



International Chamber of Commerce
The world business organization

Інтелектуальна Власність: Рекомендації для бізнесу



За сприяння
Комісії з інтелектуальної власності ICC

An ICC initiative
BASCAP
Business Action to Stop
Counterfeiting and Piracy

Робота ICC спрямована на розвиток гармонійної і стійкої системи для захисту інтелектуальної власності, яка, на думку ICC, покликана підтримувати інновації та розвиток наукомістких галузей, сприяє міжнародній торгівлі і формує сприятливий клімат для прямих іноземних інвестицій і трансферу технологій. Ця публікація є результатом спільних зусиль Комісії ICC з інтелектуальної власності та Ініціативи ICC BASCAP – Бізнес проти контрафакції та піратства.

Про Комісію з інтелектуальної власності ICC

Позиція ICC з питань інтелектуальної власності формується Комісією з інтелектуальної власності ICC, яка об'єднує більше 300 представників бізнес-структур і приватних експертів з 50 країн. Комісія з інтелектуальної власності ICC представляє точку зору міжнародного бізнесу в ході урядових і міждержавних дебатів з ключових питань інтелектуальної власності, з якими стикається бізнес-спільнота. Також Комісія працює в напрямку підвищення інформованості суспільства в галузі інтелектуальної власності через такі ініціативи як щорічний випуск огляду актуальних питань інтелектуальної власності та інших публікацій. *Детальніше про Комісію: <http://www.iccwbo.org/policy/ip/id3060/index.html>*

Про BASCAP

Контрафакція та піратство перетворилися на справжню глобальну епідемію, завдаючи суттєвої шкоди бізнесу і глобальній економіці, ставлячи під загрозу інвестиції в інновації та творчість, девальвуючи визнані бренди і створюючи ризики для здоров'я і безпеки споживачів. Широке розповсюдження цієї проблеми підриває основи економічного розвитку, стійкої системи економіки, вільної торгівлі та інвестицій. Ініціатива ICC - Бізнес в боротьбі з контрафактом і піратством (BASCAP) – стала відповіддю на цей виклик і має на меті об'єднати зусилля бізнесу з різних країн, що представляє різні галузі і сектори, в їх боротьбі проти контрафакту та піратства; зміцнити голос бізнесу і донести його думку і погляди до урядів, широкої громадськості та засобів масової інформації, підвищуючи обізнаність і розуміння природи контрафактної та піратської діяльності і пов'язаної з нею економічної і соціальної шкоди; закликати держави вжити заходів і виділити ресурси для реалізації прав інтелектуальної власності; сприяти культурній трансформації та формуванню суспільного визнання і поваги прав інтелектуальної власності. *Детальніше про BASCAP: www.iccwbo.org/bascap*

Міжнародна торгова палата – Всесвітня організація бізнесу (ICC) і її український національний комітет (ICC Ukraine) дякують за переклад цієї публікації на українську мову фірмі *Due Diligence & Intelligence Intellectual Property Agency* (www.ddiip.com)



Due Diligence & Intelligence Intellectual Property Agency

DD&I IP Agency – перше в Україні спеціалізоване агентство з питань IP Due Diligence, IP Intelligence, управління та комерціалізації об'єктів інтелектуальної власності

DD&I IP Agency здійснює систематичний огляд та аналіз об'єктів права інтелектуальної власності, метою якого є оцінка потенційних ризиків і переваг компанії, пов'язаних з використанням об'єктів права інтелектуальної власності, та розробляє стратегії управління такими ризиками і перевагами.

Передмова	2
Загальні принципи	3
Вступ та рекомендації	5
Цілі.....	6
Політика компанії.....	6
Освіта	9
Поставка, виробництво та продаж.....	10
Безпека та конфіденційність.....	14
Дотримання законодавства та аудит	16
Питання, які часто виникають (FAQs)	18
Як я можу взяти участь у програмі	20
Додаток 1	21
Рекомендації Великої Вісімки (G8) для органів державної влади щодо використання програмного забезпечення з дотриманням прав інтелектуальної власності	
Вступ	21
Декларації та Рекомендації Великої Вісімки	22
1. Правила з використання програмного забезпечення	22
2. Безпека	23
3. Навчання	24
4. Співпраця з правласниками.....	25
5. Джерела: Витяги з доповідей і декларацій Великої Вісімки	25
Додаток 2:	28
Як уникнути контрафакту при державному замовленні	
Вступ	28
Проблема контрафакції при державному замовленні	29
Електронні продукти та компоненти	29
Придбання і використання програмного забезпечення.....	30
Продукція оборонного призначення, засоби забезпечення безпеки та комплектуючі	30
Медикаменти та медичне устаткування.....	31
Боротьба з контрафактом при державних закупівлях	32
1. Державна політика	32
2. Навчання	33
3. Управління каналом поставок.....	34
4. Управління активами та безпека.....	34
5. Дотримання вимог законодавства та аудит	35
Джерела.....	36

Важливість інтелектуальної власності (ІВ) для компаній, економік окремих країн та суспільства в цілому надзвичайно зросла. Авторські права, торговельні марки та інші форми ІВ необхідні для сприяння компаніям у їх розвитку та отриманню ними заслужених винагород за власні інновації, рекламу та творчість. Більше того, компанії по всьому світу все частіше використовують чужу ІВ в своїй повсякденній роботі, як у виробництві товарів та послуг, так і в управлінні власною діяльністю.

Ініціативою Міжнародної Торгової Палати (ІСС) – «Бізнес проти контрафакції та піратства» («Business Action to Stop Counterfeiting and Piracy» («BASCAP»)) був розроблений цей збірник Рекомендацій з ІВ, аби допомогти компаніям та іншим організаціям управляти інтелектуальною власністю, яку вони створили, та ІВ інших осіб, яку вони використовують у своїй діяльності. Засновані на практиці багатьох галузей економіки, дані Рекомендації надають інформацію про практичні кроки, які можна зробити для оцінки ефективності управління ІВ компанії, особливо в сфері авторського права та торговельних марок. Вони можуть допомогти більш ефективно захистити власну ІВ компанії, надати нові можливості для покращення продуктивності та навчитись управляти ризиками, пов'язаними з контрафакцією та піратством.

Рекомендації адресовані керівникам різноманітних практик компанії, пов'язаних з ІВ, від створення об'єктів ІВ до практик, пов'язаних з пошуком комплектуючих, виробництвом, оптовим та роздрібним продажем та внутрішнім корпоративним використанням. Це включає методику організації системи постачання, відносини з посередниками та користування ІВ третіх осіб. В основній частині Рекомендацій описані узагальнені корисні напрацювання із конкретними прикладами та рекомендаціями. У Додатках містяться більш докладні поради щодо конкретних типів ІВ та видів діяльності.

Цілі ICC/BASCAP пропонує наступні Рекомендації для допомоги бізнесу:

- розуміти та підтримувати цінність ІВ як основу інноваційної, творчої та економічної діяльності, що сприяє конкурентоспроможності бізнесу та нації;
- управляти своїми власними авторськими правами та правами на торговельні марки більш ефективно;
- дотримуватися законів в області ІВ, які захищають авторські права і права на торговельні марки інших компаній;
- управляти бізнес-ризиками, пов'язаними з порушеннями прав ІВ;
- попереджати та стримувати контрафакцію та піратство і
- розробити відповідні правила і здійснити практичні заходи для досягнення перерахованих вище цілей.

Політика компанії

1. **Корпоративна політика.** Створити корпоративні правила для ведення бізнесу відповідно до законів про ІВ і світової практики. Впровадити конкретні правила, методи та практики з метою сприяння дотриманню законності.
2. **Правомірне використання.** Набувати і використовувати у своїй діяльності тільки ліцензовані копії матеріалів, захищені авторськими правами і справжні вироби, які охороняються торговельними марками.
3. **Захист ІВ компанії.** Вживати необхідні заходи для виявлення та захисту власних об'єктів права інтелектуальної власності (ОПІВ) компанії.
4. **Додержання вимог законодавства.** Призначити директора або менеджера, який буде визначати та впроваджувати політику компанії щодо ІВ.

Освіта

5. **Політика щодо співробітників.** Запровадити правила щодо додержання законів у сфері ІВ та політики компанії щодо ІВ та довести їх до відома працівників.
6. **Навчання та підвищення інформованості.** Ознайомити працівників та субпідрядників (коли це необхідно) з політикою компанії щодо додержання законів у сфері ІВ.

Поставка, виробництво та продаж

7. **Попередження постачальників та клієнтів.** Повідомляти постачальників та клієнтів, що компанія дотримується законодавства в сфері ІВ і очікує від них того ж.
8. **Законні ресурси.** По можливості, використовувати для свого бізнесу ресурси, пов'язані з ІВ, отримані від легальних та перевірених постачальників.
9. **Умови контрактів.** Вести наскільки можливо детально документацію про ключові операції з об'єктами інтелектуальної власності, а також про відносини з покупцями і постачальниками.

10. **Обізнаність про клієнтів та постачальників.** Перевіряти інформацію про постачальників та покупців товарів і послуг, заснованих на об'єктах ІВ.
11. **Необхідні ліцензії.** Отримувати письмові докази підтвердження майнових прав ІВ та необхідних ліцензій до початку виробництва, поставки чи пропонування товарів та послуг, заснованих на об'єктах ІВ.
12. **Юридичний аудит.** Аналізувати документацію та супутні відомості про наявність ознак порушення прав ІВ при замовленні та поставці товарів. За необхідності, збирати додаткову інформацію для перевірки діяльності, що викликає підозри.

Безпека та конфіденційність

13. **Фізична та інформаційна безпека.** Підтримувати фізичну та інформаційну (ІТ) безпеку на достатньому рівні, щоб забезпечити недоторканність архівів і виробничих процесів компанії, а також захистити інтелектуальну власність і конфіденційні відомості.
14. **Управління активами.** Впровадити процедури з виявлення, обліку і контролю інтелектуальних активів, щоб гарантувати можливість їх аналізу та управління ними.
15. **Захист комерційної таємниці та конфіденційної інформації.** Докладати максимальних зусиль для захисту комерційної таємниці та конфіденційної інформації компанії і третіх осіб.
16. **Технічні анти-піратські заходи.** Поважати, не втручатися і підтримувати безпеку технічних анти-піратських заходів, які використовуються правовласниками для захисту їх продукції та послуг, заснованих на об'єктах ІВ.

Дотримання законодавства та аудит

17. **Облік.** Зберігати основні матеріали, що стосуються інтелектуальної власності, протягом відповідного терміну.
18. **Маркування.** Маркувати всю продукцію та упаковку, яка має відношення до ІВ, що виробляється або поставляється.
19. **Моніторинг.** Періодично переглядати правила компанії в сфері ІВ.
20. **Зразки.** Надавати правовласникам, їх підприємствам, які борються з піратством, правоохоронним органам на їх прохання зразки продукції, створеної з використанням ІВ, яка виробляється компанією.
21. **Співпраця з правовласниками та органами державної влади.** Надавати допомогу правовласникам, підприємницьким та анти-піратським організаціям, правоохоронним органам при розслідуваннях можливих порушень права ІВ.

Вступ

Зростаюча проблема контрафакції та піратства створює багато ризиків для бізнесу.

Піратство та контрафакція пов'язані з порушенням авторських прав та прав на торговельну марку, які іменуються в цих Рекомендаціях «інтелектуальною власністю» або «ІВ».

Для того, щоб допомогти компаніям краще управляти ІВ, ICC/BASCAP виробило ряд Рекомендацій з інтелектуальної власності. Рекомендації надають підприємцям інформацію про практичні заходи з оцінки ефективності методів роботи з об'єктами ІВ, захистити їх власну ІВ та віднайти нові можливості покращення продуктивності та управління ризиками, пов'язаними з контрафакцією та піратством.

Великі та малі компанії практично в усіх сегментах економіки все частіше використовують та покладаються на ІВ – авторське право, торговельні марки, комерційні таємниці та інші нематеріальні блага, які лежать в основі багатьох товарів та послуг. Для будь-якої підприємницької діяльності необхідна ІВ: наприклад, у випуску фірмових товарів чи їх складових під фірмовим брендом, використанні захищеного авторським правом програмного забезпечення, відео та аудіо, фото, книгах, інформаційних послугах, або у торговельних марках своєї компанії або інших осіб.

В результаті, компанії частіше відчують необхідність введення правил і процедур для управління своєю ІВ і попередження неправомірного використання чужої.

В сучасній економіці «інтелектуальний капітал», втілений в креативному потенціалі компанії, може бути таким же важливим для зростання економіки, як і традиційний капітал, товари та послуги. Захист ІВ допомагає отримати дохід від інвестицій в інтелектуальний капітал, необхідних для вироблення нескінченного потоку нових інновацій та винаходів. Це робить приватні компанії, підприємницький сектор та національну економіку більш конкурентоздатною, живить культурний, технологічний, соціальний та економічний розвиток та створює умови для загального покращення здоров'я та життя .

