ПРОБЛЕМИ ПРАВОВОГО ВИЗНАЧЕННЯ КОНЦЕПТУАЛЬНОЇ МОДЕЛІ РОЗУМІННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМНИЦТВА ЯК УНІВЕРСАЛЬНОГО ОБ'ЄКТА СУСПІЛЬНИХ ВІДНОСИН У СКЛАДІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

ЛИСЕНКО Сергій Олексійович - кандидат юридичних наук, доцент, доцент кафедри управління безпекою, правоохоронної та антикорупційної діяльності, Міжрегіональна Академія управління персоналом, м. Київ

Статья посвящена проблеме формирования концептуальной модели понимания информационной безопасности предпринимательства с точки зрения права. Автор анализирует специфику отечественного правового регулирования отношений между субъектами информационного права и государством через призму информационной безопасности предпринимательства.

Ключевые слова: информационное право, модель информационной безопасности, информационная безопасность предпринимательства, правовой механизм, общественные отношения.

Актуальність обраної теми

Бурхливий розвиток інформаційних технологій породжує не лише нові можливості, але й нові загрози для підприємницької діяльності. З одного боку з'являються нові технічні, інформаційні можливості для зловживань, не обмежені, оскільки банально не передбачені законодавством, з іншого – новий інструментарій для давно відомих правопорушень, що дозволяє вправно обходити чинні норми регулювання підприємницької діяльності. У таких умовах реформування вітчизняного інформаційного права є не просто нагальною потребою, а вкрай пріоритетною задачею як для теоретиків права, так і для правотворців. Національна інформаційна безпека в ідеалі повинна базуватися на концептуальних, наукових і методологічних розробках, систематизованих і об'єднаних в єдину концепцію. Лише такий підхід дозволить державі гідно відповідати вимогам часу, а вітчизняному підприємництві належним чином конкурувати в умовах розвитку інформаційних технологій.

Мета дослідження: проаналізувати специфіку вітчизняного правового регулювання відносин між суб'єктами інформаційного права та державою крізь призму інформаційної безпеки підприємництва

Аналіз попередніх досліджень та публікацій

Окремим аспектам інформаційного права в цілому та інформаційної безпеки підприємництва зокрема вже присвячували свою увагу численні вітчизняні та зарубіжні вчені: П. Д. Біленчук, О. Р. Бойкевич, Т. Г. Васильців, В. І. Волошин, Р. Гриценко, О. В. Іляшенко, С. В. Кавун, В. В. Каркавчук; Б. В. Романюк, В. С. Цимбалюк та інші. Водночас поява нових загроз безпеці підприємництва в ході бурхливого розвитку інформаційних технологій та трансформації суспільних відносин вимагає проведення нових, комплексних досліджень окресленої сфери, з метою формування концептуальної моделі розуміння інформаційної безпеки підприємництва як універсального об'єкта суспільних відносин у складі національної безпеки.

Основний зміст

У сучасній науці передбачені різні підходи до правового визначення концептуальної моделі розуміння інформаційної безпеки підприємництва. Вони представляють собою сукупність прийомів, способів правового регулювання, здійснюваних державою та адміністрацією підприємств та спрямованих на забезпечення інформаційної безпеки підприємництва. У правовій науці виділяють наступні методи правового регулювання, що містяться в законодавчих актах забезпечення інформаційної безпеки: імперативний, диспозитивний, заохочувальний і рекомендаційний. Галузеве правове регулювання забезпечується імперативним і диспозитивним методами. Хоча пояснити особливість галузевого регулювання названими методами не можна. У різних галузях права присутні різні поєднання зазначених методів. На основі правових положень та дослідження стану правового забезпечення інформаційної безпеки можна дійти висновку, що для правових норм, що містяться в законодавстві в галузі забезпечення інформаційної безпеки, характерно використання всіляких засобів і прийомів, імперативних і диспозитивних підходів, які свідчать про великі схожості з галузями публічного права, особливо з адміністративним законодавством, а також застосування методів заохочувального і рекомендаційного характеру [1, с. 89].

