центр громадських ініціатив [Електронний ресурс]. – Режим доступу: https: // docviewer.yandex.ua/?url =ya-serp%3A%2F%2 Fcivicexpert.in.ua %2Fupload% 2Ffile%2Freestr _expertiz% 2FEUCCI _CIVIL_ EXPERTISE _REPORT. pdf&name= EUCCI_ CIVIL_ EXPERTISE _ REPORT .pdf&c =561b8701ee7b.

14 Закон України «Про Службу безпеки України» від 25 березня 1992 р. № 2229-XII // Відомості Верховної Ради України. – 1992. – № 27. – Ст. 382.

Рецензенти:
кандидат юридичних наук, старший науковий співробітник І. Касперський,
кандидат юридичних наук, старший науковий співробітник В. Шлапаченко

Аннотация: В статье рассматриваются вопросы, связанные с исследованием современных тенденций отнесения информации к категории служебной.

Ключевые слова: защита информации, информационная безопасность, утечка информации, информация с ограниченным доступом, служебная информация.

Abstract: The article deals with issues related to the research of current trends of information classification as service information.

Key words: information protection, information security, information leakage, classified information , service information.

УДК: 340:35.078.3

КРАВЧЕНКО Олександр Миколайович

НОВІ ПАРАДИГМИ СУЧАСНИХ ЗАГРОЗ КОМЕРЦІЙНІЙ ТАЄМНИЦІ

Постановка проблеми. Питання захисту інформації представляє собою сукупність тісно пов'язаних проблем в галузях права, організації управління, розробки технічних засобів, програмування і математики. Очевидно, що ефективну систему захисту можна створити, об'єднавши зусилля різних фахівців. Центральним завданням проектування систем

захисту є раціональний розподіл наявних людських, матеріальних та інших ресурсів [5].

Що ж стосується захисту комерційної таємниці, то тут, крім неюридичних заходів захисту (технічних, організаційних тощо), слід укладати договори про нерозголошення зі співробітниками та третіми особами, які можуть мати до неї доступ, заздалегідь передбачаючи дієві санкції за порушення зобов'язань щодо зберігання відповідної інформації.

Актуальність аналізу. Через посилення економічної конкуренції в умовах розвитку ринкових відносин в Україні комерційна таємниця суб'єктів господарювання та її охорона набувають пріоритетного значення. Розвиток економічної конкуренції, необхідність досягнення переваги на ринку ставлять перед суб'єктами господарювання завдання захисту комерційної таємниці за допомогою правових засобів.

Аналіз досліджень. В основу написання статті покладено ґрунтовний аналіз сучасних загроз комерційній таємниці.

Основною **метою** цієї **статті** є визначення найбільш актуальних сучасних загроз комерційній таємниці та протидія їм.

Виклад основного матеріалу. У чинному законодавстві зазначено, що кожна юридична особа має у власності інформацію про себе та може встановлювати порядок її отримання іншими особами. Так, згідно зі статтею 36 Господарського кодексу України підприємство має право визначати склад та обсяг відомостей, що становлять комерційну таємницю, і порядок їх захисту [1]. У статтях 231 і 232 Кримінального кодексу України вказано, що незаконне збирання та розголошення комерційної таємниці тягне за собою кримінальну відповідальність [2]. Однак комерційною таємницею може бути не вся інформація. Виключний перелік відомостей міститься в Постанові Кабінету Міністрів України «Про перелік відомостей, що не становлять комерційної таємниці». На жаль, він включає майже всі документи, що містять інформацію про діяльність фірми [3]. Проте вся інформація, яка не може становити комерційної таємниці, може бути визначена як конфіденційна. Фірма має право самостійно визначати порядок передачі конфіденційної інформації іншим особам, тому режим її захисту на фірмі може бути тотожним режимові захисту комерційної таємниці.

Для введення режиму захисту комерційної таємниці та конфіденційної інформації наказом керівника фірми необхідно затвердити Положення про комерційну таємницю та Положення про конфіденційну інформацію, з якими працівники фірми повинні бути ознайомлені під особистий підпис.

