РОЗДІЛ 8
КРИМІНАЛЬНЕ ПРАВО ТА КРИМІНОЛОГІЯ; КРИМІНАЛЬНО-ВИКОНАВЧЕ ПРАВО

УДК 343.534
DOI https://doi.org/10.32782/2524-0374/2025-4/70

СУЧАСНІ ІНСТРУМЕНТИ І ЗАСОБИ КОМЕРЦІЙНОГО ШПИГУНСТВА ТА ЇХ НЕЙТРАЛІЗАЦІЯ В КОРПОРАТИВНОМУ СЕКТОРІ

MODERN TOOLS AND MEANS OF COMMERCIAL ESPIONAGE AND THEIR NEUTRALISATION IN THE CORPORATE SECTOR

Аркуша Л.І., д.ю.н., професор,
завідувач кафедри криміналістики, детективної
та оперативно-розшукової діяльності
Національний університет «Одеська юридична академія»

Хижняк Є.С., к.ю.н., доцент,
доцент кафедри криміналістики, детективної
та оперативно-розшукової діяльності
Національний університет «Одеська юридична академія»

Чернов О.В., д.філос.,
доцент кафедри криміналістики, детективної
та оперативно-розшукової діяльності
Національний університет «Одеська юридична академія»

У сучасних умовах стрімкої цифровізації бізнес-процесів, зростання конкуренції та глобалізації ринків, проблема комерційного шпигунства набуває особливої актуальності. Комерційне шпигунство – це цілеспрямована діяльність, що має на меті незаконне здобуття конфіденційної або комерційної інформації, яка становить цінність для конкурентів або третіх осіб. У корпоративному середовищі витік такої інформації може призвести до серйозних фінансових збитків, втрати ринкових позицій, репутаційних ризиків, а також поставити під загрозу економічну безпеку окремих підприємств і цілих галузей.

У статті досліджуються сучасні інструменти та технології, які активно використовуються для здійснення комерційного шпигунства. Зокрема, розглянуто використання шкідливого програмного забезпечення (spyware, keyloggers, backdoors), соціальної інженерії, фішингу, атак через вразливості програмного забезпечення та апаратних засобів, а також застосування засобів стеження, таких як приховані камери, аудіозаписувальні пристрої, пристрої для перехоплення трафіку тощо. Окрема увага приділяється використанню штучного інтелекту та аналітики великих даних для збору, аналізу та використання чутливої інформації у конкурентній боротьбі.

Значну увагу автори приділяють також методам нейтралізації та протидії комерційному шпигунству в корпоративному секторі. Розглянуто організаційно-технічні заходи, серед яких ключове місце займають системи кібербезпеки, шифрування даних, багаторівнева автентифікація, аудит інформаційної безпеки, політика доступу до критичної інформації, а також внутрішній комплаєнс та регулярне навчання персоналу. Підкреслено, що ефективна протидія потребує не лише технічних рішень, а й чітко регламентованих внутрішніх процедур та підвищення загального рівня інформаційної гігієни в організаціях.

У контексті правового регулювання відзначено, що законодавча база в Україні лише частково охоплює сферу протидії комерційному шпигунству, зокрема через недостатню конкретизацію термінології, відсутність спеціалізованих норм щодо відповідальності за такі діяння та низький рівень правозастосування. Проаналізовано досвід деяких іноземних держав, де створено комплексні системи правового захисту комерційної інформації та передбачено кримінальну відповідальність за її незаконне здобуття, використання чи розголошення.

У статті наголошується на необхідності комплексного підходу до захисту корпоративної інформації, що поєднує правові, технічні та управлінські інструменти. Висловлюється теза про доцільність удосконалення вітчизняного законодавства у сфері охорони комерційної таємниці, посилення співпраці з правоохоронними органами та запровадження сучасних стандартів інформаційної безпеки на рівні підприємств.

Ключові слова: комерційне шпигунство, корпоративна безпека, конфіденційна інформація, кіберзагрози, соціальна інженерія, комплаєнс, інформаційна безпека, протидія шпигунству, правове регулювання, комерційна таємниця.