Спробуємо дослідити структурні компоненти методу правового визначення в інформаційному праві: встановлення меж інформаційних відносин; видання відповідних нормативних правових актів, що визначають права і обов'язки суб'єктів; наділення учасників інформаційних відносин відповідною правоздатністю і дієздатністю; визначення заходів юридичної відповідальності у випадках порушення встановлених норм. Багатоаспектність і специфіка інформації, громадських відносин, пов'язаних зі збором, обробкою і зберіганням інформації та забезпеченням інформаційної безпеки, приводять до необхідності застосування правових норм і використання всього відомого кола методів правового регулювання в залежності від виду та призначення інформації.

Логічно зробити висновок про єдність в інформаційному праві всіх зазначених методів правового визначення та приведення всього переліку регулюючих, контрольних, примусових, каральних і стимулюючих заходів.

Особливу актуальність набуває визначення врегулювання суспільних відносин, пов'язаних із запобіганням поширенню протиправної інформації за допомогою використання інформаційно-телекомунікаційних мереж, недопущенням поширення інформації терористичного і екстремістського характеру.

Концептуальна модель інформаційної безпеки повинна приділяти увагу проблемам протидії використанню Інтернету в терористичних і екстремістських, а також в інших протиправних цілях для забезпечення інформаційної безпеки особистості, суспільства і держави, що є важливою складовою забезпечення національної безпеки. Слід визначати необхідність координувати діяльність державних органів виконавчої влади з правового забезпечення інформаційної безпеки і впровадження систем інформаційно-технологічного забезпечення адміністративних процесів на основі міжвідомчої взаємодії. Рівень взаємодії і використання сучасних інформаційних технологій недостатній для підвищення ефективності діяльності органів державної влади. В цьому вбачається сенс створення концептуальної моделі, яка торкається державного рівня виконавчої влади та регіонального, де ті ж самі проблеми вимагають єдиних позицій і підходів [2, с. 98].

Концептуальна модель вирішення проблеми забезпечення інформаційної безпеки підприємств в умовах демократичного суспільства, множинності господарюючих суб'єктів з різними організаційно-правовими формами, ставленням до власності і високим ступенем самостійності в прийнятті управлінських рішень вимагає збалансованого підходу до нормативно-правового регулювання цієї сфери діяльності. Методика оцінки рівня та достатності заходів безпеки підприємств повинна носити універ-

сальний характер і встановлювати єдиний підхід до аналізу, незалежно від відомчої належності об'єктів, їх організаційно-правових форм, форм власності та сфери діяльності. Така можливість існує і може бути реалізована при системному підході створення моделей, до формування їх правової бази у сфері забезпечення безпеки підприємств [3].

Різноманітність видів корпоративної інформації робить вкрай скрутним встановлення загальних критеріїв, на підставі яких інформація може бути віднесена до загальнодоступної. Це призводить до необхідності вирішувати питання про доступність інформації шляхом закріплення в нормативних актах підприємств. Крім того, при правовому регулюванні відносин, пов'язаних із забезпеченням доступу до інформації, необхідно акцентувати увагу на змістовному аспекті інформації і говорити про доступ до інформації як можливості сприйняти конкретний зміст.

Систему забезпечення державної політики в галузі інформаційної безпеки являє сукупність державних органів і недержавних суб'єктів, що беруть участь у здійсненні інформаційного супроводу забезпечення державної політики і встановлених нормативними правовими актами відповідних суспільних відносин. Національна інформаційна безпека повинна базуватися на концептуальних, наукових і методологічних розробках, систематизованих і об'єднаних в єдину концепцію. Концептуальну модель інформаційної безпеки слід формувати як сукупність цілей, що відображають приватні і національні інтереси в інформаційній сфері; стратегії і тактики управлінських рішень і методів їх реалізації, що розробляються і реалізуються державною владою для регулювання і вдосконалення як безпосередньо процесів інформаційної взаємодії в усіх сферах життєдіяльності суспільства і держави, так і процесів технологічного забезпечення такої взаємодії між державою та підприємством [4, с. 30].

