

ТЕМА 2

ПОНЯТТЯ ІНФОРМАЦІЙНОГО ПРОСТОРУ, ЙОГО СУБ'ЄКТИ

ПЛАН

1. Суб'єкти інформаційного простору.
2. Організація секретного діловодства. Поняття конфіденційної інформації.
3. Віднесення відомостей до комерційної таємниці.
4. Віднесення відомостей до державної таємниці.

1. Суб'єкти інформаційного простору.

Інформаційна сфера - сукупність інформації, інформаційної інфраструктури, суб'єктів, що здійснюють збір, формування, поширення і використання інформації, а також системи регулювання відповідних суспільних відносин.

Інформаційна сфера - сукупність відносин, що виникають при: формуванні і використанні інформаційних ресурсів на основі створення, збору, обробки, накопичення, зберігання, пошуку, розповсюдження і надання споживачеві документованої інформації; створенні і використанні інформаційних технологій та засобів їх забезпечення; захисту інформації, прав суб'єктів, що беруть участь в інформаційних процесах та інформатизації.

Інформаційний потік - сукупність інформації, що переміщується в інформаційному просторі через канали комунікації. Інформаційні потоки можуть протікати як усередині окремих інфосфер, так і між ними, залежно від наявності каналів комунікації.

Організаційний аспект структури інформаційного простору складають множини баз даних і банків даних, сховищ даних, технологій їх ведення, використання, інформаційних систем, мереж, застосувань, організаційних структур, що функціонують на основі певних принципів і за встановленими правилами, що забезпечують інформаційну взаємодію об'єктів.

До складу технологічних та організаційних компонентів інформаційного простору відносять інформаційну інфраструктуру - середовище, яке забезпечує можливість збору, передачі, зберігання, автоматизованої обробки і розповсюдження інформації в суспільстві.

Інформаційна інфраструктура суспільства утворюється сукупністю:

- інформаційних і телекомунікаційних систем та мереж зв'язку, індустрії засобів інформатизації, телекомунікації і зв'язку;
- систем формування і забезпечення збереження інформаційних ресурсів;
- системи забезпечення доступу до інформаційно-телекомунікаційних систем, мереж зв'язку та інформаційних ресурсів;
- індустрії інформації та ринку інформаційних послуг;
- системи підготовки кадрів, проведення наукових досліджень;
- алгоритмів і програмних засобів, що забезпечують функціонування програмно-апаратних платформ тощо.

Інформаційний простір суспільства характеризується унікальними суб'єктами і співтовариствами, що не мають прямих аналогів в інших просторах, серед яких можна назвати віртуальне співтовариство, мережеву організацію, віртуальне підприємство. Інформаційний простір завдяки відсутності меж і своїй віртуальності є інтеграційним механізмом організаційних структур у планетарному масштабі.

Основними функціями, що нині виконує інформаційний простір, є:

- інтегруюча - об'єднує в єдине просторово-комунікативне і соціокультурне середовище різні види економічної діяльності;
- комунікативна - створюється особливе середовище транскордонної, інтерактивної і мобільної комунікації різних суб'єктів економічної діяльності, у рамках якої вони здійснюють інформаційний обмін;
- актуалізуюча — в інформаційному просторі здійснюється актуалізація інтересів різних суб'єктів економічної діяльності шляхом реалізації ними інформаційної політики;

- геополітична - формуються власні ресурси і змінюється значущість традиційних ресурсів, створюючи нове середовище геополітичних відносин і конкуренції;

- соціальна – інформаційний простір трансформує суспільство і змінює характер та зміст соціально-економічних відносин у всіх сферах: політиці, культурі, науці, релігії тощо.

2. Організація секретного діловодства

Під час роботи з захисту комерційної таємниці необхідно звернути особлива увага на документи фірми, оскільки більшість комерційних структур у нашій країні основні обсяги комерційної інформації, у тому числі конфіденційної, зберігають у документах.

Керівник фірми повинний упорядкувати відповідним чином процеси фіксації секретної інформації в ділових паперах і організувати їхній рух таким чином, щоб викрадення конфіденційних документів було б утруднене настільки, щоб воно ставало економічно не вигідним для викрадача.

При роботі з документами, що містять охоронювану фірмою інформацію, слід дотримуватися наступних правил:

- строгий контроль (чи особисто через службу безпеки) за допуском персоналу до секретних документів;

- установлення конкретних облич з керівництва фірми організуючих і контролюючих секретне діловодство фірми; наділення їх відповідними повноваженнями;

- розробка інструкції (пам'ятки) по роботі із секретними документами, ознайомлення з нею відповідних працівників фірми;

- контроль за прийняттям відповідними службовцями письмових зобов'язань про збереження комерційної таємниці фірми;

- введення системи матеріального й іншого стимулювання фірми, що служить, що мають доступ до її секретів;

- впровадження в повсякденну практику механізмів і технологій захисту комерційної таємниці фірми;
- особистий контроль з боку керівника фірми служби внутрішньої безпеки і секретного діловодства.

