

Лекція 6

ПРАВОВІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ

1. Конституційні засади інформаційної безпеки суб'єктів господарювання.
2. Правове регулювання комерційної таємниці суб'єктів господарювання
3. Закони та підзаконні нормативно-правові акти, які регулюють інформаційну безпеку суб'єктів господарювання

1. Конституційні засади інформаційної безпеки суб'єктів господарювання

Забезпечення інформаційної безпеки господарської діяльності здійснюються під впливом різноманітних умов, серед яких провідне місце займають правові умови¹. Останні, у свою чергу, утворюються чотирма джерелами правових норм:

- Конституцією України,
- законодавчими актами,
- підзаконними актами,
- нормативно-правовими актами суб'єктів господарювання.

Значення правових умов у забезпеченні інформаційної безпеки полягає у тому, що:

- ✓ без правових актів, які складають такі умови процес організації інформаційної безпеки неможливий взагалі;
- ✓ визначається правомірність тих чи інших дій щодо інформації, формуються підстави для відповідальності за дії в інформаційному просторі;
- ✓ забезпечується захист суб'єктів господарювання від неправомірного посягання на їх права, інтелектуальну власність, інформацію, що може мати місце у процесі їх діяльності.

Положення ст.55 Конституції України надають право будь-якими, не забороненими законом засобами захищати свої права і свободи від порушень і

¹ Зубок М.І. Інформаційна безпека в підприємницькій діяльності. К.: ГНОЗІС, 2015. 216 с.

протиправних посягань. Під засобами, серед інших, можна розуміти і правові засоби (норми та положення Конституції та законів України, нормативно-правових актів органів влади, нормативних документів суб'єктів господарювання та інших організацій, рішення та ухвали судів, положення судових органів, Міністерства юстиції України, положення договорів, угод, укладених суб'єктами підприємництва, рішення, приписи, накази органів нагляду та контролю). А права можуть поширюватись і на інформаційну сферу.

Зокрема право на інформацію, передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів. Крім того, Конституцією України гарантується право судового захисту щодо спростування недостовірної інформації, право вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням та поширенням недостовірної інформації. Основний закон забороняє збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків визначених законом (ст. 32). Конкретизуючи зміст конфіденційної інформації про особу слід зазначити, що до такої інформації належать, зокрема, дані про національність особи, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адресу, дату і місце народження. Тобто Конституція України встановлює загальні умови поведінки суб'єктів, і громадян в інформаційному просторі.

Важливим моментом для забезпечення правової поведінки в інформаційному просторі і правомірних інформаційних відносин є регулювання доступу до інформації. Ці питання регулюються положеннями Закону України «Про інформацію» (Рис. 1).



Рис. 1 Режим доступу до інформації (Закон України «Про інформацію», ст. ст. 20, 21).

Будь-яка інформація є відкритою крім тієї, що віднесена законом до такої, що має обмежений доступ. Важливо знати, що обмеженню підлягає інформація, а не документ в якому вона міститься. Якщо документ містить таку інформацію, то він підлягає ознайомленню в частині, що не містить інформації з обмеженим доступом.

Конфіденційною є інформація про фізичну особу, доступ до якої обмежений фізичною чи юридичною особою, крім суб'єктів владних повноважень. Така інформація може поширюватись зазначеними особами за їхнім бажанням (згодою) у визначеному ними порядку відповідно до передбачених ними умов, інших випадках визначених законом. До суб'єктів владних повноважень законодавець відносить – органи державної влади, місцевого самоврядування, інших суб'єктів, що здійснюють владні управлінські функції відповідно до законодавства, в т.ч. і делеговані повноваження.

Важливим є з'ясування особи яка має право обмежувати доступ та надавати інформації категорію конфіденційної. Очевидно, що це може бути сам власник такої інформації, або особа яка отримує право розпоряджатись даною інформацією. У останньому випадку законодавець визначає перелік розпорядників інформації, види інформації, якими вони можуть розпоряджатись, їх обов'язки та функції (Закон України «Про доступ до публічної інформації» ст. ст. 13-18).

