УДК 342.9

НАШИНЕЦЬ-НАУМОВА А.Ю., *кандидат юридичних наук,*
Національний технічний університет України
“Київський політехнічний інститут”

ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОРПОРАЦІЙ

***Анотація**. Розглянуто підходи щодо визначення поняття “інформаційна безпека корпорацій”, визначено основні ознаки при формуванні теоретичних засад інформаційної безпеки, а також складові єдиної системи забезпечення інформаційної безпеки корпорацій.*

***Ключові слова:** інформаційна безпека, корпорація, системний підхід, заходи безпеки.*

***Аннотация.** Рассмотрены подходы к определению понятия “информационная безопасность корпораций”, определены основные признаки при формировании теоретических основ информационной безопасности, а также составляющие единой системы обеспечения информационной безопасности корпораций.*

***Ключевые слова:** информационная безопасность, корпорация, системный подход, меры безопасности.*

***Summary.** The approaches regarding the definition of “information security corporations” are considered, the main features in the theoretical foundations of information security and the unified system of information security corporations are defined.*

***Keywords:** information security, corporation, systematic approach, security.*

Постановка проблеми. В наш час Україна знаходиться на переломному етапі свого розвитку. Доля проведених перетворень поставлена під питання, відповіді на які багато в чому залежать від стану і тенденцій розвитку економіки та безпеки.

Становлення безпеки корпорацій в цілому та інформаційної зокрема відбувається в складних умовах вибору концептуальних шляхів формування правової системи в Україні. Практичне вирішення багатьох проблем розвитку інформаційної безпеки корпорацій ускладнюється відсутністю її теоретичних розробок. До числа таких проблем відноситься правове регулювання інформаційної безпеки корпорацій України.

Українське законодавство далеке від стану, що відповідає принципвм сучасних європейських стандартів щодо розвитку корпорацій, в тому числі і з точки зору забезпечення їх інформаційної безпеки. Сьогодні суспільство несе величезні економічні та моральні витрати через нецивілізовані відносини у сфері інформаційного права. Назріла необхідність в дослідженні публічно-правового міжгалузевого та міжсистемного механізму регулювання інформаційної безпеки корпорацій.

Крім того, сьогодні навіть в концептуальному плані не вирішено питання про величину допустимого в країні ризику для діяльності корпоративних структур. До теперішнього часу співіснують дві точки зору: перша полягає в тому, що забезпечення інформаційної безпеки своєї діяльності – це іманентно притаманна корпораціям риса, а друга зводиться до необхідності регулювання і контролю питань інформаційної безпеки корпорацій державою. Разом з тим межі такого втручання не мають достатнього теоретичного обґрунтування.

Метою статті є теоретичне дослідження проблем правового регулювання інформаційної безпеки корпорацій та розробка рекомендацій щодо його вдосконалення.

Аналіз останніх досліджень і публікацій. Поняття “інформаційна безпека” в термінології науки з’явилось зовсім нещодавно і, як будь-який новий термін, на початковому етапі існування не має загальновизнаного тлумачення.

Сучасне законодавство має вагомий масив нормативно-правового закріплення підходів до визначення інформації, інформаційної безпеки, безпеки інформації тощо. Крім нормативного визначення, тему питання інформаційної безпеки різних суб’єктів піднімали у своїх наукових працях такі науковці: В.М. Брижко, О.С. Денісова, Р.А. Калюжний, Т.А. Костецька, О.В. Кохановська, Л.В. Кузенко, О.В. Логінов, А.І. Марущак, О.В. Нестеренко, Є.В. Петров, О.В. Соснін, В.М. Фурашев; І.Л. Бачило, В.М. Лопатин, М.А. Федотов та інші. Проте вагомі напрацювання науковців не вичерпали можливостей дослідження широкого кола питань, пов’язаних з функціонуванням і використанням інформації, а також її безпеки в корпораціях.

Огляд джерел дає змогу зробити висновок, що існуючі підходи до визначення інформаційної безпеки не є універсальними та лише частково дозволяють сформувати суб’єктивну думку про реальну сутність, цінність, наукову призначеність та орієнтованість даної категорії в інформаційному просторі. Крім того, теорія інформаційної безпеки останнім часом досить стрімко розвивається, що також обумовлює необхідність актуалізації визначення цієї категорії з урахуванням сучасного стану методологічних напрацювань і практичного інструментарію.

