УДК 351:336.7:340.5
DOI https://doi.org/10.32838/2663-6468/2020.2/34

Горник В.Г.
Таврійський національний університет імені В.І. Вернадського

Кравченко С.О.
Таврійський національний університет імені В.І. Вернадського

МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ ЯК СКЛАДНИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

У статті досліджено підходи до визначення місця й ролі інформаційної безпеки в підприємницькій діяльності. Доведено, що вдосконалення правових механізмів регулювання суспільних відносин, що виникають в інформаційній сфері, є пріоритетним напрямом державної політики у сфері забезпечення інформаційної безпеки в підприємницькій діяльності в Україні. Встановлено, що інформаційна безпека в підприємницькій діяльності передбачає такі дії: оцінку ефективності застосування чинних законодавчих та інших нормативних правових актів в інформаційній сфері й вироблення програми їх удосконалення; створення організаційно-правових механізмів забезпечення інформаційної безпеки; визначення правового статусу всіх суб'єктів відносин в інформаційній сфері, зокрема користувачів інформаційних і телекомунікаційних систем, та встановлення їхньої відповідальності за дотримання законодавства України в цій сфері.

Серед основних механізмів забезпечення інформаційної безпеки підприємницької діяльності в Україні як складника інформаційної безпеки держави доцільно виділити: інформаційний патронат; інформаційний захист (судовий, адміністративний, автономний); інформаційну кооперацію; формування ефективних систем захисту інформації.

Сьогодні ефективне забезпечення безпеки підприємницької діяльності, як і всієї національної економіки, має бути системою заходів за такими взаємопов'язаними напрямами: захист від злочинного світу; захист від порушень закону з тим, щоб самим не потрапити під його санкції; захист від недобросовісної конкуренції; захист від протиправних дій власних співробітників.

Забезпечення інформаційної безпеки підприємницької діяльності в Україні має базуватися на таких специфічних принципах, як принцип превентивного характеру проведення її заходів та принцип адекватної інформованості об'єктів безпеки, в тому числі і міжнародних. У цьому зв'язку виникає потреба розробки конкретних механізмів реалізації зазначених принципів.

Ключові слова: *інформаційна безпека, підприємницька діяльність, державне управління, інформаційна безпека держави, механізми забезпечення інформаційної безпеки.*

Постановка проблеми. Інформаційна безпека характеризується мірою захищеності держави (суспільства) та стійкості основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи тощо) відносно небезпечних (дестабілізуючих, деструктивних, що уражають державні інтереси і таке інше) інформаційних впливів, причому як з упровадження, так і добування інформації. Інформаційна безпека держави визначається здатністю нейтралізувати такі впливи. Джерелами дестабілізуючих факторів можуть бути як окремі особи, так і організації та їхні об'єднання. Сукупність джерел разом із властивими їм видами дестабілізуючих факторів формують цілий спектр інформаційних загроз, що впливають на стан інформованості особистості, суспільства і держави.

Одним із складників забезпечення інформаційної безпеки в державі виступає забезпечення інформаційної безпеки підприємницької діяльності. На цей час своєчасна та об'єктивна інформація є важливим фактором виробництва, який розглядають як один з основних ресурсів розвитку суспільства. Паралельно з розвитком і ускладненням засобів, методів, форм автоматизації процесів обробки інформації підвищується залежність суб'єктів підприємництва від ступеню безпеки використовуваних ними інформаційних технологій [7, с. 205].

Аналіз останніх досліджень і публікацій. Проблематику інформаційної безпеки як склад-

ника національної безпеки, а також різноманітні аспекти державного управління та державної політики щодо забезпечення безпеки національного інформаційного простору аналізували В. Абрамов, О. Барановський, І. Бінько, З. Варналій, О. Власюк, А. Гальчинський, В. Горбулін, Н. Грицяк, А. Качинський, В. Мунтіян, Г. Почепцов, Г. Ситник, О. Соснін, А. Сухоруков, Т. Ткачук, С. Федуняк, Я. Чернятевич, С. Чукут, І. Шевчук, В. Шлемко та інші. Проте залишаються недостатньо дослідженими питання вироблення спеціалізованого інструментарію інформаційної безпеки підприємницької діяльності для забезпечення безпеки національної економіки в сучасних цивілізаційних умовах.

