Ю. І. Когут

КОРПОРАТИВНА БЕЗПЕКА

Київ
Консалтингова компанія «СІДКОН»
2021

УДК 351.746.1+004.946.5.056
К57

Рецензент:

Гордієнко Сергій Георгійович, завідувач кафедри національної безпеки навчально-наукового інституту права ім. князя Володимира Великого МАУП, доктор юридичних наук, доцент.

Когут Ю. І.

К57 Корпоративна безпека: практичний посібник / Ю. І. Когут. – Київ : Консалтингова компанія «СІДКОН», 2021. – 460 с.

ISBN 978-966-97546-8-4

Практичний посібник підготовлений експертом з 20-ти річним стажем практики в сфері кібербезпеки та корпоративної безпеки бізнесу. У посібнику особливу увагу приділено практичним питанням кібербезпеки, корпоративної безпеки, в т.ч. безпеки цифрової економіки.

У посібнику розглядаються теоретико-прикладні проблеми й питання: управління сферою національної безпеки України; державної безпеки; воєнної безпеки; економічної безпеки; гуманітарної та екологічної безпеки; захисту державної таємниці; забезпечення безпеки суб'єктів підприємницької діяльності; інформаційної сфери і права на інформацію; інноваційної діяльності та її правових аспектів; інтелектуальної власності та права на її об'єкти.

Наведена і проаналізована теорія та практика їх «життєздатності» і захисту в умовах сьогодення України.

Даний посібник орієнтований на практиків – власників бізнесу і працівників зазначених сфер життєдіяльності суспільства, а також студентів, аспірантів, докторантів, наукових і науково-педагогічних працівників і курсантів вищих навчальних закладів, що навчаються за спеціальностями 6.050100 «Маркетинг», «Менеджмент», та інших економічних спеціальностей, а також 12.125 «Кібербезпека».

УДК 351.746.1+004.946.5.056

ISBN 978-966-97546-8-4

ЗМІСТ

РОЗДІЛ І. КОРПОРАТИВНА БЕЗПЕКА ДЛЯ ВЛАСНИКІВ БІЗНЕСУ В СУЧАСНИХ УМОВАХ 14

ВСТУП ДО РОЗДІЛУ І 14

1. ІДЕНТИФІКАЦІЯ СУЧАСНИХ ЗАГРОЗ БЕЗПЕЦІ КОМПАНІЙ ТА БАНКІВ В УМОВАХ ЕКОНОМІЧНОЇ ТА ПОЛІТИЧНОЇ НЕСТАБІЛЬНОСТІ В УКРАЇНІ 21

1.1. Інформаційні загрози: крадіжки корпоративних даних, корпоративний шпіонаж, інсайдерська розвідка, зловживання доступом, витік ділової інформації 22
1.1.1. Незаконне розголошення 25
1.1.2. Необережність 26
1.1.3. Шахрайство і порушення авторських прав 26
1.2. Сучасні тенденції реалізації корпоративних загроз шляхом Web-атак, можливостей кібертероризму та кібершпіонажу 33
1.3. Цілеспрямований підрив ділової репутації для дискредитації бізнес-структури. Інформаційні (корпоративні) війни, інформаційний тероризм (медіа-тероризм) та інші недобросовісні методи, що застосовуються у інформаційному конкурентному протистоянні 46
1.4. Загрози тероризму як фактор необхідності формування нових підходів щодо безпеки суб'єктів підприємництва 55
1.5. Конкурентна розвідка, у тому числі здійснена через функціонуючі в Україні міжнародні неурядові організації 61

1.6. Кримінальні посягання (загальнокримінальна злочинність та насильство проти бізнесу). Рейдерство 67
1.7. Політичні ризики, тиск на бізнес 77
1.8. Корупція в органах державної влади та управління 84
1.9. Ризики криптовалют 90

2. ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМПАНІЇ (БАНКУ) НА ВНУТРІШНЬОМУ РИНКУ УКРАЇНИ НА СУЧАСНОМУ ЕТАПІ 94
2.1. Основні тенденції та проблеми становлення і розвитку системи безпеки підприємництва в Україні. Співвідношення безпеки підприємництва з національною безпекою держави 94
2.2. Система безпеки підприємництва в Україні: проблемні питання її забезпечення на законодавчому рівні 99
2.3. Суперечності антикорупційного законодавства та недієвість створених державних спеціально уповноважених суб'єктів протидії корупції 105
2.4. Недоліки існуючої моделі судової та правоохоронної системи у контексті неефективності захисту бізнесу від протиправних (неправомірних) посягань 116
2.5. Безпека договірних відносин в Україні у забезпеченні безпеки діяльності суб'єкта підприємництва 132
2.6. Стан забезпечення безпеки та ризики інвестиційної діяльності в умовах економічної нестабільності в Україні 136
2.7. Проблеми забезпечення безпеки агропромислових компаній в Україні – аграрне рейдерство: підгрунття та наслідки 149

3. ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМПАНІЇ ПРИ ВИХОДІ НА МІЖНАРОДНІ РИНКИ 163

3.1. Основні ризики безпеки зовнішньоекономічного співробітництва українських компаній на міжнародних ринках 163

3.2. Основні джерела ризиків при виконанні зовнішньоторговельних контрактів 165
3.3. Захист інтересів вітчизняних товаровиробників на зовнішніх ринках. Інструменти торговельного захисту (антидемпінгові, компенсаційні та захисні заходи) 169
3.4. Основні положення міжнародних стандартів ISO щодо забезпечення безпеки та ризик-менеджменту компаній. Пріоритети розвитку системи безпеки та ризик-менеджменту підприємництва України в контексті сучасної міжнародної практики 173
3.5. Європейські та міжнародні стандарти у сфері судочинства 181
3.6. Механізм врегулювання суперечок у рамках Світової Організації Торгівлі 187
3.7. Роль Інтерполу та міжнародних торговельно-промислових палат (ICC) в забезпеченні безпеки підприємництва 196
3.8. Інституції Євросоюзу та НАТО з питань забезпечення безпеки бізнесу. Перспектива створення в Україні за підтримки НАТО єдиного центру з кібербезпеки 205

4. АУДИТ ІСНУЮЧОЇ СИСТЕМИ БЕЗПЕКИ В КОМПАНІЯХ (БАНКАХ) 214

4.1. Обґрунтування необхідності проведення аудиту корпоративної системи безпеки бізнесу 214
4.2. Чинники (індикатори), які свідчать про послаблення безпеки в компаніях (банках) 218
4.3. Напрямки проведення аудиту системи безпеки в компаніях (банках) на відповідність вимогам нормативно-правових актів України та міжнародним стандартам з безпеки 225
4.4. Аналіз існуючої політики ризик-менеджменту та корпоративної безпеки у компаніях (банках) 227
4.5. Взаємозв`язок системи ризик-менеджменту, корпоративної безпеки та корпоративного управління в компаніях (банках) .. 233