Введення режиму захисту комерційної таємниці та конфіденційної інформації надає фірмі такі переваги:

– представники контролюючих органів змушені будуть надсилати

детальні письмові запити на отримання тих чи інших документів чи відомостей з обґрунтуванням необхідності їх отримання. На будь-які усні запити з приводу надання інформації можна буде відповісти відмовою на тій підставі, що інформація, яка є конфіденційною або становить комерційну таємницю, надається лише на письмові запити;

– працівники фірми матимуть законну підставу для відмови від спілкування з представниками контролюючих органів, оскільки підписали зобов'язання про нерозголошення відомостей, які є конфіденційною інформацією або комерційною таємницею, а відтак нестимуть відповідальність за їх порушення;

– у такий спосіб можна обмежити коло спілкування перевіряючих лише зі спеціально визначеними особами, а отже, уникнути множинності варіантів відповідей з боку працівників фірми на запитання перевіряючих. Керівник фірми зможе попередити поширення працівниками інформації про діяльність установи і таким чином захиститися від конкурентів.

Нині з розвитком і повсюдним поширенням ІТ, як для окремих компаній, так і для цілих галузей економіки, інтелектуальна власність часто має більшу цінність, ніж власність традиційна – нерухомість, земля, машини. На щастя, багато власників бізнесів (і, напевно, всі власники успішних бізнесів) усвідомили цей факт і приділяють значну увагу безпеці своїх компаній у сфері інтелектуальної власності. При цьому захист вимагається як від зовнішніх, так і від внутрішніх загроз.

Зрозуміло, стратегії захисту інтелектуальної власності компаній в однакових сферах відрізняються. Так, більшості компаній, для яких створення об'єктів інтелектуальної власності не є предметом основної діяльності (торгівля матеріальними товарами, надання не ІТ-послуг та інші), варто сфокусувати увагу на захисті своїх торговельних марок, комерційних найменувань і, звичайно, комерційної таємниці. При цьому слід проводити періодичний моніторинг ринку насамперед щодо основних конкурентів з метою своєчасного виявлення (або, якщо можливо, навіть попередження) порушення і намагатися врегулювати проблемні питання у рамках позасудових (досудових) процедур. Необхідно пам'ятати, що чим більша компанія і ширший спектр її товарів/послуг, тим складніше вчасно реагувати на недобросовісну конкуренцію та доцільніше залучати до таких процесів зовнішніх фахівців (юридичні фірми). Як відомо, такі фірми мають можливість сконцентрувати окремих спеціалістів на тих напрямках, які вкаже клієнт, тоді як in-house юристи змушені займатися паралельно багатьма рутинними справами і не завжди можуть оперативно реагувати на «нештатні ситуації». У разі замовлення розробки логотипів, реклами, сайтів важливо приділяти особливу увагу

договорам із відповідними дизайн-студіями, рекламними агентствами. Останні можуть (навмисно чи ні) порушити при такій розробці права інтелектуальної власності інших осіб, внаслідок чого «підставити» компанію-замовника. Тому для керівництва важливо максимально убезпечити себе від таких випадків ще на стадії укладання договору.

Особливу ж увагу захисту інтелектуальної власності повинні приділяти компанії, що виробляють інтелектуальний продукт – програмне забезпечення, веб-сайти, рекламу, фільми тощо. Адже в цьому випадку порушення їх прав – це не просто упущена вигода, але часто й втрата результатів праці, а то й втрата бізнесу в цілому. Тому для компаній такого типу охорона їх інтелектуальної власності, як від зовнішніх загроз, так і загроз всередині компанії, повинна мати пріоритет не менший, ніж створення інтелектуального продукту. І якщо в питанні захисту від зазіхань ззовні необхідно, як і при захисті своїх торговельних марок, моніторити можливі порушення та вчасно на них реагувати, то про захист інтелектуальної власності компанії всередині неї самої потрібно дбати іншим чином, причому ще до початку створення якогось продукту. Варто враховувати, що безпосередніми творцями інтелектуальних продуктів є конкретні люди – автори, а не компанії в цілому.

Щоб урівноважити права й інтереси обох сторін таких відносин, потрібно заздалегідь обрати оптимальну схему співпраці. Законодавство про авторське право захищає насамперед інтереси автора як творця продукту [4]. На практиці ж, однак, автор часто виступає в ролі виконавця замовлення, і замовник, який заплатив за створення певного продукту, повинен мати можливість комерціалізувати такий продукт. Тому важливо знайти оптимальний баланс між інтересами роботодавців (замовників) і співробітників (виконавців). Потрібно заздалегідь обрати оптимальну схему співпраці (у рамках трудових або цивільно-правових відносин) із конкретними людьми та відповідний тип договору, що дозволяє замовнику використовувати в необхідному обсязі плоди праці виконавця.