In today's environment of rapid digitalisation of business processes, increasing competition and globalisation of markets, the problem of commercial espionage is becoming particularly relevant. Commercial espionage is a targeted activity aimed at illegally obtaining confidential or commercial information that is valuable to competitors or third parties. In the corporate environment, the leakage of such information can lead to serious financial losses, loss of market position, reputational risks, and threaten the economic security of individual companies and entire industries.

The article examines modern tools and technologies that are actively used for commercial espionage. In particular, the article examines the use of malware (spyware, keyloggers, backdoors), social engineering, phishing, attacks through software and hardware vulnerabilities, as well as the use of surveillance tools such as hidden cameras, audio recording devices, traffic interception devices, etc. Particular attention is paid to the use of artificial intelligence and big data analytics to collect, analyse and use sensitive information in the competitive struggle.

The authors also pay considerable attention to methods of neutralising and counteracting commercial espionage in the corporate sector. Organisational and technical measures are considered, among which cybersecurity systems, data encryption, multi-level authentication, information security audit, critical information access policy, as well as internal compliance and regular staff training are key. It is emphasised that effective counteraction requires not only technical solutions, but also clearly regulated internal procedures and an increase in the overall level of information hygiene in organisations.

In the context of legal regulation, it is noted that the legislative framework in Ukraine only partially covers the area of countering commercial espionage, in particular, due to insufficient specification of terminology, lack of specialised rules on liability for such acts and low level of law enforcement. The author analyses the experience of some foreign countries with comprehensive systems of legal protection of commercial information and criminal liability for its unlawful acquisition, use or disclosure.

The article emphasises the need for an integrated approach to the protection of corporate information, which combines legal, technical and managerial tools. The author suggests that it is expedient to improve domestic legislation in the field of trade secret protection, strengthen cooperation with law enforcement agencies and introduce modern information security standards at the enterprise level.

Key words: commercial espionage, corporate security, confidential information, cyber threats, social engineering, compliance, information security, counter-espionage, legal regulation, trade secrets.

Комерційне шпигунство в Україні розглядається як один із проявів економічного шпигунства, що має вже вужчу спеціалізацію, зосереджену на здобутті конфіденційної або стратегічно важливої інформації про одного або кількох безпосередніх конкурентів шляхом застосування нелегітимних, часто протиправних засобів. На відміну від економічного шпигунства, яке здебільшого асоціюється з діяльністю державних структур, зокрема розвідувальних органів іноземних країн, комерційне шпигунство зазвичай здійснюється приватними особами, суб'єктами господарювання, а також окремими компаніями або юридичними/фізичними особами, зацікавленими в отриманні переваг на ринку.

Комерційне шпигунство переслідує дві основні цілі. По-перше, це збір інформації про діяльність конкурентів, зокрема стратегії розвитку, бізнес-плани, технологічні інновації, фінансову звітність, логістику, клієнтську базу, маркетингові стратегії тощо. По-друге, це досягнення конкурентної переваги шляхом дискредитації, витіснення або усунення конкурента з ринку, використовуючи здобуту інформацію в корисливих цілях.

У науковій літературі комерційне шпигунство класифікується як одна з форм недобросовісної конкуренції. Йдеться про незаконну діяльність, спрямовану на здобуття, використання або розголошення інформації, яка має економічну або комерційну цінність, зазвичай захищену режимом комерційної таємниці. Ключовим елементом цього явища є саме його незаконність, тобто порушення норм права під час здобуття інформації, яка не призначена для відкритого доступу.

Історично комерційне шпигунство має витоки у військовій та політичній розвідці, однак із розвитком глобального бізнесу ця діяльність трансформувалася в окремий напрям – бізнес-шпигунство. У відповідь на це в країнах з розвиненою ринковою економікою виник легітимний інструмент аналізу ринку – конкурентна розвідка. Її мета – систематичний збір, обробка та аналіз публічно доступної або добровільно переданої інформації про конкурентів, партнерів, ринкові тренди та інші чинники бізнес-середовища з метою прийняття обґрунтованих управлінських рішень. Важливо підкреслити, що конкурентна розвідка діє виключно в межах чинного законодавства та етичних норм ведення бізнесу.

