УДК 342.9

С. О. ЛИСЕНКО
Міжрегіональна Академія управління персоналом, м. Київ

ОРГАНІЗАЦІЙНО-ПРАВОВІ ШЛЯХИ ВИЗНАЧЕННЯ ОСНОВНИХ ДИСФУНКЦІЙ КОНЦЕПТУАЛЬНОЇ МОДЕЛІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМНИЦТВА

Наукові праці МАУП. Серія Юридичні науки, 2017, вип. 54(3), с. 12–23

Досліджуються можливі дисфункції моделі інформаційної безпеки підприємництва крізь призму права. Значна увага приділяється ідентифікації джерел загроз інформаційній безпеці підприємництва, наводиться аргументація важливості збереження цілісності моделі інформаційної безпеки конкретного підприємства.

Стрімкий розвиток інформаційних технологій зумовлює не лише нові можливості, але й нові загрози для підприємницької діяльності. В таких умовах реформування вітчизняного інформаційного права є не просто нагальною потребою, а вкрай пріоритетним завданням як для теоретиків права, так і для правотворців. Одним із перших етапів досліджень у сфері оптимізації інформаційної безпеки підприємництва та її правового регулювання має стати ідентифікація джерел загроз інформаційній безпеці. У свою чергу, науковцям необхідно враховувати, що загрози інформаційній безпеці не виникають безпідставно, їх джерела випливають з певних недоліків (дисфункцій), наявних у моделі інформаційної безпеки того чи іншого підприємства. Особливостям ідентифікації таких загроз, в їх взаємозв'язку з недоліками (дисфункціями), притаманними певним моделям інформаційної безпеки підприємництва, і присвячено це дослідження.

Сформулюємо критерії для визначення потенціалу загроз інформаційній безпеці підприємництва.

Окремим питанням інформаційної безпеки, в тому числі інформаційної безпеки підприємництва, присвячували свої праці О. Р. Бойкевич, Т. Г. Васильців, В. І. Волошин, В. Г. Герасимчук, Р. Гриценко, О. В. Іляшенко, С. В. Кавун, В. В. Каркавчук, В. Р. Краліч, М. Медников, С. Л. Рубінштейн, І. О. Тарасенко, В. С. Цимбалюк, С. М. Шкарлет, О. М. Штаєр. Водночас генерація нових загроз у сукупності з постійною трансформацією форм підприємницької діяльності, бурхливим розвитком інформаційних технологій спричиняє необхідність системних, ґрунтовних досліджень, спрямованих

на формування концептуальної моделі інформаційної безпеки підприємництва.

Сучасна організація забезпечення безпеки інформації повинна мати комплексний характер і ґрунтуватися на глибокому аналізі можливих негативних наслідків. Важливо враховувати всі основні аспекти охоронюваної інформації підприємства. Навіть у прийнятій Доктрині інформаційної безпеки України вказано, що забезпечення інформаційної безпеки можливо при захисті всіх важливих інтересів держави та своєчасному реагуванні на протиправні посягання на інформаційні права населення [1]. Тому можливі негативні наслідки від загроз інформаційній безпеці українського підприємництва виникають залежно від наявних дисфункцій моделі інформаційної безпеки, що ним використовується. Аналіз цих наслідків передбачає обов'язкову ідентифікацію можливих джерел загроз, чинників, що сприяють їх появі, а також визначення актуальних проблем та дисфункцій обраної моделі безпеки. Ідентифікація та визначення всього переліку можливих і реальних джерел загроз інформаційній безпеці дає змогу визначити максимальний перелік ознак для порівняння, що використовуватимуться в запропонованому підході визначення надійності концептуальної моделі інформаційної безпеки підприємництва.

В ході такого аналізу суб'єктам забезпечення безпеки необхідно переконатися, що всі можливі джерела загроз ідентифіковані, всі можливі недоліки (дисфункції) зіставлені з джерелами загроз, властиві даній моделі інформаційної безпеки підприємств. Виходячи з цього принципу, класифікацію джерел загроз і їх проявів доцільно проводити на основі аналізу взаємодії логічного ланцюжка:

джерело загрози – дисфункція (недолік) – загроза (дія) – наслідки (атака, збитки).

