останньому випадку передбачалося м'якше покарання, проте навіть повне сп'яніння не було причиною безвідповідальності [12, с.413]. Тяжким злочином проти особи було нанесення тілесних ушкоджень — усікання руки, ноги та інші шкоди тілу. Від них законодавець відрізняє образу дією — удар чашею, рогом, мечем у пах. Це діяння каралося ще суворіше, аніж легкі тілесні ушкодження, побої.

***Висновок.*** Отже, для образи в Київській Русі як і для сучасного злочину характерні певні елементи, які утворюють їхній склад. Тому і не дивно, що сучасні науковці під злочином за Руською Правдою розуміють образу. Проте в порівнянні з Кримінальним кодексом України 2001 р. елементи складу злочину в Руській Правді є мало виражені. Це і не дивно, бо Руська Правда є першим кодифікованим актом, в якому були присутні норми кримінального права, які послужили фундаментом для подальшого розвитку кримінального права.

**ЛІТЕРАТУРА:**


1. *Кульчицький В. С., Тищик Б. Й. Історія держави і права України: Підруч. для студ. вищ. навч. закл. — К.: Видавничий Дім «Ін Юре», 2008. - 624 с.*
2. *Терлюк І.Я. Огляд історії кримінального права України. Навчальний посібник. - Львів: Ліга-Прес, 2007. - 92 с.*
3. *Іванов В. М. Історія держави і права України: Навчальний посібник - К.: Атіка, 2007. – 728 с.*
4. *Заруба В. М. Держава і право Київської та Галицько-Волинської Русі (кінець VIII ст. — початок XIV ст.): Навчальний посібник. — К.: Істина, 2007. - 128 с.*
5. *Єрєгян А.Р. Поняття правопорушення в джерелах права Київської Русі // Право і суспільство. – 2010. - №6. – с.54-59.*
6. *Вакула І. Стадії вчинення злочину: історико-правовий аспект // Вісник Львівського університету. Серія юридична. – 2011. – Вип.53. – с.314-321*
7. *Кульчицький В., Тищик Б., Бойко І. Галицько-Волинська держава (1199—1349) / Монографія - Львів, 2005. – 280 с.*
8. *Єрєгян А.Р. Поняття злочину та покарання в джерелах права Київської Русі //Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка. – 2008. - №4.*
9. *Бурдін В.М. Особливості кримінальної відповідальності неповнолітніх в Україні: Монографія,- К.: Атіка, 2004. - 240 с.*
10. *Гончар Т.О. Неповнолітній як суб'єкт відповідальності за кримінальним правом України: дис. на здобуття наук. ступеня канд. юрид. наук: спец. 12.00.08. – Одеса, 2004.*
11. *Федорова А.Н. Правонарушение и юридическая ответственность по Русской Правде: автореферат дис. … к.ю.н. по спец. 12.00.01. – Казань, 2005. – 22 с.*
12. *Бурдін В. Кримінальна відповідальність за злочини, вчинені в стані сп'яніння (історичний аспект) // Вісник Львівського національного університету ім. Івана Франка. Серія юридична. - 2004. - Вип. 39. - с. 413-420.*



**УДК: 340+35.078.3**



**Чистоклетов Л.Г.**
*кандидат юридичних наук, доцент*


## ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА – ЯК СКЛАДОВА ЕКОНОМІЧНОЇ БЕЗПЕКИ : СУЧАСНІ РЕАЛІЇ ТА ЗАГРОЗИ


**У даній статті розглянуті найбільш актуальні питання інформаційної безпеки підприємства у сучасних умовах, акцентована увага на основних правових напрямках визначення комерційної таємниці на підприємстві, досліджено найбільш типові для сучасних реалій внутрішні та зовнішні загрози інформаційній безпеці бізнесу, а також встановлені найбільш поширені канали витоку конфіденційної інформації та можливі шляхи локалізації таких загроз.**



**Ключові слова:** *інформаційна безпека, комерційна таємниця, загрози безпеці бізнесу, витік інформації.*



**В данной статье рассмотрены наиболее актуальные вопросы информационной безопасности предприятия в современных условиях, акцентировано внимание на основных правовых направлениях определения коммерческой тайны на предприятии, исследовано наиболее типовые для современных реалий внутренние и внешние угрозы информационной безопасности бизнеса, а также установленные**

**наиболее распространены каналы утечки конфиденциальной информации и возможны пути локализации таких угроз.**
**Ключевые слова:** *информационная безопасность, коммерческая тайна, угрозы безопасности бизнеса, утечка информации.*