Кожна з можливих форм співпраці має свої переваги і недоліки. Наприклад, якщо трудовий договір можна назвати кращим з точки зору саме захисту прав компанії-роботодавця на виготовлений співробітником продукт, то цивільно-правовий договір про створення за замовленням і використання об’єкта права інтелектуальної власності позбавить замовника від податкових, трудових та інших клопотів. Вибір оптимальної форми співпраці бажано заздалегідь обговорити з фахівцем, який підкаже, які плюси й мінуси різних форм у кожному конкретному випадку, а також допоможе скласти зразки відповідних договорів, котрі можна буде використовувати як стандартні в подальшій діяльності.

Звичайно, складно говорити про якийсь універсальний рецепт захисту інтелектуальної власності будь-якої компанії. Адже якщо для наукомістких виробництв ключовим аспектом є охорона винаходів, то для ІТ-компаній важливий передусім захист авторських прав, а правові режими цих об'єктів права інтелектуальної власності мають багато відмінностей. Однак одне правило все ж можна назвати загальним для всіх: зазвичай, простіше запобігти (або хоча б мінімізувати ризики) порушенню своїх прав, ніж захищати їх згодом.

Що може створювати небезпеку для бізнесменів чи комерсантів, зацікавлених, зрозуміло, в дотриманні комерційної таємниці? Як правило, це:

– розвідувальна діяльність конкурентів;

– несанкціоновані дії співробітників власної фірми;

– неправильна політика фірми в галузі безпеки.

Інформація, що представляє інтерес при збиранні та аналізуванні відомостей:

Відомості комерційного змісту:

– статутні документи фірми;

– зведені звіти з фінансової діяльності фірми (щомісячні, квартальні, річні, за кілька років);

– кредитні договори з банками;

– договори купівлі та продажу;

– відомості про перспективні ринки збуту, джерела коштів або сировини, товари та вигідних партнерів;

– будь-яка інформація, надана партнерами, якщо за її розголошення передбачені штрафні санкції;

– дані про конкурентів, їх слабкі та сильні сторони;

– умови фінансової діяльності;

– технологічні секрети;

– заходи, які вживаються конкурентами щодо своїх супротивників;

– дані про потенційних партнерів, перевірка їх на недобросовісність;

– інформація про місце зберігання вантажів, часу і маршрутах їх перевезення;

– виявлення вразливих ланок серед співробітників;

– виявлення осіб, перспективних для вербування шляхом підкупу, шантажу чи іншого методу;

– зв'язки і можливості керівництва;

– виявлення кола постійних відвідувачів.

Відомості особистого характеру:

– джерела доходів;

– істинне ставлення до тих чи інших суспільних явищ, «сильних світу цього»;

– уклад в особистому житті керівника та членів його сім'ї;

– розклад та адреси зустрічей – ділових та особистих;

– дані про розміри фінансового благополуччя;

– інформація про людські слабкості;

– згубні пристрасті;

– шкідливі звички;

– сексуальна орієнтація;

– дані про друзів, подруг, місцях проведення дозвілля, способах і маршрутах пересування;

– інформація про місця зберігання цінностей;

– місце проживання;

– подружня невірність;

– проблеми батьків і дітей.

Необхідно відзначити, що безпека як система заходів вимагає забезпечення необхідного рівня захищеності з таких напрямків захисту:

– від організованої злочинності;

– від порушень закону;

– від недобросовісної конкуренції.

Ці напрями реалізуються на ділянках:

– виробничої діяльності;

– комерційної діяльності;

– інформаційного забезпечення;

– кадрового забезпечення;

– страхування;

– та інших.

На сьогодні найбільш типовими формами і методами економічного шпигунства є:

– підкуп або шантаж співробітників фірми – 40 %;

– знімання інформації з ПЕОМ спецтехнікою (проникнення в бази даних, копіювання програм) – 30 %;

– копіювання або розкрадання документів, креслень, експериментальних і товарних зразків – 10 %;

– прослуховування телефонних розмов, підслуховування розмов у приміщеннях і автомобілях – 20 %.