Об'єм ІВ, з якою компанії мають справу, зростає. Неправильне управління своєю ІВ може призвести до втрати ринкових можливостей та витіснення легальних товарів контрафактом. Неправильне поводження з чужими матеріалами, які охороняються торговельними марками або авторськими правами, може призвести до цивільних або кримінальних правопорушень, виплат великих компенсацій, а також шкоди і перешкод для ведення бізнесу.

На додаток до цього, існує великий підприємницький та соціальний ризик неправильного управління ІВ, такий, як ушкодження здоров'я та інші збитки від контрафактних автозапчастин, продуктів споживання, чи фармацевтичних препаратів.

Рекомендації з ІВ надають корисну допомогу широкому колу підприємств різних секторів економіки, можуть допомогти оцінці ефективності їх правил управління ІВ.

ICC/BASCAP визнає, що правила та вимоги до управління ІВ відрізняються у різних галузях, не існує єдиної найкращої практики для всіх сфер бізнесу. Проте, є цінні уроки, які надають компанії в різних галузях, з яких підприємства різних видів діяльності зможуть взяти для себе щось корисне. Деякі з прикладів, зібрані в Рекомендаціях можуть підказати корисні ідеї, які можуть бути втілені в різних сферах або ланок в ланцюзі поставок.

Вони можуть використовуватися як керівництво для компанії, наприклад, для вироблення внутрішніх корпоративних правил або інструкцій для працівників. Положення цих Рекомендацій можуть бути включеними до договорів між правовласниками та постачальниками матеріалів, такими як заводи-виробники.

В окремих сегментах промисловості Рекомендації також підходять для прийняття за основу при проведенні процедур підтвердження відповідності або створення галузевих кодексів поведінки добровільної, чи примусової.

Рекомендації повинні стати «живим документом», який буде змінюватися відповідно до нових технологій та напрацювань різних галузей. Як і система ІВ в цілому, Рекомендації є демонстрацією поваги до інтересів правовласників, бізнесу та суспільства в цілому.

Цілі

ICC/BASCAP пропонує наступні Рекомендації для допомоги діловому співтовариству:

- розуміти та підтримувати цінність ІВ як основу інноваційної, творчої та економічної діяльності, що сприяє конкурентоспроможності бізнесу та національної конкурентоспроможності;
- управляти своїми авторськими правами та торговельними марками більш ефективно;
- дотримуватися законів в області ІВ, які захищають авторські права і торговельні марки інших компаній;
- управляти бізнес-ризиками, пов'язаними з порушеннями прав на ІВ;
- запобігати контрафакції і піратству та попереджувати її;
- розробити відповідні правила і вжити практичних кроків для дійсного дотримання прав ІВ.

Політика компанії

- 1. Організаційні правила.** Затвердити в організації правило вести діяльність у відповідності до законів про ІВ та світової практики. Впровадити конкретні правила, процедури та методки з метою сприяння дотримання законності.

Рекомендації

- 1.1. Цілеспрямована політика вищого керівництва компанії про необхідність дотримання законодавства в сфері ІВ допоможе значно зміцнити цю ідею в рамках компанії. Це можливо здійснити, наприклад, за допомогою затвердження правил компанії рішенням її виконавчого органу або іншого органу управління.
- 1.2. Під «Інтелектуальною власністю» або «ІВ» в цих Рекомендаціях розуміється правовий захист інтелектуальних прав на творчі витвори та бренди, зокрема, авторського права та торговельних марок, а також комерційних таємниць, промислових зразків та ін. Питання патентування є більш складними і не розглядаються в цих Рекомендаціях.
- 1.3. Управління ІВ відрізняється в різних галузях промисловості, немає єдиної ідеальної практики застосування Рекомендацій для будь-якого підприємства. Проте, є цінні уроки,

які надають компанії з різних сфер економіки, які серйозно ставляться до захисту ІВ. Деякі з існуючих правил варті уваги, в тому числі методика виробництва оптичних носіїв (IFPI Good Business Practices for Optical Disc Mastering & Manufacturing Plants). В галузі створення програмного забезпечення та ІТ, рекомендації та стандарти з матеріально-технічного забезпечення та управління активами містять корисні практики дотримання норм законодавства по захисту ІВ, включаючи Business Software Alliance Software Management Guide, ІТ Governance Institute's Control Objectives for Information and Related Technology (COBIT®) version 4.1 та ІSO standard ISO/IEC 19770-1, Software Asset Management. Зверніть увагу, що багато керівних принципів Рекомендацій з ІВ ICC/BASCAP можуть допомогти сформуванню корисної основи політики компанії.

- 2. Правомірне використання.** Купувати і використовувати під час ведення справ тільки ліцензовані копії матеріалів, захищені авторськими правами і справжні вироби, які охороняються торговельними марками.

Рекомендації

- 2.1 Дана пропозиція поширюється на всю діяльність із закупівлі, використання та продажу товарів та послуг, заснованих на об'єктах ІВ. Далі більш детально описується пропозиція купувати виключно матеріали, в яких законно використовується ІВ, для використання в господарській діяльності або в окремій ланці ланцюга потсавок.
- 2.2 Продукція, яка використовується в підприємницькій діяльності, але не є безпосередньо результатом виробництва, така як програмне забезпечення, довідники, інформаційні послуги тощо, захищені авторськими правами та торговельними марками, якій може бути завдано шкоди при її неліцензованому копіюванні та поширенні. Ця пропозиція вимагає відмови підприємства від використання незаконних матеріалів у своїй діяльності.
- 2.3. Виготовлення та збут продукції, заснованої на об'єктах ІВ, без дозволу правовласника також є порушенням. Цією продукцією можуть бути диски, що містять неліцензійний матеріал (фільми, музику, програмне забезпечення, ігри) та підроблені брендові товари (наприклад, комп'ютерне програмне забезпечення, промислові продукти, їжа, цигарки, автозапчастини, товари народного вжитку та фармацевтичні препарати). Цей обов'язок означає заборону виготовляти, рекламувати, продавати, поставляти, поширювати або іншим способом використовувати таку нелегальну продукцію.
- 2.4. Потрібно виділяти достатній бюджет для всіх матеріалів, заснованих на правах ІВ, які використовуються в підприємницькій діяльності для того, щоб у працівників не виникало стимулу використовувати матеріали, що порушують право ІВ.

- 3. Захист ІВ компанії.** Вживати необхідних заходів для виявлення та захисту ІВ компанії.

Рекомендації

- 3.1 Розуміння компанією цінності ІВ та необхідності її захисту, що належать їй, не тільки допомагає компанії отримувати користь від власної творчості та інноваторства, але й показує гарний приклад поваги до прав ІВ третіх осіб.

- 3.2. Захист ІВ компанії може приймати різні форми залежно від сфери її діяльності та виду конкретного підприємства. Перевірка комерційних найменувань та символів, реєстрації та правильного використання торговельних марок можлива на багатьох підприємствах. В деяких випадках може знадобитися документальне оформлення оригінальних робіт, захищених авторським правом, а в деяких випадках їх реєстрація або повідомлення про авторські права є обов'язковим. Що ж до промислових винаходів, може знадобитися реєстрація промислових зразків. Особливо уважно треба здійснювати процеси продовження дії таких прав, документування та інші докази існування таких прав.
- 3.3. Існує широке коло стратегій, до яких компанія може вдаватися щоб захистити себе від порушення її прав ІВ іншими особами. Залежно від виду діяльності компанії та сектору ринку, вони можуть включати:
- Використання технічних засобів захисту продуктів та процесів, пов'язаних з ІВ.
 - Вибір ділових партнерів, які дотримуються належних методів управління ІВ.
 - Співпрацю з правоохоронними органами на національному, регіональному та міжнародному рівнях.
 - Співпрацю з правовласниками та їх посередниками (включаючи оптовиків, перевізників,
 - підприємства роздрібної торгівлі, Інтернет-провайдерів та інших постачальників он-лайн послуг) для протидії правопорушенням і продажу контрафактних та піратських товарів.
 - Звернення з заявами про порушення кримінальних справ та вчинення інших правових дій в разі необхідності.
 - Співпраця з господарськими об'єднаннями для боротьби з різними видами контрафакції та піратства.
- 3.4. Митні органи, як правило, потребують від компанії особливої допомоги у захисті ІВ. Реєстрація заяв в Митних органах, надання їм інформації про продукцію, роз'яснень та оперативних відповідей на запити Митних органів про допомогу можуть суттєво покращити спроби Митних органів зупинити постачання через кордон продукції, що порушує права ІВ.
- 4. Додержання вимог законодавства.** Призначити директора або менеджера, який буде визначати та впроваджувати політику компанії щодо ІВ.

Рекомендації

- 4.1 Для того, щоб на підприємстві виконувались вимоги законодавства щодо ІВ, необхідно призначити надійного працівника, який би ніс за це персональну відповідальність. Ця особа повинна бути наділена необхідними повноваженнями для можливості мати або отримати у майбутньому повне уявлення про діяльність організації; мати змогу розробляти та вводити в дію методики, процедури та правила компанії з дотримання законодавства у сфері ІВ, а також розглядати спори та скарги. Кваліфікований старший керівник, чи топ-менеджер має бути гарною кандидатурою для виконання цієї функції.

5. Політика щодо співробітників. Запровадити правила щодо додержання законів у сфері ІВ та політики компанії щодо ІВ та довести їх до відома працівників.

Рекомендації

- 5.1. Так само, як у випадку з правилами охорони здоров'я та безпеки праці, а також іншими вимогами законодавства, працівники повинні бути заохочені до дотримання законів, правил, методики та процедур компанії в сфері ІВ. Наприклад, працівників можна зобов'язати не займатись протиправною діяльністю, яка порушує права ІВ третіх осіб під час виконання своїх трудових обов'язків на території компанії, використовуючи її обладнання, зберігати конфіденційність та комерційні таємниці компанії та третіх осіб.
- 5.2. Вимога про дотримання прав ІВ може бути включене, як умова трудового договору з працівником, або частина правового посібника, який би розповсюджувався серед працівників. Вимоги до захисту ІВ доповнюють умови трудових договорів з працівниками або інструкції, які регулюють питання виключних прав на вироби, створені працівниками.
- 5.3. Схожі вимоги та умови можуть бути включені також до письмових трудових договорів з підрядниками.
- 5.4. Працівники та підрядники, які взяли на себе обов'язок поважати право ІВ, повинні дотримуватись цього обов'язку не тільки в рамках виконання їх прямих обов'язків в компанії, – такі як закупівля, створення продукції, виготовлення, маркетинг тощо, – але також на всю їх діяльність на території компанії та в роботі з устаткуванням. Багато компаній захищають себе від несанкціонованих дій у цій сфері, забороняючи працівникам інстальовати, чи використовувати нелегальні копії програмного забезпечення, музики, друкованих матеріалів, чи ігор на комп'ютерах компанії, або дозволяти доступ до комп'ютерної мережі компанії стороннім з метою нелегального доступу, передання чи зберігання матеріалів, захищених авторським правом, чи комерційною таємницею.

6. Навчання та підвищення інформованості. Ознайомити працівників та субпідрядників (коли це необхідно) з політикою компанії щодо захисту ІВ.

Рекомендації

- 6.1. Навчання персоналу може включати в себе ознайомлення з діючим законодавством в сфері ІВ, вимогами до ліцензування, належності виключних прав у підприємницькій діяльності, а також правила, процедури та методики компанії.
- 6.2. Керівник, відповідальний за захист прав ІВ повинен знати закони про ІВ, так само, як і правила ліцензування в сфері ІВ, що має відношення до діяльності компанії, для розроблення та впровадження правил захисту ІВ, процесів та практик, які є

ефективними, необхідними та дієвими для компанії. Наприклад, керівник в компанії, яка займається виготовленням компакт-дисків, повинен бути ознайомлений із законами про авторське право, пов'язаними з музикою, ліцензійними договорами, які використовуються компаніями звукозапису та іншими правовласниками, а, також, інформацією про правовласників у належних сферах, яку можна знайти через доступні бази даних.

- 6.3. Працівники та підрядники також потребують навчання та інформування в сфері ІВ, пов'язаної з їх роботою. Наприклад, керівник з виробництва компакт-дисків повинен розуміти, що тиражування CD- та DVD-дисків з програмним забезпеченням, музикою чи фільмами без підписання ліцензійного договору з правовласником є правопорушенням. В багатьох компаніях менеджер із закупівель повинен розуміти, що використання відомої торговельної марки для маркування підробки є контрафакцією.
- 6.4. Керівникам з контролю за дотриманням законодавства, так само, як і рядовим працівникам буде корисно проходити таке навчання, коли вони працюють з об'єктами ІВ, і періодично після цього, з урахуванням зміни робочих кадрів та лінії продукції, а також, еволюції ліцензійних та бізнес-практик в усіх сферах. Відповідні промислові професіональні об'єднання, так само, як і юридичні фірми та спільноти пропонують такі тренінги в більшості країн.

Поставка, виробництво та продаж

7. **Попереджати постачальників та клієнтів.** Повідомляти постачальників та покупців про те, що компанія дотримується законодавства в сфері ІВ і чекає від них того ж.