Основна відмінність між конкурентною розвідкою та комерційним шпигунством полягає в методах отримання інформації. Якщо конкурентна розвідка базується на відкритих джерелах та правових засобах доступу до інформації, то комерційне шпигунство вдається до прихованих, неправомірних або кримінально караних способів. Серед найбільш поширених методів комерційного шпигунства варто виділити: незаконне проникнення до інформаційних систем конкурента, використання шкідливого програмного забезпечення, приховане прослуховування телефонних розмов або встановлення засобів відеоспостереження, шантаж працівників з метою отримання відомостей, підкуп або вербування співробітників конкурентних фірм, викрадення носіїв інформації тощо.

Сучасні методи, що використовуються для здійснення комерційного шпигунства як у країнах Європи, так і в Україні, умовно поділяються на дві основні категорії: розвідувальні методи та технічні засоби збору інформації. Розвідувальні методи, по суті, становлять основу будь-якої шпигунської діяльності, незалежно від сфери її застосування. Найпоширенішими з них є рекрутинг (вербування) осіб, які мають доступ до комерційно значущої інформації, та залучення третіх осіб – агентів, які впроваджуються до структури підприємства-конкурента.

Варто зазначити, що практично в кожній великій компанії працюють фахівці, котрі мають доступ до внутрішніх баз даних, стратегічних документів і технологічної інформації. Такі особи, особливо якщо вони незадоволені умовами праці або перебувають під фінансовим чи іншим тиском, можуть стати об'єктами рекрутингу з боку суб'єктів комерційного шпигунства. При цьому використання зовнішніх агентів часто вважається безпечнішим способом ведення шпигунської діяльності, оскільки зменшує ризик викриття замовника та забезпечує більшу лояльність і контрольованість виконавця.

Щодо технічних методів комерційного шпигунства, які є особливо актуальними для українських реалій, то вони охоплюють широкий спектр засобів прихованого збору інформації. Законодавство України частково регулює виробництво, обіг і використання таких пристроїв, однак у практиці їх застосування залишаються суттєві прогалини в контролі та правозастосуванні. Серед найбільш уживаних технічних засобів – пристрої для аудіозапису: мікрофони, електронні стетоскопи, радіомікрофони, лазерні мікрофони, магнітофони тощо. Ці пристрої дозволяють здійснювати приховане перехоплення розмов у приміщеннях, автомобілях або на робочих місцях.

Сучасне комерційне шпигунство є складним, багатогранним явищем, що активно використовує найновіші інформаційні технології, психолого-комунікативні методи та інструменти кіберзлочинності для досягнення своїх цілей. Основна мета зловмисників – здобуття стратегічно важливої інформації про діяльність компаній, новітні розробки, комерційні плани, бази клієнтів, фінансові показники тощо. З огляду на це, комерційне шпигунство дедалі частіше здійснюється не через традиційні форми стеження, а через складні цифрові атаки та технологічні маніпуляції, які складно виявити без спеціалізованих знань і засобів кіберзахисту.

Одним із найбільш поширених інструментів сучасного комерційного шпигунства є шкідливе програмне забезпечення (malware). До нього належать spyware, keyloggers та backdoors. Spyware – це шпигунське програмне забезпечення, яке інсталюється на комп'ютери або мобільні пристрої без згоди користувача. Таке програмне забезпечення виконує функції непомітного моніторингу, фіксуючи кожен крок користувача – від перегляду вебсторінок і введення паролів до копіювання вмісту електронної пошти та документів. Інформація передається на віддалені сервери зловмисників, що дозволяє їм отримувати повну картину внутрішньої діяльності компанії в режимі реального часу.

Keyloggers – це специфічний тип spyware, який фіксує натискання клавіш на клавіатурі. Такий інструмент дозволяє викрадачам отримувати точні логіни, паролі, коди доступу до внутрішніх систем, CRM, бухгалтерських програм або корпоративних акаунтів. Особливо небезпечними є апаратні keyloggers, які можуть бути вмонтовані у клавіатури або підключені до комп'ютера фізично, що практично унеможливлює їхнє виявлення без технічного обстеження.

Backdoors (бекдори) – ще один небезпечний інструмент шпигунства, який дозволяє обійти стандартні механізми автентифікації і отримати повний доступ до системи. Бекдори можуть бути навмисно закладені в програмне забезпечення ще на етапі його розробки, або створені в результаті злому інформаційної інфраструктури. Вони забезпечують прихований контроль над мережевими ресурсами, базами даних, поштовими серверами, файлами та іншими критично важливими елементами інформаційної системи підприємства.