Цікаво порівняти результати цього опитування з думкою групи експертів країн Європейського співтовариства про форми і методи несанкціонованого доступу до комерційних секретів конкуруючих фірм:

– підкуп або шантаж співробітників фірми, впровадження туди своїх агентів – 45 %;

– знімання інформації з ПЕОМ спецтехнікою – 30 %;

– копіювання або розкрадання документів, креслень, експериментальних і товарних зразків – 5 %;

– прослуховування і підслуховування – 15 %;

– інші способи – 5 %.

Як бачимо, висновки близькі один одному.

Що ж стосується умов, які сприяють витоку комерційних секретів фірм, маємо такі результати:

– балакучість співробітників, особливо у зв’язку зі споживанням алкоголю і в дружніх компаніях – 40 %;

– прагнення співробітників заробити гроші будь-яким способом – 15%;

– відсутність служби безпеки фірми – 15 %;

– звичка співробітників «ділитися передовим (іншим) досвідом», давати поради стороннім – 10 %;

– безконтрольне використання інформаційних і копіювальних засобів на фірмі – 10 %;

– психологічні конфлікти між співробітниками, між співробітниками і керівництвом, набір випадкових людей, здатних «продатися» або «помститися» – 10 %.

Отримати достовірну інформацію про діяльність фірми незаконним

шляхом малоймовірно, якщо фірма з розумінням ставиться до збереження комерційної таємниці та створення відповідної системи захисту. У той же час багато під безпекою розуміють перш за все фізичну захищеність, іноді включаючи окремі вимоги інформаційного захисту комерційних інтересів, що не сприяє вирішенню проблем безпеки в комплексі.

Офіс звичайної сучасної фірми або банку являє собою насичені електронікою приміщення, де інформація, що представляє собою комерційну таємницю, може перебувати на паперових та магнітних носіях, передаватися телефоном, факсом, електронною поштою, оброблятися, зберігатися і розповсюджуватися засобами обчислювальної техніки, записуватися й відтворюватися.

Нарешті інформація присутня в повітряному середовищі у вигляді акустичних сигналів при переговорах.

Існують загрози нанесення збитків системам обробки даних, що викликаються фізичними впливами стихійних природних явищ, які не залежать від людини. Однак найбільш широке і небезпечне коло штучних загроз, викликаних людською діяльністю, серед яких, виходячи з мотивів, можна виокремити:

– ненавмисні загрози, викликані помилками в проектуванні, в діях обслуговуючого персоналу, програмному забезпеченні, випадковими збоями в роботі засобів ПЕОМ і ліній зв'язку, енергопостачання, упущеннями користувачів, впливом на апаратуру фізичних полів тощо;

– навмисні загрози, зумовлені несанкціонованими діями обслуговуючого персоналу та несанкціонованим доступом до інформації сторонніх осіб.

Результатом реалізації загроз інформації може бути:

– втрата (руйнування, знищення);

– витік (витяг, копіювання, підслуховування);

– спотворення (модифікація, підробка);

– блокування.

Найбільш типовою природною загрозою в системах обробки даних, не завжди пов'язаної з діяльністю людини, є пожежа. Тому при проектуванні та експлуатації систем обробки даних в обов'язковому плані вирішуються питання протипожежної безпеки. Особливу увагу при цьому слід приділити захисту від пожежі носіїв комп'ютерних даних, серверів, окремих ПЕОМ, центрів зв'язку, архівів та іншого устаткування і приміщень, де сконцентровані величезні масиви дуже важливої інформації. Для цих цілей можуть бути використані спеціальні вогнетривкі сейфи, металеві шафи, контейнери тощо.

Інша загроза для систем обробки даних в комп'ютерних системах – удари блискавки. Ця проблема виникає не часто, але збитки можуть бути нанесені дуже великі. Причому не стільки матеріальні, а пов'язані з ремонтом або заміною техніки, що вийшла з ладу, і відновленням втраченої ін-

формації, яка циркулює в комп'ютерних мережах. Але перш за все, якщо не вжито необхідних технічних заходів захисту від потужних електромагнітних випромінювань грозових розрядів, виходять з ладу окремі робочі станції або сервери мережі, й на значний час паралізується робота об'єкта, всі операції припиняються. Фірма і особливо банк у такій ситуації втрачає свій імідж надійного партнера і, як наслідок, клієнтів.