Ймовірність витоку секретної інформації з документів особливо велика в процесі їхнього пересилання. Тому доставку секретних документів і цінностей приходится здійснювати власними силами із залученням охоронців фірми чи звертатися в спеціальні фірми.

Фірми, відповідальні за збереження, використання і своєчасне знищення секретних документів, повинні бути захищені від спокуси торгівлі секретами фірми простим, але радикальним способом — гарною платою за роботу.

У процесі збереження і пересилання секретних документів фірми можуть бути застосовані засоби захисту і сигналізації про несанкціонований доступ до них. Одна з новинок — невидиме світлочутливе покриття, наносимо на документи, що виявляється під впливом світла, указуючи тим самим на факт несанкціонованого ознайомлення з чи документами їхнього фотографування.

Фахівцям з питань захисту комерційної інформації відомі й інші технології і системи охорони конфіденційних документів фірми від несанкціонованого до неї чи доступу можливого витоку охоронюваних зведень. За інформацією з даного питання варто звертатися в організації і служби, що спеціально займаються даною проблемою.

Для ведення секретного діловодства повинні залучатися люди, що пройшли спеціальну перевірку, і в чесності яких немає сумнівів. Крім того, ці люди повинні бути відповідним чином підготовлені і навчені, тому що професійні недоліки і відступ від правил у їхній роботі можуть занадто дорого коштувати фірмі.

Приміщення, у яких ведеться робота із секретними документами, повинні добре охоронятися, а доступ туди повинний бути закритий для сторонніх облич. Ці приміщення повинні мати міцні перекриття і стіни, посилену металеві двері, міцні віконні рами з подвійним склом і ґратами, щільні штори. Сховище

повинне бути обладнане охороною і пожежною сигналізацією і ретельно охоронятися силами внутрішньої охорони. Доступ у сховище строго обмежений. Не рекомендується розташовувати таке приміщення на першому й останньому поверхах будинку. Секретні документи зберігаються в сейфах чи металевих шафах з надійними замками і запорами.

Різні прийоми ведення секретного діловодства спрямовані на запобігання витоку комерційних секретів. Наприклад, документи, що містять комерційну таємницю, підрозділяються по ступені таємності відображеної в них інформації і забезпечуються відповідним грифом таємності.

Навіть ретельно охоронювані таємниці фірми можуть стати надбанням конкурентів зі звичайних публікацій, якщо пустити цю справа на самоплив. Тому один зі службовців фірми обов'язково повинний бути наділений самими широкими владними повноваженнями, щоб займатися попередньою цензурою брошур, що готуються, рекламних оголошень, прес-релізів і інших матеріалів для симпозіумів, виставок, конгресів, а також виступів, наукових і інших публікацій співробітників фірми.

Інтереси охорони секретів фірми найчастіше знаходяться у важко розв'язному протиріччі з особистими амбіціями, самолюбством, академічною незалежністю співробітників фірми, що бажають професійно само затверджуватися в ученому світі, серед своїх колег, у суспільній чи груповій думці.

Не менш легкий для дозволу конфлікт між прагненням зберегти комерційні таємниці фірми і бажанням використовувати в рекламних цілях деякі найбільш вражаючі дані зі строго охоронюваної інформації, особливо ті з них, що, безсумнівно, допомогли б розширити збут вироблених товарів і послуг.

3. Віднесення відомостей до комерційної таємниці

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.

Ст. 505 ЦК України містить легальне визначення поняття комерційної таємниці.

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 має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

Секретною або таємною прийнято називати інформацію, що складає державну та військову таємницю. Поняття комерційної таємниці, яке міститься в коментованій статті, вказує на юридично значущі ознаки комерційної таємниці.

Ознаками комерційної таємниці є:

- а) інформаційність комерційної таємниці (в тому розумінні, що комерційна таємниця - це інформація);
- б) конфіденційність;
- в) комерційна цінність та
- г) захищеність інформації, яка становить комерційну таємницю.

Ці ознаки комерційної таємниці є істотними, необхідними та невіддільними.

Конфіденційність комерційної таємниці полягає в тому, що інформація, яка становить комерційну таємницю, в цілому чи в певній формі та сукупності її складових має бути невідомою та не бути легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить.