В області правового визначення концептуальної моделі забезпечення інформаційної безпеки можна виділити наступні основні напрямки:

- захист прав особистості, інтересів суспільства і держави;

- захист інформації;

- забезпечення сталого функціонування інформаційно-телекомунікаційних систем і мереж;

- розвиток міжнародного співробітництва в галузі безпеки глобального інформаційного простору;

- відкритість у реалізації функцій органів державної влади, регіональних органів державної влади, громадських об'єднань та підприємств, що передбачає інформування суспільства про їх діяльність з урахуванням обмежень, встановлених законодавством України;

- правова рівність усіх учасників процесу інформаційної взаємодії незалежно від їх політичного, соціального та економічного статусу, що ґрунтується на конституційному праві громадян на вільний пошук, отримання, передачу, виробництво і поширення інформації будь-яким законним способом [4, с. 31].

Отже, правовий механізм у складі механізму функціонування моделі інформаційної безпеки підприємства слід розглядати як сукупність правових норм та формальних інституцій, з використанням яких регулюються інформаційні взаємовідносини підприємства у межах чинного законодавства у забезпеченні його інформаційної безпеки.

Сукупність правових норм, що регулюють інформаційні взаємовідносини підприємства в межах чинного законодавства у забезпеченні інформаційної безпеки підприємства достатньо велика, що зумовлює необхідність деякого упорядкування цих норм:

- норми внутрішніх правових процедур та правовідносин на підприємстві;

- норми зовнішніх правовідносин підприємства;

- норми арбітражного процесуального права;

- механізми виконання рішень [5, с. 228].

Норми правових процедур на підприємстві регулюють інформаційні процеси у підприємстві, прописують процедури їх

реорганізації та ліквідації. Норми внутрішніх правовідносин на підприємстві регулюють інформаційні правовідносини всередині підприємства, вирішують правові питання, пов'язані із забезпеченням стану захищеності інформації. Норми зовнішніх правовідносин підприємства регулюють інформаційні правовідносини підприємства і держави, інших суб'єктів зовнішнього середовища (суб'єктів права), дозволяють вирішити правові питання взаємовідносин цих суб'єктів господарювання у сфері захисту від небезпек зовнішнього середовища. Норми арбітражного процесуального права регулюють функцію арбітражного процесуального права, вирішують питання розгляду господарських спорів. Механізми виконання рішень реалізують процедуру виконання рішень арбітражного суду, сприяють практичній реалізації вирішення арбітражних спорів між суб'єктами господарської діяльності [6, с. 26].

Основним завданням визначення моделі інформаційної безпеки підприємств є встановлення її місця в системі національної безпеки. Кожна концептуальна модель інформаційної безпеки повинна бути складовою цеглиною загальної національної безпеки України. В такому сенсі, доля недержавних суб'єктів інформаційної безпеки буде перевищувати кількість державних, що дасть можливість розвитку здорової конкуренції та фінансової економії. Скорочення державних суб'єктів повинно відбуватись паралельно із наданням їм додаткових повноважень нагляду за недержавними суб'єктами, одночасно із підвищенням відповідальності обох видів суб'єктів за невиконання або неналежне виконання своїх обов'язків.

Правові відносини між підприємством та державою реалізуються за рахунок надання гарантій інформаційних прав суб'єктам підприємницької діяльності. Держава гарантує всім підприємствам, незалежно від організаційно-правової форми діяльності, рівні права і створює рівні можливості у доступі до інформаційних ресурсів. Гарантії інформаційних прав полягають у тому, що держава гарантує недоторканність права на інформацію і забезпечує захист права власності підприємця. У моделі інформаційної безпеки підприємства відносини із державою відображаються у повноваженнях які надано державними органами суб'єктам підприємства У цих відносинах домінуючі позиції належать державі [7]. Проте не менш важливим елементом інформаційно-правових відносин підприємства з державою є відносини з приводу ліцензій, дозволів та нормативів, дотримання яких убезпечує підприємство від непродуктивних витрат (наприклад, штрафи) [8, с. 8].

Механізм правових відносин з суб'єктами зовнішнього та внутрішнього сфери діяльності підприємства дозволяє сформувати відносини у правовому полі. При формуванні правових відносин підприємства із суб'єктами зовнішньої сфери обов'язково слід враховувати, що інформаційна безпека підприємства суттєво залежить від дотримання норм чинного законодавства у відносинах з діловими партнерами. Залежність рівня інформаційної безпеки підприємства від його правової поведінки зростатиме в залежності від розвитку інформаційного суспільства в Україні, що зумовлює зростання значення механізму правових відносин підприємства з державою [9, с. 31].