Таємною є інформація, доступ до якої обмежується відповідно до вимог ст.6 Закону України «Про доступ до публічної інформації» і розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить відомості, що складають державну, професійну, банківську, комерційну та інші передбачені законом види таємниць.

До службової інформації належить така, що міститься в документах суб'єктів владних повноважень, а також зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Доступ до таємної інформації визначається відповідно до чинного законодавства установами, органами, які володіють такою інформацією. Доступ до службової інформації визначається відповідно до Закону України «Про доступ до публічної інформації» в порядку передбаченому внутрішніми документами суб'єкта владних повноважень.

Відносини у сфері доступу до публічної інформації регулюються Законом України «Про доступ до публічної інформації». Зокрема, закон дає визначення

поняття «публічна інформація» згідно з яким це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні таких суб'єктів, інших розпорядників, крім випадків встановлених законом.

Відповідно до зазначеного вище закону, доступ до публічної інформації здійснюється шляхом її оприлюднення у встановленому порядку та шляхом подання запитів до розпорядників інформації. Інформація надається безкоштовно.

Суб'єктами відносин у сфері доступу до публічної інформації є запитувачі інформації, розпорядники інформації, їх структурні підрозділи або відповідальні особи з питань виконання запитів.

Окремо регулюється система відносин щодо доступу до інформації про особу. Тут маємо брати за основу положення Закону України «Про захист персональних даних», Закону України «Про доступ до публічної інформації», Закону України «Про інформацію». Зокрема передбачається, що збирання, зберігання, використання та поширення інформації про особу не можливе без згоди саме особи, крім випадків передбачених законом. Обсяг такої інформації має бути максимально обмеженим і використовуватись лише з метою та у спосіб, визначений законом.

Суб'єктами відносин у сфері доступу до інформації про особу виступають самі особи, володільці та розпорядники баз персональних даних, треті особи (особи яким володільцями чи розпорядниками баз персональних даних здійснюється передача персональних даних відповідно до закону), уповноважений державний орган з питань захисту персональних даних, інші державні органи, органи місцевого самоврядування, до повноважень яких належить здійснення захисту персональних даних.

Про збір даних про осіб, включення інформації про них в базу персональних даних особи мають повідомляти про їх права володільцем, чи розпорядником бази даних протягом 10 днів з дня формування даних. Разом з тим, коли персональні дані збираються з загальнодоступних джерел таке повідомлення не здійснюється.

Питання правового регулювання доступу до персональних даних нормами міжнародного права, забезпечуються положеннями Конвенції Ради Європи «Про захист фізичних осіб при автоматизованій обробці персональних даних» від 28.01.1981р. зі змінами внесеними у 1999р., додаткового протоколу

до Конвенції «Про захист фізичних осіб при автоматизованій обробці персональних даних щодо органів нагляду і трансграничних потоків даних» від 08.11.2001 року., Директивою Ради Європейського Союзу «Про захист фізичних осіб при автоматизованій обробці персональних даних і про вільний обіг таких даних» (1995р.), а також Директивою «Про обробку персональних даних і захист прав фізичних осіб у телекомунікаційному секторі» (1997р.). Основними принципами захисту персональних даних викладених у зазначених правових актах є: збір і обробка персональних даних мають здійснюватись коректно і законно; використання персональних даних повинно бути адекватним визначеній меті, та обмежуватись за термінами; персональні дані повинні бути точними, оброблюватись лише з дозволу суб'єктів цих даних, бути доступними для них; персональні дані повинні бути надійно захищені [42].

2.Правове регулювання комерційної таємниці суб'єктів господарювання

Важливе значення, з точки зору інформаційної безпеки, має правове регулювання відносин у сфері захисту інформації з обмеженим доступом. Для підприємницької діяльності важливими питаннями є захист комерційної та банківської таємниці, а також комерційної інформації.