Окрему загрозу становить використання методів соціальної інженерії, які ґрунтуються не на технологіях, а на маніпуляції людською психологією. Зловмисники, видаючи себе за співробітників компанії, представників технічної підтримки, постачальників або навіть керівництво, здійснюють телефонні дзвінки, надсилають електронні листи або вступають у прямий контакт з працівниками компанії. Їхня мета – змусити людину добровільно розкрити паролі, надіслати конфіденційні файли або здій-

снити дії, які відкриють доступ до інформаційної інфраструктури. Часто жертви навіть не усвідомлюють, що стали джерелом витоку важливої інформації.

Серед методів, які базуються на соціальній інженерії, особливу небезпеку становить фішинг – надсилання підроблених електронних повідомлень із посиланнями на фальшиві сайти, що імітують реальні корпоративні ресурси або платформи для входу до внутрішніх систем. Користувач вводить на такому сайті свій логін і пароль, після чого ці дані миттєво потрапляють до зловмисників. Різновиди фішингу включають spear phishing – цілеспрямовані атаки на конкретних осіб, зазвичай – представників бухгалтерії або IT-відділу, whaling – атаки на керівництво компаній, smishing – фішинг через SMS, та vishing – голосові дзвінки з метою маніпуляції.

Не менш небезпечним є використання вразливостей програмного забезпечення, особливо так званих «нульових днів» (zero-day vulnerabilities), які ще не були виявлені або не усунуті розробниками. Через такі вразливості хакери можуть проникнути до корпоративної мережі, викрасти файли, змінити дані або впровадити додаткові шкідливі програми. Атаки часто здійснюються через неправильно налаштовані сервери, застаріле або неоновлене програмне забезпечення, а також через популярні веб-застосунки, які містять вразливості типу SQL-ін'єкцій, міжсайтових скриптів (XSS) або підробки міжсайтових запитів (CSRF).

У сучасних умовах значну роль відіграє також фізичне впровадження шпигунських пристроїв до апаратного середовища компаній. Це можуть бути апаратні keyloggers, мініатюрні відеокамери, стетоскопи для перехоплення звуку через стіни, GPS-трекери, закладені в обладнання, або навіть модифіковані флеш-накопичувачі, які запускають шкідливі скрипти одразу після підключення до комп'ютера. Злочинці можуть впровадити такі пристрої через постачальників, ремонтників, кур'єрів або під виглядом звичайних офісних приладів.

Зі зростанням популярності хмарних технологій та віддаленої роботи також зросли ризики, пов'язані з неправильним налаштуванням хмарних сервісів. У багатьох випадках конфіденційні файли залишаються доступними без автентифікації або з використанням надто слабких паролів. Особливо вразливими є хмарні сховища типу Amazon S3, Google Drive, Dropbox, API, що використовуються у мобільних застосунках, а також IoT-пристрої, які підключені до корпоративної мережі (наприклад, розумні принтери, IP-камери, системи доступу та датчики). Через ці слабкі місця зловмисники можуть не лише перехопити трафік, а й отримати доступ до систем управління безпекою або логістикою компанії.

Таким чином, сучасне комерційне шпигунство використовує поєднання технічних, програмних, організаційних та психологічних методів для досягнення своїх цілей. Протидія таким загрозам потребує комплексного підходу, що включає не лише використання сучасних систем інформаційної безпеки, а й постійне навчання персоналу, аудит внутрішніх процедур, впровадження політик управління ризиками та створення систем моніторингу підозрілої активності на всіх рівнях функціонування компанії.

Згідно з позицією низки українських дослідників, одним із найрозповсюдженіших способів незаконного отримання інформації в Україні залишається негласне підключення до телефонних ліній. Такий метод популярний через відносну простоту реалізації, доступність необхідного обладнання та низьку вартість. У той же час використання засобів відеоспостереження, хоча й менш поширене, також має місце, особливо в контексті стеження за ключовими особами підприємства.

Комерційне шпигунство включає також непрямі засоби здобуття інформації, такі як дезінформація, шантаж співробітників, підкуп, зловживання службовим становищем, а також використання окремих представників правоохоронних або контролюючих органів для доступу до конфіденційної інформації під прикриттям перевірок, розслідувань чи іншої офіційної діяльності.