Інформаційні відносини підприємства із суб'єктами зовнішньої сфери діяльності базуються виключно на договірних засадах. Відповідно до Господарського кодексу України майново-господарські зобов'язання, які виникають між суб'єктами господарської діяльності або між суб'єктами господарської діяльності і негосподарюючими суб'єктами – юридичними особами на основі господарських договорів, є господарсько-договірними зобов'язаннями [10]. Така норма господарського права забезпечує стан захищеності обох сторін укладеного договору.

Механізм правових відносин з суб'єктами зовнішньої та внутрішньої сфери діяльності, що мають або реалізують злочинні наміри відносно інформаційної діяльності підприємства, призначений для безпосереднього забезпечення надійності інформаційної моделі підприємства. Такий механізм реалізує попереджувальну функ-

цію моделі інформаційної безпеки підприємства.

Складність моделі інформаційної безпеки підприємництва виявляється не лише у чисельності її елементів, а також й у наявності багатьох процесів, що забезпечують взаємозв'язок та взаємодію цих елементів. Взаємодію елементів моделі інформаційної безпеки підприємництва (об'єктів безпеки, суб'єктів та способів захисту), реалізацію організаційних стосунків та виконання моделлю функцій, забезпечує механізм функціонування моделі. Метою дії механізму функціонування моделі інформаційної безпеки підприємництва є забезпечення безперервного та результативного функціонування моделі інформаційної безпеки підприємства шляхом виконання функцій моделі у певному режимі для захисту об'єктів безпеки системи від небезпек та загроз [11, с. 114].

Функціонування моделі інформаційної безпеки підприємництва побудовано з використанням сукупності принципів, відповідно до яких немає «важливих» та «неважливих» або головних та другорядних елементів. Враховуючи, що модель інформаційної безпеки підприємства за своєю суттю є інформаційною системою, механізм функціонування, що приводить систему в дію, також є інформаційним. Тому методичною основою побудови функціонування моделі на конкретному підприємстві є кінематичний та динамічний аналіз руху інформації, що стосується захисту об'єктів безпеки моделі інформаційної безпеки підприємства. Такий аналіз повинен визначити траєкторії руху інформації між елементами кінематичних ланцюгів, можливості цих елементів здійснювати утримання та оброблення інформації, зіставити швидкість та можливості зміни швидкості дії окремих елементів та виявити на цій основі проблемні місця, обрахувати наявну та потрібну потужність руху, встановити номенклатуру та характеристики сил спротиву роботі механізму та рушійних сил, здатних долати цей спротив [12, с. 142].

За правовим розумінням функціонування моделі інформаційної безпеки підприємства є ієрархічним, тобто містить сукупність елементів, що розташовуються за рівнями ієрархії. Численність рівнів і елементів у механізмі функціонування моделі інформаційної безпеки підприємництва пояснюється тим, що ця діяльність, як і будь-яка підприємницька діяльність, пов'язана з використанням ресурсів та нематеріальних активів, що мають ринкову ціну та беруть участь у загальноринкових відносинах. Це визначає принциповий набір елементів у складі функціонування моделі інформаційної безпеки підприємництва.

У складі процесу функціонування моделі інформаційної безпеки підприємництва провідну роль відіграє завдання захисту інформаційної діяльності підприємства. Другорядним завданням є підтримання національної інформаційної безпеки. Процес захисту інформаційної діяльності підприємства розуміється як сукупність взаємопов'язаних структурних елементів, що у послідовних діях формують стан захищеності об'єктів безпеки моделі інформаційної безпеки підприємства, тим самим забезпечуючи безпеку його інформаційної діяльності. Процес забезпечення інформаційної безпеки підприємства слугує вмикачем процесів у більшості механізмів, що входять до його складу, які необхідні для захисту об'єктів моделі інформаційної безпеки підприємництва. Відповідно до вимог системного підходу, забезпеченню інформаційної безпеки підприємництва притаманні цілеспрямованість, подільність, унікальність елементів, відкритість, динамізм [13].

