УДК 342.9

ЛИСЕНКО С.О.

ГНУЧКА МОДЕЛЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМНИЦТВА В КОНТЕКСТІ ВИКОРИСТАННЯ АДМІНІСТРАТИВНОГО РЕСУРСУ

Статтю присвячено формуванню гнучкої моделі інформаційної безпеки підприємництва в цілому й особливостям адміністрування такої моделі зокрема. Окрему увагу приділено особливостям становлення вітчизняного законодавства, орієнтованого на регулювання інформаційної безпеки.

Ключові слова: *інформаційна безпека, моделювання інформаційної безпеки, підприємництво, адміністративно-правове регулювання.*

Статья посвящена формированию гибкой модели информационной безопасности предпринимательства в целом и особенностям администрирования такой модели в частности. Главное внимание уделено особенностям становления отечественного законодательства, ориентированного на регулирование информационной безопасности.

Ключевые слова: *информационная безопасность, моделирование информационной безопасности, предпринимательство, административно-правовое регулирование.*

The article is devoted to the problem of forming a flexible model of information security of entrepreneurship in general and the peculiarities of administering such a model in particular. The attention paid to the peculiarities of the development of domestic legislation, oriented on regulating information security.

Key words: *information security, information security modeling, entrepreneurship, administrative and legal regulation.*

Актуальність обраної теми. Сила та добробут країни забезпечується рівнем розвитку її економіки. Економіка будь-якої демократичної держави будується на засадах вільного підприємництва. Саме здатність економіки відповідати потребам часу забезпечує країні відповідний розвиток та безпеку. Найважливішою якістю, що притаманна підприємництву, яка забезпечує зростання економіки, формування належної фінансово-економічної бази, а відтак – зміцнення безпеки держави, є здатність підприємництва оперативно трансформувати свої напрями діяльності. Тобто йдеться про певну гнучкість підприємництва.

Сучасне підприємництво скрізь побудоване на інформаційних потоках, обміні інформацією, її зберіганні. Не існує галузі підприємництва, яка б не залежала від певного обсягу інформації, що забезпечує його діяльність на достатньому рівні конкурентоспроможності. Обіг та обмін інформацією, її обсяг та форми доступу регулюються певною моделлю інформаційної безпеки. Саме тому ми стверджуємо, що модель інформаційної безпеки підприємництва мусить мати певну гнучкість, достатню для того, щоб відповідати потребам держави та її економіки. Ця модель має відповідати потребам часу та світу загалом. У таких умовах особливої гостроти набуває потреба адміністративно-правового регулювання такої моделі.

Огляд попередніх досліджень у цій сфері. Окремим елементам, проявам моделей інформаційної безпеки та їх правового регулювання присвячували свої дослідження вітчизняні та зарубіжні вчені, зокрема К.І. Бєляков, В.Д. Гавловський, В.В. Гриценко, В.С. Цимбалюк, однак комплексного дослідження гнучкості моделі інформаційної безпеки в контексті адміністративного права у вітчизняній науці ще не проводилось.

Основний зміст дослідження. Створення моделі інформаційної безпеки підприємництва відбувається за алгоритмом, що включає три складники, що вже розглядалися в попередніх

© ЛИСЕНКО С.О. – кандидат юридичних наук, докторант (Навчально-науковий інститут права імені князя Володимира Великого Міжрегіональної академії управління персоналом)

публікаціях автора [1, с. 168–171]. Зазначений алгоритм був допрацьований та апробований на практиці. Завдяки цьому було досягнуто необхідну гнучкість моделі, яка в подальшому створить підстави для прогресивного розвитку всього підприємництва.

Забезпечення інформаційної безпеки підприємництва реалізується за рахунок специфічних прийомів моделювання. Ми відходимо від розгляду традиційних моделей, які випливають із різновидів підприємницької діяльності. Наше завдання та мета – розроблення гнучких моделей інформаційної безпеки без прив'язування до галузей, сфер та видів діяльності соціальних систем, їх суб'єктів та підприємництва в цілому. Ми ставимо за мету розроблення моделей інформаційної безпеки, придатних для вживання будь-якою організацією.

