SIDCON
CONSULTING COMPANY

КОРПОРАТИВНА БЕЗПЕКА

ДЛЯ ВЛАСНИКІВ БІЗНЕСУ В СУЧАСНИХ УМОВАХ

UKRAINE
INTERNATIONAL
CHAMBER OF COMMERCE
The world business organization

У *посібнику з позицій системного підходу розглядаються концептуальні положення, основні напрями та практичні рекомендації" щодо забезпечення корпоративної· безпеки в сучасних умовах. Розкрито сутність і сучасний стан інформаційної економічної· та корпоративної· безпеки Украї"ни. Проведено ідентифікацію загроз безпеці компаній і банків в умовах економічної· кризи та політичної· нестабільності. Показано шляхи забезпечення безпеки національних компаній у разі виходу на міжнародні ринки, запропоновано механізми й інструменти забезпечення сучасної· системи безпеки підприємництва.*

Особливе місце в посібнику посідають питання забезпечення безпеки компанії" (банку) на внутрішньому ринку Украї"ни на сучасному етапі.

Посібник розрахований на власників і менеджмент украї·нського бізнесу, на спеціалістів, які працюють у сфері підприємництва, займаються питаннями забезпечення економічної· безпеки підприємств, а також на викладачів, аспірантів, студентів економічних факультетів.

ЗМІСТ

1. ІДЕНТИФІКАЦІЯ СУЧАСНИХ ЗАГРОЗ БЕЗПЕЦІ КОМПАНІЙ І БАНКІВ В УМОВАХ ЕКОНОМІЧНОЇ ТА ПОЛІТИЧНОЇ НЕСТАБІЛЬНОСТІ В УКРАЇНІ

Ідентифікація загроз безпеці компаній і банків є початковим етапом системи заходів з управління ризиками. На сучасному етапі кожна компанія або банківська установа займається систематичним виявленням і класифікацією загроз, а також оцінюванням їх суттєвості. У результаті формується перелік значущих (істотних) загроз, для кожного банку або компанії він свій і залежить від багатьох факторів [3, с. 80]. Нижче ми систематизували сучасні загрози безпеці компаній і банків в Україні в умовах мінливого зовнішнього середовища та нестабільного розвитку національної економіки.

Важливість цього етапу управління пов'язана з тим, що ідентифікація дає змогу визначити вид або категорію загроз і можливість їх кількісної оцінки. У процесі ідентифікації також з'ясовують можливість впливу на ту чи іншу загрозу.

Пріоритетним завданням для кожного суб'єкта підприємництва стає побудова ефективної системи безпеки, яка зможе забезпечити сталий розвиток і захистить від можливих негативних факторів або мінімізує їх вплив на діяльність компанії (банку) [99].

1.1. Інформаційні загрози: крадіжки корпоративних даних, корпоративний шпіонаж, інсайдерська розвідка, зловживання доступом, витік ділової інформації

У 2016 р. американська компанія «Spiceworks» провела дослідження проблем безпеки серед користувачів розробленої нею програми аудиту мережі. Аналіз ситуації дав несподіваний результат: основну загрозу безпеці становлять самі користувачі всередині підприємства [103]. При чому ядро інсайдерської активності формується за рахунок елементарної необізнаності, низького порогу пильності внутрішніх користувачів і відсутності внутрішньої корпоративної культури захисту від загроз.

Те саме дослідження компанії «Spiceworks» показало ще кілька цікавих цифр щодо диверсифікації джерел загроз для інформаційної безпеки [103]:

- 36% – інсайдери;
- 25% – організовані угруповання зловмисників;
- 12% – терористичні угруповання;
- 12% – хакери.

Питома вага внутрішніх загроз прямо свідчить про те, що серйозні

зусилля потрібно спрямовувати на запобігання витоку конфіденційної інформації всередині компанії, на підвищення рівня свідомості й обізнаності співробітників, оскільки найчастіше інциденти відбуваються не навмисне, а через незнання та необережність.

Поряд із цим існує певне коло «внутрішніх» зловмисників, які діють під впливом цілком усвідомлених мотивів. У звіті про інсайдерські загрози у фінансовому секторі США (липень 2012 р.) наведені такі статистичні дані: 80% компрометувальних дій здійснено співробітниками на робочому місці в робочий час [103]; 81% із них планували саботаж заздалегідь; у більше ніж 80% випадків мотивом слугувала фінансова вигода, у 23% – зловмисниками рухало почуття помсти [103].