Як показують дослідження, зокрема праця Якубівської Ю.Є., вплив комерційного шпигунства на сферу інтелектуальної власності в Україні проявляється у двох основних напрямах:

1. Незаконне отримання знань, ноу-хау та інформації, що становить об'єкти інтелектуальної власності – таких як виробничі технології, унікальні рецептури, формули, методи обробки, алгоритми та технічні розробки.

2. Здобуття матеріальних прав на результати чужої інтелектуальної діяльності, включаючи бази даних клієнтів, інформацію про ціноутворення, продажі, маркетингову політику, внутрішні звіти про дослідження та розробки, плани стратегічного розвитку, зміни у виробничих процесах тощо [1].

У межах цього процесу можуть мати місце такі протиправні дії, як крадіжка комерційної таємниці, технічне стеження, підкуп посадових осіб, шантаж та інші злочини, спрямовані на доступ до критично важливої для бізнесу інформації.

При цьому суб'єктами комерційного шпигунства в Україні виступають не лише окремі підприємства чи приватні особи, але й державні установи або посадові особи, які можуть зловживати службовим становищем для маніпуляцій у сфері, наприклад, державних закупівель, отримуючи конфіденційні дані про умови тендерів і передаючи їх обраним учасникам для формування вигідніших пропозицій та штучного зниження конкуренції.

У сучасних умовах успішне здійснення розвідувальної діяльності у сфері бізнесу значною мірою ґрунтується на ефективному функціонуванні конкурентної розвідки. Своєчасне отримання достовірної, перевіреної та аналітично обробленої інформації про дії, наміри, стан справ і стратегії конкурентів стає ключовим чинником, що визначає здатність компанії адаптуватися до змін, захищати власні ринкові позиції та приймати стратегічно обґрунтовані управлінські рішення. Проте межа між легітимними методами збору та аналізу відкритої інформації і діями, що вже мають ознаки комерційного шпигунства, часто є настільки розмитою, що на практиці відокремити одне від іншого буває вкрай складно. Особливо це стосується ситуацій, коли підприємства використовують методи, які формально не заборонені законом, але по суті спрямовані на отримання інформації обхідними, маніпулятивними або прихованими способами.

Комерційне шпигунство, на відміну від конкурентної розвідки, передбачає протиправне втручання в діяльність іншого суб'єкта господарювання з метою заволодіння конфіденційними даними. Йдеться про викрадення ноу-хау, технологічних розробок, ділових планів, списків клієнтів, схем цінової політики, персональних даних працівників тощо, які можуть бути використані для недобросовісної конкуренції, шантажу, підриву ділової репутації або створення штучних переваг на ринку. Подібна діяльність суперечить принципам етичного ведення бізнесу і прямо порушує норми чинного законодавства.

Натомість конкурентна розвідка базується на відкритих і дозволених законом джерелах інформації. Її основна мета – вивчити діяльність конкурентів у легальний спосіб для того, щоб своєчасно виявити потенційні загрози, оцінити ринкові тенденції та визначити стратегічні переваги, які можна використати для зміцнення позицій власного бізнесу. Практично це зводиться до аналізу того, як функціонують конкуруючі компанії: які обсяги продажів вони демонструють, як реалізують маркетингові стратегії, які нововведення впроваджують, як знижують собівартість продукції, які напрями розвитку обирають.

Методи конкурентної розвідки, залежно від характеру джерел, умов збору інформації та рівня ризику, поділя-

ються на два основні типи: «кабінетний» і «польовий». «Кабінетний» метод полягає у зборі та аналізі даних із загальнодоступних джерел. Це можуть бути аналітичні звіти державних органів, економічна статистика, галузеві огляди, публікації у засобах масової інформації, експертні прогнози, річні звіти компаній-конкурентів, інформація з офіційних сайтів, біржових новин тощо. Завдяки цифровим інструментам і спеціалізованим базам даних аналітики можуть з мінімальними витратами отримувати значні обсяги актуальної інформації для подальшої обробки і використання в стратегічному плануванні.

«Польовий» метод, на відміну від кабінетного, передбачає безпосереднє взаємодію з конкурентним середовищем. Наприклад, підприємство може здійснити замовлення продукції конкурента, щоб оцінити якість товару, рівень сервісу, швидкість і вартість доставки. Такий підхід дозволяє виявити як сильні, так і слабкі сторони діяльності суперника, після чого внести відповідні корективи у власні бізнес-процеси чи сформулювати привабливі пропозиції для переманювання клієнтів.

