві, щоб перешкодити виникненню загроз, які можуть проникнути через власні мережі. Даний процес є доволі важким, саме тому, найголовніше, що можуть зробити компанії, це визначити ризики, а потім здійснювати

відповідні протоколи економічної безпеки.

Очевидно, що у сфері бізнесу сьогодні інформація є більш цінним об'єктом, ніж будь-коли. Кожна організація є уразливою для крадіжки інформації. У зв'язку з цим компанії повинні змінити спосіб мислення в контексті формування економічної безпеки підприємства, тобто визначити свої цінні ресурси та інформацію, в яких можуть бути зацікавлені їхні конкуренти. Вони повинні вирішити, на якому участку необхідна охорона і де знайти потрібних людей, котрі можуть її надати. Важливим аспектом виступає якість на надійність персоналу, що задіяний у забезпеченні безпеки підприємства. Адже маючи безпосередній доступ до арсеналу інформації про компанію, промислові шпигуни в особі недобросовісних програмістів можуть внедрити вірус «троянського коня» в корпоративну комп'ютерну систему, і тим самим створити «чорний хід» доступу до конфіденційних даних компанії.

Цільові атаки належать до найпоширеніших форм промислового шпигунства в контексті постійних загроз у сфері промислової власності. На них припадає приблизно один із числа двох мільйонів повідомлень електронної пошти. Тим не менш, кількість спеціально створених шкідливих програм в цілому виросла в обсязі та складності в останні роки, але так як вони призначені для крадіжки секретів компаній, може бути досить важким завданням для одержувачів дізнатися, коли зловмисник використовує методи соціальної інженерії.

Цільові атаки вперше з'явилися в 2005 році і набули свого поширення в зв'язку з розвитком комп'ютерної сфери. Спеціалізовані комп'ютерні програми ідентифікують і блокують такий напад приблизно на тижневий період, після чого необхідна ліквідація такої загрози та її наслідків. Протягом наступного року їхня кількість зросла до одного або двох нападів на день, а в наступні роки відбулася активізація даного процесу до наступної кількості: приблизно 60 за день в 2010 році та 154 в 2011 році.

Точність цільової атаки, як правило, забезпечується використанням шкідливих документів, котрі пересилаються електронною поштою до конкретної людини або невеликої групи осіб. Такі листи наділені соціальним елементом, що робить їх більш цікавими і актуальними.

Цільові атаки водночас можуть мати ознаки міжнародного шпигунства або саботажу. Цілі таких атак коригуються від військових, політичних до економічних в контексті порушення діяльності розвідувальної діяльності, порушення надійності комерційних таємниць. Метою здійснення такого роду атак може бути крадіжка даних або втручання в діяльність цільової організації чи компанії, саме тому вони можуть становити загрозу для мережі, котра контролюється шкідливими програмами конкурентних організації. Останні просуваються за допомогою спеціальних зашифрованих трафіків, замаскованих під звичайні. У гіршому випадку такі програми набирають характеру шкідливості, закріплюючись безпосередньо в компютерно-інформаційній системі організації чи підприємства, що виступає об'єктом посягань, з метою віддаленого закачування необхідної інформації конкурентами або ж управління базами даних. Нападники мають дуже чіткі і конкретні цілі, вони добре фінансуються і є добре організованими, у зв'язку з чим відсутність належного рівня захисту від такого роду шкідливих програм, існує велика потенційна загроза для досягнення ними бажаних цілей. Визначення того, що мається на увазі під поняттям цільових атак є необхідним, щоб краще зрозуміти природу цієї наростаючої загрози.
Типами організацій, що стають мішенню цільових атак, як правило, є великі, добре відомі багатонаціональні організації, котрі переважно працюють в державному секторі, обороні, енергетиці і фармацевтичній діяльності. В останні роки даний перелік розширився, включивши в себе усі форми організацій, в тому числі малого і середнього бізнесу.