Рекомендації

- 7.1. Одним із способів додержання постачальниками та клієнтами прав ІВ є повідомлення відповідних постачальників та клієнтів про те, що компанія поважає ІВ, дотримується правил, методик та процедур із захисту ІВ та чекає від постачальників і клієнтів такого ж відношення. Конкретні обов'язки можуть бути винесені на обговорення та включені до відповідних договорів або в окремі почтові повідомлення чи декларації на веб-сайті. Це дає правильне уявлення про ділові відносини та може попередити проблемні замовлення і дії з боку контрагентів, наприклад, замовлення на поставку контрафактної продукції.
- 7.2. Договори компанії з постачальниками та клієнтами можуть також включати умови про розподіл відповідальності за контрафактну продукцію та інші порушення прав ІВ. Такі умови можуть включати гарантії від шкоди, фінансові гарантії, обов'язки усунути порушення, пов'язані з ІВ, обов'язок виключити правопорушника зі списку постачальників чи клієнтів та розірвання договору. За допомогою цього компанія може керувати ризиками в сфері ІВ у випадку, коли її постачальники чи клієнти порушують право ІВ третіх осіб без відома компанії, її згоди або участі.

- 8. Законні ресурси.** По можливості використовувати для свого бізнесу ресурси, отримані від легальних та перевірених постачальників.

Рекомендації

- 8.1. Дії по отриманню ресурсів, такі як закупівля сировини та компонентів, проектування, дизайн, а бо інші послуги, виконані третіми особами, часто мають на увазі використання авторського права і торговельних марок. Компанія в більшості випадків може домовитись із продавцями про постачання товарів та послуг, які б не порушували законів про ІВ.
- 8.2. Зокрема, при здійсненні виготовлення компанії корисно отримувати матеріали від перевірених постачальників, які пропонують продукцію тільки від оригінальних виробників, ліцензованих дистриб'юторів, чи первинних власників товарів та виключно у постачальників, які проходять повну аудиторську перевірку.
- 8.3. Більш детально про «передові практики» отримання легальних ресурсів та інші питання поставки йдеться у спеціальних галузевих посібниках та публікаціях Торгової палати США «Жодної торгівлі підробками: інструментарій системи поставок» («No Trade in Fakes: Supply Chain Tool Kit»).

- 9. Умови контрактів.** Вести наскільки можливо детально документацію про ключові операції з об'єктами інтелектуальної власності, а також про відносини з покупцями і постачальниками.

Рекомендації

- 9.1. Відсутність або недостатність документації є однією з ознак того, що підприємство знаходиться в серйозній небезпеці, пов'язаної зі зневагою проблем ІВ або з активною участю у контрафакції або іншій протиправній діяльності. Для компаній, які займаються виробництвом продуктів на базі ІВ, надзвичайно важливим є документування своєї діяльності і проведення аудиту.
- 9.2. Конкретні особливості документообігу залежать від галузі економіки та сфери діяльності компанії, але обов'язково повинна бути включена фіксація «ключової» діяльності з використання товарів та послуг, заснованих на об'єктах ІВ. Це можуть бути детальні та максимально точні письмові ліцензійні та промислові договори про створення об'єкту ІВ, замовлення на закупівлю чи продаж продукції, виробнича документація, інвойси та транспортні накладні. Фіксація ключової діяльності повинна бути достатньо детальною для того, щоб ідентифікувати сам матеріал, заснований на об'єктах ІВ (наприклад, оригінальну промислову установку, чи споживчий товар, музичний трек, назва комп'ютерного програмного забезпечення чи фільму, ліки чи хімічна сполука, їжа, чи торговельна марка), кількість, ціну або роялті, та точне місце призначення і відправлення.
- 9.3. Для деяких сфер господарської діяльності дуже важливим є збереження виробничих матриць та зразків продукції, тому що вони можуть слугувати засобом захисту ІВ для компанії, її постачальників та клієнтів, так само, як і для правовласників. Зокрема, в разі

позову або претензії про порушення прав ІВ, матриці та зразки продукції можуть стати в нагоді для виявлення джерела незаконної продукції або її компонентів та притягнення до відповідальності належної сторони.

- 9.4. Передання виключних прав та ліцензій на об'єкти ІВ повинне бути виражене у письмовій формі. Це є особливо важливим у випадку, коли компанія передає право на виготовлення продукції, захищеної правом ІВ, третім особам, тому що згідно законів більшості країн, таке передання прав і ліцензій є недейсним без додержання письмової форми. Письмова форма договорів може попередити суперечки щодо права власності та можливі позови про правопорушення.
- 9.5. Угоди про використання ІВ повинні бути чіткими і охоплювати всі важливі питання достатньо детально для того, щоб уникнути плутанини і проблем в майбутньому. Такі угоди, як правило, включають інформацію про технологію або матеріал, який використовується, коло прав, які відчужуються, умови користування та продажу (якщо потрібно), обов'язки зберігати конфіденційність, обов'язки проводити моніторинг та аудит, а також, умови розірвання угоди та способи відшкодування шкоди в разі порушення її умов.

10. Обізнаність про постачальників та клієнтів. Отримувати письмові докази підтвердження майнових прав ІВ та необхідних ліцензій до початку виробництва, поставки чи пропонування товарів та послуг, заснованих на об'єктах ІВ.

Рекомендації

- 10.1. Більша частина торгівлі контрафактною продукцією існує та робиться на користь анонімних постачальників та клієнтів, особа яких не була належним чином встановлена. Псевдоніми, абонентські поштові скриньки, невизначені електронні адреси та мізерна контактна інформація можуть свідчити про те, що постачальник, або клієнта, бере участь у торгівлі контрафакцією, так само, як відсутність підтвердженої діяльності в тій галузі, економіки, для якої характерна специфічна продукція, заснована на об'єктах ІВ.
- 10.2. Достовірна інформація, що ідентифікує постачальників та покупців, включає в себе дані про справжні імена, повні адреси та номери телефонів. Посередникам також належить отримувати та мати можливість надати таку інформацію по відношенню до їх кінцевих споживачів.
- 10.3. «Знай свого постачальника та покупця» – це дуже добра ділова практика. Фіксація достовірної ідентифікуючої інформації, збір довідкової та контактної інформації про постачальників та покупців є не тільки стримуючим фактором проти контрафакції і піратства, але й допомагає компанії керувати іншими видами ризиків, включаючи проблеми, пов'язані з поставкою, оплатою, якістю та ін.

11. Необхідні ліцензії. Отримайте письмовий доказ належності майнових прав ІВ та необхідні ліцензії перед виробництвом, поставкою чи пропонуванням продуктів або послуг, заснованих на ІВ.

Рекомендації

- 11.1. Копіювання, розповсюдження, передання чи інше використання товарів і послуг, захищених торговельними марками і авторським правом, в підприємницькій діяльності без отримання дозволу майже завжди є правопорушенням, за умови відсутності ліцензій від правовласників.
- 11.2. Ліцензії мають бути оригіналами документів, які звичайно визначають всі захищені твори, чи торговельні марки, строк дії ліцензії, особливості використання та кількість об'єктів, на які надається ліцензія.
- 11.3. Необхідні ліцензії повинні бути надані в письмовій формі. Справжні ліцензії на об'єкти авторського права і торговельних марок, і рідко покривають весь ряд продукції, прав та торговельних марок правовласника, і рідко видаються на невизначений строк. Компанії повинні наполягати на тому, щоб в ліцензіях на копіювання, виготовлення, чи розповсюдження продукції, пов'язаної з ІВ, чітко визначалися предмет ліцензії, строк, на який вона видана та особливості її використання.

12. Юридичний аудит. Аналізувати документацію та супутні відомості про наявність ознак порушення прав ІВ при замовленні та поставці товарів. За необхідності, збирати додаткову інформацію для перевірки діяльності, що викликає підозри.

Рекомендації

- 12.1. Ігнорування контрафакції і піратства не може мати виправдань. У відношенні багатьох порушень прав ІВ передбачена презумпція винуватості, наприклад, у відношенні неліцензійного відтворення та розповсюдження матеріалів, захищених авторським правом або товарів, захищених відомими торговельними марками без ліцензії, навіть якщо вказана діяльність здійснювалась по замовленню покупця. Проведення юридичної перевірки ліцензій, товарів, зразків, замовлень, інформації та інших предметів, пов'язаних з товарами і послугами, захищеними правом ІВ, може знизити ризик скоєння правопорушення.
- 12.2. Інформація про постачальників та споживачів, ліцензії, отримані товари, зразки продукції та умови замовлень можуть нести сигнали того, що поставлені або замовлені матеріали є нелегальними, ефективна програма регулярної або вибіркової перевірки може допомогти виявити такі сигнали попередження. Якщо сигнали попередження були виявлені, може знадобитися подальше розслідування, включаючи консультації з відповідними правовласниками чи галузевою анти-піратською організацією для визначення статусу підозрілої діяльності.
- 12.3. Сигнали про небезпеку у різних галузях різні. Ними, наприклад, можуть бути замовлення великої кількості немаркованих копій відомих товарів; використання відомих торговельних марок невідомими компаніями, запити від невідомих компаній на отримання ліцензій; оплата готівкою великих сум; неякісне оздоблення чи упаковка; видалення, відновлення чи окрема доставка товарів та етикеток з торговельними марками або засобів технічного захисту; неправильне, чи неповне зазначення змісту, місця походження або виготовлення товару на етикетці.

12.4. Деякі правовласники самостійно пропонують інформацію та допомогу для того, щоб покупець мав змогу перевірити, чи є продукція або ліцензія законними; інші виконують це при посередництві галузевих анти-піратських організацій. Договори зі споживачами та постачальниками повинні передбачувати можливість консультування з відповідними правовласниками або галузевими анти-піратськими організаціями, якщо виникне підозра у правопорушенні.

Безпека та конфіденційність

13. Фізична та інформаційна безпека. Підтримувати фізичну та інформаційну (ІТ) безпеку на достатньому рівні, щоб забезпечити недоторканність архівів і виробничих процесів компанії, а також захистити інтелектуальну власність і конфіденційні відомості.

Рекомендації

- 13.1. Компанії, задіяні у виготовленні та продажі товарів, заснованих на об'єктах ІВ, функціонують добре, якщо їх територія захищена і проводиться профілактична робота з персоналом для попередження крадіжок, незаконного доступу, «третіх робочих змін», чи інших несанкціонованих дій по виготовленню або використанню товарів, розголошенню комерційної таємниці та інших незаконних дій.
- 13.2. Компанії, задіяні у використанні ліцензованої продукції часто повинні бути здатними надати докази та звітувати про здійснювану ліцензовану діяльність. Це вимагає зберігання договорів, пов'язаних з ІВ, ліцензій, фінансових звітів та іншої документації у безпеці – гарна ділова практика в будь-якому випадку.
- 13.3. Копії інформаційних матеріалів про секрети виробництва, продукції, заснованої на об'єктах ІВ, комерційних таємниць та іншої конфіденційної інформації, звіти компанії все частіше зберігаються на комп'ютерах та в комп'ютерних мережах. Надійна ІТ-охорона може допомогти зберігати конфіденційність такої інформації, а також запобігти порушенню ІВ у формі незаконного електронного доступу, зберігання, копіювання, розміщення, передання або розкриття ІВ третім особам.
- 13.4. ІТ-охорона звичайно включає такий захист, як програмне забезпечення проти вірусів та шпійських програм, внутрішні обмеження доступу до комп'ютерів та комп'ютерної мережі, брандмауери та інші обмеження доступу через Інтернет до комп'ютерів і комп'ютерної мережі компанії (включаючи пірингові файлообмінні мережі) та заборону несанкціонованої інсталяції чи поширення матеріалів, захищених правом ІВ, на комп'ютерах або комп'ютерних мережах компанії. Для отримання подальшої інформації про ІТ-захист, пов'язаний з порушеннями ІВ, звертайтеся до публікації Міжнародної федерації виробників фонограм / Американської асоціації кінокомпаній / Міжнародної асоціації виробників відео (IFPI/MPAA/IVF) – «Керівництво з авторського права та безпеки для організацій та органів влади» (Copyright and Security Guide for Companies and Governments).

- 14. Управління активами.** Впровадити процедури з виявлення, обліку і контролю інтелектуальних активів, щоб гарантувати можливість їх аналізу та управління ними.

Рекомендації

- 14.1. Гарною бізнес-практикою є проведення інвентаризації товарів, вироблених з використанням ІВ, використовуваних підприємством у внутрішній діяльності програмного забезпечення та іншої ІТ-продукції, а також управління такими товарами, як і іншими ключовими активами, на протязі всього циклу їх використання.

- 15. Захист комерційної таємниці та конфіденційної інформації.** Докладати максимальних зусиль для захисту комерційної таємниці та конфіденційної інформації компанії і третіх осіб.