Ще один поширений спосіб – маскування під звичайного покупця. Представник компанії під виглядом клієнта відвідує магазин чи офіс конкурента, щоб особисто оцінити якість обслуговування, асортимент продукції, цінову політику, атмосферу в точці продажу. У разі потреби додаткової інформації, зокрема про менеджмент, можна інсценувати конфліктну ситуацію чи скаргу, щоб отримати доступ до вищого керівництва або відповідальних осіб компанії.

Також досить ефективним є метод маскування під претендента на роботу. Подаючи документи для участі в конкурсі на вакантну посаду, представник компанії-конкурента може отримати уявлення про внутрішню організацію праці, систему мотивації персоналу, рівень заробітних плат, специфіку корпоративної культури, технологічні аспекти бізнесу. Ця інформація особливо цінна в умовах кадрової конкуренції або за наявності потреби у формуванні нових команд.

Конкурентна розвідка виконує два ключові завдання. По-перше, вона має забезпечити оперативне виявлення зовнішніх загроз, можливостей, змін у ринковому середовищі та передавати сигнали керівництву ще до того, як ситуація стане очевидною для інших учасників ринку. Завчасність отримання таких повідомлень дозволяє компанії діяти проактивно – адаптувати стратегії, мінімізувати ризики або, навпаки, скористатися можливостями, які ще не усвідомлені конкурентами. По-друге, розвідка повинна забезпечувати керівництво компанії об'єктивною, актуальною та всебічною інформацією про реальний стан справ на підприємстві у контексті загальної ринкової ситуації. Незалежно від того, наскільки позитивною чи критичною є ця інформація, вона має бути правдивою, адже тільки за таких умов можливе прийняття ефективних рішень, спрямованих на розвиток і довгострокову стабільність компанії [2].

Методи, характерні для комерційного шпигунства, умовно поділяються на дві основні категорії: агентурні та технічні.

Агентурні методи є ключовими в системі будь-якого шпигунства, оскільки передбачають безпосередню участь людини в процесі отримання конфіденційної інформації. Здебільшого реалізація цього підходу здійснюється двома основними шляхами:

1. Впровадження власного агента до структури підприємства-конкурента.

2. Вербування вже наявного співробітника цієї структури.

Кожен із цих способів має свої специфічні переваги. Впроваджений агент, який поступово здобуває довіру в колективі, з часом може отримати доступ до критично важливої інформації, особливо якщо він наближається до вищої управлінської ланки. У свою чергу, вербування передбачає залучення особи, яка вже займає певну посаду в компанії. Особливо ефективним є вербування так званих «других» або «третіх» осіб – керівників середньої ланки чи досвідчених фахівців, які мають глибокі знання про діяльність підприємства та можуть діяти автономно, реалізуючи власні цілі.

У разі успішного вербування можливе перенаправлення прибуткових контрактів на користь сторони, яка організувала шпигунську діяльність. Якщо мета промислового шпигунства полягає не лише в здобутті інформації, а й у підриві діяльності конкурента (наприклад, через дискредитацію чи банкрутство), то впровадження агента вважається більш ефективним інструментом. Це зумовлено тим, що до «своєї» людини в колективі, як правило, формується більший рівень довіри.

Об’єктами агентурного впливу можуть бути не лише керівники чи аналітики, а й співробітники нижчої ланки – обслуговуючий або технічний персонал. Саме такі працівники часто мають змогу непомітно встановити технічні засоби стеження – мікрофони, пристрої для зчитування даних, системи аудіоконтролю («жучки», «комарі» тощо). Установка таких пристроїв зазвичай триває від кількох секунд до кількох хвилин, що робить цей процес практично невловимим для оточення [3].

Технічні методи корпоративного шпигунства ґрунтуються на використанні спеціалізованих технічних засобів, виробництво, обіг та застосування яких регулюється національним законодавством.

З метою перехоплення та реєстрації акустичної інформації (зокрема розмов і звукових сигналів), зловмисники користуються широким спектром пристроїв: електронними стетоскопами, високочутливими мікрофонами, лазерними мікрофонами, радіопередавачами (так званими «радіозакладками»), апаратами для магнітного або цифрового запису тощо.