Мета статті – виділення механізмів забезпечення інформаційної безпеки підприємницької діяльності як складника інформаційної безпеки держави.

Виклад основного матеріалу дослідження. У найзагальнішому випадку інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави. Під інформаційним середовищем розуміють сферу діяльності суб'єктів, пов'язану зі створенням, перетворенням і споживанням інформації. Інформаційне середовище умовно поділяється на такі предметні частини:

− створення і розповсюдження вихідної та похідної інформації;

− формування інформаційних ресурсів, підготовки інформаційних продуктів, надання інформаційних послуг;

− споживання інформації;

− створення і застосування інформаційних систем, інформаційних технологій і засобів їхнього забезпечення;

− створення і застосування засобів і механізмів інформаційної безпеки.

Слід відзначити, що задоволення в будь-якій мірі потреб в інформації призводить до оволодіння відомостями про навколишній світ та процеси, що протікають в ньому, тобто інформованості особистості, суспільства та держави [1, с. 46–48].

Концепція інформаційної безпеки держави – це систематизована сукупність відомостей про інформаційну безпеку держави та шляхи її забезпечення. У цій концепції проводиться системна класифікація дестабілізуючих факторів і інформаційних загроз безпеці особистості, суспільства і держави; обґрунтовуються основні положення з організації забезпечення інформаційної безпеки держави; розробляються пропозиції щодо способів і форм забезпечення інформаційної безпеки [1, с. 24–25].

Важливе місце у забезпеченні інформаційної безпеки держави посідає інформаційна безпека підприємницької діяльності. Загрозами інформаційній безпеці сучасного підприємства є: протизаконна діяльність деяких економічних структур у сфері формування, поширення і використання інформації; порушення встановлених регламентів збору, обробки та передачі інформації; навмисні дії та ненавмисні помилки персоналу інформаційних систем; помилки в проектуванні інформаційних систем; відмова технічних засобів і проблеми програмного забезпечення в інформаційних і телекомунікаційних системах тощо [1, с. 28].

Джерелами негативних впливів на інформаційну безпеку підприємства можуть бути:

1) свідомі чи несвідомі дії окремих посадових осіб і суб'єктів господарювання (органів державної влади, міжнародних організацій, підприємств-конкурентів);

2) збіг об'єктивних обставин (стан фінансової кон'юнктури на ринках певного підприємства, наукові відкриття і технологічні розробки, форс-мажорні обставини тощо). Залежно від суб'єктної зумовленості негативні впливи на безпеку можуть бути об'єктивними і суб'єктивними. Об'єктивними вважаються негативні впливи, які виникають не з волі конкретного підприємства або його окремих працівників. Суб'єктивні впливи можливі внаслідок неефективної роботи підприємства загалом або окремих його працівників (передовсім керівників і функціональних менеджерів).

Головна мета інформаційної безпеки підприємства полягає в тому, щоб гарантувати його стабільне й максимально ефективне функціонування тепер та високий потенціал розвитку в майбутньому.

Одним із джерел загроз інтересам суспільства в інформаційній сфері є безперервне ускладнення інформаційних систем і мереж зв'язку критично важливої інфраструктури забезпечення життя суспільства.

Ці загрози можуть проявлятися у вигляді як навмисних, так і ненавмисних помилок, збоїв і відмов техніки і програмного забезпечення, шкідливого впливу з боку злочинних структур і кримінальних елементів. Об'єктами реалізації таких структур можуть виступати системи енергетичної, транспортної, трубопровідної і деяких інших елементів інфраструктури.