**In this article the most actual and widespread questions of information safety of enterprise are considered, attention is accented on basic legal directions of determination of commercial secret on an enterprise, investigated the most widespread for modern realities internal and external threats to information safety of business, and also set the most widespread sources of confidential information loss and the possible ways of the such threats localization.**
**Keywords:** *informative safety, commercial secret, threat business safety, information loss .*

***Постановка проблеми.*** Поняття «інформація» сьогодні вживається досить широко і різносторонньо. Важко знайти таку галузь знань, де б воно не використовувалося. Величезні інформаційні потоки буквально захлипають людей. Обсяг наукових знань, за оцінкою фахівців, подвоюється кожні п'ять років. З цього можна зробити висновок, що XXI століття буде інформаційним століттям.

Стабільне функціонування, зростання економічного потенціалу будь-якого підприємства в умовах шаленого розвитку інформаційних відносин багато в чому залежить від наявності надійної системи інформаційної безпеки. Дане і зумовлює **актуальність** наукових пошуків даного напрямку

***Аналіз останніх досліджень.*** Останнім часом наукові доробки з розв'язання різних проблем інформаційної безпеки бізнесу значно активізувались. Це зумовлена як потребами часу, адже ми є активними учасниками розвитку інформаційного суспільства, так і пріоритетними вимогами бізнесу, адже не володіючи достовірною, своєчасною, цінною тощо інформацією щодо різних аспектів функціонування підприємства, керівник, тай весь бізнес, вразливий до впливу як внутрішніх так і зовнішніх інформаційних загроз. Дослідженню окремих напрямків даної проблеми присвятили свої праці Ю. Бабенко, О. Бєліков, К. Бєляков, Ю. Мірошник, А. Марущак, О. Івченко, П. Пригунов, Д. Прокоф'єва та ін. Проте, такі питання як внутрішні загрози інформаційній безпеці підприємства та шляхи їх попередження залишаються мало дослідженні, потребують подальшого наукового осмислення питання конфіденційного та секретного діловодства на підприємстві як важливої складової системи інформаційної безпеки підприємства.

Мета дослідження**.** Виходячи з зазначеного, основною метою даної статті є визначення найбільш актуальних проблем формування системи інформаційної безпеки бізнесу у сучасних умовах.

Досягнення поставленої мети реалізовувалось через постановку та послідовне вирішення таких основних завдань:

- *обґрунтувати* правові напрямки визначення комерційної таємниці на підприємстві;
- *дослідити* основні загрози інформаційній безпеці підприємства;
- *встановити* канали витоку конфіденційної інформації та можливі шляхи локалізації таких загроз.

***Виклад основного матеріалу.*** Пріоритетним напрямком у процесі формування та забезпечення інформаційної безпеки будь-якої компанії є збереження в таємниці комерційно важливої інформації, що дозволяє успішно конкурувати на ринку виробництва та збуту товарів і послуг. Це, природно, вимагає конкретних дій, спрямованих на захист інформації з обмеженим доступом. Як свідчить вітчизняна і закордонна преса, кількість злочинів в інформаційній сфері не тільки не зменшується, але й має досить стійку тенденцію до росту.

Досвід показує, що для боротьби з цією тенденцією необхідна цілеспрямована організація процесу захисту інформаційних ресурсів. Причому в цьому повинні брати активну участь професіонали, адміністрація та співробітники, що і визначає значимість організаційної сторони питання.

Аналіз стану справ в сфері інформаційної безпеки свідчить, що на сьогоднішній день концепція і структура захисту інформації вже склалася, і її основу становлять:

– досить розвинутий арсенал технічних засобів захисту інформації;
– значна кількість фірм, що спеціалізуються на вирішенні питань захисту інформації;
– чітко окреслена система поглядів на цю проблему;
– наявність значного практичного досвіду тощо.

Досвід також показує, що:

– забезпечення безпеки інформації не може бути одноразовим актом. Це безперервний процес, що полягає в обґрунтуванні і реалізації найбільш раціональних методів, способів та шляхів удосконалювання і розвитку системи захисту, безперервному контролі її стану, виявленні її слабких місць та протиправних дій;
– безпека інформації може бути забезпечена лише за умови комплексного використання всього арсеналу наявних засобів захисту у всіх структурних елементах виробничої системи і на всіх етапах

технологічного циклу обробки інформації. Найбільший ефект досягається тоді, коли всі засоби, методи і заходи поєднуються в єдиний цілісний механізм – систему захисту інформації (СЗІ). При цьому функціонування системи повинно контролюватися, оновлюватися і доповнюватися залежно від зміни зовнішніх і внутрішніх умов;

– ніяка СЗІ не може забезпечити необхідного рівня безпеки інформації без належної підготовки користувачів і дотримання ними усіх установлених правил, спрямованих на її захист [1].