Комерційну цінність інформації, яка становить комерційну таємницю, розуміють таким чином, що її використання надає володільцю інформації певні економічні переваги в силу того, що його конкуренти або інші особи такою інформацією не володіють. Комерційна цінність може виражатися в отриманні

більших прибутків від реалізації продукції, виробленої з використанням конфіденційних технологій, від розширення ринків збуту тощо.

Інформація, що становить комерційну таємницю, має бути предметом адекватних існуючим обставинам заходів щодо збереження її конфіденційності, вжитих особою, яка законно контролює цю інформацію. Відповідно до ч. 2 ст. 505 ЦК України 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.

Закон не встановлює будь-яких вимог до формалізації об'єктивного вираження інформації, яка становить комерційну таємницю. Відтак, нею можуть бути й відомості, повідомлені усно, зафіксовані письмово, виражені графічно тощо. Не може бути віднесена до комерційної таємниці інформація, яка згідно з Законом України "Про інформацію" підпадає під режим таємної (державна таємниця) або, навпаки, відкритої інформації, наприклад, правила страхування, розроблені страховиком (див. Закон України "Про страхування"). Так само не можуть становити комерційної таємниці відомості, які підлягають обов'язковому опублікуванню, наданню на запит необмеженого кола заінтересованих осіб, а також відомості, щодо яких в законодавстві міститься пряма заборона на поширення на них режиму обмеженого доступу.

Наприклад, у ч. 2 ст. 50 Конституції України встановлено, що інформація про стан довкілля, про якість харчових продуктів і предметів побуту ніким не може бути засекречена. Закон України "Про бухгалтерський облік та фінансову звітність в Україні" передбачає, що фінансова звітність підприємств не становить комерційної таємниці, крім випадків, передбачених законодавством. В Законі України "Про сертифіковані товарні склади та прості і подвійні складські свідоцтва" закріплено норму про те, що регламент сертифікованого складу не може становити комерційної таємниці.

Обмеження на застосування режиму комерційної таємниці встановлені також постановою Кабінету Міністрів України від 9 серпня 1993 р. N 611 "Про

перелік відомостей, що не становлять комерційної таємниці". Так, комерційну таємницю не становитимуть:

- 1) установчі документи, документи, що дозволяють займатися підприємницькою діяльністю та її окремими видами;
- 2) інформація за всіма встановленими формами державної звітності;
- 3) дані, необхідні для перевірки обчислення і сплати податків та інших обов'язкових платежів;
- 4) відомості про чисельність і склад працюючих, їхню заробітну плату в цілому та за професіями й посадами, а також наявність вільних робочих місць;
- 5) інформація про забруднення навколишнього природного середовища, недотримання безпечних умов праці, реалізацію продукції, що завдає шкоди здоров'ю, а також інші порушення законодавства України та розміри заподіяних при цьому збитків;
- 6) документи про платоспроможність;
- 7) відомості про участь посадових осіб підприємства в кооперативах, малих підприємствах, спілках, об'єднаннях та інших організаціях, які займаються підприємницькою діяльністю;
- 8) відомості, що відповідно до чинного законодавства підлягають оголошенню.

Зазначена постанова Кабінету Міністрів України N 611 від 09.08.93 р. сьогодні не відповідає вимогам ч. 2 ст. 505 ЦК України, оскільки відомості, які не можуть бути віднесені до комерційної таємниці, повинні визначатися не підзаконним нормативно-правовим актом, а законом, якого, однак, в Україні поки що не прийнято.

4. Віднесення відомостей до державної таємниці

Державна таємниця - це вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди

національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою.

Гриф секретності - реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності даної інформації;

Засекречування матеріальних носіїв інформації - введення у встановленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом надання відповідного грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації;

Категорія режиму секретності - категорія, яка характеризує важливість та обсяги відомостей, що становлять державну таємницю, які зосереджені в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях;

Криптографічний захист секретної інформації - вид захисту, що реалізується шляхом перетворення інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

Матеріальні носії секретної інформації - матеріальні об'єкти, в тому числі фізичні поля, в яких відомості, що становлять державну таємницю, відображені у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів тощо;

Охорона державної таємниці - комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв;

Ступінь секретності ("особливої важливості", "цілком таємно", "таємно") - категорія, яка характеризує важливість секретної інформації, ступінь обмеження доступу до неї та рівень її охорони державою;

Технічний захист секретної інформації - вид захисту, спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності та унеможливлення блокування інформації.

Стаття 2. Законодавство України про державну таємницю

Відносини у сфері охорони державної таємниці регулюються Конституцією України, Законом України "Про інформацію", цим Законом, міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України та іншими нормативно-правовими актами.