Рекомендації

- 15.1. Компанії, задіяні у виробництві або продажі товарів чи послуг, заснованих на об'єктах ІВ, часто потребують у своїй діяльності доступу до комерційної таємниці чи конфіденційної інформації, яка належить правовласнику. Доступ до комерційної таємниці і конфіденційної інформації зумовлений договірними чи юридичними обов'язками, покликаних захищати, не розголошувати та не використовувати комерційну таємницю і конфіденціальну інформацію правовласника йому на шкоду, крім випадків, спеціально дозволених правовласником. Такі обмеження звичайно не поширюються на випадки, коли інформація була розкрита правовласником без обмежень, або коли урядове чи судове рішення вимагає такого розкриття.

- 15.2. В цілому, для збереження конфіденційності корисно скласти з користувачами і постачальниками договір, який би дозволяв консультації з правоохоронними органами або відповідними анти-піратськими організаціями і правовласниками у випадку підозри у порушенні прав ІВ, таких, як клієнтське замовлення на завідомо контрафактну продукцію.

- 16. Технічні анти-піратські заходи.** Поважати, не втручатися і підтримувати безпеку технічних анти-піратських заходів, які використовуються правовласниками для захисту їх продукції та послуг, заснованих на об'єктах ІВ.

Рекомендації

- 16.1. Правовласники все частіше покладаються на різні види технічних анти-піратських засобів, які використовуються ними в упаковці продукції і її дистрибуції для попередження і припинення контрафакції. Компанії, задіяні у виробництві, маркетингу та поширенні продукції, заснованої на об'єктах ІВ, повинні підтримувати такі дії шляхом виконання вказівок правовласників по використанню даних технічних засобів безпеки, не повинні прибирати, відключати чи обходити дані засоби, або вживати інші засоби, які б знизили їх ефективність.
- 16.2. Ліцензована продукція, виготовлена з використанням ІВ, яка використовується у внутрішній діяльності компанії також може містити анти-піратські заходи, які також потрібно поважати. Більш того, сучасні закони про авторське право класифікують уникнення цих заходів як правопорушення.

Дотримання законодавства та аудит

- 17. Облік.** Зберігати основні матеріали, що стосуються інтелектуальної власності, протягом відповідного терміну.

Рекомендації

- 17.1. Правильного ведення фінансової звітності вимагають практично всі стандарти бухгалтерського обліку та податкові органи у всьому світі. Фінансові звіти та записи, пов'язані з ІВ, повинні зберігатись разом з іншими звітами компанії не менше трьох років після їх використання (цей період є довшим у деяких країнах). Звіти та матеріали повинні містити копії фінансових угод, замовлень, виробничих записів, транспортних накладних, ліцензій та зразків продукції, виробленої з використанням ІВ.

- 18. Маркування.** Маркувати всю продукцію та упаковку, яка має відношення до ІВ, що виробляється або поставляється.

Рекомендації

- 18.1. Явною ознакою контрафактної продукції є відсутність маркування. Вироби, упаковки або пакувальні коробки можуть свідчити про інший вміст, чи можуть не мати маркування взагалі. Місце походження чи виробництва на таких товарах може не вказуватися або бути хибним. Списки товарів у змішаних поставках можуть не мати згадки про контрафактні вироби, включені до них разом з іншим товаром.

- 18.2. Не дивлячись на те, що вимоги можуть відрізнятися, залежно від галузі промисловості, маркування виробів, пов'язаних з ІВ, які поставляються, повинне бути повним та точним в частині специфікації товарів, їх кількості та місця походження. Маркування повинне містити ідентифікаційні маркувальні знаки та коди, розроблені самим правовласником, або передбачені стандартами галузі промисловості, містити інформацію про завод-виробник, ідентифікацію виробу, номер партії та інші зазначення.

- 18.3. Окремі правовласники можуть мати власні вимоги до маркування. Існують також стандартні вимоги до маркування, які використовуються у певних галузях, наприклад, стандарти кодів Міжнародно федерації виробників фонограм / Філіпс «Ідентифікація джерел» (IFPI/Philips Source Identification disc and mould codes), які застосовують при виробництві оптичних дисків. Найкращою практикою для підприємців є використання стандартного маркування, яке застосовують точно і без винятків всі правовласники та індустрії.

- 19. Моніторинг.** Періодично переглядати правила компанії в сфері ІВ.

Рекомендації

- 19.1. Для того, щоб правила компанії, процедури та методики дотримувались працівниками та були здійсненними, необхідно здійснювати постійний моніторинг, виправлення недоліків та покращення правил компанії з дотримання законодавства в сфері ІВ.

20. Зразки. Надавати правовласникам, їх підприємствам, які борються з піратством, правоохоронним органам на їх прохання зразки продукції, створеної з використанням ІВ, яка виробляється компанією.

Рекомендації

20.1. Легальним підприємствам немає що приховувати. Надання зразків, наприклад, зразка диску з кожної партії виготовлених оптичних дисків, допомагає попереджати контрафакцію та викривати порушників, які займаються піратством.

21. Співпраця з правовласниками та органами державної влади. Надавати допомогу правовласникам, підприємницьким та анти-піратським організаціям, правоохоронним органам при розслідуваннях можливих порушень права ІВ.

Рекомендації

21.1. Компаніям, які здійснюють операції з товарами і послугами, заснованими на об'єктах ІВ, вигідно об'єднуватись і співпрацювати, коли виникають проблеми з порушеннями прав ІВ, наприклад, пред'явлення ліцензій та іншої інформації, пов'язаної з підозрілими творами, замовленнями та діяльністю. Боротьба з тіньовою Економікою, піратством та контрафактною продукцією вимагає завзятості і співпраці з іншими правовласниками, органами влади та компаніями в кожній ланці ланцюга поставок.

П. Що означають «Рекомендації з інтелектуальної власності для бізнесу» ІСС/BASCAP?

- В.** Бізнес проти контрафакції і піратства (BASCAP), ініціатива Міжнародної торгової палати (ІСС), виробила низку Рекомендацій з ІВ, які надають інформацію, за допомогою якої підприємства зможуть вжити практичних заходів для оцінки ефективності управління своєю ІВ, особливо в сфері авторського права та торговельних марок; захистити власну ІВ підприємства; розглянути додаткові можливості покращення продуктивності та управління ризиками, пов'язаними з контрафакцією та піратством. Ці Рекомендації направлені на внутрішнє управління ІВ, практику роботи з постачальниками, стосунки з посередниками та використання ІВ, яка належить третім особам. Рекомендації розглядають управління ІВ в усіх її формах в компаніях, від розробки ІВ до пошуку компонентів, виробництва, продажу та використання в межах корпорації.

П. Чому BASCAP це робить?

- В.** BASCAP розробив ці Рекомендації для допомоги компаніям всіх рівнів знизити ризик крадіжки об'єктів ІВ, і боротися з піратством та контрафакцією. Піратство і контрафакція негативно впливають на економіку і мають серйозні та руйнуючі наслідки для компаній, які працюють в цій сфері. Це трапляється тому, що контрафакція і піратство мають більш значні наслідки: вони перешкоджають створенню нових винаходів і креативності, позбавляють держави податкових надходжень, недобросовісно конкурують з правомірною економічною діяльністю та шкодять зайнятості населення, послаблюють впевненість споживачів у добре відомих легальних товарах, викликають серйозну небезпеку для здоров'я і безпеки людей та живлять організовану злочинність. Бізнес та уряд разом, кожний у своїй ролі, зможуть знизити рівень крадіжок ІВ і шкоду бізнесу та суспільству, яку вони наносять.

П. Чому потрібні Рекомендації?

- В.** Компанії можуть багато що зробити для захисту своєї власної креативності та інновацій, втілених у товарах і послугах, заснованих на об'єктах ІВ, а також зменшити ризики порушення прав ІВ третіх осіб. Глобальна економічна тенденція полягає у підвищенні інвестицій у ІВ та більшу віру в ІВ, як суттєвий елемент економічного зростання. Проблема полягає в тому, що ІВ є нематеріальним активом, який потребує не лише правового захисту, але й правильного керування та використання з метою розкриття її повного потенціалу. Рекомендації розроблені для підвищення обізнаності та надання компаніям корисної інформації щодо управління ІВ.

П. Хто буде їх використовувати?

- В.** Великі та малі компанії майже у кожній галузі все частіше використовують та покладаються на ІВ, і це може покращитись при використанні якісних правил з управління ІВ, розроблених на основі цих Рекомендацій. Малі та середні підприємства та великі компанії, задіяні у створенні, виробленні, поставці, чи продажі заснованих на ІВ товарів і послуг, так само, як і велика кількість інших комерційних формувань, які використовують деякі із заснованих на ІВ матеріалів в своїй діяльності, тільки виграють.

П. Це обов'язкова програма?

- В. Рекомендації з ІВ були розроблені як путівник, який компанії можуть використовувати, або на який можуть спиратися при виробленні власних правил, процедур чи посадових інструкцій для працівників, що працюють з ІВ.
- Будучи свого роду довідковим посібником, ці Рекомендації можуть бути частково включеними до договорів між правовласниками та постачальниками, такими як заводи. Вони, також, можуть бути взятими за основу при проведенні сертифікації відповідності або при створенні галузевого кодексу правил, добровільних чи обов'язкових в певних галузях господарства.
- Ці Рекомендації розроблялися для того, щоб приносити користь широкому колу підприємств в різних галузях та можуть бути адаптовані у певних сегментах або ланках ланцюгу поставок.

П. Як Рекомендації були створені?

- В. Рекомендації були створені після дослідження та перегляду напрацювань та прецедентів у різних секторах промисловості, пов'язаних з ІВ, та являють собою набір інструментів, які компанії використовують у багатьох галузях для підвищення ефективності управління ІВ. В цьому дослідженні були використані наступні джерела, багато з яких були процитовані у різних секціях Рекомендацій:
- Рекомендації для окремих індустрій («Керівництво з авторського права та безпеки» (Copyright Use and Security Guide) та «Належна методика виробництва для заводів-виробників оптичних носіїв» (Good Business Practices for Optical Disc Manufacturing) для кіно- та музичних галузей; для індустрії програмного забезпечення – «Контрольні цілі для технології обробки інформації та суміжної технології» COBIT та Стандарти Міжнародної організації зі стандартизації (ISO) для управління ІТ та програмним забезпеченням).
 - «Інструментарій системи поставок» (Supply Chain Tool Kit) Коаліції проти контрафакції і піратства США: (<http://www.thecacp.com/portal/truercosts/resources/supplychain.htm>).

П. Як вони будуть поширені?

- В. ICC співпрацює з національними комісіями та компаніями-членами для поширення Рекомендацій серед галузевих груп і компаній по всьому світу. ICC робить Рекомендації доступними шляхом оприлюднення їх на веб-сайті (www.iccwbo.org/bascap), а, також, співпрацює з урядами для сприяння обізнаності про необхідність правильного управління ІВ, як це описано в Рекомендаціях.

П. Чому ICC?

- В. Основними цілями ICC є представництво від імені всього світового бізнесу, підтримка глобалізації економіки як джерела економічного розвитку, створення робочих місць та процвітання. З 1919 року, ICC працювало над створенням міжнародної ринкової економіки, заснованої на єдиних правилах торгівлі та інвестування. Ця робота включає створення кодексів правил ведення бізнесу та типових договорів, які використовуються підприємствами по всьому світі. На сьогодні, вони охопили багато сфер, включаючи міжнародні комерційні терміни, банківські правила та корпоративну етику, і зараз поширилися на питання обізнаності в сфері корпоративного управління ІВ.

Як я можу взяти участь у програмі?

- 1. Перегляньте методи управління ІВ у Вашій компанії.** Рекомендації надають корисні ідеї та інструменти для оцінки ефективності правил, процедур, методик та договорів, пов'язаних з управлінням ІВ, особливо у сферах авторського права та торговельних марок, а також для нових можливостей покращити рівень керування ризиками, пов'язаними з контрафакцією та піратством.
- 2. Надайте інформацію про Ваші правила з управління ІВ** Вашим постачальникам, клієнтам та іншим особам. Ви можете зробити це на Вашому веб-сайті, за допомогою електронної пошти або у ваших договорах. Якщо Ви бажаєте, ICC/BASCAP схвалює та підтримує розміщення прямих посилань на ці Рекомендації на веб-сайті Вашої компанії.
- 3. Поширюйте Рекомендації** серед ділових та господарських груп. Якщо Ви бажаєте, то заохочуйте Вашу чи пов'язану з Вами галузеву групу ознайомитись та поширити ці Рекомендації.
- 4. Доведіть до відома Вашого уряду,** що Рекомендації пропонують корисну інформацію для допомоги компаніям здійснювати управління ІВ, чому, влада, можливо, захоче сприяти. Покажіть владі, що бізнес робить свій вклад у боротьбу з піратством і контрафакцією.

Додаток 1: Рекомендації Великої Вісімки (G8) для органів державної влади щодо використання програмного забезпечення із дотриманням прав інтелектуальної власності

Вступ

Ініціативою Міжнародної Торгової Палати (ICC) – «Бізнес проти контрафакції та піратства» («Business Action to Stop Counterfeiting and Piracy» («BASCAP»)) був розроблений цей збірник Рекомендацій з інтелектуальної власності (ІВ) для надання інформації про практичні заходи, які підприємці та інші організації можуть здійснити для більш ефективного корпоративного управління авторськими правами, маркованими та захищеними іншими об'єктами ІВ товарами та послугами.