Для захисту інформаційної діяльності підприємства визначено складові концептуальної моделі та побудовано алгоритм її компонування. Створення моделі інформаційної безпеки підприємства базується на поєднанні процесного, предметно-функціонального та об'єктного підходів до впровадження безпекозабезпечувальних заходів. Структура процесу захисту інформаційної діяльності підприємства складається з механізмів, які регулюють конкретні зони відповідальності, де розташовані об'єкти моделі інформаційної безпеки підприємства. Формування моделі інформаційної безпеки

підприємства відбувається за кількома етапами [14, с. 128].

Правове розуміння функціонування моделі інформаційної безпеки підприємства уособлює та відображає вплив інституційного середовища на захист об'єктів моделі інформаційної безпеки підприємства. Таке розуміння розглядається як складна система інституційних заходів, інструментів, важелів, спрямованих на захист об'єктів моделі інформаційної безпеки підприємства від внутрішніх та зовнішніх загроз за рахунок такого поєднання формальних та неформальних інституцій, яке дозволяє не лише захистити об'єкти безпеки, а й дотриматися інформаційних інтересів суспільства.

Дія інституційного механізму у складі функціонування моделі інформаційної безпеки підприємництва характеризується надзвичайною складністю завдяки наявності численних формальних та неформальних інституції. Проте складність моделі інформаційної безпеки підприємства виправдовує використання такого складного інструмента. Дію інституційного механізму спрямовано переважно на налагодження взаємозв'язку із суб'єктами зовнішнього середовища, звідки надходить більшість загроз об'єктам моделі інформаційної безпеки підприємства [15, с. 264].

Інституційний напрям у розумінні забезпечення інформаційної безпеки підприємства потребував значного поглиблення правової складової, яку реалізовано шляхом дії правового механізму у складі механізму функціонування моделі інформаційної безпеки підприємства. Такий правовий механізм становить собою організовану сукупність правових інституцій та норм господарського, адміністративного та карного характеру або є системою правових засобів (способів і форм), за допомогою яких забезпечується відповідність дій підприємства щодо захисту об'єктів моделі вимогам правових норм. Складна структура правового механізму зумовлена чинниками, під впливом яких відбувається його імплементація, цілями та завданнями [16, с. 112].

Дія правового механізму моделі інформаційної безпеки підприємництва дозволяє сформувати відносини з державою щодо правил та обмежень безпекозабезпечувальних заходів, з працівниками підприємств, контрагентами та суб'єктами зовнішнього середовища. Дозволяє визначити межі законності діяльності підприємства, з потенційними та реальними суб'єктами злочинних дій відносно підприємства щодо межі можливого втручання [6, с. 84]. Таким чином, правовий механізм є складовою інституційного механізму в частині реалізації формальних інституцій (норм, правил, законів тощо) і розглядається як сукупність норм та інститутів права, що динамічно розвиваються та регулюють господарські взаємовідносини суб'єктів господарювання у межах чинного законодавства для забезпечення інформаційної безпеки підприємства. Проте правовий механізм може існувати як самостійний у ситуації, коли інституційний механізм не використовується або його роль є другорядна.

Висновки

Сучасні тенденції у галузі права характеризується утворенням нових підгалузей права, норми яких поширюються на специфічні види діяльності, що не може позитивно не позначитися на правовідносинах у сфері інформаційної безпеки. Проте в Україні відсутній окремий закон, що регулює відносини між суб'єктами інформаційного права та державою, щодо захисту комерційної діяльності та корпоративних прав від зазіхань з боку злочинних угруповань і корумпованих владних структур. Отже, норми права, які регулюють вказані відносини, містяться в окремих законах України та в підзаконних нормативних актах. Найчастіше у цих нормах права особа (як суб'єкт права) виступає не як підприємець (тобто особа, що займається підприємницькою діяльністю), а як фізична особа (тобто незалежно від роду занять).

Вищезгадане правове розуміння моделі інформаційної безпеки підприємництва дозволяє в перспективі сформувати відносини з державою, що впровадить загальний для всіх процес спілкування та інформаційних відносин.