За нашим переконанням гнучкість та придатність моделі інформаційної безпеки підприємництва надасть підхід до її створення, побудований на трьох складниках:

– залежно від сфери застосування та категорії конфіденційності інформації, щодо якої створюється модель інформаційної безпеки підприємництва;

– залежно від складності соціальної системи (організації), в якій створюється модель інформаційної безпеки підприємництва;

– залежно від складу керівників та суб'єктів-виконавців забезпечення самої моделі інформаційної безпеки підприємництва.

За сферами застосування інформації та категорії конфіденційності, що обертається в організації, модель інформаційної безпеки підприємництва будується шляхом адміністративно-правового розгалуження ступенів доступу до інформації та трирівневого процесу прийняття рішень. Останнім часом вітчизняний законодавець усе ж почав приділяти увагу інформаційній безпеці. Так, у 2013 році Розпорядженням Кабінету Міністрів України було схвалено Стратегію розвитку інформаційного суспільства в Україні [2], а в 2015 р. на розгляд Верховної Ради України подано проект Закону «Про основні засади забезпечення кібербезпеки України» [3]. Вже два десятиліття точиться дискусія щодо необхідності прийняття Інформаційного кодексу.

Відтак, використовуючи профільні закони, адаптуючи їх у корпоративні акти, будується найвищий рівень доступу до інформації для керівників та засновників, що ухвалюють загальні рішення. Другий рівень доступу придатний для суб'єктів, що забезпечують інформаційну безпеку, підтримують працездатність моделі інформаційної безпеки та контролюють виконання іншими співробітниками прийнятих керівництвом норм. У третій черзі залишаються інші відповідальні особи, що працюють з інформацією та беруть участь у потоках інформації. В адміністративній діяльності, що забезпечує організацію процесу створення інформаційної безпеки підприємництва, профілактики правопорушень і витоку інформації, об'єктами гнучкої моделі інформаційної безпеки підприємництва будуть:

– процес утворення та забезпечення зберігання конфіденційної інформації;

– процес обігу та використання конфіденційної інформації суб'єктами відносин;

– взаємодія керівництва та підлеглих співробітників підприємства під час робочого процесу;

– дії суб'єктів, що забезпечують інформаційну безпеку (керівники, охоронці, співробітники та ін.) щодня та під час виникнення нештатних ситуацій.

У цьому разі можуть використовуватися плани та розпорядження стосовно моделі, що забезпечує життєздатність системи інформаційної безпеки підприємства, розмежовує функції співробітників залежно від ступеня доступу до інформації і їхні дії як буденні, так і під час виникнення нештатних ситуацій. Створюються моделі характерних правопорушень, їх причини, механізми виконання, утворення слідів та напряму службового розслідування. За відповідного правового оформлення можливе створення моделі за допомогою комп'ютера, для вирішення адміністративно-правових завдань з великим обсягом інформації, одночасно і швидко проводиться оцінка рівнів розвитку та безпеки підприємства для виявлення слабких місць, що не під силу людині. За допомогою комп'ютерної програми можуть моделюватися можливі наслідки за заздалегідь розробленим алгоритмом та надаватися поради щодо усунення недоліків та негативних наслідків.

Різновиди адміністративно-правової діяльності залежать від розміру самого підприємства, кількості рівнів доступу та обміну конфіденційною інформацією, наявності та кількості співробітників служби безпеки. Але єдиним залишається те, що у разі створення моделей інформаційної безпеки підприємництва необхідно залучати та враховувати весь наявний персонал підприємства, лише так можна врахувати всі можливі шляхи розвитку подій і наслідків. При чому кожен співробітник має бути визначений суб'єктом інформаційної безпеки, знати та дотримуватись прийнятого (затвердженого) правила поведінки та відносин.