Небезпечним джерелом загроз виступає можливість концентрації засобів масової інформації в руках невеликої групи власників. Ці загрози можуть проявлятися у вигляді маніпуляції суспільною думкою по відношенню до тих чи інших суспільно значимих подій, а також руйнування моральних устоїв суспільства шляхом нав'язування чужорідних цінностей.

Нарешті, небезпечним джерелом загроз є розширення масштабів вітчизняної і міжнародної комп'ютерної злочинності. Ці загрози можуть проявлятися у вигляді спроб здійснення шахрайських операцій з використанням глобальних або вітчизняних інформаційно-телекомунікаційних систем, відмивання фінансових коштів, одержаних протиправним шляхом, одержання неправомірного доступу до фінансової, банківської та іншої інформації, яка може бути використаною з корисливою метою [6, с. 19–20].

Крім цього, існують три загальні зовнішні джерела загрози функціонуванню фірми.

Передусім це несприятлива для підприємства економічна політика держави. Маніпулювання (з метою регулювання економіки) валютним курсом, ставками митного тарифу, податків тощо можуть входити в протиріччя з виробництвом, комерційною і фінансовою політикою держави. Крім вищезгаданого, реальну загрозу для підприємства являють адміністративні дії влади, насильницьке звуження сфери товарно-грошових відносин, порушення (з боку державних органів) законів, що регламентують підприємницьку діяльність, перевищують встановлену компетенцію у взаємовідносинах з підприємством, необґрунтоване втручання в його виробничу, фінансову і комерційну діяльність, зазіхання на власність підприємства тощо. Під час виходу на зовнішні ринки підприємство може також зазнати негативного впливу в результаті несприятливої економічної політики іноземних держав.

Іншим джерелом зовнішньої загрози для комерційної діяльності підприємства є дії деяких господарчих суб'єктів. Насамперед йдеться про недобросовісну конкуренцію, яка, до речі, різними джерелами трактується по-різному. Так, наприклад, згідно з міжнародно-правовими нормами вирізняють три види недобросовісної конкуренції: всі дії, що ведуть до того, щоб комерційну діяльність однієї фірми представити споживачу як комерційну діяльність іншої; дискредитація комерційної діяльності конкурента за допомогою розповсюдження неправдивої інформації; неправомірне використання в процесі комерційної діяльності позначок, що можуть ввести споживача в оману.

Як показує закордонна статистика, втрати від промислового шпигунства у світі оцінюються десятками мільярдів доларів. Тільки в США з цієї причини в системах захисту таємної інформації приватного сектора зайнято біля 1,5 млн чоловік, що набагато більше, ніж чисельність державних служб безпеки. На промисловому шпигунстві спеціалізуються і наживаються окремі фірми, використовуючи у своїй роботі фахові і найчастіше протизаконні методи добування інформації.

Забезпечення інформаційної безпеки – це сукупність заходів, призначених для досягнення стану захищеності потреб особистостей, суспільства і держави в інформації.

Держава здійснює свої заходи через відповідні органи, а громадяни – через суспільні організації і об'єднання, що мають відповідні повноваження. В основу забезпечення інформаційної безпеки держави повинні бути покладені такі принципи:

− законність, дотримання балансу інтересів особистості, суспільства і держави;

− взаємна відповідальність суб'єктів забезпечення інформаційної безпеки;

− інтеграція систем національної і міжнародної безпеки.

Специфічними принципами забезпечення інформаційної безпеки є:

− превентивний характер проведення її заходів стосовно заходів інших видів безпеки;

− адекватна інформованість об'єктів безпеки, в тому числі і міжнародних.

Превентивність зумовлена властивою людині послідовністю виконання операцій, що складає будь-яку елементарну дію. Усе починається з приймання (добування) інформації, а закінчується активною дією: реакцією на одержану інформацію. Оскільки це справедливо по відношенню до будь-якого виду діяльності, то можна стверджувати, що цей принцип є загальним, і його дія розповсюджується на всі сфери безпеки особистості, суспільства та держави.