Атака може розглядатися як цільова, якщо вона призначена для конкретної особи або організації і створюється в обхід традиційного захисту та безпеки, використовуючи передові методи соціальної інженерії. Однак, не всі цільові атаки призводять до промислового шпигунства. Наприклад, вірусна програма-троян «Zeus» у сфері банківської діяльності може бути спрямована і буде використовувати соціальну інженерію, щоб стимулювати одержувача в активації шкідливих програм, але не є методом здійснення промислового шпигунства. Атакуючий не обов'язково піклується про те, хто є одержувачами окремої загрози, оскільки вони, можливо, були обрані просто тому, що він має можливість користуватися інформацією, зібраною зазвичай через соціальні мережі та веб-сайти. Соціальна інженерія завжди була на передньому плані в контексті більш складних видів атак, спеціально розроблених, щоб прорвати оборону компанії і отримати доступ до інтелектуальної власності або з метою втручання у фізичну систему контролю роботи організації чи підприємства. Без сильної складової соціальної інженерії навіть самі технічно витончені атаки навряд чи реалізуються. Оскільки велика кількість цільових атак методом соціальної інженерії заснована на інформації, зібраній за допомогою соціальних мереж та соціальних медіа та Web–сайтів, зловмисники в змозі зрозуміти їхні цілі, інтереси, хобі, розпізнати партнерів, з якими вони спілкуються; завдяки такій інформації вони в змозі побудувати більш правдоподібну і переконливу атаку.

Основні показники результативності цільових атак в мережі Інтернет за 2012 рік:

- кількість цільових атак зросла на 42 % в 2012 році порівняно із 2011 роком;
- 31% атак був направлений на підприємства з кількістю працівників менше 250 чоловік;
- однієї атаки було достатньо, щоб заразити 500 організацій за один день;
- виявлено 14 новітніх вразливих елементів систем;
- 32 % усіх мобільних загроз здійснюють крадіжку інформації;
- одна загроза стала джерелом зараження для 600000 комп'ютерів в 2012 році;
- зниження кількості спаму (69 % електронних повідомлень містять спам);
- кількість сайтів, атакуючих соціальні мережі, зросла на 125 %;
- активність веб-атак зросла на 30%;
- кількість нових уражень, виявлених в 2012 році, склала 529, при цьому 415 з них були направлені на мобільні операційні системи [1].

Компанія «ESET» у 2012 році повідомила про виявлення шкідливого програмного забезпечення, що отримало назву «ACAD / Medre.A». Виявлений вірус-«хробак» був націлений на розкрадання файлів, створених у спеціалізованих програмних продуктах «AutoCAD», які використовуються для створення конструкторських проектів та креслень у сфері машинобудування, будівництва, архітектури та інших галузях промисловості. Спалах вірусної атаки був зафіксований в Перу службою «ESET Live Grid». Фахівці компанії виявили, що вірусний файл викрадає інформацію і відправляє її на облікові записи електронної пошти в Китаї. З метою припинення передачі інформації та файлів аналітики «ESET» зв'язалися з китайським інтернет-провайдером «Tencent», Національним центром КНР з реагування на вірусні загрози, а також з компанією «Autodesk», творцем «AutoCAD». На момент ідентифікації вірусу було викрадено тисячі креслень. Через масштабність даної цільової атаки з метою промислового шпигунства фахівці «ESET» звернулися до власника домену qq.com, компанії «Tencent». Завдяки негайним діям «ESET» і «Tencent» облікові записи, що використовувалися для передачі креслень, були заблоковані, що запобігло подальшому витоку даних [2]. Велика кількість комп'ютерних програмних заражень в Перу могла бути пов'язана з тим, що шкідливе програмне забезпечення, модифіковане під файл формату «AutoCAD», могло бути запроваджене компаніями, що співпрацюють з державними службами саме в Перу. Тобто основною мішенню творців даного шкідливого вірусного програмного забезпечення були ці установи та організації. А це у свою чергу є яскравим прикладом промислового шпигунства на макрорівні.