Найбільш складним завданням на шляху вирішення цих проблем є кодування ознак, що характеризують складну нештатну ситуацію, кримінально-правові, кримінально-процесуальні, цивільно-правові, цивільно-процесуальні, адміністративні та інші норми права. Ці моделі на підприємствах закріплюються в мережевих планах, що забезпечують наочність планування та затверджуються наказами [4].

Одночасно модель інформаційної безпеки підприємництва має забезпечувати надійність від зовнішніх негативних впливів. Створення позитивного іміджу підприємства під час конкурентної боротьби із конфліктним супротивником, який може вести інформаційну боротьбу проти підприємства, має бути частиною наявної моделі. Бажано враховувати в наявній моделі інформаційної безпеки засади, націлені на припинення протиправних та конфліктних дій. Особливо на початкових етапах, та превентивні дії під час оцінки надійності моделі. Такі заходи, відображені в моделі, мають бути адекватні розміру загрози, можливим наслідкам та збиткам від інформаційної атаки зловмисника.

Об'єктами моделі інформаційної безпеки підприємництва в такому разі можуть бути:

– організація роботи підприємства;

– відносини між керівниками та підлеглими;

– зовнішній імідж підприємства та його керівників;

– позитивна думка співробітників підприємства та пересічних громадян стосовно керівництва та самого підприємства.

Як прийоми моделювання використовують уявні та логіко-математичні моделі, які приймуть керівники підприємства, що затверджують стратегію інформаційної політики підприємства. Які зможуть створити всі суб'єкти інформаційної безпеки підприємства. А також які найбільш коректно відповідатимуть інтересам, цілям та завданням підприємства [1].

Розробляючи моделі інформаційної безпеки підприємництва для соціальних систем (організацій), залежно від її величини та складності варто враховувати таке:

– психологічну модель управління, що діє в організації,

– складність структури соціальної системи.

Психологічні різновиди управління організаціями можуть поділятись на авторитарні та колегіальні. При цьому важливим складником є відносини всередині соціальної системи (організації). Отто Кернберг описував у своїх численних дослідженнях, як можуть складатися відносини між суб`єктами забезпечення безпеки та членами організації, між самими членами організації, між керівництвом, всіма іншими тощо. Встановлено, якщо соціальна система (організація) була створена штучно, то правила відносин між членами та суб'єктами є нав'язаними зверху, а значить усередині системи обов'язково виникнуть зв'язки неофіційного характеру [5].

У цьому контексті можна зробити деякі висновки. У зв'язку з примусовістю, заданою із самого початку певної ієрархії в організації, не маючи права впливу та вибору адміністративної структури, співробітники так чи інакше, безпосередньо або опосередковано укладатимуть «власну» ієрархію. Чим більше організаційна структура буде асоціюватися у свідомості співробітників зі станами домінування, небезпеки, незадоволення потреб, тим більше актуалізуватиметься неформальна організаційна структура, що популяризуватиме альтернативні організаційні цінності та схеми взаємодії. Наскільки відомо, їх поведінка реалізовувала почуття, спрямовані на аналітика, але які суб'єкт боявся відчувати або допустити до усвідомлення, особливо в присутності психоаналітика. Пізніше цей термін почали використовувати в основному для опису поведінки, зумовленої несвідомою потребою впоратися з тривогою, асоційованою з внутрішньо забороненими почуттями та бажаннями, а також із нав'язливими страхами, фантазіями і спогадами.

У зв'язку з цим, екстраполюючи зміст такого процесу на контекст адміністративно-правової структури, зазначимо, що неформальна поведінка сприяє механізму витоку інформації, пошуку середовища, яке б відповідало ідеальним уявленням. Часто такий підхід сприяє становленню опозиції, просуванню ідей зовнішніх агентів тощо, тобто формує джерело загрози безпеці.

Одночасно з неформальними лідерами в соціальних системах (організаціях) є офіційне керівництво, яке діє згідно зі статутами та інструкціями. Залежно від того, скільки керівників у соціальній системі (організації) та яким чином приймаються рішення, їх поділяють на авторитарні (керує одна особа) та колегіальні (двоє та більше осіб) [5].