Адекватна інформованість об'єктів безпеки означає, що всі вони мають право володіти інформацією про явища і процеси, що їх цікавлять, яке обмежене тільки законодавчо з метою охорони особистої, сімейної, професійної, комерційної та державної таємниці, а також моралі [3, с. 34].

Права та свободи суспільства в питаннях пошуку, володіння та розповсюдження інформації повинні регулюватися законодавчими актами, які видаються щодо специфіки діяльності суспільних

об'єднань та організацій або змісту інформації. Наприклад, адекватна інформованість суспільства про його матеріальні цінності досягається у сфері нормотворчості та правозастосування законодавства про захист комерційної таємниці. Права та свободи суспільства в духовній сфері повинні захищати законодавчі акти, які визначають порядок освіти та функціонування освітніх, просвітницьких, культурних, релігійних організацій, а також засобів масової інформації. В основі прав і свобод держави у сфері її інформованості з питань світової політики, економіки, науки, ресурсів, екології, оборони тощо лежать діючі норми та принципи міждержавного права. Головним слід вважати принцип рівної безпеки. Щодо інформаційної сфери, то можна говорити про його трансформацію в принцип адекватної інформованості держав світового співтовариства, який передбачає право кожної держави на інформаційну безпеку, забезпечення інформаційної безпеки усіх членів співтовариства рівною мірою, врахування інтересів усіх сторін без будь-якої дискримінації, виключення односторонніх переваг, відмова від дій, що наносять шкоду іншій державі.

Законодавча база, яка визначає перелік відомостей, що віднесені до державної таємниці, механізм та порядок її захисту повинні розроблюватися з огляду на наведений принцип, а також багатосторонні угоди держав, які входять до міжнародної системи інформаційної безпеки. Формування останньої буде, очевидно, справою далекої перспективи, яка ознаменує собою вищий рівень прояву довіри та зацікавленості держав світового співтовариства в забезпеченні виконання на практиці принципу адекватної інформованості. Така система повинна стати підсистемою у системі колективної безпеки [4].

Державна система забезпечення інформаційної безпеки країни являє собою організаційне об'єднання державних органів, а також сил та засобів інформаційної безпеки, що виконують свої функції на основі закону під контролем і захистом судової влади. Державна система складає найважливішу ланку системи інформаційної безпеки особистості, суспільства і держави в правовій державі. Основними завданнями такої системи є:

а) виявлення і прогнозування дестабілізуючих факторів і інформаційних загроз життєво важливим інтересам особистості, суспільства та держави;

б) здійснення комплексу оперативних і довготривалих заходів з їхнього попередження і усунення;

в) створення і підтримання в готовності сил та засобів забезпечення інформаційної безпеки.

Органи (служби) інформаційної безпеки можуть створюватися (на законодавчих засадах) і в недержавних структурах для захисту своїх потреб в забезпеченні необхідною інформацією. Ці органи на основі укладення відповідних угод можуть бути приєднані до єдиної державної системи інформаційної безпеки.

Натепер окремі елементи системи інформаційної безпеки створені та функціонують (органи зовнішньої розвідки, інформаційні служби різноманітних міністерств, система технічного та криптографічного захисту інформації держави і таке інше). Проте для їхнього функціонування ще недостатня правова база. Зміст діяльності органів інформаційної безпеки також ще не повною мірою відповідає покладеним на них завданням. Це пояснюється в першу чергу недостатнім опрацюванням питань, що стосуються форм і способів забезпечення інформаційної безпеки [5, с. 2–3].

