



SIDCON
CONSULTING COMPANY



КОРПОРАТИВНА БЕЗПЕКА

**ДЛЯ ВЛАСНИКІВ БІЗНЕСУ
В СУЧАСНИХ УМОВАХ**

18C

UKRAINE
INTERNATIONAL
CHAMBER OF COMMERCE

Купити книгу на сайті kniga.biz.ua >>>

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 України. 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 підприємства.

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

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



[Купити книгу на сайті kniga.biz.ua >>>](http://kniga.biz.ua)



ЗМІСТ

ПЕРЕДМОВА.....	3
ВСТУП. ХТО МАЄ ВІДПОВІДАТИ ЗА КОРПОРАТИВНУ СИСТЕМУ БЕЗПЕКИ В КОМПАНІЇ (БАНКУ).....	12
1. ІДЕНТИФІКАЦІЯ СУЧАСНИХ ЗАГРОЗ БЕЗПЕЦІ КОМПАНІЙ І БАНКІВ В УМОВАХ ЕКОНОМІЧНОЇ ТА ПОЛІТИЧНОЇ НЕСТАБІЛЬНОСТІ В УКРАЇНІ.....	18
1.1. Інформаційні загрози: крадіжки корпоративних даних, корпоративний шпionaж, інсайдерська розвідка, зловживання доступом, витік ділової інформації.....	18
1.2. Сучасні тенденції реалізації корпоративних загроз шляхом web-атак, можливостей кібертероризму та кібершпionaжу.....	26
1.3. Цілеспрямований підрив ділової репутації для дискредитації бізнес-структури. інформаційні (корпоративні) війни, інформаційний тероризм (медіа-тероризм) та інші недобросовісні методи, що застосовуються в інформаційному конкурентному протистоянні.....	36
1.4. Загрози тероризму як фактор необхідності формування нових підходів до безпеки суб'єктів підприємництва.....	42
1.5. Конкурентна розвідка, у тому числі здійснена через функціонуючі в Україні міжнародні неурядові організації.....	46
1.6. Кримінальні посягання (загальнокримінальна злочинність і насильство проти бізнесу). Рейдерство.....	50
1.7. Політичні ризики, тиск на бізнес.....	58
1.8. Корупція в органах державної влади та управління.....	62
1.9. Ризики криптовалют.....	67
2. ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМПАНІЇ (БАНКУ) НА ВНУТРІШНЬОМУ РИНКУ УКРАЇНИ НА СУЧАСНОМУ ЕТАПІ.....	70
2.1. Основні тенденції та проблеми становлення й розвитку системи безпеки підприємництва в Україні. Співвідношення безпеки підприємництва з національною безпекою держави.....	70

2.2. Система безпеки підприємництва в Україні: проблемні питання її забезпечення на законодавчому рівні.....	74
2.3. Суперечності антикорупційного законодавства та недовість створених державних спеціально уповноважених суб'єктів протидії корупції.....	78
2.4. Недоліки чинної моделі судової та правоохоронної системи в контексті неефективності захисту бізнесу від протиправних (неправомірних) посягань.....	86
2.5. Безпека договірних відносин в Україні в забезпеченні безпеки діяльності суб'єкта підприємництва.....	98
2.6. Стан забезпечення безпеки й ризику інвестиційної діяльності в умовах економічної нестабільності в Україні.....	102
2.7. Проблеми забезпечення безпеки агропромислових компаній в Україні – аграрне рейдерство: підгрунття й наслідки.....	112

3. ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМПАНІЙ ПІД ЧАС ВИХОДУ НА МІЖНАРОДНІ РИНКИ.....122