У створенні моделі інформаційної безпеки підприємництва варто враховувати, що авторитарну модель управління слід супроводити додатковим колегіальним органом, якому необхідно передати дорадчі та оціночні функції. Це має знайти своє відображення у статутах та наказах.

Навпаки колегіальне управління потребує певної єдиної адміністративної сили. Це може бути забезпечене шляхом введення посади головного управлінця чи менеджера або передачі йому певних керівних прав для вирішення складних та термінових питань. Особливо певна свобода прийняття рішень корисна, коли гаяння часу на роздуми та наради може завдати великих збитків організації.

Виходячи із вищевказаного, вважаємо, що неможливо створювати модель інформаційної безпеки підприємництва, не враховуючи наявних офіційних та неофіційних міжособистісних зв'язків та особливостей управління.

Складність структури соціальної системи відіграє важливу роль під час створення моделей інформаційної безпеки підприємництва, тому що від цього залежить комунікація між підрозділами, швидкість обміну інформацією та якість відтворення керівних команд разом із їх виконанням. Соціальні системи слід поділяти залежно від різновидів їх інтересів та видів діяльності на горизонтальні та вертикальні.

Горизонтальні мають на меті досягнення інтересів та діяльності в одній галузі, наприклад, торгівлі або будівництві. Такі соціальні системи (організації) мають у складі однорідних суб'єктів та членів системи, які займаються приблизно однаковим рівнем інтересів в ієрархії. Склад таких систем утворюється залежно від обсягів діяльності, але він однорідний. Наприклад, будівельна компанія має на меті розширення своїх потужностей і у разі збільшення підвищує кількість працівників однорідних професій та обслуговуючого чи адміністративного персоналу. Отже, необхідно створювати модель інформаційної безпеки, націлену на захист однорідних функцій від одних і тих же можливих посягань. У разі збільшення потужностей соціальної системи (організації) може збільшуватись кількість суб'єктів забезпечення безпеки по горизонталі системи. Але це не впливатиме на саму модель інформаційної безпеки підприємництва та процедури відтворення її діяльності.

Вертикальні соціальні системи створюють ті горизонтальні системи, які досягли певного розвитку та почали своє розширення в інші, не притаманні їм галузі, або створюють вертикальну ланку від видобування сировини до розповсюдження своєї продукції. Прикладом такої соціальної системи (організації) може бути нафтовидобувна компанія, яка перейшла від самого видобування нафти до її перероблення, до виготовлення певного переліку пального та мастильних матеріалів, придбавши для цього виробничі потужності, розширивши їх, а потім створила свою мережу з оптового та роздрібного збуту своєї продукції.

У такому разі ми маємо більш складну модель забезпечення інформаційної безпеки підприємництва, яка розповсюджується на горизонтальні складники соціальної системи, які мають однорідні інтереси (однорідний набір дій із забезпечення безпеки), а також вертикальні складники, що складаються із різних рівнів горизонтальних моделей для кожного різновиду інтересів окремо. Модель інформаційної безпеки підприємництва для вертикальної структури організації забезпечує комунікацію між самими горизонтальними складниками та керівництвом, вона виконує функцію склеювання та утримування соціальної системи від розгалуження та руйнування. У такому разі збільшення інтересів соціальної системи не завжди призводить до збільшення суб'єктів забезпечення безпеки, тому що у моделях інформаційної безпеки підприємництва для вертикальних організацій одні і ті ж суб'єкти можуть виконувати свої функції в різних горизонтальних структурних складниках. У таких моделях важливо приділяти увагу якості комунікацій між горизонтальними складниками та керівництвом. При цьому різні горизонтальні складники мусять мати різні ступені допусків до конфіденційної інформації, різний (свій) перелік інформації, що підлягає охороні тощо.

За аналогією можемо стверджувати, що держава є найскладнішою соціальною системою із вертикальною структурою, тому наш підхід до побудови моделей інформаційної безпеки підприємництва придатний для створення державних (національних) систем інформаційної безпеки загалом. Безумовно, це потребуватиме законодавчого закріплення.