Правову основу комерційної таємниці складають положення Господарського кодексу України, Цивільного кодексу України, Кримінального кодексу України, Кодексу України про адміністративні правопорушення, Законів України «Про захист від недобросовісної конкуренції», «Про інформацію», інших правових актів. Зокрема, сутність комерційної таємниці як виду інформації з обмеженим доступом подається у Цивільному кодексі України. Так, комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи певній формі та сукупності її складових є невід'ємною та не є легкодоступною для осіб, які звичайно мають справу з видом інформації до якого вона належить і 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. За змістом 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. Перелік відомостей, які можуть становити комерційну

таємницю подається у Постанові Кабінету Міністрів України №611 від 09.08.93р.

Відповідно до положень Господарського кодексу України склад і обсяг відомостей, що становлять комерційну таємницю, спосіб їх захисту визначається суб'єктом господарювання [44].

Таким чином, законодавець не дає конкретного змісту комерційної таємниці, подаючи лише вказівки про що мають бути відомості, які становлять таку таємницю. Слід також звернути увагу на те, що такий вид таємниці як комерційна стосується лише суб'єктів господарювання: юридичних осіб та фізичних осіб зареєстрованих як суб'єкти підприємницької діяльності. Право власності на такий вид інформації вони отримують через створення її власними силами та засобами або іншими особами на договірних засадах з суб'єктами господарювання за їх кошти і на їх користь, придбанням такої інформації у інших осіб. Створення інформації, що становить комерційну таємницю іншими особами на користь суб'єктів господарювання стосується зазвичай продуктів інтелектуальної власності. Комерційною таємницею у таких випадках захищаються інформаційні характеристики зазначених продуктів. Право власності включає право володіння, право використання і право розпорядження чи поширення. Враховуючи, що суб'єкти господарювання є власниками своєї комерційної таємниці, вони ж самі визначають умови та способи їх захисту, доступу до неї, в т. ч. і у будь-яких взаємовідносинах з іншими суб'єктами. Згідно з положеннями Цивільного кодексу України (ст. 506) право розкриття комерційної таємниці належить особі, яка володіє майновими правами інтелектуальної власності на комерційну таємницю. Тобто, підстави, умови, способи захисту відомостей, що становлять комерційну таємницю у різних суб'єктів господарювання можуть бути різними, організуються кожним із них, виходячи з особливостей їх діяльності, інформаційних потреб та можливостей. Інформаційні відносини суб'єктів господарювання щодо комерційної таємниці, як правило, будуються на договірних засадах, з врахуванням нормативних документів суб'єктів у сфері їх інформаційної безпеки.

Окремо регулюється порядок захисту комерційної таємниці суб'єктів господарювання у їх конкурентних відносинах. Так, відповідно до гл. 4 Закону України «Про захист від недобросовісної конкуренції» неправомірним визнається збирання протиправним способом відомостей, що становлять комерційну таємницю за умов коли це завдало чи могло завдати шкоди суб'єкту господарювання. Крім того, неправомірним також визнається впровадження у виробництво або врахування під час планування чи здійснення

господарської діяльності без дозволу уповноваженої на те особи (неправомірне використання) відомостей, що становлять комерційну таємницю. Неправомірним вважається розголошення чи схилення до розголошення комерційної таємниці. Такі дії є протиріччям нормам чинного законодавства і переслідуються у кримінальному, адміністративному чи цивільному (відшкодування шкоди) порядку.

Певну специфіку мають інформаційні відносини предметом яких є банківська таємниця. Згідно ст. 60 Закону України «Про банки і банківську діяльність» банківською таємницею є інформація щодо діяльності та фінансового стану клієнтів банку, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третіми особами при наданні послуг банку. Тобто, банківська таємниця виникає тоді коли суб'єкти господарювання (підприємництва) стають клієнтами банків. Останні вважаються такими у разі отримання послуг банків. Враховуючи ж, що вказані суб'єкти здійснюючи свою фінансово-господарську діяльність обов'язково вдаються до послуг банків, виникнення в них банківської таємниці є закономірним фактом. В той же час слід зазначити, що статус банківської таємниці діє навіть тоді, коли суб'єкт (клієнт) припиняє відносини з банком. Інформація, що надана банку залишається в банку і закон не передбачає, що втрата відносин клієнта з банком припиняє статус банківської таємниці.