Ще одним прикладом здійснення активної цільової атаки в контексті промислового шпигунства стали постійні випадки кібер-нападів на нафтову промисловість, котрі отримали назву «Nitro» (за даними американської компанії «Symantec»). Значна частина атак «Nitro» відбулася у 2011 році. Метою атаки було промислове шпигунство, в основному, у сферах хімічної та нафтової промисловості, в контексті збору інформації щодо об'єктів інтелектуальної власності для досягнення конкурентної переваги. Проте, учасники кібер-атаки «Nitro» цільові напади здійснювали водночас і на оборонну промисловість та аерокосмічний комплекс у жовтні 2011 року. Щоб зрозуміти природу цільових атак компанія «Symantec» зібрала дані про більш ніж 26 000 атак, які могли бути ідентифіковані як цільові. Ці атаки були направлені на електронну пошту та містили деструктивні дії щодо функціональності комп'ютерів. При використанні додаткового аналізу компанією було застосовано програму «Triage», за допомогою якої було ідентифіковано різні цільові атаки, а також визначено характеристики і динаміку цих військові цільових атак в контексті промислового шпигунства. За ініціативи компанії «Symantec» в рамках

європейської кампанії «Wombat», направленої на удосконалення методології виявлення потенційних та існуючих цільових атак та аналізу різних типів загроз, була впроваджена і використовується техніка багатокритеріального алгоритму з розробки програмного забезпечення «Triage» [6]. На сьогодні дана програма удосконалюється за підтримки європейського проекту «Vis-sense» в рамках співпраці «Symantec» з іншими п'ятьма партнерами [5].

Такі галузі промисловості, як сільське господарство, будівництво, нафтова промисловість та енергетика часто підпадають під мішень цільових атак, що спрямовані на отримання комерційних таємниць. Це не означає, що уряд і оборонна промисловість не стикаються з цільовими атаками. Дві третини військових компаній підпадають під одноразові або обмежену кількість нападів від організацій, що працюють в тому ж секторі. Ці атаки здійснювалися з використанням шкідливих програм «Sykipot». Дані програми отримали значне поширення у 2006 році, а остання хвиля їх використання припала на кінець 2011 року і характеризувалася застосуванням шкідливої програми, вміщеної у PDF форматі файлу Adobe Reader і Acrobat (CVE -2011- 2462) [4]. Нападники, які використовують «Sykipot», свою увагу переважно зосереджують на оборонній промисловості. Особливої уваги заслуговують шкідливі PDF – файли, котрі в значній мірі продовжують застосовуватися для цільової атаки (в середньому цей показник становить більше третини всіх атак). Поштовий і RAR-архіви використовуються зловмисниками приблизно у 27% всіх атак. Варто відзначити, що файли PE32, які приходять у якості поштових повідомлень, рідко використовуються в контексті цільових атак. Найчастіше цілями такого роду атак є урядові сайти чи поштові скриньки державних організацій.

Висновки та пропозиції.

Підводячи підсумок про характер цільових атак в контексті промислового шпигунства, можемо зробити акцент на загальновизнаних в економічній літературі припущеннях про їхні особливості, внісши відповідні сучасному розвитку даної сфери корективи:

1. Вважається, що тільки великі корпорації, уряди та оборонна промисловість стають мішенню для промислового шпигунства в контексті застосування цільових атак. Однак, загальне число цільових атак, спрямованих на малі та середні підприємства та організації приблизно дорівнює кількості атак, спрямованих на великі підприємства та організації.

2. Вважається, що тільки топ-менеджери і експерти з інтелектуальної власності стають мішенню цільової атаки. Однак, зловмисники прагнуть захопити інформацію від працівників, які мають доступ до інтелектуальної власності, але вони не атакують їх безпосередньо, а використовують працівників нижчих рангів, щоб отримати необхідну інформацію.

3. Вважається, що промислове шпигунство є результатом лише одного виду цільової атаки. Однак, доволі часто керівництва організацій вважають, що якщо вони не стали ціллю здійснення цільової атаки високого профілю, або якщо поодинокі атаки на організацію чи підприємство були заблоковані, то цільова атака закінчилася. Проте, цільова атака в середньому може тривати протягом місяця і більше. А промислове шпигунство потенційно буде змінюватися з плином часу, з використанням нового виду соціальної інженерії, цільових атак, нових шкідливих програм.