Серед користувачів товарів та послуг, заснованих на об'єктах ІВ, є і уряди, які зацікавлені в розробці правил з ефективного управління товарами та послугами, заснованими на об'єктах ІВ, які ними купуються та використовуються, та відповідальності за них. Демонструючи своє лідерство в цій сфері, Велика Вісімка окреслила конкретні напрямки, дотримуючись яких, уряди зможуть керувати використанням одного важливого продукту, заснованого на об'єктах ІВ, – програмного забезпечення – з дотриманням правил ІВ.

Нижче описані та проілюстровані основні принципи управління ІВ, схвалені Великою Вісімкою, а також надані корисні приклади з основного тексту Рекомендацій з ІВ ICC/BASCAP, а також інших найкращих напрацювань галузей та органів влади.

Органам державної влади будь-якого рівня буде корисно ознайомитись з цими Рекомендаціями для органів державної влади з використання програмного забезпечення, ми сподіваємося, що цей Додаток зможе стати корисним джерелом інформації та рекомендацій для органів державної влади в рамках Великої Вісімки та всього світу.

«Ефективний захист прав інтелектуальної власності та їх популяризація важливі для створення творчих продуктів, технологій та економік... Ми підтверджуємо нашу позицію про те, що уряд повинен використовувати програмне забезпечення відповідно до діючих міжнародних договорів та закликаємо інші країни підтримати нашу позицію»

**Декларація Великої Вісімки,
8 липня 2008 р.**

http://www.mofa.go.jp/policy/economy/summit/2008/doc/doc080714_en.html

Група восьми країн – Велика Вісімка (G8), до якої входять Канада, Франція, Німеччина, Італія, Японія, Росія, Великобританія і Сполучені Штати, не раз підкреслювала важливість інтелектуальної власності для економічного зростання, інновацій, творчості та інших соціальних благ.

Лідери G8 зробили особливі заяви в 2000 і 2008 роках про важливість використання урядами у своїй внутрішній діяльності програмного забезпечення (найважливішої інновації, заснованої на об'єктах інтелектуальної власності) з повним дотриманням прав ІВ. У декларації 2009 р. Лідери G8 схвалили звіт експертної групи з інтелектуальної власності, який, зокрема, включає «Рекомендації для органів державної влади щодо використання програмного забезпечення з дотриманням прав інтелектуальної власності» (Guidelines for Governments Use of Software in Compliance with Intellectual Property Rights). (Відповідні положення декларацій лідерів G8 та експертної групи G8 з інтелектуальної власності викладені в Додатку).

Ці Рекомендації G8 на високому рівні розглядають приклади правил, приписів та законів, якими повинні оперувати органи державної влади для «зменшення ризику використання державних комп'ютерних ресурсів з метою порушення прав ІВ, подання прикладу приватному сектору економіки і користувачам інформаційних технологій у боротьбі проти контрафакції та піратства, і в той же час забезпечення інтересів безпеки та прозорості їх власних адміністрацій». Рекомендації G8 висвітлюють такі питання: правила використання програмного забезпечення, безпека, інформація та обізнаність, і співробітництво держави та представників бізнесу.

Рекомендації Великої Вісімки для органів державної влади щодо використання програмного забезпечення будуть корисні для органів державної влади будь-якого рівня. Рекомендації Великої Вісімки, так само, як і приклади впровадження таких правил, що містяться в Рекомендаціях з ІВ ICC / BASCAP і різних передових практиках галузей економіки та органів державної влади, надають інформацію про практичні кроки, які уряди можуть зробити для оцінки ефективності правил управління ІВ та управління ризиками, пов'язаними з контрафакцією і піратством.

1. Правила використання програмного забезпечення

Рекомендація G8: Програмне забезпечення. Органи державної влади не повинні порушувати права ІВ при купівлі та встановленні програмного забезпечення, і повинні прийняти необхідні заходи для забезпечення виконання даного зобов'язання. Компетентні органи повинні здійснювати контроль над тим, щоб на комп'ютерах, що використовуються державними адміністративними органами, було встановлено виключно законне програмне забезпечення.

Коментарі та приклади

- 1.1 Правильне внутрішнє управління програмним забезпеченням та іншими продуктами, компонентами, та послугами, заснованими на інтелектуальній власності, ніколи не є випадковим, а, як правило, являє собою результат конкретних розпоряджень та безперервних програм, які роблять здійснення такого управління ефективним. Рекомендації з ІВ ICC/BASCAP описують декілька корисних елементів таких вимог, які можуть бути цікаві державним органам, в тому числі:
 - Специфічні правила, процедури та методики здійснення діяльності з дотриманням прав ІВ.

- Відповідні правила фінансування та закупівлі матеріалів, заснованих на об'єктах ІВ.
 - Призначення виконавчого директора або менеджера, обов'язки якого включатимуть спостереження та дотримання правил у сфері ІВ.
 - Ефективні правила щодо інформування постачальників, практика укладення договорів та ліцензування, юридичний аудит та інші правила для забезпечення законних каналів поставок.
- 1.2 Міжнародна Організація Стандартизації (ISO) та інші промислові стандарти можуть надати наступні рекомендації та приклади для розробки ефективних правил управління використання органами державної влади програмного забезпечення та інших продуктів та послуг, заснованих на об'єктах ІВ. Корисні рекомендації включають:
- Стандарт ISO/IEC 19770-1, Управління програмними активами, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=33908.
 - Альянс виробників програмного забезпечення (Business Software Alliance), Рекомендації урядам щодо управління програмним забезпеченням (Government Guide to Software Management), <http://www.bsa.org/~media/C72B329D6F7E4B46A7467DE0151210A1.ashx>.
 - Інститут з управління інформаційними технологіями (IT Governance Institute), Задачі інформаційних та суміжних технологій (Control Objectives for Information and Related Technology (COBIT®) версія 4.1, <http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981>.
- 1.3 Можливості використання цих Рекомендацій G8 багаточисельні та різноманітні. Корисні приклади:
- 1.3.1 Деякі органи державної влади на національному, регіональному чи локальному рівнях видають міністерські чи інші декрети, якими вимагають від держслужбовців придбання та використання лише легальних копій програмного забезпечення або матеріалів та послуг, заснованих на ІВ в цілому.
- 1.3.2 Деякі органи державної влади включають такі ж вимоги до трудових договорів.
- 1.3.3 Деякі органи державної влади розробляють деталізовані інструкції із державних закупівель та укладення державних договорів, які містять вимоги про легальні поставки програмного забезпечення та інших матеріалів, заснованих на ІВ.

2. Безпека

Рекомендація G8: Використання комп'ютерних мереж державних органів.

Компетентні державні органи повинні впровадити необхідні міри, щоб упевнитись, що при користуванні комп'ютерними мережами державних органів, включаючи, наприклад, ті, які використовуються підрядниками, не порушуються права інтелектуальної власності.

Коментарі та приклади

- 2.1 Відповідно до Рекомендацій G8, комп'ютери та мережі державних службовців потребують відповідної охорони та управління для захисту проти умисного або необережного використання всіх видів матеріалів, заснованих на ІВ, включаючи програмне забезпечення.

- 2.2 Деякі види заходів безпеки корисні в цьому випадку, вони можуть не тільки допомогти протидіяти неправильному використанню ІВ, але і захистити від більшої шкоди, завданої системам та інформації державних органів. Більш деталізовано це описують Рекомендації з ІВ ICC/BASCAP:
- Забезпечити фізичну та інформаційну безпеку для гарантування недоторканності архівів та діяльності державних органів, а також захистити конфіденційні відомості та матеріали, засновані на ІВ.
 - Впровадити процедури з виявлення, обліку і контролю інтелектуальних активів, щоб гарантувати можливість їх аналізу та управління ними.
 - Забезпечити фізичний, інформаційний та організаційний захист комерційних таємниць та конфіденційних матеріалів.
 - Підтримувати у робочому стані пристрої проти піратства, що використовуються правовласниками.

3. Інформація та навчання

Рекомендація G8: Інформація та навчання. Державні органи виконавчої влади повинні проводити заходи і акції з метою підвищення обізнаності працівників про важливість прав інтелектуальної власності для інновацій і створення нових продуктів та стимулювання належного використання інформаційних технологій. Державні службовці повинні бути інформовані про правила і процедури користування мережею і про наслідки незаконного або неналежного використання державних комп'ютерних систем.

Коментарі та приклади

- 3.1. Знання працівників і навіть підрядників про те, чому так важливо захищати інтелектуальну власність, а також розуміння, яким чином вони в рамках своєї діяльності можуть сприяти підтримці безпеки інтелектуальної власності, надзвичайно важливе для ефективного управління державними органами програмним забезпеченням та іншими об'єктами інтелектуальної власності.
- 3.2. Рекомендації з ІВ ICC/BASCAP пропонують декілька напрямів проведення тренінгів для працівників та відповідних підрядників:
- Тренінги, присвячені діючим законам у сфері ІВ, ліцензійним вимогам, правовласникам і законам, правилам, процедурам і методикам державних органів у сфері ІВ.
 - Деталізований тренінг для службовців, відповідальних за дотримання законодавства.
 - Відповідні тренінги для інших працівників залежно від характеру їх трудової діяльності, тобто є вони звичайними користувачами, фахівцями у сфері інформаційних технологій або співробітниками відділу закупівель.
 - Вступний тренінг у разі необхідності, наприклад, коли працівник приступає до роботи або займає нову позицію, пов'язану з ІВ; регулярні тренінги надалі, беручи до уваги зміну кадрів та обіг товарів, а також зміни в ліцензуванні ІВ та методах підприємництва. Зверніть увагу, що відповідні професійні галузеві об'єднання, а також юридичні фірми і спільноти пропонують проведення таких тренінгів у більшості країн.

4. Співпраця із правовласниками

Рекомендація G8: Співпраця держави та бізнесу. Знаючи про вирішальне значення державних закупівель для розвитку інновацій в галузі програмного забезпечення, державні органи можуть співпрацювати з представниками бізнесу та іншими зацікавленими особами з метою обміну передовим досвідом законного придбання та використання програмного забезпечення.

Коментарі та приклади

- 4.1. Боротьба з тінговою економікою контрафакту і піратських товарів вимагає великих зусиль і взаємодії всіх зацікавлених осіб: уряду, правовласників, органів державної влади і компаній на кожному рівні каналу поставок. Співпраця з правовласниками / розробниками програмного забезпечення, а також з іншими відповідними зацікавленими особами в діловому середовищі та уряді може стати надзвичайно вигідним для державних органів, тому що вони розробляють і стежать за виконанням правил по управлінню ІВ, включаючи програмне забезпечення.
- 4.2. Як зазначено в Рекомендаціях з ІВ ICC / BASCAP, у разі виявлення контрафакту чи інших проблем, пов'язаних з порушенням прав ІВ, державним органам, можливо, доведеться співпрацювати з правовласниками або правоохоронними органами. Таке співробітництво може включати, наприклад, надання ліцензій на об'єкти ІВ та іншої інформації, пов'язаної з підозрілими предметами, замовленнями і діяльністю.
- 4.3. Численні бізнес-організації, включаючи ICC / BASCAP, галузеві асоціації промислових підприємств, окремі постачальники, бухгалтерські фірми та інші консультаційні компанії можуть надати в якості прикладу загальні або конкретні рекомендації безкоштовно або за номінальною вартістю, а також платну консультацію з тим, щоб допомогти державним органам розробити та впровадити правила, процедури та методики з управління ІВ.

5. Джерела: Витяги з доповідей і декларацій Великої Вісімки

Доповідь за результатами зустрічі експертної групи Великої Вісімки з інтелектуальної власності (G8 Intellectual Property Experts Group Report of Discussions)
Аквіла, Італія, липень 2009

http://www.g8italia2009.it/static/G8_Allegato/ITALY%20G8%20IPEG%20Final%20Report.0.pdf

Окінавська Хартія про використання програмного забезпечення з дотриманням прав інтелектуальної власності

У державних органів є особливий обов'язок – подавати приклад у боротьбі з піратством і контрафакцією. Дотримуючись цього принципу, лідери повторно схвалили Окінавську Хартію на Саміті Хоккайдо-Токіо в 2008 р., щоб забезпечити використання державними органами програмного забезпечення в повній відповідності із захищеними правами інтелектуальної власності. IPEG (Експертна група з інтелектуальної власності) розробила і схвалила доданий набір рекомендацій (Додаток 1), щоб внести свій внесок в роботу по зниженню ризику використання державних мереж з метою порушення прав ІВ.