Зміст банківської таємниці конкретизовано у зазначеному законі і він є остаточним аж до поки в закон в установленому порядку не буде внесено відповідних змін. Зокрема вказується, що до складу банківської таємниці віднесено:

- відомості про банківські рахунки клієнтів, в т. ч. кореспондентські рахунки банків у НБУ;
- операції, які були проведені на користь чи за дорученням клієнтів, здійснені ними угоди;
- фінансово-економічний стан клієнтів;
- відомості про системи охорони банку і клієнтів;
- інформація про організаційно-правову структуру юридичної особи клієнтів, їх керівників, напрями діяльності;
- відомості стосовно комерційної діяльності клієнтів чи їх комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація;

- інформація щодо звітності по окремому банку за винятком тієї, що підлягає опублікуванню (ст. 70) Закону України «Про банки і банківську діяльність»;

- коди, що використовуються банками для захисту інформації.

Тут слід додати, що у зв'язку з появою законодавства про захист персональних даних, НБУ вніс певні доповнення до змісту банківської таємниці. Відповідно до постанови Правління НБУ від 11.07.2012р. №292 банківською таємницею є відомості або сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована, що стали відомі банку під час обслуговування фізичної особи та взаємовідносин з нею та взаємовідносин з нею чи третіми особами при наданні послуг банку [40].

Тобто, за своєю суттю і змістом банківська таємниця є єдиною для всіх банків і їх клієнтів, на відміну від комерційної таємниці.

Необхідно звернути увагу на те, що перераховані відомості не стають автоматично банківською таємницею з встановленням стосунків з банками. Інформація має стати відомою банку тільки в результаті обслуговування клієнта, що має підтверджуватись відповідною угодою про надання (отримання) банківських послуг. Крім того, фактом, що підтверджує отримання банком відповідної інформації про клієнта мають бути певні документи, які вимагаються банками від їх клієнтів для надання їм тих чи інших послуг. Скажімо, інформація про систему охорони клієнта не є фінансовою інформацією, не стосується послуг банку і тому не може бути відома останньому, а звідси і не може бути банківською таємницею. Тобто, факт надання інформації має бути пов'язано з наданням клієнту послуг банку і засвідчено документально.

Необхідність дотримання такої процедури обумовлюється тим, що інформація, яка становить банківську таємницю залишаючись власністю клієнта захищається банком. Законодавець поклав на банк відповідні обов'язки щодо організації захисту банківської таємниці, зокрема визначив заходи захисту і встановив порядок доступу до неї. У даному випадку порядок доступу до відомостей, що становлять банківську таємницю є єдиним і не залежить від волі чи бажання власника таємниці або банку.

Зокрема, ст. 62 Закону України «Про банки і банківську діяльність» визначає порядок розкриття банківської таємниці.

Банківська таємниця розкривається:

- на письмовий запит або з письмового дозволу власника даної інформації;

- за рішенням суду;
- органам прокуратури, Служби безпеки України, Міністерства внутрішніх справ України, Антимонопольного комітету України – на їх письмову вимогу стосовно операцій за рахунками конкретної юридичної особи або фізичної особи – суб'єкта підприємницької діяльності за конкретний проміжок часу;
- центральному органу виконавчої влади, що реалізує державну податкову політику: на його письмову вимогу щодо наявності банківських рахунків; за рішенням суду щодо відомостей, зазначених у деклараціях про майно, доходи, витрати і зобов'язання фінансового характеру, у зв'язку з проведенням перевірки їх достовірності;
- центральному органу влади, що реалізує державну політику у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом на його запит щодо фінансових операцій, пов'язаних з фінансовими операціями, що стали об'єктом фінансового моніторингу (аналізу) згідно із законодавством щодо запобігання та протидії легалізації (відмиванню) доходів одержаних злочинним шляхом або фінансового тероризму, а також учасників зазначених операцій;
- органам державної виконавчої служби на їх письмову вимогу з питань виконання рішень судів та рішень, що підлягають примусовому виконанню відповідно до Закону України «Про виконавче провадження» стосовно стану рахунків конкретної юридичної особи або фізичної особи;
- Національній комісії з цінних паперів і фондового ринку у випадках самостійного подання банком інформації про банк як емітент та адміністративних даних відповідно до законодавства про цінні папери і фондовий ринок.