Виклад основного матеріалу. Актуальність питань інформаційної безпеки обумовлює доцільність формування науково обґрунтованої теоретичної бази, спрямованої на удосконалення аспектів і перегляд системи інформаційної безпеки корпорацій з огляду на сьогоднішнє розуміння даної правової категорії, тенденцій розвитку корпорацій в інформаційному середовищі.

Основні проблеми, які постають при формуванні теоретичних засад інформаційної безпеки корпорацій, можна згрупувати за такими ознаками:

- невідкладні – проблемні питання, які потребують термінового вирішення та перегляду;
- конститутивні – актуальні проблемні питання, які виникають при розгляді основних аспектів інформаційної безпеки, але несуттєво впливають на формування системи безпеки;
- складні – проблемні питання, які обов’язково мають бути взяті до розгляду в майбутньому та потребують інноваційних рішень.

Це ще не повний перелік питань, які вимагають відповідей, перегляду та переоцінки. Запропонована систематизація проблем при формуванні теоретико-методологічного апарату інформаційної безпеки корпорацій дає змогу сконцентрувати увагу на об'єктивному розгляді та розробці найбільш пріоритетних базових аспектів системи інформаційної безпеки, що є дуже цінним для забезпечення його практичного використання для захисту корпорацій та підтримки сталого функціонування з точки зору інформаційної безпеки [1, с. 60].

Кожна система інформаційної безпеки – це свого роду “кібернетичний продукт”. Її потрібно будувати, виходячи з сутнісних зв’язків і діючих інформаційних нормативно-правових актів, а також кожного конкретного суб’єкта господарювання, оскільки корпорація, холдинг і фінансова компанія дуже відрізняються один від одного. Крім того, необхідно враховувати, що побудова системи інформаційної безпеки в корпорації неминуче наштовхується на різні протистояння, які необхідно врегульовувати в

установленому в корпорації порядку з урахуванням норм чинного законодавства. Існують типові алгоритми локалізації загроз і етапи формування системи інформаційної безпеки, які застосовуються при створенні будь-якої системи безпеки. Так, наприклад, цілісна система інформаційної безпеки повинна передбачати як профілактичну, так і внутрішню оперативну роботу. Профілактична робота допускає використання технічних методів і способів контролю, однак можливість їх проведення стосовно співробітників повинна бути, в обов’язково порядку, закріплена письмовою згодою самого працівника. Внутрішня оперативна робота – це процес виявлення інформації небезпечного характеру. До основних етапів формування системи інформаційної безпеки корпорацій можна віднести наступні: ідентифікація джерел загроз і ризиків для бізнесу; оцінка ступеня серйозності загрози; вибір та застосування оптимального алгоритму локалізації загроз (побудова системи захисту) з урахуванням виділеного на це бюджету [2, с. 63].

Головною діючою особою ринку в недержавному секторі економіки і стрижнем будь-якої економічної системи, побудованої не на державно-монополістичних, а на конкурентних засадах, є корпорації. Але необхідно зазначити, що повсякденна практика недержавних об’єктів свідчить про їх підвищену порівняно з державними структурами уразливість від протиправних та інших посягань з боку різного роду кримінальних структур, а також окремих осіб. Власність тепер зобов’язує корпорації займатись діяльністю, яка раніше була виключно прерогативою спеціальних державних органів. Забезпечення безпеки приватної діяльності стає важливою необхідністю, є підґрунтям функціонування недержавних об'єктів. Отже, охорона корпорацій і забезпечення інформаційної безпеки корпоративної діяльності є стрижневою проблемою, що обіймає комплекс організаційно-правових, техніко-технологічних, інформаційних, адміністративних, виховних, фінансових і спеціальних заходів, спрямованих на виявлення, попередження і припинення загроз і зазіхань на стабільність функціонування і розвитку корпорацій. Цей процес містить у собі безпеку інформації, охорону приватної власності корпорацій і фізичний захист його персоналу. При цьому до власності відносять, по-перше, основне матеріальне майно: приміщення, земельна ділянка, парк техніки, сировина й інвентар, а також допоміжне устаткування, призначене для збереження, переробки і перевезення вантажів. По-друге, сюди ж варто віднести інтелектуальну власність, що складає інформацію, яка є активом компанії про власність власника, а також знання і досвід співробітників корпорацій, їхні професійні секрети і винаходи. Корпорації, які прагнуть мати власну службу безпеки, не повинні розглядати витрати на її створення, як необґрунтовано високі, оскільки життя та репутація цінується набагато вище. Нещастям корпорацій є те, що, заробивши великі гроші, вони не хочуть усвідомлювати, що багатство неминуче переводить їх у “групу ризику”. Як показує сумний досвід, наші корпорації починають здійснювати суттєві кроки із забезпечення власної безпеки, безпеки інформації лише після того, як у них починаються неприємності [1, с. 61].