Рекомендації Великої Вісімки для органів державної влади щодо використання програмного забезпечення з дотриманням прав інтелектуальної власності

Слідуючи прогресивним змінам в області інформаційних і комунікаційних технологій, лідери Великої Вісімки на Саміті Кюсю-Окінава в 2000 р. прийняли Окінавську Хартію глобального інформаційного суспільства, яка закликає органи державної влади використовувати програмне забезпечення з повним дотриманням охоронюваних прав ІВ. У 2008 р. на Саміті Хоккайдо-Токіо лідери Великої вісімки повторно схвалили цей документ і закликали інші держави наслідувати йому.

Після Окінавського Саміту технологічні розробки, включаючи пірингові файлообмінні мережі, зіткнулися з новими проблемами.

Державні мережі являють собою значну частину інформаційних Інтернет-ресурсів а, отже, схильні до ризиків і проблем, пов'язаних з порушенням прав інтелектуальної власності.

Шляхом повторного схвалення Окінавської Хартії, прийняття законів, директив і правил для мінімізації ризиків використання комп'ютерних ресурсів держави для порушення прав ІВ, державні органи можуть подати бізнесу і користувачам інформаційних технологій приклад у боротьбі з контрафакцією і піратством, і, разом з тим, державні органи отримують можливість забезпечити безпеку і прозорість роботи, в яких вони зацікавлені.

Відповідно до цього, Експертна група з інтелектуальної власності розробила наступний набір рекомендацій, який може служити інструментом для удосконалення захисту прав ІВ в рамках роботи органів державної влади.

Рекомендації:

- **Програмне забезпечення**
Державні органи не повинні порушувати права інтелектуальної власності при придбанні та установці програмного забезпечення і повинні вживати належні заходи, щоб забезпечити виконання даного зобов'язання. Компетентні органи повинні здійснювати контроль над тим, щоб на комп'ютерах, що використовуються державними органами, було встановлено виключно легальне програмне забезпечення.
- **Використання державних комп'ютерних мереж**
Компетентні державні органи повинні вжити необхідних заходів, щоб користування державними комп'ютерними мережами, включаючи, наприклад, мережі, які обслуговуються підрядниками, здійснювалося без порушень прав інтелектуальної власності.
- **Інформація та обізнаність**
Державні органи повинні проводити інформаційні заходи і акції з метою підвищення обізнаності службовців про важливість прав інтелектуальної власності для інновацій, створення нових продуктів та стимулювання належного використання інформаційних технологій. Державні службовці повинні бути інформовані про правила і процедури користування мережею і про наслідки незаконного або неналежного використання державних комп'ютерних систем.

- **Співробітництво держави та представників бізнесу**

Органи державної влади, будучи інформовані про вирішальне значення державних закупівель для розвитку інновацій в галузі програмного забезпечення, можуть співпрацювати з представниками бізнесу та іншими зацікавленими особами з метою обміну передовим досвідом законного придбання та використання програмного забезпечення.

**Декларація лідерів Великої Вісімки: «Відповідальне управління в ім'я стабільного майбутнього» (Responsible Leadership for a Sustainable Future)
Аквіль, Італія, 8 липня 2009**

http://www.g8italia2009.it/static/G8_Allegato/G8_Declaration_08_07_09_final.0.pdf

Інновації та знання – це ключові чинники здатні допомогти одужанню економіки та відновленню її стабільного зростання ... Створення правил і ділового середовища, у якому поважаються права інтелектуальної власності, необхідно для стимулювання інновацій, знань, підприємництва і творчості ... Контрафакція і піратство продовжують загрожувати глобальній економіці, здоров'ю та добробуту населення. Через це ми схвалюємо результати роботи, проведеної нашими експертами, які відображені в Доповіді за результатами зустрічі експертної групи Великої Вісімки з інтелектуальної власності.

**Декларація лідерів Великої Вісімки. Саміт Хоккайдо-Токіо (G8 Hokkaido Tokyo Summit Leaders Declaration)
Хоккайдо-Токіо, Японія, 8 липня 2008**

http://www.mofa.go.jp/policy/economy/summit/2008/doc/doc080714_en.html

Ефективне стимулювання і захист прав ІВ мають надзвичайне значення для розробки творчих продуктів, технологій та розвитку економік. Ми вдосконалюємо існуючі ініціативи проти контрафакції та піратства ... Ми підтверджуємо нашу позицію про те, що державні органи повинні використовувати програмне забезпечення в повній згоді з відповідними міжнародними договорами, і закликаємо інші країни приєднатися до нашого рішення.

**«Окінавська Хартія Великої Вісімки про глобальне інформаційне суспільство»
(G8 Okinawa Charter on Global Information Society)
Саміт Кюсю-Окінава, Японія, липень 2000**

<http://www.mofa.go.jp/policy/economy/summit/2000/pdfs/charter.pdf>

Щоб максимізувати переваги Інформаційного суспільства для економіки та населення, ми розробили такі ключові принципи та методики і рекомендуємо їх усім:

- Захист прав інтелектуальної власності стосовно інформаційних технологій вкрай необхідний для стимулювання інновацій в сфері інформаційних технологій, конкуренції та трансферу нових технологій; ми вітаємо поточну спільну роботу державних органів, зайнятих у сфері інтелектуальної власності, а також закликаємо наших експертів до обговорення подальших кроків у цій сфері;
- Повторне схвалення урядами позиції про використання програмного забезпечення в повній відповідності з правами інтелектуальної власності, також дуже важливе.

Додаток 2: Як уникнути контрафакту при державному замовленні

Вступ

*«Практично все ризикує
виявитися підробленим»*

**Головне контрольне управління
США**, [http://www.gao.gov/products/
GAO-10-389](http://www.gao.gov/products/GAO-10-389)

*«Сенс у тому, що [виробників
контрафакту] мотивує лише
жага до грошей і жадібність»*

**Марсі Форман, Директор
Департаменту розслідувань
Імміграційної і митної поліції
США**, [http://news.bbc.co.uk/1/hi/
health/7865569.stm](http://news.bbc.co.uk/1/hi/health/7865569.stm)

Органи державної влади, так само, як і підприємці та споживачі можуть стати жертвами контрафакції та піратства.

Іноді контрафактні або піратські товари і послуги поставляються в результаті державних закупівель таких товарів, як електроніка, оборонні вироби, комплектуючі, програмне забезпечення та медикаменти. Цілком очевидно бажання постачальників заробити більше, поставивши дешеві підробки, і часом очевидна спокуса осіб, відповідальних за державні закупівлі, придбати дешеві компоненти незалежно від їх походження та якості. Результатом можуть стати всілякі ризики і збитки, включаючи вихід обладнання та систем з ладу, проблеми з безпекою, втрачений час, витрачені державні кошти і, в багатьох випадках, загроза людському здоров'ю та життю.

Органи державної влади можуть і повинні застосовувати ефективні правила з тим, щоб виявляти контрафактні і піратські товари та послуги при державних закупівлях, протидіяти їм і відшкодувати збиток від таких товарів і послуг. Ініціатива Міжнародної Торгової Палати (ІСС) «Бізнес

проти контрафакції і піратства» (BASCAP), розробила широкий спектр рекомендацій з ІВ для надання інформації з практичних заходів, які можуть взяти підприємства та інші організації для більш ефективного корпоративного управління своїми авторськими правами, торговельними марками та іншими об'єктами ІВ. Див.: <http://www.iccwbo.org/bascap/index.html?id=24276>.

Цей Додаток до Рекомендацій з ІВ ІСС/BASCAP описує конкретні стратегії поведінки з контрафакцією і піратством при державному замовленні. Грунтуючись на загальних принципах і практичних пропозиціях, викладених у Рекомендаціях з ІВ, даний Додаток описує конкретні заходи, здійснюючи які, органи державної влади зможуть дотримуватися законодавства і захистити від контрафакції та піратства свою систему закупівель.

Останнім часом проблема масштабності та серйозності контрафакції та піратства в поставках при державній закупівлі знаходиться в центрі уваги. Дві урядові установи США, дослідивши проблему контрафактних товарів у сфері оборонних закупівель в 2010 р., встановили, що «практично все ризикує опинитися підробленим» [1] і висловили співчуття з приводу того, що «Міністерство оборони (DOD) не має наразі правил або особливих процедур для виявлення та протидії контрафакту. Існуючі процедури закупівлі та контролю якості, що використовуються для ідентифікації неякісних товарів, не мають достатніх можливостей, щоб виявити і запобігти появі контрафакту при закупівлях для потреб Міністерства оборони.

Дослідження Європейської комісії виявило 27 випадків потрапляння контрафактних медикаментів в законні поставки у період 2001-2005 років в Євросоюзі, де медикаменти часто замовляються безпосередньо органами державної влади чи медичними установами, що перебувають під контролем держави. В той же час, Всесвітня організація охорони здоров'я і ООН встановили, що в таких розвинених країнах підробленим є 1% від обороту ліків, ця статистика збільшується до 50% контрафактних медикаментів в країнах, що розвиваються і в продажах через Інтернет. [2]

Органи державної влади іноді широко використовують термін «контрафакт», включаючи в це поняття не тільки підробки, пов'язані з інтелектуальною власністю (такі як товари під фальшивими брендами та інші товари, вироблені або поставлені з порушенням торговельної марки, авторського права або інших об'єктів прав ІВ), але і браковані товари. [3] Даний документ, головним чином стосується державних закупівель товарів, які є контрафактними або піратськими в сенсі порушення прав інтелектуальної власності, але ці товари також регулярно виявляються і бракованими. Представлені в даному документі методики роботи з товарами, контрафактність яких обумовлена порушенням прав інтелектуальної власності, також будуть корисні в роботі з контрафактом у більш широкому сенсі при державних закупівлях.

Виявлено безліч контрафактної та піратської продукції, придбаної відділами закупівель органів державної влади, наслідком цього є ризики проілюстровані на наступних прикладах.

- **Електронні продукти та компоненти.**

Підроблені **роутери і їх компоненти** фірми Cisco, як з'ясувалося, були закуплені декількома урядовими агентствами США, включаючи Військово-повітряні сили, Морську піхоту, ВМС США, Федеральне авіаційне управління США, їх підрядниками в оборонній сфері, і, навіть, ФБР. Розслідування проводилося ФБР, у ньому брало участь п'ять інших урядових агентств США і Канади. У рамках розслідування було видано 36 ордерів на обшук і виявлено 3 500 контрафактних компонентів роутерів Cisco, оціночна роздрібна вартість яких склала більше 3,5 млн. дол. більш ніж за дворічний період 2006-2008. Було порушено більше 15 кримінальних справ, винесено 10 вироків. Це розслідування було частиною більш глобальної ініціативи ФБР, в рамках якої було конфісковано понад 400 екземплярів підроблених етикеток і мережевого устаткування Cisco, оціночна вартість яких склала понад 76 млн. дол. [4]

Рисунок 1. Підроблені мережеві адаптери
(ФБР, Розслідування ФБР: Роутери Cisco, <http://www.abovetopsecret.com/forum/thread350381/pg1>, виявлені Andover Network Liquidators, <http://www.andovercrg.com/services/cisco-counterfeit-wic-1dsu-t1.shtml>).



У державних закупівлях зустрічалися поставки іншої підробленої електроніки, такої як **мікропроцесори** для керуючого комп'ютера винищувача F15, **випромінювачі GPS** для бойових систем, **електронні підсилювачі, діоди і мікросхеми**. [5] Близько двох третин сумнівних і знайдених контрафактних деталей, про які повідомило Міністерство оборони США, включали в себе електронні елементи або деталі кріплення. [6]

Зазначені типи закупаваної контрафактної електроніки містять у собі різного роду ризики для органів державної влади, в інтересах яких проводяться закупівлі. Крім звичайної проблеми, яка полягає в тому, що такі компоненти не зможуть довго функціонувати або взагалі не зможуть працювати, контрафактна електроніка може давати недостатню продуктивність, невірні результати або навіть представляти серйозний ризик для безпеки тих, хто від неї залежить. Наприклад, як підкреслило Головне контрольне управління США (US General Accountability Office (GAO)), контрафактні системи GPS, встановлені у військових командних приладах, «можуть спричинити собою провал місії» [7] з очевидними ризиками для життя і здоров'я людей.