Під термінами цього ланцюжка слід розуміти:

1. Джерело загрози — це потенційні антропогенні, техногенні або стихійні носії загрози безпеки.

2. Загроза (дія) — це можлива небезпека (потенційна або реальна, внутрішня або зовнішня) вчинення будь-якого діяння (дії або бездіяльності), спрямованого проти об'єкта захисту (інформаційних ресурсів), що завдає шкоди власнику, підприємству, яка проявляється в небезпеці спотворення і втрати інформації.

3. Дисфункція (недолік) — це властиві обраній моделі інформаційної безпеки причини, що призводять до порушення безпеки інформації на конкретному об'єкті і обумовлені недоліками процесу функціонування самої моделі, властивостями архітектури автоматизованої системи, апаратною платформою та умовами експлуатації носіїв інформації.

4. Наслідки (атака, збитки) — це можливі наслідки реалізації загрози (можливі дії) при взаємодії джерела загрози через наявні недоліки (дисфункції). Як видно з визначення, атака — це завжди пара "джерело – фактор", що реалізує загрозу і призводить до збитку. При цьому аналіз наслідків передба-

чає проведення прогнозування та оцінки можливих збитків і вибору методів знешкодження загроз безпеки інформації [2, *37*].

Загроз моделі інформаційної безпеки не так вже й багато. Загроза — це небезпека заподіяння шкоди цілісності або сутності інформації, яка виявляється через зв'язок дисфункцій моделі із збитком підприємству. У загальному вигляді можливі загрози прийнято розділяти на внутрішні і зовнішні [3, *122*]. Але перші і другі ми спробуємо класифікувати частинами нижченаведених категорій.

Прояви можливих збитків можуть виглядати у такому переліку [3, *123*]:

- моральний і матеріальний збиток діловій репутації підприємства;
- моральний, фізичний чи матеріальний збиток, пов'язаний з розголошенням персональних даних окремих осіб;
- матеріальний збиток від розголошення конфіденційної інформації, що захищається;
- матеріальний збиток від необхідності відновлення порушених інформаційних ресурсів, що захищаються;
- матеріальні збитки від неможливості виконання взятих на себе зобов'язань перед третьою стороною;
- моральний і матеріальний збиток від дезорганізації діяльності підприємства;
- матеріальні та моральні збитки від порушення міжнародних відносин.

Якщо збиток заподіяний навмисно будь-якою особою, в цьому випадку є склад правопорушення. В іншому разі збиток може бути наслідком незалежних від особи проявів (наприклад, стихійних чи інших впливів, таких як прояви техногенних властивостей цивілізації). У першому випадку ми маємо винну особу, якій пред'являється заподіяна шкода, як частина складу правопорушення, вчиненого зі злого мотиву або з необережності, і заподіяний збиток повинен кваліфікуватися, як частина складу правопорушення, обумовлена деліктним правом. У другому випадку збиток носить імовірнісний характер і повинен бути порівняний з тим ризиком, який обумовлюється цивільним, адміністративним або арбітражним правом, як предмет розгляду [4, *212*].

У теорії права під збитком розуміються невигідні для власника майнові наслідки, що виникли в разі правопорушення. Збиток виявляється у зменшенні майна або в недоотриманні доходу, який був би отриманий за відсутності правопорушення (упущена вигода) [5, *72*]. При розгляді шкоди, завданої особою, необхідно довести, що саме ця особа заподіяла даний збиток, тобто діяння особистості необхідно кваліфікувати як склад правопорушення. В цьому випадку при класифікації загроз безпеки інформації доцільно враховувати вимоги чинного кримінального та адміністративного законодавства, що визначають склад правопорушення. Однак говорити про злий намір кого-небудь у знищенні інформації в результаті стихійних лих неможливо, як і той факт, що навряд чи стихія зможе скористатися конфіденційною інформацією для власної вигоди. Хоча в обох випадках власнику інформації завдано збитків. Тут є правомочним застосування категорії "заподіяння шко-

ди майну" й інформація виступає інтелектуальним майном. При цьому мова піде не про кримінальну відповідальність за знищення або пошкодження чужого майна, а про випадки, що підпадають під цивільне право в частині відшкодування заподіяної шкоди (ризик випадкової загибелі майна — тобто ризик можливого нанесення збитків у зв'язку з загибеллю або псуванням майна з причин, не залежних від особи). За загальним правилом у цьому випадку збитки у зв'язку з загибеллю або псуванням майна несе власник, однак цивільне право передбачає й інші варіанти компенсації заподіяної шкоди [6, *45*].