Систему захисту інформації можна визначити як сукупність спеціальних органів, засобів, методів і заходів, що забезпечують захист інформації від внутрішніх та зовнішніх загроз.

Перш ніж починати роботу над СЗІ необхідно визначитися, по-перше, яку інформацію слід відносити до конфіденційної інформації, а яку до комерційної таємниці.

Відповідно до статті 28 Закону України «Про інформацію» [2], інформацію поділяють за режимом доступу (на відкриту та інформацію з обмеженим доступом), а остання за своїм правовим режимом поділяється на конфіденційну, службову і таємну (ст. 30).

Відкрита інформація, окрім тієї, доступ до якої не може бути обмежено відповідно до згаданого Закону (ст. 29), здатна переходити до категорії конфіденційної за рішенням її власника або уповноваженої ним особи; відомості, які становлять конфіденційну або таємну інформацію, можуть належати до об'єктів права інтелектуальної власності; інформація, що визнана конфіденційною за рішенням її власника або уповноваженої ним особи, може також бути віднесена до категорії таємної у випадках, передбачених законодавством.

Закон України „Про інформацію" не містить чіткого розмежування понять конфіденційної інформації та комерційної таємниці. В цьому Законі не встановлено, в чому саме полягає особливість правового режиму інформації комерційного та банківського характеру, але однозначно встановлюється, що такі відомості не можуть бути конфіденційною інформацією.

Згідно зі статтею 505 Цивільного кодексу України [7], комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить. У зв'язку з цим, як зазначає вітчизняний дослідник О. Бєліков, такий вид інформації має комерційну цінність; вона є предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію. Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці [4].

Створення ефективної системи інформаційної безпеки є неможливим без **чіткого визначення загроз інформації, що охороняється**. Під загрозами інформації з обмеженим доступом прийнято розуміти потенційні або реально можливі дії стосовно інформаційних ресурсів, що призводять до неправомірного оволодіння інформацією.

Джерелами зовнішніх загроз є: несумлінні конкуренти; злочинні угруповання і формування; окремі особи та організації адміністративно-управлінського апарата.

Джерелами внутрішніх загроз можуть бути: адміністрація підприємства; персонал; технічні засоби забезпечення виробничої і трудової діяльності.

Фахівці встановлюють, в середньому, наступне співвідношення зовнішніх і внутрішніх загроз: 82% загроз створюються співробітниками фірми або за їх прямої або опосередкованої участі; 17% загроз виникає ззовні – зовнішні загрози; 1% загроз створюється випадковими особами [9].

***Основними загрозами інформації є її розголошення, витік і несанкціонований доступ до її джерел.***

З урахуванням викладеного залишається розглянути питання, які умови сприяють неправомірному оволодінню конфіденційною інформацією. В літературі вказуються наступні умови:

– розголошення (зайва балакучість співробітників) – 32%;

– несанкціонований доступ шляхом підкупу і схиляння до співробітництва з боку конкурентів і злочинних угруповань – 24%;

– відсутність на фірмі належного контролю і жорстких умов забезпечення інформаційної безпеки – 14%;

– традиційний обмін виробничим досвідом – 12%;

– безконтрольне використання інформаційних систем – 10%;

– наявність передумов виникнення серед співробітників конфліктних ситуацій – 8% [9].

***Розголошення інформації.*** Розголошення комерційних секретів, мабуть, найбільш розповсюджена дія власника (джерела), що призводить до неправомірного оволодіння конфіденційною інформацією за мінімальних витратах зусиль з боку зловмисника. Для цього він користується в основному легальними шляхами і мінімальним набором технічних засобів.

Реалізується розголошення формальними і неформальними каналами поширення інформації.

До формальних каналів поширення інформації належать:

– ділові зустрічі, наради, переговори та інші форми спілкування;

– обмін офіційними діловими, науковими і технічними документами засобами передачі офіційної інформації (пошта, телефон, телеграф, факс тощо.)