Ще більше занепокоєння викликає той факт, що контрафактна електроніка потенційно ставить під загрозу безпеку та інформаційні ресурси комп'ютерних систем органів державної влади. Розслідування ФБР виявило наступні ризики: потенційна можливість для користувачів отримувати дистанційний доступ до комп'ютерних систем, знижувати ефективність державних шифрувальних систем і виводити комп'ютерні системи з ладу. [8]

- **Придбання та використання комп'ютерного програмного забезпечення.** Іноді органи державної влади виявляють, що їм було поставлено контрафактне або піратське (тобто неліцензійне) програмне забезпечення або надані послуги підрядниками, які користуються таким програмним забезпеченням. Державний орган Шотландії закупив у постачальника контрафактні ліцензії на програму Microsoft Office, і опинився втягнутим у цивільний процес з виплатою компенсації у розмірі 42 500 фунтів, а крім того, у 2002 році змушений був придбати 470 додаткових ліцензій на використання програмного забезпечення на суму 102 229 фунтів. [9] У тому ж році контрафактне програмне забезпечення, встановлене на комп'ютерних системах вартістю 1,3 мільйона фунтів, було поставлено 10 Британським поліцейським відділкам та «Спеціальному підрозділу» Скотланд-Ярду. [10]

Органи державної влади, які отримують контрафактне і піратське програмне забезпечення або послуги у підрядників, які використовують таке програмне забезпечення, піддаються наступним ризикам:

- недоліки якості, надійності та продуктивності програмного забезпечення (Контрафактне програмне забезпечення частіше атакується вірусами, троянами та іншими хакерськими програмами),
- судові спори та штрафи, і
- неефективний контроль за інформаційними системами, ресурсами та коштами. [11]

- **Продукція оборонного призначення, засоби забезпечення безпеки та комплектуючі.** Найпоширенішим контрафактним товаром, що поставляється в рамках державних закупівель у сфері оборони і безпеки, є комплектуючі. Нещодавно уряд США розглянув проблеми Міністерства оборони США, пов'язані із закупівлею матеріалів і комплектуючих, і виявив, що були поставлені наступні види контрафактних товарів: **самоконтрящіся гайки**, титанові **авіаційні деталі**, алюмінієві **деталі для зброї і бойових машин**, герметичні **контейнери**

для мікрохвильових печей, компоненти для системи кондиціонування і навіть ремені безпеки. Також в рамках державних тендерів поставлялися підроблені автомобільні запчастини, включаючи **гальмові колодки**, зроблені з водоростей, і **бронезилети** нібито волокнистого матеріалу бренду Kevlar®. [12]

Головне контрольне управління США повідомило, що такі товари, компоненти та деталі можуть призвести до серйозного порушення поставок, затримці поточних місій, підриву цілісності збройних систем, поставити під загрозу цивільні та військові програми, спричинити матеріальні збитки, а також втрати в особовому складі.

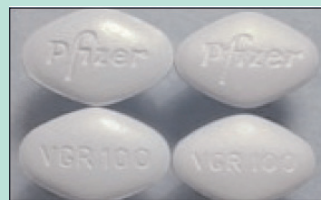
- **Медикаменти та медичне устаткування.** Навіть у тих державах, де постачання ліків та медичного обладнання регулюються на високому рівні, а їх закупівля і продаж здійснюється або фінансується державою, контрафакту все одно вдається пробратися в систему закупівель. «Усі види ліків підроблялися, як захищені торговельними марками, так і не захищені, починаючи від медикаментів для лікування хвороб, що загрожують життю, і закінчуючи недорогими аналогами патентованих знеболюючих і антигістамінних препаратів», повідомляє Всесвітня організація охорони здоров'я. [13]

Серед 1% контрафактних препаратів, які потрапили в європейські системи закупівель медикаментів за державної фінансової підтримки, були виділені наступні контрафактні препарати: ліки від **хвороб серця** та **інсульту** (Плавікс (клопідогрель)), **раку простати** (Casodex (бікалутамід)), **надлишку холестерину** (Lipitor), **ожиріння** (Reductil (Сибутрамін)), **астми** (Seretid) і **шизофренії** (Zyprexa (оланзапін)), не кажучи вже про препарати для лікування сексуальних дисфункцій, які продавалися через легальні традиційні канали постачання медикаментів та поза ними. Серед контрафактних медичних пристроїв, виявлених в Європі, були **лінзи для окулярів, контактні лінзи, продукти для регуляції функції сечового міхура, тест-смужки для визначення рівня глюкози, зубні філлери, міхури з льодом, голки для введення інсуліну** та навіть **набори експрес-тестів на ВІЧ**. [14]

Ризик для здоров'я і життя людини тут, на жаль, очевидний. Вміст контрафакту може бути небезпечним або може не мати активних інгредієнтів. В результаті їх застосування лікування може виявитися невдалим або в організмі може виробитися опір до легальних ліків, якщо вміст активних інгредієнтів в підробці занадто малий. Підробки навіть можуть стати причиною смерті. Контрафактні версії наркотичних ліків фентанілу і оксикодону призвели до безлічі смертей в США і Європі. [15]

На відміну від справжніх ліків, коли будь-які проблеми у виробничому процесі можуть бути виявлені і усунені відомим виробником, контрафактні медикаменти виготовляються з метою обману. Марсі Форман (Marcy Foreman), що займає посаду Директора Департаменту розслідувань Імміграційної і митної поліції США і працює з таким контрафактом, коротко торкнулася даного питання в ефірі БіБіСі (BBC): Основний момент полягає в тому, що виробниками контрафакту рухає «виключно жага наживи і жадібність». [16]

Рисунок 2. Контрафактні медикаменти.
Цей контрафактний препарат Viagra® був виявлений в Угорщині. Замість належного активного інгредієнту, ці підробки містили лише амфетамін – більш відомий як «спід». Пфайзер, Аналіз справи: Контрафактний склад (Pfizer, Case Study: Counterfeit Contents), <http://media.pfizer.com/files/products/CounterfeitContents.pdf>.



Методики закупівель та управління активами, описані в Рекомендаціях з ІВ ICC / BASCAP, корисні як для компаній, що працюють з товарами і послугами, заснованими на об'єктах ІВ, так і для органів державної влади, які прагнуть виявляти контрафактні і піратські товари та послуги, протидіяти їх закупівлям і відшкодувати збиток від таких закупівель.

Поряд з п'ятьма основними типами стратегій і процедур, представленими в Рекомендаціях з ІВ (робота з правилами, обізнаність, канали поставок, безпека та дотримання вимог законодавства), нижче описані заходи, які органи влади можуть вжити щодо своїх правил і методик закупівлі. Також далі розглянуті кілька наочних прикладів практики, що вже існує в деяких країнах. Посилання на свіжі рекомендації органам влади, підготовлені на тлі зростаючої в усьому світі стурбованості проникненням контрафакту в поставки для державних потреб, також представлені далі.

1. Політика держави

Закон повинен чітко говорити про те, що поставка і використання контрафактних товарів у зв'язку з державними закупівлями незаконні. Чітка державна політика, узгоджена між відповідними міністерствами, надзвичайно важлива.

Рекомендації

- 1.1 Нелегальність контрафакту.** Складається враження, що в деяких країнах поставка контрафактної продукції та компонентів за державним замовленням не є такою вже незаконною. Наприклад, у Німеччині, Іспанії та Литві є особливе законодавство, яке забороняє контрафактні медикаменти, але більшість держав Євросоюзу, маючи справу з контрафактом, задовольняються уривками із законів про інтелектуальну власність і про реєстраційні посвідчення лікарських засобів. [17] Дуже важливо, щоб законодавство про закупівлі містило окрему і чітку заборону на постачання всіх видів контрафактної продукції та компонентів.
- 1.2 Форма заборони.** Правило, що забороняє контрафакту брати участь у тендерах, може бути виражено у формі простої заборони на участь в тендерах будь-яких товарів, компонентів або інших матеріалів, придбання або використання яких може порушити права ІВ третіх осіб. В якості альтернативи така вимога може бути окремо згадана у більш загальних правилах про дотримання законодавства або про боротьбу з шахрайськими діями, які містять заборону на участь у тендерах товарів, чия автентичність, історія, джерело походження або якість були сфальсифіковані. Також необхідна наявність адекватних і досить жорстких санкцій, щоб запобігти порушенню закону. Наприклад, китайський проект Правил застосування Закону про державні закупівлі передбачає такі санкції стосовно постачальника, який виставив підроблені товари на тендер: повернення незаконно отриманого прибутку, штраф, заборона на участь в тендерах від одного до трьох років, відкликання ліцензії на здійснення господарської діяльності або кримінальну відповідальність. [18]
- 1.3 Законне використання.** Внутрішні правила органів влади для департаментів і службовців повинні містити положення про неприпустимість придбання та / або використання контрафактних матеріалів, або матеріалів, які будь-яким іншим чином порушують права ІВ. Опис таких правил міститься у Рекомендаціях з інтелектуальної власності ICC / BASCAP та Додатку 1: Рекомендації Великої Вісімки для органів влади щодо використання програмного забезпечення з дотриманням прав інтелектуальної власності. Ще одне рекомендоване правило відповідає цим же принципам, воно виникло в результаті недавніх дискусій урядових установ США і полягає в тому, щоб до підрядників також пред'являлася вимога дотримуватися законодавства в сфері інтелектуальної власності при наданні послуг державі, наприклад, використовуючи тільки законне програмне забезпечення у своїй діяльності. [19]

1.4 Відповідальність та погодження дій. Державні закупівлі, за визначенням, вимагають участі і покладають обов'язки на цілий ряд міністерств і відомств. Необхідні також скоординовані дії всіх відповідних підрозділів, а також чітке розмежування сфер відповідальності за розробку необхідних правил і процедур. Це необхідно для того, щоб забезпечити єдиний підхід і максимальну ефективність виявлення контрафактних товарів, протидії їх закупівлям та відшкодування збитків від таких закупівель. Наприклад, Уряд США нещодавно скликав робочу групу з даного питання, яка складається з семи урядових установ і очолюється Адміністраторами Правил надання державних послуг та здійснення державних закупівель, координатором Білого дому з контролю за дотриманням прав інтелектуальної власності та Заступником Міністра оборони.

Особливому підрозділу в рамках Управління з контролю за обігом лікарських засобів і виробів медичного призначення Великобританії (the UK Government's Medicines and Healthcare Products Regulatory Agency (MHRA)) передали повноваження щодо розслідування та виявлення порушень, а також координації правоохоронної діяльності щодо контрафактних медикаментів і медичних пристроїв у законних і незаконних каналах поставок. Особливий підрозділ співпрацює з Міністерством праці та пенсій, співробітниками Міністерства торгових стандартів та іншими урядовими департаментами згідно комплексної Стратегії по боротьбі з контрафактом. [20]

2. Освіта та інформованість

Тренінги та інформування про правила та ризики роботи з контрафактом у сфері державних закупівель будуть корисні державним службовцям, підрядникам та суспільству в цілому.

Рекомендації

- 2.1 Інформованість службовців.** Однією з найважливіших умов, необхідних для зменшення розповсюдження контрафакту в сфері державних закупівель, є розуміння правил і ризиків, та здатність виявляти контрафактні товари. На запит Головного контрольного управління США (GAO) прийшли відповіді від кількох посадових осіб Міністерства оборони про те, що «персонал, відповідальний за збірку і ремонт обладнання, не навчений ідентифікації контрафактних деталей». З цією проблемою стала працювати команда співробітників міністерства, яка не тільки вивчає процеси та процедури зі зберігання, виявлення, обігу та розпорядження контрафактними деталями, а й розробляє тренінги та курси з метою підвищення обізнаності співробітників про контрафактні деталі і про методи їх виявлення. [21]
- 2.2 Інформування/попередження постачальників.** Рекомендації ICC / BASCAP з IB радять компаніям повідомляти постачальників про те, що компанія дотримується законодавства про інтелектуальну власність і очікує від них того ж. Органам влади буде також корисно інформувати своїх постачальників про це.
- 2.3 Інформування споживачів.** Органи влади вважають, що проведення тренінгів та інформування підрядників і споживачів про контрафактну продукцію, буде корисним щодо деяких типів товарів, що потрапляють у сферу державних закупівель, особливо медикаментів та медичних пристроїв. Наприклад, Управління з контролю за обігом лікарських засобів і виробів медичного призначення Великобританії (UK MHRA) не обмежується наданням лише фармацевтам інформації про ризики, пов'язані з контрафактною продукцією, і про те, як її визначати, а й розміщує на своєму сайті для попередження населення інформацію про конкретні контрафактні медикаменти, виявлені в каналах поставок у Великобританії. [22]

3. Управління каналом постачання

Контракти на поставку повинні передбачати заборони, гарантії та санкції, пов'язані з поставками і/або використанням контрафакту. Юридична перевірка підрядників у ланцюзі поставок може допомогти викоринити поставки контрафакту.

Рекомендації

- 3.1 Умови контракту.** Згідно з Рекомендаціями з IB ICC / BASCAP щодо питань договорів поставки в приватному секторі економіки, важливо, щоб державні тендери із закупівель і самі контракти включали особливі умови, присвячені ризикам, пов'язаним з контрафактною продукцією. Такими умовами можуть бути: заборони на постачання та / або використання контрафактної продукції, гарантії дотримання таких вимог та ефективні санкції щодо порушень цих вимог. Знову ж, ці вимоги можуть бути оформлені як окремі положення, присвячені інтелектуальній власності, а також в якості частини більш загальних положень про дотримання законодавства та протидію шахрайству.
- 3.2 Необхідні ліцензії.** У відповідних випадках сертифікати відповідності чи аналогічна документація, що надається державними постачальниками, також може включати копії або інші письмові докази наявності необхідних ліцензій чи інших прав ІВ, як викладено в Рекомендаціях з IB ICC / BASCAP.
- 3.3 Юридичний аудит.** Хоча такі інструменти, як реєстраційні свідоцтва для визначення надійних постачальників є загальноприйнятими в сфері закупівлі медикаментів, переваги використання перевірених постачальників часто недооцінюються в багатьох областях державних закупівель. Авіакосмічна галузь і галузь з виробництва електронних компонентів розробили корисні правила в цій сфері. Наприклад, розроблено стандарти, стимулюючи закупівлю компонентів у перевірених постачальників (тобто оригінальних виробників, схвалених дистриб'юторів та інших осіб, які погодилися дотримуватися правил і процедур, що лежать в основі стандартів, розроблених для скорочення обсягів контрафакту) та / або проведення юридичних перевірок щодо нових постачальників. Відповідно до цих принципів Міністерство оборони США прийняло Стандарти Системи статистичного аналізу AS5553 (SAS Standart AS5553). [23]

4. Управління активами та безпека

Контроль органів влади та постачальників за просуванням товару при поставках, адекватне управління активами, фізична та інформаційна безпека можуть знизити ризики і наслідки, пов'язані з контрафактним товаром.