Форми і способи забезпечення інформаційної безпеки утворюють власне інструмент, з допомогою якого сили інформаційної безпеки вирішують весь комплекс завдань із захисту життєво важливих інтересів особистості, суспільства та держави. Тому необхідне чітке юридичне оформлення під час розробки нормативних актів, які регулюють діяльність органів інформаційної безпеки.

Інформаційний патронат – форма забезпечення інформаційної безпеки фізичних і юридичних осіб з боку держави. Він припускає забезпечення органів управління системи інформаційної безпеки держави відомостями про дестабілізуючі фактори і загрози стану інформованості фізичних і юридичних осіб (інформаційне забезпечення інформаційної безпеки) і, власне, захист життєво важливих інтересів цих осіб від інформаційних загроз або, як ще кажуть, – інформаційний захист [8].

При цьому інформаційне забезпечення інформаційної безпеки включає збирання (добування) відомостей про дестабілізуючі фактори та інформаційні загрози, їхню обробку, обмін інформацією між органами керування і силами та засобами системи інформаційної безпеки. Його основу складає збирання (добування) необхідних відомостей, здійснюване в процесі розвідувальної, контррозвідувальної, оперативно-розшукової і оперативно-інформаційної діяльності.

Інформаційний захист досягається шляхом внесення в порядок законодавчої ініціативи законопроектів, здійснення судового захисту,

проведення оперативних заходів силами і засобами інформаційної безпеки.

Інформаційна кооперація – це форма забезпечення інформаційної безпеки між рівноправними суб'єктами інформаційного процесу (фізичними, юридичними, міжнародними), який включає сукупність їхніх взаємоузгоджених дій, спрямованих на одержання відомостей про дестабілізуючі фактори, дестабілізуючі й інформаційні загрози та захист від них доступними законними способами і засобами.

Для конкретної особистості такими способами і засобами можуть бути:

− судовий захист прав і свобод у використанні інформації;

− адміністративний захист її життєво важливих інтересів у інформованості з боку територіальних або відомчих органів інформаційної безпеки;

− автономний захист своїх прав і свобод в основному із застосуванням технічних засобів захисту, особистої, сімейної і професійної таємниці.

Це ж характерно і для суспільних об'єднань, організацій (підприємств). Водночас, за наявності у них власних органів інформаційної безпеки, їхні можливості у сфері автономного захисту суттєво розширюються [2, с. 220–225].

Оскільки в будь-якій системі всі елементи та підсистема є взаємопов'язаними, більшість завдань інформаційної безпеки виконується разом із основними та допоміжними підсистемами системи економічної безпеки підприємства.

Технічний складник покликаний забезпечити захист інформації та об'єктів підприємства, а також виявлення фактів витікання інформації та неправомірних дій персоналу та сторонніх осіб щодо цього підприємства за допомогою технічних засобів.

Організаційний складник повинен, на нашу думку, забезпечити належне поводження персоналу підприємства із секретною інформацією та іншими об'єктами захисту господарюючого суб'єкта.

Дозвільний складник системи інформаційної безпеки має здійснювати розподіл інформації підприємства за рівнями секретності та визначити ступінь доступу до неї. Для уникнення ефекту дезінформації та прийняття внаслідок цього хибних управлінських рішень, а також максимального зниження ймовірності витікання секретної інформації система інформаційної безпеки має включати попереджувальний складник. Правовий складник покликаний забезпечити правовий захист інтересів підприємства щодо захисту інформації, а також закріплення прав підприємства щодо комерційної таємниці в установчих документах, договорах та інших нормативних актах. Системи захисту інформації, що пропонуються науковцями та практиками, не відображають повною мірою вирішення завдань та виконання функцій, які стоять перед захистом інформації в системі інформаційної безпеки, інформаційного забезпечення та економічної безпеки загалом, у сучасних умовах. Основними завданнями системи захисту інформації можна вважати наступні:

− організація особливого діловодства та контролю за секретними документами;

− виявлення, попередження та присікання каналів витікання інформації;

− створення посадових інструкцій, а також положень, пам'яток, методичних вказівок для роботи з відомостями, що складають комерційну таємницю;

− захист інформації під час використання комп'ютерної техніки та інших технічних засобів обробки та передавання даних;

− виявлення необхідності, обґрунтування та організація встановлення необхідних технічних засобів забезпечення збереження інформації;

− захист у судових та інших державних органах інтересів підприємства щодо комерційної таємниці;

− розроблення нормативної документації щодо комерційної таємниці на підприємстві;

− навчання правилам інформаційної безпеки працівників.