Побудова правового поля в Україні поступово зумовлює створення системи забезпечення інформаційної безпеки корпорацій відповідно до світової практики. Важливим чинником цього процесу є утворення функціонування державних і недержавних структур як єдиного цілого.

Складовими єдиної системи забезпечення інформаційної безпеки корпорацій є:

- державна система, що представлена правоохоронними органами та спецслужбами (наприклад, Служба безпеки України, Рада національної безпеки і оборони України);
- недержавна система, яка представлена приватними охоронними, охоронно-технічними підприємствами, комерційними службами безпеки, підприємства різної

форми власності, інформаційними бюро, службами безпеки банків, профільними факультетами, кафедрами вищих навчальних закладів (прикладом є кафедра інформаційної безпеки Національного технічного університету України “Київський політехнічний інститут” м. Києва).

Слід зауважити, що велику частину недержавної системи складають професіонали, колишні співробітники служби безпеки, органів внутрішніх справ, збройних сил і підрозділів спеціального призначення.

Для порівняння, в західних країнах в корпоративному секторі головну роботу по захисту бізнесу здійснюють недержавні служби безпеки, численність яких, наприклад, в США, вдвічі перевищує штат поліції. А це, в свою чергу, знижує витрати держави на утримання поліції [3, с. 20].

Розглядаючи недержавну систему, необхідно зазначити, що її побудова повинна здійснюватись на основі дотримання таких принципів, як:

- законність;
- дотримання прав і свобод громадян;
- централізоване керування;
- координація і взаємодія з правоохоронними органами;
- самостійність;
- відповідальність за забезпечення безпеки;
- відповідність зовнішнім і внутрішнім загрозам безпеки;
- передова матеріально-технічна оснащеність;
- прогресуюче стимулювання суб’єктів системи;
- компетентність;
- конфіденційність;
- корпоративна етика;
- комплексне використання сил і засобів.

Системний підхід до інформаційної безпеки корпорацій має бути:

- постійним – вимога, яка не дає можливості зловмисникам обійти захист для досягнення своїх протиправних цілей;
- централізованим – у межах визначеної корпорації повинна гарантуватися організаційно-функціональна самостійність процесу забезпечення інформаційної безпеки;
- цілеспрямованим – розробка планів дій щодо забезпечення захищеності корпорації всіма компонентами його структури;
- універсальним – незалежність заходів інформаційної безпеки від місця їхнього можливого впливу;
- рухливим – захисні заходи перетворюються в життя з достатнім ступенем наполегливості;
- безпечним – надійність методів, засобів і форм захисту з одночасним дублюванням засобів і заходів інформаційної безпеки;
- комплексним – застосовування усіх видів і форм захисту в повному обсязі.

Висновки.

На підставі дослідження, закріплення права корпорацій на забезпечення інформаційної безпеки, крім використання типових алгоритмів локалізації загроз і етапів формування системи інформаційної безпеки, на нашу думку доцільно забезпечити: регулювання діяльності служби інформаційної безпеки корпорацій здійснювати на підставі поєднання державного нормативно-правового регулювання та локального; відносини з регулювання діяльності служби інформаційної безпеки

корпорацій більшою мірою здійснюються локальними актами і в меншій – спільними нормативно-правовими актами, прийнятими державою; право служби безпеки корпорацій на здійснення діяльності щодо забезпечення інформаційної безпеки, закріпленої в локальних актах, інтеграцію системи управління інформаційною безпекою в існуючу систему корпорацій забезпечити шляхом обліку діючих в корпорації правил та положень при розробці локальних актів нормативно-правового регулювання.

Використана література

1. Назаров В.В. Деякі аспекти забезпечення безпеки підприємницької діяльності / В.В. Назаров : матеріали Всеукраїнської науково-практичної конференції [“Недержавна система безпеки підприємництва як складова національної безпеки України”]. – К. : ЛТД, 2013. – С. 60-61.

2. Нашинець-Наумова А.Ю. Питання забезпечення інформаційної безпеки підприємства / А.Ю. Нашинець-Наумова : зб. наук. праць Національного авіаційного університету. – Сер. “Юридичний вісник “Повітряне і космічне право”. – 2012. – № 3(24). – С. 58-63.

3. Соловьев И.Н. Информационная и правовая составляющая безопасности предпринимательской деятельности / И.Н. Соловьев // Налоговый вестник. – 2011. – № 10, 11. – С. 19-20.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~