Рекомендації

- 4.1 Контроль за просуванням товару.** Дивно, що не завжди можливо прослідкувати походження товарів і компонентів, які державні органи замовляють для своїх потреб. Такі правила, як описані вище SAS Стандарти AS5553 заохочують якісне управління підрядниками та деталями, а також облік у рамках ланцюга поставок з тим, щоб можна було відстежити будь-які товари або деталі аж до їхнього джерела. Це може допомогти як у протидії контрафакту, так і у відшкодуванні шкоди від контрафактної продукції. [24]
- 4.2 Управління активами, безпека.** В цілому, сумлінне внутрішнє управління і облік щодо товарів, компонентів і послуг, заснованих на об'єктах інтелектуальної власності, а також ефективна фізична та інформаційна безпека для запобігання несанкціонованого доступу та інших правопорушень, є найважливішими факторами в роботі органів влади та бізнесу щодо зниження

розповсюдження контрафакту і наслідків такого поширення. Рекомендації з IB ICC / BASCAP пропонують кілька типів корисних правил і процедур для таких цілей.

5. Додержання законності та аудит

Регулярний аудит товарів, що беруть участь в тендері, проведення розслідувань і переслідування виробників контрафакту, а також співробітництво з правоохоронними органами та бізнесом також є корисною практикою при роботі з контрафактом в рамках державних закупівель.

Рекомендації

- 5.1 Відповідність якості та аудит.** Урядові програми з закупівлі часто включають процедури підтвердження відповідності якості та перевірки поставлених товарів і компонентів, а також більш ретельні інспекції діяльності підрядників. Такі інспекції повинні включати перевірку наявності контрафактних деталей або компонентів і дій, які мало перешкоджають постачанню контрафакту. Міжнародний комітет з контролю за обігом наркотиків Організації об'єднаних націй рекомендує, наприклад, проводити «регулярні інспекції організацій, залучених у виробництво, торгівлю і дистрибуцію медикаментів». Аналогічні перевірки постачальників товарів і компонентів іншого типу можуть також знадобитися в разі підозри того, що контрафакт був або може бути поставлений.
- 5.2 Розслідування, правозастосування.** Гарні закони і процедури рідко бувають повністю ефективними без оперативних розслідувань і правозастосування проти правопорушень. Деякі державні органи організували особливі підрозділи в рамках їх департаментів із закупівель, які здійснюють розслідування і забезпечують відшкодування збитків, завданих такими правопорушеннями, як поставка контрафакту, наприклад, згадане вище Управління з контролю за обігом лікарських засобів і виробів медичного призначення Великобританії.
- 5.3 Співпраця з представниками бізнесу.** Бізнес, яким створюється більшість товарів, придбаних державою, володіє цінною інформацією про те, як розпізнати контрафактні товари та компоненти, джерела та схеми розповсюдження таких товарів, а також володіє готовими тренінгами і матеріалами, а також інформацією про правила і передові напрацювання, які можуть бути запозичені з метою виявлення контрафактних товарів, протидії контрафакції та відшкодування пов'язаних з нею збитків. У звіті Головного контрольного управління США (GAO) перераховані кілька приватних організацій, які можуть взяти участь у державно-приватному співробітництві з питань контрафактного товару при державних закупівлях, включаючи не тільки ICC / BASCAP, але також і Асоціацію космічної промисловості США (Aerospace Industries Association), Громадянську коаліцію електронної промисловості (Electronic Industry Citizenship Coalition), Міжнародну коаліцію по боротьбі з контрафактною продукцією (International Anti-Counterfeiting Coalition), Міжнародне товариство інженерів з автомобілебудування (SAE International), Асоціація напівпровідникової промисловості (Semiconductor Industry Association) та інші. [25]
- 5.4 Моніторинг/оновлення правил.** Виявлення контрафакту та інших незаконних товарів при державних закупівлях, протидія їх поставці та використанню, а також відшкодування збитків, пов'язаних з такими товарами, – це проблема, яка, на жаль, не може бути вирішена відразу. Якщо узагальнити рекомендації у відношенні правил щодо дотримання прав ІВ, представлених в Рекомендаціях з IB ICC / BASCAP, державам слід займатися постійним моніторингом своїх правил по боротьбі з контрафактною продукцією при державних закупівлях, виправляти недоліки і, в разі необхідності, час від часу допрацьовувати свої правила з тим, щоб переконатися в тому, що вони насправді працюють і дотримуються державними службовцями та постачальниками.

- ^[1] US Government Accountability Office, Report to Congressional Requesters, Defense Supplier Base: DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts, p. 2 (March 2010) («GAO 2010»), <http://www.gao.gov/products/GAO-10-389>; see also U.S. Department of Commerce, Defense Industrial Base Assessment: Counterfeit Electronics (Jan. 2010), http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf.
- ^[2] See, e.g., WHO, International Medical Products Anti-Counterfeiting Taskforce, <http://www.who.int/mediacentre/factsheets/fs275/en/index.html>.
- ^[3] SAE Aerospace Standard 5553, for example, defines a counterfeit part as a suspect part that is a copy or substitute without legal right or authority to do so or one whose material, performance, or characteristics are knowingly misrepresented by a supplier in the supply chain. By contrast, one US Defense Logistics Agency supply centre defines a part as counterfeit only when it misrepresented the part's trademark. (GAO 2010, p. 2).
- ^[4] J. Markoff, F.B.I. Says the Military Had Bogus Computer Gear, New York Times (9 May 2008), http://www.nytimes.com/2008/05/09/technology/09cisco.html?_r=1&ref=technology, citing ATSNNews, FBI Fears Chinese Hackers Have Back Door Into US Government & Military, <http://www.abovetopsecret.com/forum/thread350381/pg1>; US Dep't of Justice, Departments of Justice and Homeland Security Announce International Initiative Against Traffickers in Counterfeit Network Hardware (9 Feb. 2008), http://www.justice.gov/opa/pr/2008/February/08_crm_150.html.
- ^[5] GAO 2010, pp. 7-8.
- ^[6] GAO 2010, p. 7.
- ^[7] GAO 2010, p. 24.
- ^[8] Markoff 2008, ATS News 2008.
- ^[9] Cliff Saran, How a council got clobbered for software piracy, Computer Weekly (21 Jan. 2002), <http://www.computerweekly.com/Articles/2002/01/21/184723/How-a-council-got-clobbered-for-software-piracy.htm>.
- ^[10] Richard Alleyne, 'Pirated' software at Special Branch, Daily Telegraph (20 Nov. 2002), <http://www.telegraph.co.uk/news/uknews/1413725/Pirated-software-at-Special-Branch.html>; see also BBC, How Cyber Piracy Affects You (9 Apr. 2003), <http://news.bbc.co.uk/1/hi/uk/2924531.stm>.
- ^[11] BSA, Government Guide For Software Management, <http://www.bsa.org/~media/C72B329D6F7E4B46A7467DE0151210A1.ashx>
- ^[12] GAO 2010, pp. 25-26.
- ^[13] WHO, Counterfeit Medicines, <http://www.who.int/mediacentre/factsheets/fs275/en/index.html>.
- ^[14] A.C.P. de Bruijn, C.G.J.C.A. de Vries, H.P.H. Hermsen, Counterfeit medical devices: A risk indication, RIVM National Institute for Public Health and the Environment, Letter report 360060001/2009 (August 2009), <http://www.rivm.nl/bibliotheek/rapporten/360060001.pdf>.
- ^[15] Statement by Dr. P. Emafo, President of the International Narcotics Control Board, Third Global Congress on Combating Counterfeiting and Piracy (30-31 January 2007), http://www.wipo.int/enforcement/en/global_congress/docs/philippe_emafo.doc.
- ^[16] BBC, How Fake Drugs Got into the NHS, (3 Feb. 2009), <http://news.bbc.co.uk/1/hi/health/7865569.stm>.
- ^[17] Europe Economics, Compilation of Material Relating to Counterfeit Medicines (8 Jul. 2008), http://ec.europa.eu/health/files/counterf_par_trade/counterfeit_doc/11-11-2008/counterfeit-study-main-report_en.pdf.
- ^[18] See <http://lawprofessors.typepad.com/.../government-procurement-regulations---draft-for-comment---1-11-10-en.pdf>.
- ^[19] See Executive Office of the President, 2010 Joint Strategic Plan on Intellectual Property Enforcement, pp. 7-8 (June 2010) («Use of Legal Software by Federal Contractors»), http://www.whitehouse.gov/sites/default/files/omb/assets/intellectualproperty/intellectualproperty_strategic_plan.pdf.
- ^[20] Medicines And Healthcare Products Regulatory Agency (MHRA), Anti-Counterfeiting Strategy 2007-2010, <http://www.mhra.gov.uk/home/groups/ei/documents/websiteresources/con2033156.pdf>.
- ^[21] GAO 2010, pp. 9-10.
- ^[22] MHRA, Guidance for Pharmacists: Counterfeit Medicines, http://www.mhra.gov.uk/home/idcplg?IdcService=GET_FILE&dDocName=CON2023831&RevisionSelectionMethod=LatestReleased; MHRA, Counterfeit Medicines and Devices, <http://www.mhra.gov.uk/Safetyinformation/Generalsafetyinformationandadvice/Adviceandinformationforconsumers/Counterfeitmedicinesanddevices/index.htm>.
- ^[23] See SAE, Standard AS5553, Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition, <http://standards.sae.org/as5553>; TechAmerica, Engineering Bulletin TB-0003, http://www.techstreet.com/standards/TechAmerica/TechAmerica_TB_0003?product_id=1608325; SAS, DOD adopts SAE's AS5553 standard on counterfeit electronic parts (14 Oct. 2009), <http://www.sae.org/mags/aem/7058>.
- ^[24] See Phil Zulueta, Counterfeit Electronic Parts, Avoidance, Detection, Mitigation and Disposition: AS5553 Standards Development Progress (Oct. 2008), http://supplychain.gsfc.nasa.gov/2008/SC2008-Zulueta_a.pdf.
- ^[25] GAO 2010, pp. 15-18.

Будь ласка, завітайте на веб-сайт BASCAP для отримання оновленої копії Рекомендацій з ІВ:
www.iccwbo.org/bascap

Бізнес проти контрафакції і піратства – це бізнес-ініціатива, яку створив, очолив та профінансував міжнародний бізнес, в тому числі власники відомих брендів, і яка була організована Міжнародною торговою палатою для підвищення політичної та громадської уваги до проблеми контрафакції і піратства, спонукання держави до дій та поширення поваги до інтелектуальної власності.

Для того, щоб дізнатись більше про BASCAP, будь ласка, зв'яжіться з:

Jeffrey P. Hardy

Coordinator, BASCAP

E-mail: bascap@iccwbo.org

BASCAP Initiative Group in Ukraine

Business Action to Stop Counterfeiting and Piracy

Наталія Мещерякова

Голова Ініціативної групи BASCAP в Україні

E-mail: n.meshcheriakova@bascap.com.ua

04071, Київ

Вул. Рейтарська 19Б

Тел.: +380 44 361 12 78

Факс: +380 44 361 14 49

bascap@bascap.com.ua

<http://bascap.com.ua>

© 2008, 2011 Опубліковано у березні 2011 Міжнародною торговою палатою (ICC)

© Photographer: Putnik | Agency: Dreamstime.com, оформлення, обкладинка

© Due Diligence & Intelligence Intellectual Property Agency (www.ddiip.com), український переклад

Всі права захищені. Жодна з частин цього тексту не може бути відтворена чи скопійована в якій би то не було формі і якими б то не було засобами, - графічними, електронними, механічними, включаючи фотозйомку, сканування, грамзапис, друк або інші пристрої для відтворення інформації, та з будь-якими намірами без письмової згоди Міжнародної торгової палати.

International Chamber of Commerce

38 Cours Albert 1er, 75008 Paris, France

Tel +33 (0)1 49 53 28 28 Fax +33 (0)1 49 53 29 42

E-mail: icc@iccwbo.org

Website: www.iccwbo.org

ICC Publication No. 848

ISBN: 978-92-842-0060-3