АНОТАЦІЯ

Статтю присвячено проблемі формування концептуальної моделі розуміння інформаційної безпеки підприємництва з точки зору права. Автор аналізує специфіку вітчизняного правового регулювання відносин між суб'єктами інформаційного права та державою крізь призму інформаційної безпеки підприємництва

Ключові слова: інформаційне право, модель інформаційної безпеки, інформаційна безпека підприємництва, правовий механізм, суспільні відносини.

SUMMARY

The article was devoted to the problem of forming a conceptual model for understanding the information security of entrepreneurship in terms of law. The author analyzes the specifics of the domestic legal regulation of relations between the subjects of information law and the state through the prism of information security of entrepreneurship

Key words: information law, model of information security, information security of entrepreneurship, legal mechanism, social relations.

Література

1. Цимбалюк В. Інформаційна безпека підприємницької діяльності: визначення сутності та змісту поняття за умов входження України до інформаційного суспільства (глобальні кіберцивілізації) //Підприємництво, господарство і право. – 2004. – № 3. – С. 88-91

2. Біленчук П. Д., Романюк Б. В., Цимбалюк В. С. та ін. Комп'ютерна злочинність. Навчальний посібник.- Київ: Атіка, 2002.-240 с.

3. Близнюк І. Інформаційна безпека України та заходи її забезпечення //Науковий вісник Національної академії внутрішніх справ України. – 2003. – № 5. – С. 101-214

4. Цимбалюк В. С. Суб'єкти інформаційного права та інформаційної діяльності / В. С. Цимбалюк // Правова інформатика. – 2010. – № 3 (27). – С.29-32.

5. Бут В. В. Проблеми безпеки в інформаційній сфері – сутність понять та їх термінологічне тлумачення //Науковий вісник Національної академії внутрішніх справ України. – 2003. – № 5. – С. 225-232.

6. Фінансово-економічна безпека підприємств України: стратегія та механізми забезпечення : [монографія] / Т. Г. Васильців, В. І. Волошин, О. Р. Бойкевич, В. В. Каркавчук; за ред. Т. Г. Васильціва. – Львів: Ліга-Прес, 2012. – 386 с.

7. О. В. Потій, А. В. Лєншин, Харківський університет Повітряних Сил ім. І. Кожедуба, Харківський національний університет радіоелектроніки, Харків // Збірник наукових праць Харківського університету Повітряних Сил. – 2010. – Випуск 2(24)

8. Вертузаєв М. С., Попов А. Ф. Проблеми боротьби зі злочинністю в сфері комп'ютерної інформації // Інформаційні технології та захист інформації. – 1998. – №1. – Ст. 4-14.

9. П. Д. Біленчук, А. П. Гель, Г. С. Семаков, Криміналістична тактика і методика розслідування окремих видів злочинів. Навчал. посібник, К. : МАУП 2007 – 512с.

10. Господарський процесуальний кодекс України. // Відомості Верховної Ради України: закон від 06.11.1991, редакція від 01.05.2016 [Електронний ресурс] – режим доступу:http://zakon4.rada.gov.ua/laws/show/1798-12

11. В. С. Цимбалюк, Інформаційне право, концептуальні положення, монографія, К, Освіта України, 2011 – 426с.

12. Экономика и организация безопасности хозяйствующих субъектов / М. Медников и др. – СПб: Питер, 2004. – 288 с.

13. Holovatyi, M. (2015). The state and society: The conceptual foundations and social interaction in the context of formation and functioning of states. Economic Annals-XXI, 9-10, 4-8.

14. Шкарлет С. М. Первинні засади структурної моделі економічної безпеки підприємства / С. М. Шкарлет // Сіверянський літопис. – 2006. – No 1. – С. 124–130.

15. Штаєр О. М. Напрями забезпечення та основні складові економічної безпеки банку / О.М.Штаєр // Європейський вектор економічного розвитку. – 2011. – No 2. – С. 263–270.

16. Чорней Н. Б. Теорія систем і системний аналіз / Н. Б. Чорней, Р. К. Чорней. – К.: МАУП, 2005. – 256 с.