Одним із найрозповсюдженіших способів отримання інформації є непомітне впровадження передавальних пристроїв у робочі або службові приміщення. Часто такі пристрої замасковані під побутові предмети або елементи інтер’єру. Вони можуть автономно працювати протягом кількох годин або днів – до повного розрядження джерела живлення. Для тривалішого використання шпигунських засобів іноді передбачено підключення до мережі електроживлення, що забезпечує їх безперервну роботу протягом тривалого часу й суттєво ускладнює їх виявлення.

Асортимент таких «жучків» на нелегальному ринку надзвичайно широкий: від дешевих, кустарно виготовлених пристроїв вартістю 10–20 доларів США, до професійних систем із вартістю 100–200 доларів і більше. Недорогі моделі нерідко використовуються для організації прослуховування відкритих територій – їх можна непомітно розміщувати в листі, траві чи інших природних укриттях, створюючи своєрідну «мережу спостереження». За умови співпраці з особами, обізнаними у сфері радіоелектроніки, ці пристрої можна вільно придбати, зокрема, на радіоринках.

За даними експертів, в Україні найпоширенішим технічним способом отримання конфіденційної інформації залишається приховане підключення до телефонних ліній. Такий метод залишається популярним через його технічну простоту та відносну дешевизну. Випадки прихованого відеоспостереження у корпоративному секторі – рідші, але також мають місце.

Сучасні методи перехоплення телефонних переговорів варіюються від найпримітивніших (перехоплення сигналу радіотелефонів) до складних технічних рішень – наприклад, високочастотного нав’язування сигналу. У таких випадках телефонна лінія використовується не лише для передачі розмов, а й як канал для передавання інформації, зібраної, наприклад, акустичним «жучком», а також як

джерело енергоживлення для шпигунських пристроїв, що передають дані по радіоканалах.

Прослуховуючі пристрої, які встановлюють в офісах, класифікуються за типом живлення на автономні та стаціонарні. Автономні «жучки» зазвичай живляться від батарейок або акумуляторів, до яких підключені мікромікрофони та передавачі. Такі пристрої залишають у приміщенні непомітно – вони працюють, поки не розрядиться елемент живлення (зазвичай 7–10 діб).

Окрему категорію становить мобільне шпигунство – тобто використання мобільних телефонів як засобу негласного збору інформації. Цей напрям стрімко розвивається, як і засоби протидії йому. Згідно з даними продавців техніки безпеки, останніми роками значно зріс попит на пристрої для блокування сигналів мобільних телефонів.

Існують спеціальні зовнішні пристрої, які здатні активувати навіть вимкнений мобільний телефон (за умови, що з нього не вийнято акумулятор), перетворюючи його на мікрофон, що передає усі звуки в приміщенні, включно з приватними розмовами власника. Для протидії таким загрозам розроблено шумогенератори, які створюють перешкоди у відповідному радіочастотному діапазоні. Найпростіші з них коштують від 250–300 доларів США. Вітчизняні моделі, які мають складніший функціонал – зокрема, точково блокують синхронізаційні імпульси між телефоном і базовою станцією, залишаючись при цьому непомітними – можуть коштувати до 1200 доларів США [4].

Загроза комерційного шпигунства є однією з найбільших проблем для сучасних компаній, що прагнуть зберегти свою конкурентоспроможність і конфіденційну інформацію. З огляду на це, важливо розглянути можливі способи нейтралізації та протидії комерційному шпигунству, що включає не тільки технічні, але й організаційні, кадрові та правові заходи.

Одним із основних напрямів захисту є розробка організаційної структури, яка передбачає чітке регулювання обігу конфіденційної інформації. Для цього необхідно створити систему, що включає політики щодо доступу до важливих даних, визначення меж доступу для кожного співробітника залежно від їхніх обов'язків. Це дозволить мінімізувати ймовірність несанкціонованого доступу до інформації або її витоку через недбалість персоналу. Крім того, вкрай важливим є забезпечення чіткої фізичної безпеки корпоративних приміщень. Встановлення систем відеонагляду, контрольно-пропускних пунктів, а також періодичні інспекції допомагають запобігти несанкціонованому доступу в зони, де обробляються чутливі дані.