Неформальними каналами поширення інформації є:

– особисте спілкування (зустрічі, переписка, телефонні переговори тощо.);
– виставки, семінари, конференції, з'їзди, колоквіуми та інші масові заходи;
– засоби масової інформації (преса, інтерв'ю, радіо, телебачення тощо).

Як правило, причиною розголошення конфіденційної інформації є:

– слабке знання (або незнання) вимог захисту конфіденційної інформації;
– помилковість дій персоналу через низьку виробничу кваліфікацію;
– відсутність системи контролю за оформленням документів, підготовкою виступів, реклами і публікацій;
– злісне, навмисне невиконання вимог захисту комерційної таємниці.

Наведена нижче таблиця дає уявлення про фактори, що сприяють розголошенню комерційних секретів [9].

| № | **ФАКТОРИ** | % |
|---|---|---|
| 1. | Зайва балакучість співробітників | 32 |
| 2. | Прагнення співробітників заробляти гроші будь-якими способами і за будь-яку ціну | 24 |
| 3. | Відсутність на фірмі служби безпеки | 14 |
| 4. | "Радянські" звички співробітників фірми ділитися один з одним (тобто традиційний обмін досвідом) | 12 |
| 5. | Безконтрольне використання інформаційних систем | 10 |
| 6. | Наявність передумов для виникнення серед співробітників конфліктних ситуацій: відсутність психологічної сумісності, випадковий підбір кадрів. | 8 |

***Витік інформації*** загалом можна розглядати як неправомірний вихід конфіденційної інформації за межі організації або кола осіб, яким ця інформація була довірена.

Витік інформації за своєю суттю завжди припускає протиправне (таємне або явне, усвідомлене або випадкове) оволодіння конфіденційною інформацією, незалежно від того, яким шляхом це досягається.

Причини витоку полягають, як правило, у недосконалості норм щодо збереження комерційних секретів, порушенні цих норм, а також відступі від правил поводження з відповідними документами, технічними засобами, зразками продукції та іншими матеріалами, що містять конфіденційну інформацію.

Умови включають різні фактори і обставини, що складаються в процесі наукової, виробничої, рекламної, видавничої, звітної, інформаційної та іншої діяльності підприємства (організації) і створюють передумови для витоку комерційних секретів. До таких факторів і обставин можуть, наприклад, відноситися:

– недостатнє знання працівниками підприємства правил захисту комерційної таємниці і нерозуміння (або непорозуміння) необхідності їх ретельного дотримання;
– використання не атестованих технічних засобів обробки конфіденційної інформації;
– слабкий контроль за дотриманням правил захисту інформації правовими, організаційними та інженерно-технічними заходами;
– плинність кадрів, у тому числі які володіють інформацією, що становить комерційну таємницю.

Таким чином, значна частина причин і умов, що створюють передумови і можливість неправомірного оволодіння конфіденційною інформацією, виникають через недбалість керівників підприємств та їхніх співробітників.

***Несанкціонований доступ.*** Несанкціонований доступ (НД) можна визначити як сукупність прийомів і порядок дій з метою одержання (добування) охоронюваних даних протиправним шляхом.

До таких способів відносяться:

1. Таємне спостереження.
2. Підкуп службовця конкуруючої фірми або особи, що займається її постачанням.
3. Використання агента для одержання інформації.
4. Перехоплення телеграфних повідомлень.
5. Підслуховування телефонних переговорів.
6. Крадіжки креслень, зразків, документів тощо.
7. Шпигунство і вимагання.

До інших способів несанкціонованого доступу до інформації, які не порушують норм закону, але знаходяться на грані такої ситуації, можна віднести:

- Співбесіди про найм на роботу зі службовцями конкуруючих фірм (хоча опитувач зовсім не має наміру приймати дану людини на роботу).
- Так звані "помилкові" переговори з фірмою-конкурентом щодо придбання ліцензії, створення спільного підприємства, підписання партнерської угоди.
- Найм на роботу службовця конкуруючої фірми для одержання необхідної інформації.
- Працевлаштування «свого» працівника на підприємство-конкурента.

У закордонних матеріалах наводяться окремі показники співвідношення способів несанкціонованого доступу, зокрема:

| № | Спосіб НД | % |
|---|---|---|
| 1. | Підкуп, шантаж, переманювання службовців, впровадження агентів | 43 |
| 2. | Підслуховування телефонних розмов | 5 |
| 3. | Крадіжка документів | 10 |
| 4. | Проникнення в ПЕОМ | 18 |
| 5. | Знімання інформації з каналів зв'язку | 24 |

Аналіз наведених даних показує, що значна частина дій (2, 4, 5) реалізуються в кримінальній практиці за допомогою використання тих або інших технічних засобів і складають загалом 47% від загального їхнього числа. Це зайвий раз підтверджує небезпека технічних способів добування інформації в практиці здійснення підприємницької діяльності [5].