Отже, цільові атаки виступають проблемою для всіх організацій, великих і малих підприємств. Керівники вищої ланки, працівники, які мають пряме відношення до інтелектуальної власності компанії, повинні бути обережними, оскільки усі співробітники знаходиться під загрозою стати об'єктом цільових атак. Це особливо стосується працівників, які в ході своєї роботи зазвичай отримують електронну пошту від осіб, котрих вони не знають. Зрештою, незалежно від розміру або типу організації існує фактор загрози виникнення цільової атаки, особливо в контексті промислового шпигунства.

На мікрорівні керівництва компаній повинні зосереджувати свою увагу не лише на реактивних методах забезпечення економічної безпеки, але і формувати систему превентивних заходів з метою уникнення випадків виникнення факту промислового шпигунства:

- здійснювати постійний моніторинг потенційних загроз у вигляді шкідливого програмного забезпечення;
- здійснювати періодичну та неперіодичну атестацію персоналу з метою визначення рівня його надійності;
- обов'язково підписувати договори про нерозголошення комерційної таємниці між керівниками підприємств та працівниками, чия професійна діяльність пов'язана з такого роду інформацією.

На макрорівні необхідними умовами формування системи захисту від промислового шпигунства є:

- формування ефективного механізму державного регулювання експорту-імпорту товарів, які містять отриману незаконним шляхом інтелектуальну власність, особливо у якості комерційної таємниці, чи виготовлені на її основі;

- податкове регулювання процесу переміщення через кордон продукції, що виготовлена або реалізовується із порушенням права інтелектуальної власності;

- гармонізація законодавства, що стосується захисту від недобросовісної конкуренції у контексті промислового шпигунства, особливо щодо питань, пов'язаних із охороною та захистом комерційної таємниці;

- стимулювання розвідувальної та контррозвідувальної діяльності у контексті боротьби з промисловим шпигунством як на національному, так і на міжнародному рівні, контроль за дотриманням чинного законодавства.

Необхідно поєднувати як методи захисту національних суб'єктів господарювання від промислового шпигунства, так і провадити активну діяльність по недопущенню проявів даного процесу з їхнього боку. Для цього необхідна не лише державна підтримка, але в першу чергу гармонізація законодавства у сфері інтелектуальної власності, особливо, що стосується захисту від недобросовісної конкуренції. Таке поєднання повинно нейтралізувати можливість виникнення загроз, а також стимулювати економічне зростання в контексті формування ефективної системи економічної безпеки. Перспективними вважаються подальші дослідження процесу промислового шпигунства, захисту від цільових атак, нейтралізації інсайдерських загроз.

СПИСОК ДЖЕРЕЛ:

1. Отчет об угрозах безопасности в Интернете за 2013 год: [Електронний ресурс] / Публикации службы Securuty Response. - 2013. – Том 18. - Режим доступу: http://www.symantec.com/ru/ru/security_response/publications/threatreport.jsp?inid=ru_ghp_thumbnail3_istr-2013
2. Унікальний випадок промислового шпигунства виявлений фахівцями ESET : [Електронний ресурс] / Інформативне місце КЕРНпр. – 2012. - Режим доступу: http://kernpro.info/unikalnyj-vypadok-promyslovoho-shpyhunstva-vyjavlenyj-fahivcjamy-eset/
3. Nasheri H. Economic Espionage and Industrial Spying / Nasheri Hedieh . – Cambridge: Studies in Criminology, 2004. - 288 p.
4. The Sykipot Attacks : [Електронний ресурс] / Symantec. – 2012. - Режим доступу: http://www.symantec.com/connect/blogs/sykipot-attacks
5. Visual Analytics for Securitiy. Vis-sense. : [Електронний ресурс] .- Режим доступу: http://www.vis-sense.eu/Project/
6. Worldwide Observatory of Malicious Behaviors and Attack Threats : [Електронний ресурс] / Wombat. – 2012 .- Режим доступу: http://www.wombat-project.eu/