Інсайдерами можуть бути середньостатистичні співробітники компанії: бухгалтер, менеджер з продажу, маркетолог, офіс-менеджер тощо, тобто будь-який працівник зі штату, який має доступ до певної корпоративної інформації. Інсайдери можуть володіти паролями, тобто законним доступом до комп'ютерних систем, якими вони оперують у своїй щоденній роботі. Співробітники також часто мають прямий доступ до конфіденційної інформації компанії. Це спрощує завдання обходити захисні бар'єри й робить цінні для компанії активи уразливими.

Доступ до внутрішньої інформації означає, що у співробітників немає необхідності незаконно проникати в мережу крізь зовнішній периметр, вони вже й так перебувають у системі.

Загрозу також можуть становити програми, навмисно встановлені на комп'ютерах співробітниками, яких звільнили.

Так, звільнені співробітники нерідко можуть становити для компанії загрозу більш серйозну, ніж хакери. При тому що це можуть бути як звільнені, так і працівники, які пішли за власним бажанням, у яких залишилися претензії до роботодавця або осад від минулих конфліктів.

Фахівці з інформаційної безпеки констатують, що неуважність компаній до закриття облікових записів та обмеження доступу для колишніх співробітників – це справжня кіберзагроза, іноді навіть більш згубна, ніж втручання сторонніх осіб.

Агентство «Osterman Research» провело опитування в США й Канаді, яке показало, що 89% звільнених співробітників підприємств малого та середнього бізнесу зберігають доступ до корпоративних веб-додатків та електронної пошти. Кількість тих, хто вважає, що це дало б їм змогу отримувати конфіденційну інформацію про роботу компанії, – 45% [104]. Стільки ж зізналося, що й після звільнення іноді користувалися своїм корпоративним обліковим записом, а 68% переносили робочі файли в приватне «хмарне»

сховище за межами контролю корпоративної IT-служби [104], іноді для забезпечення конкурентної переваги в новій компанії. Ці цифри – вагомий аргумент серйозно замислитися власнику бізнесу про інформаційну безпеку та не ігнорувати заходи безпеки щодо колишніх працівників.

У багатьох із цих ситуацій крадіжка конфіденційної інформації стала можливою завдяки використанню доступу до «хмарних» сховищ та особистих облікових записів електронної пошти. Частина інцидентів виникла, коли колишні співробітники намагалися вимагати у свого роботодавця гроші, щоб скасувати зміни або обмеження доступу до веб-сайтів компанії [104]. Змінивши декілька паролів або ж «підправивши» деякі настройки, вони отримали козир, який дав можливість і помститися, і заробити [104].

Аналогічна ситуація спостерігається й у Росії: компанії «ESET» і «FutureToday» провели дослідження, яке також показало сумну картину щодо корпоративних інформаційних ризиків. 17% опитаних співробітників компаній зізналися, що їм доводилося знищувати цінні документи, листування або програмне забезпечення, щоб нашкодити колишньому роботодавцеві. 13% опитаних забирали із собою бази клієнтів, плани, звіти й інші дані для подальшого продажу або використання на новому місці роботи [104]. Близько 4% співробітників після звільнення користувалися недоробками IT-фахівців колишньої компанії, зокрема заходили на робочу пошту або продовжували віддалено відвідувати корпоративні ресурси [104]. Ще 4% респондентів публікували корпоративну інформацію (від фінансових документів до особистих даних керівництва) в Інтернеті.

Ці інциденти інформаційної безпеки можуть коштувати компаніям тисячі й навіть мільйони доларів, залежно від їх масштабів. Під час останніх досліджень ФБР дійшло невтішних висновків: компанії втрачають від $ 5000 до $ 3 000 000 у зв'язку з інцидентами, пов'язаними з втручанням у роботу незадоволених співробітників [104]. Серед головних складових втрат – вартість украдених даних, витрати з відновлення інформаційної безпеки, створення контрзаходів, на юридичні послуги, а також втрати доходів і/або клієнтів.

Щоб сформувати дієву систему захисту в бізнес-структурі, необхідно класифікувати загрози, які надходять від інсайдерів, у зв'язку з чим нижче наведемо кілька класичних сценаріїв інсайдерських загроз [103].

1.1.1. Незаконне розголошення

У результаті незаконного розголошення, іншими словами, витоку, конфіденційні відомості залишають внутрішній периметр і потрапляють до рук осіб, які не мають прав на їх використання. Наприклад, це можуть бути база даних клієнтів, інформація про контрагентів, інтелектуальна власність.