Перехід від абстрактного до конкретного захисту, звичайно, починається з виявлення та аналізу найбільш уразливих місць. Таким місцем, безумовно, є джерела, що містять інформацію конфіденційного характеру.

Джерелами інформації, що є комерційною таємницею, а, отже, потенційними джерелами витоку можуть бути:

***1. Документація*** *підприємства або просто документи (вхідні-вихідні, накази, бізнес плани, ділова переписка тощо).*

Важливою особливістю документів є те, що вони іноді є єдиним джерелом найважливішої інформації (наприклад, контракт, боргова розписка), а, отже, їхня втрата, викрадення чи знищення може завдати непоправної шкоди. Розмаїття форм і змісту документів за призначенням, спрямованістю, характером руху і використанням є досить привабливим джерелом для зловмисників, що, природно, привертає їхню увагу до можливості одержання цінної інформації. Важливим напрямком інформаційної безпеки у даному напрямку буде створення системи секретного та конфіденційного діловодства на підприємстві.

***2.*** *Робочий персонал або просто* ***особи*** *(до цього поняття належать усі без винятку працівники підприємства).*

Фізичні особи серед джерел конфіденційної інформації займають особливе місце як активний елемент, здатний виступати не тільки джерелом, але й суб'єктом зловмисних дій. Люди є і власниками, і розповсюджувачами інформації в рамках своїх функціональних обов'язків. Крім того, що вони мають інформацію, вони ще здатні її аналізувати, узагальнювати, запам’ятовувати, робити відповідні висновки, а також, за певних умов, ховати, продавати, змінювати тощо.

***3. Партнери, контрагенти або клієнти.*** Всі знають, що відносини між партнерами завжди мають правову форму. Зміст цих документів, у більшості випадків, містить для конкурентів цінну комерційну інформацію. Тому необхідно забезпечити конфіденційність таких документів, або ж передбачити відповідальність за протиправне розголошення змісту таких документів третім особам.

Забезпечити комерційну таємницю, що міститься в угодах з партнерами можна двома шляхами:

- включити до змісту договору окремі пункти про збереження комерційної таємниці, де передбачити, яка інформація становить комерційну таємницю, які підстави і порядок розголошення цієї інформації третім особам (контролюючим органам, судовим інстанціям, іншим підприємствам тощо), яка відповідальність за несанкціоноване розголошення комерційної таємниці;
- якщо ж відносини з партнерами і контрагентами носять тривалий і стійкий характер, то доцільним буде окремий договір (угода) про збереження комерційної таємниці, де більш детально буде розроблений режим збереження комерційної таємниці.

***4. Продукція підприємства або послуги, що надаються.*** Продукція є особливим джерелом інформації, за характеристиками якої досить активно полюють конкуренти. Особливої уваги заслуговує нова, що готується до виробництва продукція. Вважають, що для продукції існують визначені етапи "життєвого циклу": задум, макет, зразок, іспити, серійне виробництво, експлуатація, модернізація і зняття з виробництва. Кожний з цих етапів супроводжується специфічною інформацією, що виражається у вигляді різних фізичних ефектів, які можуть розкрити інформацію, яка охороняється

***5. Технічні засоби забезпечення виробничої діяльності.*** Технічні засоби як джерела конфіденційної інформації є широкою в інформаційному плані групою джерел. Засоби забезпечення виробничої діяльності можуть бути найрізноманітнішими, такі, зокрема, як телефони і телефонний зв'язок, телевізори і промислові телевізійні установки, радіоприймачі, радіотрансляційні системи, системи гучномовного зв'язку, підсилювальні системи, охоронні і пожежні системи тощо, котрі, за своїми параметрами, можуть бути джерелами перетворення акустичної інформації в електричні та електромагнітні поля, здатні утворювати електромагнітні канали витоку конфіденційної інформації.