Ми вважаємо, що інформація – основний продукт інформаційного суспільства й особливий об'єкт правового регулювання в сферах публічного і приватного права. Вона відіграє вирішальну роль у сучасному суспільстві, всі галузі життєдіяльності суспільства опосередковуються інформаційними засобами і здійснюються в інформаційному просторі. Саме тому інформаційна безпека стала одним із головних факторів, що визначають національну, регіональну і міжнародну безпеку, а її забезпечення – одним із головних пріоритетів держави [6].

Забезпечення самої інформаційної безпеки здійснюється суб'єктами (людьми) соціальної системи, які відрізняються між собою і мають власні інтереси та проблеми. На нашу думку,

до процесу участі в забезпеченні інформаційної безпеки мають бути причетні всі суб'єкти, і ті, що безпосередньо займаються її здійсненням, і ті, до основних обов'язків яких це не входить. Загалом такими суб'єктами можуть бути звичайні співробітники, якщо на підприємстві немає окремого підрозділу служби безпеки. У такому разі функції із забезпечення інформаційної безпеки покладаються в повному обсязі на весь персонал.

Варто також зазначити, що не можна ототожнювати поняття «захист інформації» та «інформаційна безпека». Інформаційна безпека – це не тільки захист інформації, але й організаційні, адміністративно-правові та інші заходи, спрямовані на забезпечення сталого, стабільного розвитку окремої соціальної системи і суспільства у цілому. У зв'язку з цим дуже важливо розуміти, що інформаційна безпека є соціальним, а не суто технічним явищем. Поняття «інформаційна безпека», «безпека інформації», «захист інформації» взаємодоповнюють один одного. При цьому кожна наступна категорія є складовою частиною попередньої, а всі разом вони утворюють модель інформаційної безпеки підприємництва.

У своїх моделях ми розробляємо такі механізми, які мають призвести до мінімізації впливу людського фактора на здійснення інформаційної безпеки підприємництва. Поняття «людський фактор» у нашій країні традиційно пов'язується з проблемою аварійності та правопорушень, оскільки саме людина, як правило, є тією «слабкою ланкою» в технологічному ланцюгу сучасного підприємництва.

У численних наукових дослідженнях є спроби розробити концептуальний підхід для системного розгляду впливу людського фактора на статичні та динамічні процеси в організаціях. Визначено специфіку зв'язків ініціативності і різних параметрів активності людини. Розкрито міжрівневий зв'язок між динамічними, інструментальними, особистісними і соціально-психологічними властивостями суб'єкта: зв'язок властивостей темпераменту і акцентуацій характеру, спрямованості міжособистісних відносин у колективах, зв'язок акцентуації характеру і міжособистісних відносин.

Проблема людського фактора полягає у відсутності достатніх знань про природні закони поведінки людини, про причинно-наслідкові зв'язки впливу на людину різних чинників. Проблема починається з відсутності визначення поняття «людський фактор», з відсутності методології кількісної оцінки і врахування впливу людського фактора на безпеку соціальної системи, держави [7].

Як методологічний орієнтир може виступити математичний апарат теорії нечітких множин, теорії ймовірностей і математичної статистики, сучасні спеціальні діагностичні методики для визначення типологічних ознак, що характеризують структуру міжособистісних відносин членів групи, а також результати тестування діяльності членів колективу [8].

Одне із основних завдань створених моделей інформаційної безпеки підприємництва, враховуючи суб'єктні особливості, полягає в тому, щоб мінімізувати вплив особистості на роботу моделей інформаційної безпеки, унеможливити ненавмисне втручання в діяльність соціальної системи, виключивши фактори помилок та неналежний рівень кваліфікації суб'єктів підприємництва.