Визначаючи в якості суб'єкта, який завдав шкоди, будь-яке природне або техногенне явище, під завданими збитками можна розуміти невигідні майнові наслідки, викликані цими явищами і які можуть бути компенсовані за рахунок коштів третьої сторони (наприклад, страхування ризиків настання події) або за рахунок власних коштів власника інформації, тобто підприємства.

З урахуванням викладеного радше вірним є такий загальний перелік загроз безпеці інформації, наведений авторами навчального посібника "Економічна безпека" [7]:

- розкрадання (копіювання) інформації;
- знищення інформації;
- модифікація (спотворення) інформації;
- порушення доступності (блокування) інформації;
- заперечення автентичності інформації;
- нав'язування неправдивої інформації.

Зважаючи на положення проекту Концепції інформаційної безпеки України, можемо класифікувати джерела загроз за нищенаведеними критеріями. Носіями загроз безпеці інформації є джерела загроз. В якості джерел загроз можуть виступати живі особи та об'єктивні прояви. Причому джерела загроз можуть знаходитися як всередині підприємства, яке захищається, — внутрішні джерела, так і поза ним — зовнішні джерела. Запропонований розподіл джерел на суб'єктивні і об'єктивні виправданий, виходячи з попередніх міркувань з приводу провини або ризику шкоди інформації. А поділ на внутрішні і зовнішні загрози виправданий тим, що для однієї і тієї ж загрози методи знешкодження для зовнішніх і внутрішніх джерел можуть бути різними [7].

Згідно з поглядами багатьох українських науковців всі джерела загроз безпеці інформації можна розділити на три основні групи [7]:

– заподіяні діями людини (антропогенні джерела загроз);
– заподіяні технічними засобами (техногенні джерела загрози);
– заподіяні стихійними лихами.

Антропогенними джерелами загроз безпеки інформації виступають особи, дії яких можуть бути кваліфіковані, як умисні або випадкові правопорушення. Тільки в такому сенсі можна стверджувати про заподіяння шкоди. Ця група є найрозповсюдженішою і становить найбільший інтерес з точки зору дослідження організації захисту, тому що дії особи можна оцінити, спрогнозувати і вжити адекватних заходів. Методи протидії в цьому випадку завжди скеровані і безпосередньо залежать від волі керівників моделі інформаційної

безпеки підприємств. В якості антропогенного джерела загроз інформаційній безпеці можна розглядати, як стверджує О. Гордєєв, "певну особу, яка має доступ (санкціонований або несанкціонований) до роботи зі штатними засобами інформаційної безпеки підприємства. Особи (джерела), дії яких можуть призвести до порушення надійності моделі інформаційної безпеки, можуть бути як зовнішні (джерела зовнішні), так і внутрішні (джерела внутрішні)" [8].

Зовнішні антропогенні джерела безпеці можуть мати як випадковий характер, так і навмисний, як наслідок, буде різний рівень суспільної важкості. Тож більшість дослідників до таких джерел відносить [9]:

- кримінальні структури;
- потенційні злочинці і хакери;
- недобросовісні партнери;
- технічний персонал постачальників телекомунікаційних послуг;
- представники контролюючих наглядових організацій та аварійних служб;
- представники силових структур.

Внутрішні антропогенні джерела — це висококваліфіковані фахівці в галузі розробки й експлуатації програмного забезпечення і технічних засобів підприємства. Такі особи не лише завжди знайомі зі специфікою завдань, які вирішуються, структурою та основними функціями і принципами роботи програмно-апаратних засобів захисту інформації, але й мають можливість використання штатного обладнання і технічних засобів мережі. Деякі з них мають доступ до всіх носіїв конфіденційної інформації, навіть до паперових. До зазначених джерел Л. Сафонов відносить такі категорії [9]:

- основний персонал (канцелярія, менеджмент, користувачі, програмісти, розробники);
- представники служби захисту інформації;
- допоміжний персонал (прибиральники, охорона);
- технічний персонал (життєзабезпечення, експлуатація).