Оскільки система захисту інформації становить найбільш вагому частку в інформаційній безпеці, отже, й більшість складників у системі інформаційної безпеки становлять саме складники захисту інформації. Так, технічний, організаційний та правовий складник належать саме до системи захисту інформації. Також до системи захисту інформації належить попереджувальний складник у частині передбачення, виявлення та перекриття каналів витікання інформації.

Сьогодні ефективне забезпечення безпеки підприємницької діяльності, як і всієї національної економіки, уявляється спеціалістам в цій сфері як система заходів, яка працює у таких взаємопов'язаних напрямах:

а) захист від злочинного світу;

б) захист від порушень закону з тим, щоб самим не потрапити під його санкції;

в) захист від недобросовісної конкуренції;

г) захист від протиправних дій власних співробітників.

Через те, що чинників, що являють загрозу для фірми, достатньо багато, доцільно всю роботу із забезпечення безпеки координувати з єдиного виконавчо-розпорядчого органу, який називають «службою (відділом) безпеки». Ця служба «тримає руку на пульсі» практично всіх ланок фірми і запроваджує ефективні заходи протидії руйнівним чинникам, використовуючи для цього, за необхідності, не тільки свої сили, але і сили усієї фірми, а в окремих випадках – і сили зовнішніх організацій.

Безпека сучасного комерційного підприємства забезпечується за допомогою таких режимів:

1) конфіденційності і захисту об'єктів інтелектуальної власності, що складає інформаційну безпеку;

2) фізичної охорони, тобто забезпечення фізичної безпеки майна і персоналу фірми.

За тих умов, що існують на українському ринку, розраховувати на ефективний захист своїх життєво важливих інтересів підприємець може лише: якщо він здатний організувати процедурно-орієнтований процес, який повинен бути націлений на позбавлення потенційного супротивника інформації про виробничі і торговельні можливості і наміри підприємства, головним чином шляхом виявлення та усунення індикаторів (тобто демаскуючих ознак, каналів витоку інформації), пов'язаних з плануванням і здійсненням підприємницької діяльності; якщо в цьому процесі будуть задіяні всі службовці підприємства, а не тільки служба безпеки.

Ідея методу системного підходу до проблем забезпечення інформаційної безпеки полягає в тому, щоб припинити, скоротити або, в крайньому разі, обмежити виток тих часток цінної інформації, які можуть дати конкурентам можливість наперед виявити, що саме в певний момент керівництво фірми планує та здійснює.

На жаль, в Україні майже повністю відсутні такі необхідні для реалізації системного підходу складники, як:

− достатньо повна законодавча база, що регулює основні відносини у сфері бізнесу, наприклад, у нас недостатньо розвинуте приватне право і юридичне забезпечення економічної діяльності;

− відпрацьований механізм економічної реформи на загальнодержавному і регіональному рівні;

− достатній рівень включення суспільства в процеси економічних перебудов;

− державна програма боротьби з розповсюдженою у сфері національної економіки корупцією;

− ефективна національна статистика і контроль.

Будь-яке ігнорування законів ринкової економіки і потреб економічної безпеки дуже часто призводить до того, що марнуються корисні угоди, укладаються контракти з недобросовісними партнерами, приймаються на роботу особи з низькими моральними устоями або такими, що являються «підставою» недобросовісних конкурентів чи навіть організованої злочинності. Отже, легше, дешевше і корисніше зберігати необхідний рівень економічної безпеки, ніж вести довгі і не завжди перспективні судові процеси, що вимагають значних витрат, намагаючись захистити свої права.