3.1. Основні ризики безпеки зовнішньоекономічного співробітництва українських компаній на міжнародних ринках.....	122
3.2. Основні джерела ризиків під час виконання зовнішньоторговельних контрактів.....	124
3.3. Захист інтересів вітчизняних товаровиробників на зовнішніх ринках. Інструменти торговельного захисту (антидемпінгові, компенсаційні й захисні заходи).....	126
3.4. Основні положення міжнародних стандартів ISO щодо забезпечення безпеки й ризик-менеджменту компаній. Пріоритети розвитку системи безпеки та ризик-менеджменту підприємництва України в контексті сучасної міжнародної практики.....	129
3.5. Європейські й міжнародні стандарти у сфері судочинства.....	136
3.6. Механізм врегулювання суперечок у рамках Світової організації торгівлі.....	140
3.7. Роль Інтерполу й міжнародних торговельно-промислових палат (ICC) у забезпеченні безпеки підприємництва.....	147
3.8. Інституції Євросоюзу й НАТО з питань забезпечення безпеки бізнесу. Перспектива створення в Україні за підтримки НАТО єдиного центру з кібербезпеки.....	154

4. АУДИТ ІСНУЮЧОЇ СИСТЕМИ БЕЗПЕКИ В КОМПАНІЯХ (БАНКАХ).....161

4.1. Обґрунтування необхідності проведення аудиту корпоративної системи безпеки бізнесу.....	161
4.2. Чинники (індикатори), які свідчать про послаблення безпеки в компаніях (банках).....	164
4.3. Напрями проведення аудиту системи безпеки в компаніях (банках) на відповідність вимогам нормативно-правових актів України та міжнародним стандартам з безпеки.....	169
4.4. Аналіз існуючої політики ризик-менеджменту й корпоративної безпеки в компаніях (банках).....	171
4.5. Взаємозв'язок системи ризик-менеджменту, корпоративної безпеки й корпоративного управління в компаніях (банках).....	176
4.6. За що має нести відповідальність служба безпеки компанії (банку)?.....	183

5. НАПРЯМИ Й ІНСТРУМЕНТИ СТВОРЕННЯ ЕФЕКТИВНОЇ СИСТЕМИ БЕЗПЕКИ ПІДПРИЄМНИЦТВА.....189

5.1. Напрями забезпечення й основні складові системи безпеки в компаніях (банках).....	189
5.2. Створення приватних моделей загроз безпеці бізнесу.....	193
5.3. Необхідність створення інформаційно-аналітичних центрів і систем підтримки прийняття рішень.....	195
5.4. Бізнес-розвідка в системі забезпечення безпеки суб'єктів підприємництва.....	200
5.5. Завдання щодо досягнення надійної системи безпеки компанії (банку), яка б відповідала міжнародним стандартам безпеки й управління ризиками. Головні заходи щодо забезпечення ефективності системи безпеки та захисту корпоративних даних у компанії (банку).....	207
5.6. Аутсорсинг окремих питань безпеки у сфері організації захисту підприємництва й бізнесу. Хто має займатися питаннями організації забезпечення безпеки в компаніях (банках) і підготовкою кадрів для їхніх служб безпеки?.....	209
5.7. Доцільність розроблення корпоративного стандарту	

й концепції безпеки компаній (банків) з позицій системного підходу та ризик-менеджменту.....	214
5.8. Розроблення пакета документів для впровадження та подальшого функціонування комплексної системи управління безпекою й ризиками суб'єкта підприємництва.....	218
ВИСНОВКИ.....	223
ТЕРМІНИ, ЩО ЗАСТОСОВУЮТЬСЯ У СФЕРІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ БІЗНЕСУ.....	227
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	235
СПИСОК НОРМАТИВНО-ПРАВОВИХ АКТІВ З ПИТАНЬ БЕЗПЕКИ Й РИЗИК-МЕНЕДЖМЕНТУ КОМПАНІЙ (БАНКІВ).....	246
ДОДАТКИ.....	251



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 захистити від можливих негативних факторів або мінімізує їх вплив на діяльність компанії (банку) [99].

1.1. Інформаційні загрози: крадіжки корпоративних даних, корпоративний шпionаж, 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 неухважність 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 ІТ-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]. Змінюючи 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 компанії 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 ІТ-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 невтїшних 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 сформувавши 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.