Для більшості організацій втрата імені, поява будь-яких чуток про внутрішні проблеми є багато в чому неприємнішими від фінансових збитків, часом навіть і досить відчутних.

Для будівель, де розміщуються технічні засоби обробки інформації, розташованих в долинах річок або на узбережжі, досить імовірною загрозою є затоплення. У цих випадках апаратні кімнати не повинні знаходитися на нижніх поверхах будівель, необхідно вживати й інших запобіжних заходів.

Заподіяння збитків ресурсам систем обробки даних може також бути викликане землетрусами, ураганами, вибухами газу та технічними аваріями, наприклад, при раптовому відключенні електроживлення.

Загрози, пов'язані з діяльністю людини, можуть виявлятися в системі обробки інформації в результаті:

– несанкціонованого використання штатних технічних і програмних засобів, а також їх розкрадання, псування, руйнування;

– використання спеціальних засобів, що не входять до складу системи обробки даних (побічні випромінювання, наведення по ланцюгах напруги, використання апаратури звукопідсилення, прийом сигналів з ліній зв'язку, акустичні канали);

– використання спеціальних методів і технічних засобів (фотографування, електронні закладки, передавальні засоби, що руйнують або спотворюють оброблювану або мовну інформацію);

– опромінення технічних засобів зондувальними сигналами, які можуть призвести до спотворення або руйнування інформації, а при значній потужності опромінень і до виведення з ладу апаратури.

Зарубіжні фахівці до числа найбільш імовірних каналів витоку конфіденційної інформації відносять такі:

– спільна діяльність з іншими фірмами;

– ведення переговорів;

– екскурсії та відвідування фірми;

– реклама, публікації у пресі, інтерв'ю;

– консультації сторонніх фахівців, які отримують доступ до документації та виробничої діяльності;

– фіктивні запити про можливість роботи у фірмі, укладення з нею угод, здійснення спільної діяльності;

– розсилка окремим співробітникам різних анкет і запитальників під маркою наукових або маркетингових досліджень;

– приватні бесіди зі співробітниками фірми, нав'язування їм незапланованих дискусій з тих чи інших проблем.

Аналіз системи захисту комерційних секретів, моделювання ймовірних загроз дозволяє намічати (при необхідності) додаткові заходи безпеки. При цьому ступінь їх доцільності визначається досить просто: витрати на забезпечення належної секретності повинні бути меншими за можливі економічні збитки.

Однак, як образно висловився один експерт, «ступінь надійності будь-якого шифру визначається не його складністю, а непідкупністю шифрувальника». Іншими словами, ключовими фігурами систем захисту комерційних секретів є співробітники фірми. Причому не тільки ті, які працюють із закритою інформацією (хоча ця категорія в першу чергу). Рядовий співробітник, який не має доступу до комерційної таємниці, теж може надати допомогу конкурентам у проведенні електронного шпигунства, забезпечити умови для розкрадання носіїв інформації, для вивідування, зняття копій.

На думку зарубіжних фахівців, імовірність витоку відомостей, що становлять комерційну таємницю, при проведенні таких дій, як підкуп, шантаж, переманювання співробітників фірми, впровадження своїх агентів, становить 40 %; отримання відомостей шляхом їх вивідування у співробітників – 20 %.

Західні фахівці з економічної безпеки вважають, що від правильного добору, розстановки і стимулювання персоналу збереження фірмових секретів залежить, як мінімум, на 80 %.

Американський психолог А. Маслоу виділяє у людини п'ять груп основних потреб, а саме:

– фізіологічні;

– забезпечення безпеки;

– спілкування й контакти з іншими людьми;

– суспільне визнання своєї значущості, придбання, можливо, більш високого соціального статусу;

– самореалізація [6].

Знаючи цей науково встановлений факт, грамотний керівник будь-якої фірми повинен так організовувати роботу, щоб кожен співробітник отримував від роботи максимальне задоволення (повертаючись в цьому зв'язку до проблеми підбору персоналу зазначимо, що найбільше задоволення людина отримує від тієї діяльності, яка максимально відповідає її здібностям та інтересам).