4.6. За що має нести відповідальність служба безпеки компанії (банку)? 242

5. НАПРЯМКИ ТА ІНСТРУМЕНТИ СТВОРЕННЯ ЕФЕКТИВНОЇ СИСТЕМИ БЕЗПЕКИ ПІДПРИЄМНИЦТВА 250

5.1. Напрями забезпечення та основні складові системи безпеки в компаніях (банках) 250
5.2. Створення приватних моделей загроз безпеці бізнесу 255
5.3. Необхідність створення інформаційно-аналітичних центрів та систем підтримки прийняття рішень 258
5.4. Бізнес-розвідка в системі забезпечення безпеки суб'єктів підприємництва 264
5.5. Завдання щодо досягнення надійної системи безпеки компанії (банку), яка б відповідала міжнародним стандартам безпеки та управління ризиками. Головні заходи щодо забезпечення ефективності системи безпеки та захисту корпоративних даних в компанії (банку) 273
5.6. Аутсорсинг окремих питань безпеки у сфері організації захисту підприємництва та бізнесу. Хто має займатися питаннями організації забезпечення безпеки в компаніях (банках) та підготовкою кадрів для їх служб безпеки? 276
5.7. Доцільність розробки корпоративного стандарту та концепції безпеки компаній (банків) з позицій системного підходу та ризик-менеджменту 282
5.8. Розробка пакету документів для впровадження та подальшого функціонування комплексної системи управління безпекою та ризиками суб'єкта підприємництва 287

ВИСНОВКИ ДО РОЗДІЛУ І 293

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ДО РОЗДІЛУ І 298

РОЗДІЛ ІІ. КІБЕРБЕЗПЕКА ЦИФРОВОЇ ЕКОНОМІКИ ДЛЯ ВЛАСНИКІВ БІЗНЕСУ 308

ВСТУП ДО РОЗДІЛУ ІІ 308

1. СТАНОВЛЕННЯ І РОЗВИТОК ЦИФРОВОЇ ЕКОНОМІКИ У СВІТІ ТА В УКРАЇНІ 311

1.1. Що таке цифрова економіка? Ключові фактори, які впливають на її розвиток 311

1.2. Роль держави (державних інституцій, органів влади та управління) у розвитку цифрової економіки, формуванні її основних трендів та забезпеченні безпеки 321

1.3. Глобальні наслідки зростання впливу цифрових платформ у світі 328

2. МОЖЛИВОСТІ ТА РИЗИКИ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ЦИФРОВОЇ ЕКОНОМІКИ В БІЗНЕСІ 347

2.1. Загрози кібербезпеці в умовах розвитку цифрової економіки для держави, суспільства, бізнесу та особистості 347

2.2. Основні напрямки та ризики використання цифрових технологій у сучасній економіці та суспільстві 354

2.2.1. Електронна комерція 354

2.2.2. Блокчейн. Токенізація активів у блокчейні. Смарт-контракти 360

2.2.3. Створення державних реєстрів, систем електронних ідентифікаційних документів, державних електронних послуг. Можливість розроблення глобальної мобільної платформи «Електронна Україна» 371

2.2.4. Електронні гроші, цифрова валюта (криптовалюта). Bitcoin-ф'ючерси 376

2.2.5. Технології Інтернету речей. Промисловий Інтернет, нові виробничі технології, комп'ютерний інжиніринг 388

2.2.6. Сучасні технології бездротового зв'язку 394

2.2.7. Стартапи у сфері цифрової економіки. Поширення нових бізнес-моделей в умовах використання передових цифрових технологій 399
2.3. Вимоги до компетенції кадрів компаній щодо забезпечення корпоративної кібербезпеки в умовах розвитку цифрової економіки 402

3. ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В КОМПАНІЯХ В УМОВАХ ФОРМУВАННЯ ЦИФРОВОЇ ЕКОНОМІКИ 409
3.1. Необхідні умови для впровадження системи кібербезпеки в компаніях 409
3.2. Основні заходи щодо організації ефективної системи кібербезпеки в компаніях у сучасних умовах розвитку цифрової економіки 411
3.3. Управління інцидентами кібербезпеки в компаніях 417

ВИСНОВОК ДО РОЗДІЛУ II 420

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ДО РОЗДІЛУ II 423

СПИСОК НОРМАТИВНО-ПРАВОВИХ АКТІВ З ПИТАНЬ БЕЗПЕКИ ТА РИЗИК-МЕНЕДЖМЕНТУ КОМПАНІЙ (БАНКІВ) 431

ТЕРМІНИ, ЩО ЗАСТОСОВУЮТЬСЯ У СФЕРІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ БІЗНЕСУ 436

ДОДАТКИ 443