Зазначене може бути досягнуто з урахуванням таких принципів моделювання інформаційної безпеки підприємництва, як:

– адекватність актуального стану моделі інформаційної безпеки підприємництва цілям прогресивного розвитку суспільства;

– використання адміністративно-правових складників моделі як одного з головних засобів суспільно-державного управління;

– відповідність моделей інформаційної безпеки життєво важливим інтересам підприємництва, суспільства, особистості та національним інтересам країни у цілому;

– спрямованість на недопущення зовнішніх і внутрішніх інформаційних загроз;

– реальна можливість вростання інформаційної політики підприємництва в Україні в міжнародний інформаційний простір;

– забезпечення збереження інформаційних ресурсів, їх адміністративний і організаційний захист як одного з головних елементів стратегічного розвитку підприємництва;

– здатність моделей інформаційної безпеки підприємництва створювати всі необхідні умови для впровадження національних і регіональних інформаційних систем і технологій [7].

Ідея забезпечення такого гнучкого механізму роботи моделі інформаційної безпеки підприємництва полягає в тому, що всі суб'єкти за напрямами разом із своїми обов'язками відслідковують основні показники організації за переліком, прийнятим для оцінювання рівнів розвитку

та безпеки. При чому не має значення, це суб'єкти служби безпеки чи відповідальні працівники. Такі функції на них покладаються трудовим договором або корпоративними розпорядженнями. Після чого за алгоритмом оцінювання проводиться оцінка рівнів розвитку та безпеки організації, а потім її загальний рівень надійності.

Висновки. Базою забезпечення фактора гнучкості інформаційної безпеки є аналіз потенційних та наявних загроз, який має проводитись з максимальною об'єктивністю. Отримавши результати оцінки, керівники та власники бачать реальну картину роботи організації з конкретизацією її сильних та слабких місць. На основі отриманих результатів робляться висновки про подальші напрями роботи підприємництва та знешкодження виявлених реальних або латентних загроз. Згідно з висновками видаються адміністративно-правові акти підприємництва, спрямовані на вдосконалення роботи організації та знешкодження загроз. На наступному етапі робота адміністративного ресурсу полягатиме у відслідковуванні виконання керівних вказівок згідно з отриманими після оцінювання висновками. У подальшому адміністративний ресурс буде регулярно збирати вищевказані показники організації за визначеним переліком, контролюючи виконавців тих чи інших рівнів.

Доречно регулярно (наприклад, раз у квартал) проводити оцінювання рівнів розвитку, безпеки та надійності моделі інформаційної безпеки підприємництва для виявлення позитивних або негативних змін. Такий підхід дасть змогу мінімізувати загрози від людського фактора як в отриманні висновків, так і в процесі обрання оптимальних адміністративно-правових рішень для подальшого розвитку інформаційної безпеки підприємництва.

Список використаних джерел:

1. Лисенко С.О. Методи моделювання у забезпеченні інформаційної безпеки підприємств / С. О. Лисенко // Митна справа. – 2015. – № 3(2). – С. 167–172.

2. Про схвалення Стратегії розвитку інформаційного суспільства в Україні: Розпорядження Кабінету Міністрів України від 15.05.2013 № 386-р // База даних «Законодавство України»: Верховна Рада України. [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/386-2013-%D1%80.

3. Про основні засади забезпечення кібербезпеки України: Проект Закону України № 2126а від 19.06.2015 // База даних «Законодавство України»: Верховна Рада України. [Електронний ресурс]. – Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657.

4. Бєляков К.І. Інформація в праві: теорія і практика: [монографія]. – К.: Вид-во «КВІЦ», 2006. – 118 с.

5. Отто Кернберг (2015) «Конфлікт, лідерство, ідеологія в групах та організаціях». – 458 с.

6. Юзвишин И.И. Основы информациологии: [учебник.] Изд. 3-е, исп. и доп. – М.: Издательство «Высшая школа», 2001. – 600 с.

7. Основи інформаційного права України: [підручник] / [В.С.Цимбалюк, В.Д.Гавловський, В.В. Гриценко та ін.], 2004, видавництво «Знання». – 356 с.

8. Prisniakova, L.M., Prisniakov, V.F. Mathematical model of the interpersonal conflict on the spacecraft during long mission (2005). / International Astronautical Federation – 56th International Astronautical Congress 2005, 1, pp. 219–227.