Порядок надання банками інформації, що становить банківську таємницю визначений у Законі України «Про банки і банківську діяльність» і конкретизовано Правилами зберігання, захисту використання та розкриття банківської таємниці, затвердженими постановою Правління НБУ №267 від 14.07.2006р.

Таким чином, доступ до банківської таємниці суворо регламентовано чинним законодавством дотримання якого законодавець поклав на банки та інших суб'єктів предметом відносин яких є саме інформація, що становить банківську таємницю.

Узагальнюючи викладене необхідно вказати, що основними особливостями банківської таємниці як інформації з обмеженим доступом є наступні:

зміст банківської таємниці визначено законом, законодавець встановив вичерпний перелік відомостей, які становлять банківську таємницю, зміст банківської таємниці для всіх суб'єктів, які мають до неї відношення є одним і тим же; банківська таємниця не є різновидом інших таємниць, а становить самостійний вид таємної інформації; інформація, що становить банківську таємницю торкається насамперед клієнтів банків, причому режимом таємності охоплюються відомості, які банки отримують від своїх клієнтів офіційно, в процесі безпосереднього здійснення своєї діяльності. Слід також зазначити, що інформацію про клієнта банк може отримати як безпосередньо від нього, так і інших (третіх) осіб, з якими банк вступає у взаємовідносини, при наданні банківських послуг. Інформація, яка становить банківську таємницю може міститись в документах, що характеризують взаємовідносин банку і клієнта, документах, що характеризують самого клієнта і його діяльність, а також документах банку, що характеризують самого клієнта і його діяльність.

За посягання на банківську та комерційну таємницю законодавство України передбачає дисциплінарну, кримінальну, адміністративну та цивільну відповідальність.

Тут слід виділити дві основні групи суб'єктів посягань на таку інформацію. Особи, що незаконно заволоділи інформацією банку та особи, що правомірно отримали таку інформацію, але порушили зобов'язання щодо збереження її в таємниці (працівники, контрагенти, партнери, клієнти, державні службовці).

Кримінальна відповідальність передбачена за умисні дії, які спрямовані на отримання відомостей, що становлять комерційну або банківську таємницю, з метою розголошення чи іншого використання цих відомостей, а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб'єкту господарської діяльності.

Крім того, кримінальна відповідальність настає також за умисне розголошення комерційної або банківської таємниці, без згоди її власника, особою, якій ця таємниця відома, у зв'язку з професійною або службовою діяльністю якщо воно вчинене з корисливих чи інших особистих мотивів і завдало істотної шкоди суб'єкту господарської діяльності.

Адміністративна відповідальність може наступати у разі отримання, використання, розголошення комерційної таємниці, з метою заподіяння шкоди діловій репутації або майну конкурента.

Цивільний кодекс України відносить інформацію до об'єктів цивільних прав і визначає, що суб'єкт відносин у сфері інформації може вимагати

усунення порушень його права та відшкодування майнової і моральної шкоди, завданої такими правопорушеннями.