***6. Непрямі джерела (сміття, реклама, публікації).*** Велика частина інформації добувається саме з непрямих джерел. Професійно проведена аналітична робота дозволяє іноді одержати чудовий результат. Крім того, цьому джерелу, звичайно, не надається особливої уваги а, отже, він найбільш доступний. Наприклад, відходи виробництва, що називається непридатний матеріал, можуть багато чого розповісти про використовувані матеріали, їхній склад, особливості виробництва, технології. Тим більше їх одержують майже безпечним шляхом на смітниках, місцях збору металобрухту, у кошиках кабінетів. Вмілий аналіз цих "відходів"

може багато чого розповісти про секрети виробництва. Публікації - це інформаційні носії у вигляді найрізноманітніших видань: книги, статті, монографії, огляди, повідомлення, рекламні проспекти, доповіді, тези тощо, в яких Ви можете, самі того не бажаючи, розкрити всі таємні секрети.

Джерела конфіденційної інформації дають повні зведення про склад, зміст і напрямок діяльності підприємства (організації), що досить цікаво для конкурентів. Природно, що така інформація їм вкрай необхідна, і вони докладуть усіх зусиль, знайдуть необхідні способи, щоб одержати необхідну їм інформацію. Тому грамотна система захисту, розроблена з урахуванням всіх особливостей дозволить запобігти багатьом проблемам.

***Висновок.*** Беручи до уваги все викладене вище, забезпечення інформаційної безпеки можна поділити на наступні основні напрямки:

- В будь-якій організації необхідно розробляти і вводити просту систему класифікації ступеня конфіденційності інформації, що обробляється (гриф обмеження доступу). Гриф можна присвоїти за допомогою штампів, спеціальних оцінок, а можна і просто за допомогою кольору (наприклад, документи загального користування - білого кольору, документи службового - жовті, а таємні - червоного).
- Обов'язково встановити процедуру передачі конфіденційної інформації від одного співробітника іншому, порядок її обробки і збереження залежно від ступеня таємності. (Це неминуче призведе до включення до цієї процедури аспектів забезпечення комп'ютерної безпеки, а також порядку ведення діловодства загалом і встановлення правил роботи з конфіденційними документами). Краще, якщо робота з контролю за документами буде доручена окремому співробітнику (наприклад, інспектору по режиму роботи з документами), в ідеалі цим повинна займатися група режиму служби безпеки підприємства.
- Необхідно постійно проводити з персоналом компанії роботу про правила поводження з конфіденційною інформацією.

Таким чином, створення системи інформаційної безпеки є масштабною роботою, яка вимагає серйозних зусиль. Тому фахівці радять, насамперед, найбільш точно визначити ризики, які існують для інформаційної безпеки підприємства, і не вживати додаткових заходів забезпечення безпеки, якщо це реально не відобразиться на підвищенні росту самого бізнесу.

**Література:**


1. *Антирейдерский союз предпринимателей Украины Консультационный центр «Корпоративная безопасность предприятия (фирмы)» - «Информационная безопасность предприятия (фирмы)» – Курс лекций - Библиотека Антирейдера.*

2. *Про інформацію: Закон України від 2 жовтня 1992 р. № 2657-XII // Відомості Верховної Ради України. — 1992. — № 48. —Ст.. 650. із наступними змінами та доповненнями*

3. *Бєляков К. І., Мірошник Ю. П. Проблеми законодавчого регулювання у сфері користування інформацією з обмеженим доступом в Україні. - Держава і право - №12 - 2001 - ст.190-197*

4. *Бєліков О. Комерційна таємниця в чинному законодавстві: перспективи розвитку та застосування / О. Бєліков . – Електронний ресурс. – Режим доступу: www.yur-gazeta.com*

5. *Антирейдерский союз предпринимателей Украины Консультационный центр «Корпоративная безопасность предприятия (фирмы)» - «Коммерческая тайна. Секрет Полишинеля или тайна за семью печатями. (зарубежный опыт)» – Курс лекций - Библиотека Антирейдера.*

6. *Антирейдерский союз предпринимателей Украины Консультационный центр «Корпоративная безопасность предприятия (фирмы)» -«Промышленный шпионаж – угроза экономической безопасности предприятия (фирмы)» - Курс лекций - Библиотека Антирейдера.*

7. *Цивільний кодекс України від 16.01.03 р. – № 435 // Відомості Верховної Ради. – 2003. – № 40-44. – Ст. 356*

8. *Постанова Кабінету Міністрів України Про перелік відомостей, що не становлять комерційної таємниці від 09.08.93 р. - № 611 // Офіційний сайт Верховної Ради України. Режим доступу: www.rada.gov.ua.*

9. *Об'єднання професіоналів конкурентної розвідки Росії // Офіційний сайт. Режим доступу: www.rscip.ru*