Створюючи умови для задоволення співробітником потреб в самореалізації, суспільному визнанні його значущості, можна в рамках фірми встановити такий сприятливий соціально-психологічний клімат, який дасть змогу максимально зменшити плинність кадрів. У такій обстановці малоймовірна поява працівника, котрий намагатиметься самоствердитися шляхом передачі

конкурентам секретів, тобто шляхом зради.

Виходячи зі сказаного, необхідно в роботі з персоналом керуватися наступними правилами:

– створити дієву систему матеріальних стимулів;

– забезпечити кожного співробітника довготривалою роботою;

– ставитися до них як до самостійних індивідів;

– забезпечити участь у прибутках;

– створити можливості для просування по службі;

– залучати персонал до вирішування виробничих проблем;

– створити гнучку систему звільнень.

Крім того, американські фахівці в галузі протидії промисловому шпигунству рекомендують використовувати будь-яку можливість для пропаганди програм забезпечення економічної безпеки фірми; не забувати періодично винагороджувати співробітників фірми за успіхи в цій роботі; всіляко стимулювати участь співробітників фірми у реалізації програм забезпечення секретності.

Висновки. Кожен комерційний об'єкт повинен будувати свою систему захисту інформації на концептуальній основі, виходячи з призначення об'єкта, його розмірів, умов розміщення, характеру діяльності, фінансових можливостей тощо. При розробці концепції захисту необхідно виходити з детального аналізу напрямків діяльності підприємницької структури і комплексних вимог захисту. Особливо, якщо комерційні об'єкти застосовують у своїй діяльності засоби інформатизації.

Враховуючи різноманіття потенційних загроз інформації в системі обробки даних, складність структури і функцій, а також участь людини в технологічному процесі обробки інформації, вважаємо, що мета захисту комерційної таємниці може бути досягнута тільки шляхом створення системи захисту інформації на основі комплексного підходу. І починати цю роботу треба з оцінки загроз безпеки діяльності комерційного об'єкта, а виходячи з отриманих результатів аналізу, приймати рішення про побудову всієї системи захисту комерційної таємниці.

Таким чином, можна зробити висновок, що персонал фірми, з одного боку, є найважливішим ресурсом підприємницької діяльності, а з іншого – пам'ятати, що деякі співробітники в силу різних обставин можуть стати джерелом великих втрат і навіть банкрутства фірми. Саме тому організаційні й адміністративні заходи захисту комерційної таємниці необхідно поєднувати з соціально-психологічними заходами, серед яких можна виділити два основних напрямки: це, по-перше, правильний підбір і розстановка кадрів, по-друге, використання матеріальних та моральних стимулів.

Список використаних джерел

1 Господарський кодекс України // Голос України. – 2003. – № 49.

2 Кримінальний кодекс України від 5 квітня 2001 р. // Відомості Верховної Ради України. – 2001. – № 25–26. – Ст. 131.

3 Постанова Кабінету Міністрів України «Про перелік відомостей, що не становлять комерційної таємниці» від 9 серпня 1993 р. [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/611-93-п.

4 Цивільний кодекс України // Голос України. – 2003. – № 45.

5 Організаційно-правові основи охорони комерційної таємниці / укладачі В. І. Журавель, Т. Ю. Ткачук ; за заг. ред. О. Д. Довганя. – К. : НА СБ України, 2013. – 321 с.

6 Маслоу А. Мотивація і особистість / А. Маслоу. – СПб., 2002.

Рецензенти:
кандидат юридичних наук, доцент
Я. Журавель,
кандидат юридичних наук, доцент
Т. Ткачук

Аннотация: В статье исследованы актуальные вопросы современных угроз коммерческой тайны. Проанализировано многообразие потенциальных угроз коммерческой тайны в современном обществе. Определены направления совершенствования защиты коммерческой тайны. Цель защиты коммерческой тайны может быть достигнута только путем создания системы защиты информации на основе комплексного подхода.

Ключевые слова: информация с ограниченным доступом, коммерческая тайна, промышленный шпионаж, право интеллектуальной собственности, недобросовестная конкуренция, конфиденциальная информация.

Abstract: The article explores current issues of modern threats of a trade secret. It analyzes the diversity of potential threats to a trade secret in modern society. The ways of improving the protection of a trade secret are defined. The aim of protection of a trade secret can be achieved only by creating a system of information security based on an integrated approach.

Key words: classified information, a trade secret, industrial espionage, intellectual property right, unfair competition, confidential information.