3. Закони та підзаконні нормативно-правові акти, які регулюють інформаційну безпеку суб'єктів господарювання

Враховуючи особливий статус та значний обсяг електронної інформації в діяльності суб'єктів підприємництва законодавець передбачив відповідні правові умови відносин у сфері такої інформації. Основним правовим документом тут є Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». Згідно закону основним об'єктом захисту виступають: інформація, що використовується в інформаційно-телекомунікаційних системах та програмне забезпечення, яке використовується для обробки інформації суб'єктами відносин є: власники інформації, власники систем, користувачі, уповноважений орган виконавчої влади з питань організації спецзв'язку та захисту інформації. Взаємовідносини суб'єктів здійснюється на договірних засадах. Порядок доступу до інформації, що оброблюється в системі, перелік користувачів та їх повноваження визначає власник інформації. У випадках коли в системах оброблюється інформація з обмеженим доступом, доступ до неї визначається законодавством. Положеннями закону врегульовано відносини поміж власниками інформації і власниками інформаційно-телекомунікаційних систем, між власниками різних систем, власниками систем і користувачами. Організація захисту інформації, що оброблюється у системах покладається на власників систем. За порушення порядку і правил захисту інформації, що оброблюється в інформаційно-телекомунікаційних системах може наступати адміністративна та кримінальна відповідальність.

Документообіг в електронному інформаційному просторі на сьогоднішній час є одним із елементів документування підприємницької діяльності. Безумовно, що він має бути в правовому плані врегульованим і захищеним. Це питання регулюється двома законодавчими актами: Закони України «Про електронні документи та електронний документообіг» і «Про електронний цифровий підпис», а також Положеннями «Про технічний захист інформації в Україні» і «Про порядок здійснення криптографічного захисту інформації в Україні». Зазначені правові норми визначають організаційно-правові засади електронного документообігу, використання електронних документів, правовий статус електронного підпису та регулювання відносин, що виникають при його

використанні. Зокрема, в законодавчих актах надається поняття електронного документу та наголошується на його юридичному статусі (документ не може бути заперечений через те, що він має електронну форму). Крім того, регулюються питання обігу документів, які містять інформацію з обмеженим доступом та їх особливого захисту в електронних мережах і носіях. Також встановлюється, що електронний підпис є обов'язковим реквізитом електронного документу: за своїм правовим статусом прирівнюється до власноручного підпису (печатки) за умов передбачених Законом України «Про електронний цифровий підпис».

Вказані вище Положення визначають порядок технічного захисту інформації та виконання криптографічного захисту інформації з обмеженим доступом.

Організуючи забезпечення інформаційної безпеки суб'єктів підприємництва у стосунках з представниками засобів масової інформації необхідно досить професійно орієнтуватись у законодавстві та правових актах, що регулюють діяльність суб'єктів масової інформації. Зокрема доцільним буде ознайомлення з положеннями наступних правових актів: Законів України «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації», «Про інформацію», «Про друковані засоби масової інформації (пресу) в Україні», «Про телебачення і радіомовлення», «Про інформаційні агентства», «Про авторське право і суміжні права», «Про державну підтримку засобів масової інформації та соціальний захист журналістів», «Про захист суспільної моралі». Крім того, не зайвим буде ознайомитись з Кодексом професійної етики українського журналіста.

Враховуючи, що діяльність з забезпечення інформаційної безпеки суб'єктів підприємництва зазвичай передбачає взаємовідносини з правоохоронними та судовими органами, органами контролю та нагляду, які керуються спеціальними законодавчими актами, що регулюють їх діяльність, доцільним також буде ознайомлення з правами таких органів в інформаційній сфері. Насамперед положеннями Законів України «Про прокуратуру», «Про міліцію», «Про службу безпеки України», «Про оперативно розшукову діяльність», «Про організаційні основи боротьби з організованою злочинністю», «Про судоустрій та статус судів», «Про адвокатуру та адвокатську діяльність», «Про державну контрольно-ревізійну службу в Україні», «Про Національний банк України», «Про заходи протидії незаконному обігу наркотичних засобів, психотропних речовин і прекурсорів та

зловживання ними», а також Податкового кодексу України та іншими положеннями правових актів, що регулюють діяльність зазначених органів.