Стаття 3. Сфера дії Закону

Дія цього Закону поширюється на органи законодавчої, виконавчої та судової влади, органи прокуратури України, інші державні органи, Верховну Раду Автономної Республіки Крим, Раду міністрів Автономної Республіки Крим, органи місцевого самоврядування, підприємства, установи та організації усіх форм власності, об'єднання громадян (далі - державні органи, органи місцевого самоврядування, підприємства, установи та організації), що провадять діяльність, пов'язану з державною таємницею, громадян України, іноземців та осіб без громадянства, яким у встановленому порядку наданий доступ до державної таємниці.

Передані Україні відомості, що становлять таємницю іноземної держави чи міжнародної організації, охороняються в порядку, передбаченому цим Законом. У разі, якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, встановлено інші, ніж передбачені цим Законом, правила охорони таємниці іноземної держави чи міжнародної організації, то застосовуються правила міжнародного договору України.

Стаття 4. Державна політика щодо державної таємниці

Державну політику щодо державної таємниці як складову засад внутрішньої та зовнішньої політики визначає Верховна Рада України.

Стаття 5. Компетенція державних органів, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці

Президент України, забезпечуючи національну безпеку, видає укази та розпорядження з питань охорони державної таємниці, віднесених цим Законом та іншими законами до його повноважень.

Рада національної безпеки і оборони України координує та контролює діяльність органів виконавчої влади у сфері охорони державної таємниці. Кабінет Міністрів України спрямовує та координує роботу міністерств, інших органів виконавчої влади щодо забезпечення здійснення державної політики у сфері охорони державної таємниці.

Центральні та місцеві органи виконавчої влади, Рада міністрів Автономної Республіки Крим та органи місцевого самоврядування здійснюють державну політику у сфері охорони державної таємниці в межах своїх повноважень, передбачених законом.

Спеціально уповноваженим державним органом у сфері забезпечення охорони державної таємниці є Служба безпеки України.

Забезпечення охорони державної таємниці відповідно до вимог режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, діяльність яких пов'язана з державною таємницею, покладається на керівників зазначених органів, підприємств, установ і організацій.

Стаття 6. Здійснення права власності на секретну інформацію та її матеріальні носії

Власник секретної інформації або її матеріальних носіїв здійснює своє право власності з урахуванням обмежень, установлених в інтересах національної безпеки України відповідно до цього Закону.

Якщо обмеження права власності на секретну інформацію або її матеріальні носії завдають шкоди їх власнику, відшкодування здійснюється за рахунок держави у порядку та розмірах, що визначаються у договорі між власником такої інформації або її матеріальних носіїв і державним органом (органами), якому державним експертом з питань таємниць надається право приймати рішення щодо суб'єктів, які матимуть доступ до цієї інформації та її

матеріальних носіїв. Зазначеним договором також визначаються порядок та умови охорони державної таємниці, включаючи режим секретності під час користування і розпорядження секретною інформацією та її матеріальними носіями, обумовлюється згода власника цієї інформації та її матеріальних носіїв на здійснення права власності з урахуванням обмежень, встановлених відповідно до цього Закону, взяття власником на себе зобов'язання щодо збереження державної таємниці та ознайомлення його з мірою відповідальності за порушення законодавства про державну таємницю.

Якщо власник секретної інформації або її матеріальних носіїв відмовляється від укладення договору чи порушує його, за рішенням суду ця інформація або її матеріальні носії можуть бути вилучені у власність держави за умови попереднього і повного відшкодування власникові їх вартості.

Стаття 7. Фінансування витрат на здійснення діяльності, пов'язаної з державною таємницею Фінансування витрат на здійснення діяльності, пов'язаної з державною таємницею, в бюджетних установах і організаціях здійснюється за рахунок Державного бюджету України, бюджету Автономної Республіки Крим та місцевих бюджетів. Кошти на зазначені витрати передбачаються у відповідних бюджетах окремим рядком. Зазначені витрати інших установ і організацій, а також підприємств відносяться до валових витрат виробника продукції, виготовлення якої пов'язано з державною таємницею.

Витрати на здійснення заходів щодо віднесення інформації до державної таємниці, засекречування, розсекречування та охорони матеріальних носіїв такої інформації, її криптографічного та технічного захисту, інші витрати, пов'язані з державною таємницею, на недержавних підприємствах, в установах, організаціях фінансуються на підставі договору з замовником робіт, пов'язаних з державною таємницею.

Підприємствам, установам і організаціям, які провадять діяльність, пов'язану з державною таємницею, можуть надаватися податкові та інші пільги в порядку, встановленому законом.