Висновки. Серед основних механізмів забезпечення інформаційної безпеки підприємницької діяльності в Україні як складника інформаційної безпеки держави доцільно виділити: інформаційний патронат; інформаційний захист (судовий, адміністративний, автономний); інформаційна кооперація; формування ефективних систем захисту інформації.

Сьогодні ефективне забезпечення безпеки підприємницької діяльності, як і всієї національної економіки, має бути системою заходів за такими взаємопов'язаними напрямами: захист від злочинного світу; захист від порушень закону з тим, щоб самим не потрапити під його санкції; захист від недобросовісної конкуренції; захист від протиправних дій власних співробітників.

Забезпечення інформаційної безпеки підприємницької діяльності в Україні має базуватися на таких специфічних принципах, як: превентивний характер проведення її заходів; адекватна інформованість об'єктів безпеки, в тому числі і міжнародних. Тут виникає потреба розробки конкретних механізмів реалізації зазначених принципів, що зумовлює перспективи подальших досліджень у цьому напрямі.

Список літератури:

1. Е-майбутнє та інформаційне право / за ред. М. Швеця. 2-е вид., доп. Київ: НДЦПІ АПрН України, 2006. 234 с.

2. Информатика: учебник / под. ред. Н.В. Макаровой. 3-е перераб. изд. Москва : Финансы и статистика, 2000. 768 с.

3. Копылов В.А. Информационное право: учеб. пособие. Москва : Юристь, 1997. 472 с.
4. Корженівський О. Загальне поняття інформації. *Пульсар*. 2001. № 4. С. 7.
5. Марущак А.І. Правомірні засоби доступу громадян до інформації : наук.-практ. посібник. Біла Церква : Буква, 2006. 432 с.
6. Правове забезпечення інформаційної діяльності в Україні / за заг. ред. Ю.С. Шемшученка, І.С. Чижа. Київ : Юридична думка. 2006. 384 с.
7. Скакун О.Ф. Теорія держави і права: підручник. Харків: Консул. 2001. 656 с.
8. Субіна Т. Поняття і сутність інформації у просторі держави. *Науковий вісник Національної академії ДПС України*. 2004. № 4 (26). С. 210–211.

Hornyk V.G., Kravchenko S.O. MECHANISMS FOR PROVIDING OF INFORMATION SECURITY IN ENTREPRENEURIAL ACTIVITY AS COMPONENT OF STATE INFORMATION SECURITY

Approaches to determining the place and role of information security in business are studied. It is proved that the improvement of legal mechanisms for regulating public relations that arise in the information sphere is a priority of state policy in the field of information security in business in Ukraine. It is established that information security in business provides: assessment of the effectiveness of the application of current legislative and other normative legal acts in the information sphere and development of a program for their improvement; creation of organizational and legal mechanisms to ensure information security; determination of the legal status of all subjects of relations in the information sphere, including users of information and telecommunication systems, and establishing their responsibility for compliance with the legislation of Ukraine in this area.

The main mechanisms for providing of information security in entrepreneurial activity in Ukraine as a component of state information security are: information patronage; information protection (judicial, administrative, autonomous); information cooperation; building of efficient systems of information security in business.

Today efficient providing of information security in entrepreneurial activity similarly as in national economy must be the system of measures in such interrelated directions: protection from criminal groups; protection from violation of law; protection from unfair competition; protection from wrongful actions of own employees.

Providing of information security in entrepreneurial activity in Ukraine has to be based on such special principles: preventive nature of its measures; appropriate informing for security objects, including international. The need for development of concrete mechanisms for implementation of mentioned principles arises in this relation.

Key words: *information security, business activity, state governance, state information security, mechanisms for providing of information security.*