Питання правового регулювання інформаційної безпеки суб'єктів господарювання не буде повним без нормативно-правових документів самих суб'єктів. Саме такі нормативно-правові документи, базуючись на положеннях законодавчих та підзаконних актів утворюють правові підстави та регулюють діяльність суб'єктів щодо встановлення відповідного інформаційного режиму їх інформаційних відносин з іншими суб'єктами, контрагентами, клієнтами, кредиторами і мають певне значення для взаєностосунків з державними органами. Якраз в таких документах обґрунтовується поведінка суб'єктів підприємництва в їх інформаційному просторі за різних умов.

На сьогодні, як і взагалі у сфері інформаційної безпеки суб'єктів підприємництва, так і в питаннях правового її регулювання нормативно-правовими документами самих суб'єктів стійкої позиції немає. Беручи до уваги мету, завдання та зміст інформаційної безпеки суб'єктів підприємництва, структуру процесу її організації та напрацьований досвід, можна рекомендувати наступний перелік таких нормативно-правових документів:

- Положення про комерційну таємницю та правила її зберігання на підприємстві (у банку);
- Положення про конфіденційну інформацію підприємства (банку);
- Інструкція про порядок підготовки, обліку, зберігання та знищення документів, справ, видань і матеріалів, що містять комерційну таємницю та конфіденційну інформацію підприємства (банку);
- Положення про захист електронної інформації та електронних документів на підприємстві (у банках питання захисту електронної інформації здійснюється відповідно до нормативно-правових документів НБУ);
- Інструкція про порядок виконання документів, що надходять до підприємства (банку) від правоохоронних органів, судів та інших державних установ;
- Положення про архів і архівну діяльність підприємства (банку);
- Інструкція про проведення службових розслідувань на підприємстві (у банку);
- Положення про інформаційно-аналітичну роботу на підприємстві (у банку);
- Інструкція з службового діловодства; Інструкція з спеціального діловодства;

- Правила використання, поширення та зберігання інформації підприємства (банку) у процесі його діяльності;

- Методики розробки інформаційних документів підприємства (банку) та надання інформаційних послуг;

Пам'ятки працівникам підприємства, банку по збереженню інформації з обмеженим доступом; інші документи.

Незважаючи на значний перелік документів, всі вони утворюють правове поле суб'єкта підприємництва у сфері забезпечення його інформаційної безпеки, обґрунтовують поведінку суб'єкта у інформаційному середовищі.

Список рекомендованої літератури

1. Конституція України : Закон України від 1996 р. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.

2. Господарський кодекс України: Закон України від 16 січня 2003 р. № 436-IV. *Відомості Верховної Ради України*. 2003. №№ 18, 19–20, 21–22. Ст. 144.

3. Цивільний кодекс України від 16 січня 2003 р. № 435-IV. *Відомості Верховної Ради України*. 2003. № 40-44. Ст.356.

4. Про Концепцію Національної програми інформатизації : Закон України від 1998 р. *Відомості Верховної Ради України*. 1998. № 27-28. Ст. 182.

5. Про Державну службу спеціального зв'язку та захист інформації України: Закон України від 23 лютого 2006 року. *Відомості Верховної Ради України*. 2006. № 30. ст.258.

6. Про інформацію: Закон України від 2 жовтня 1992 р. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650.

7. Про Національну програму інформатизації : Закон України від 1998 р. *Відомості Верховної Ради України*. 1998. № 27-28. Ст. 181.

8. Стратегії розвитку України : теорія і практика; за ред. О.С. Власюка. К.: НІСД, 2002, 864 с.

9. Зубок М. І. Інформаційно-аналітичне забезпечення підприємницької діяльності. К.: ГНОЗІС, 2015. 216 с.

10. Кормич Б. А. Інформаційне право. Підручник. Харків: БУРУН і К., 2011. 334 с.

11. Крегул Ю.І., Зубок М.І. Правове регулювання безпеки підприємницької діяльності: навч. посібник. К.: КНТЕУ, 2013. 216с.

12. Шпакова О. Політика інформаційної безпеки в Україні: правовий базис. *Актуальні проблеми міжнародних відносин*. 2008. Вип.65 (Ч. 1). С. 242-249.