Важливою складовою є кадрова безпека. На етапі найму необхідно проводити ретельну перевірку кандидатів, зокрема перевірку їхнього професійного минулого та наявності можливих конфліктів інтересів. Також не слід нехтувати психологічним тестуванням співробітників для виявлення потенційних загроз. Для вже працюючих працівників необхідно регулярно проводити тренінги та інструктажі з питань інформаційної безпеки, підвищуючи їхню обізнаність щодо ризиків, пов'язаних із комерційним шпигунством.

Технічні заходи захисту відіграють важливу роль у протидії шпигунству. Встановлення спеціального обладнання для виявлення пристроїв для прослуховування та стеження (так званих «жучків»), відеокамер і мікрофонів є основним інструментом для захисту від технічного шпигунства. Використання спеціалізованих детекторів радіосигналів, спектроаналізаторів та шумових генераторів дозволяє своєчасно виявляти загрози. Крім того, для захисту від несанкціонованого запису розмов у офісах доцільно застосовувати технології екранізації приміщень або шумозаглушення.

Не менш важливим є захист інформації, що передається через цифрові канали. У цьому контексті важливо впровадити шифрування для всіх електронних комунікацій, що забезпечить захист від несанкціонованого доступу до електронної пошти та інших корпоративних систем. Також потрібно обмежити використання зовнішніх пристроїв для зберігання даних, таких як USB-флешки, а також встановити систему контролю доступу до комп'ютерних мереж і документів. Враховуючи зростаючу загрозу «мобільного шпигунства», слід вжити заходів для обмеження або блокування можливості прослуховування мобільних телефонів, наприклад, через використання генераторів шуму або радіоподавлення.

Для протидії цифровим загрозам, пов'язаним із витоком інформації через телефонні лінії, необхідно запровадити системи моніторингу і захисту, які дозволяють виявити несанкціоновані підключення до корпоративних телефонних мереж. Це дозволяє своєчасно реагувати на можливі спроби несанкціонованого доступу до конфіденційних переговорів і за допомогою сучасних технологій виявляти підслуховуючі пристрої.

Юридична складова є важливою складовою системи захисту від шпигунства. Кожна компанія повинна розробити внутрішні політики, що регулюють захист комерційної таємниці, підкріплені юридичними угодами, зокрема угодами про нерозголошення (NDA). У разі виявлення факту шпигунства або порушення інформаційної безпеки важливо мати чітко визначені кроки для реагування, що включають оперативне реагування служб безпеки, повідомлення правоохоронних органів і притягнення винних до відповідальності.

Постійний моніторинг і аудит усіх заходів безпеки також є важливими складовими ефективного захисту. Регулярні перевірки безпеки корпоративної інформаційної системи дозволяють виявити та усунути потенційні вразливості до того, як вони стануть об'єктом атаки.

Отже, ефективна протидія комерційному шпигунству вимагає системного підходу, що включає не тільки технічні, але й організаційні, кадрові та правові заходи. Важливо не лише запобігти технічним спробам витоку інформації, а й мінімізувати людські фактори, які можуть сприяти витоку через недбалість чи зловмисні дії співробітників. Комплексний захист включає розвиток корпоративної культури безпеки, чітку політику доступу до інформації, належне технічне забезпечення та активне використання правових інструментів для захисту від комерційного шпигунства.

ЛІТЕРАТУРА

1. Якубівська Ю. Є. Вплив промислового шпигунства на сферу інтелектуальної власності. *Зовнішня торгівля: право та економіка. Науковий журнал.* No 3(43) / 2013. К.: УДУФМТ, 2013. С. 158–162.

2. Базилевич В., Ільїн В. Інтелектуальна власність: креативи метафізичного пошуку : монографія. К.: Знання, 2008. 687с. (Серія "Київському національному університету імені Тараса Шевченка 175 років").

3. Радутний О. Е. Кримінальна відповідальність за незаконне збирання, використання та розголошення відомостей, що становлять комерційну таємницю (аналіз складів злочинів) : дис... канд. юрид. наук. Х., 2014. 204 с.

4. Ткачук Т. Ю. Сучасні реалії та загрози інформації з обмеженим доступом на підприємстві. *Право України.* 2011. No 3. С. 243–252.