Слід зазначити, що особливу групу внутрішніх антропогенних загроз складають особи з порушеною психікою або спеціально впроваджені і завербовані агенти сторонніх структур. Вони можуть бути в складі основного, допоміжного і технічного персоналу, а також серед суб'єктів служби інформаційної безпеки. При цьому, як формулює О. В. Ілляшенко, "дана група розглядається в складі перерахованих вище джерел загроз, але методи протидії загрозам цієї групи можуть мати свої відмінності. Кваліфікація антропогенних джерел інформації відіграє важливу роль в оцінці їх впливу і враховується при ранжуванні джерел загроз" [10, *51*].

Друга група загроз містить джерела, які зумовлюються технократичною діяльністю людини і розвитком цивілізації, — техногенні загрози. Вони особливо небезпечні, коли наслідки від такої діяльності вийшли з-під контролю людини й існують самі по собі. Такі джерела загроз менш прогнозовані, безпосередньо залежать від властивостей техніки і тому вимагають особливої уваги. Зазначений вид джерел загроз інформаційній безпеці є особливо

актуальним у сучасних умовах, оскільки саме в сучасних умовах науковці прогнозують різке зростання кількості техногенних катастроф, викликаних фізичним і моральним старінням технічних можливостей обладнання, яке використовується, а також відсутністю своєчасного його оновлення [11, *67*].

Відповідно до попереднього погляду технічні засоби, які є джерелами загроз інформаційній безпеці підприємств, можуть бути зовнішніми:

- засоби зв'язку;
- мережі інженерних комунікацій (водопостачання, каналізації);
- транспорт.

До внутрішніх джерел загроз А. Й. Присяжнюк, досліджуючи адміністративно-правовий механізм забезпечення економічної безпеки держави, відносить такі [12]:

- неякісні технічні засоби обробки інформації;
- неякісні програмні засоби обробки інформації;
- допоміжні засоби (охорони, сигналізації, телефонії);
- інші технічні засоби, що застосовуються в установі.

Щодо третьої, стихійної (або природної), групи джерел, то вона об'єднує обставини, що становлять непереборну силу, тобто такі, що мають об'єктивний і абсолютний характер, який поширюється на всі об'єкти інформаційної безпеки. До обставин непереборної сили, в цивільному законодавстві і договірній практиці, А. Й. Присяжнюк відносить "стихійні лиха або інші обставини, які неможливо передбачити, або якщо можливо, але неможливо запобігти при сучасному рівні людського знання і можливостей. Дані джерела загроз абсолютно не піддаються прогнозуванню і тому заходи захисту від них повинні застосовуватися постійно" [12].

Стихійні джерела загроз інформаційній безпеці підприємств, як правило, є зовнішніми, і під ними варто розуміти насамперед природні катаклізми:

- пожежі;
- землетрус;
- повені;
- урагани;
- різні непередбачені обставини;
- нез'ясовані явища;
- інші форс-мажорні обставини.

Звичайно, природні катаклізми заподіюють шкоду не тільки моделі інформаційної безпеки підприємства, від них страждає вся система безпеки. Тому превентивні заходи з попередження цих загроз слід вживати в комплексі, відносно всього об'єкта захисту — підприємства.

Загрози, як можливі чинники будь-якої негативної дії, спрямованої проти об'єкта захисту, виявляються не самі по собі, а через дисфункції (недоліки) на підприємстві, що призводять до порушення цілісності моделі інформаційної безпеки конкретного підприємства. Недоліки, що притаманні об'єкту інформатизації, невіддільні від нього і обумовлюються дисфункціями процесу функціонування, властивостями архітектури автоматизованих систем, протоколами обміну та інтерфейсами, що застосовуються програмним за-

безпеченням, процедурою доступу, умовами експлуатації і розташуванням тощо [7].

Джерела загроз безпеці можуть використовувати дисфункції моделі інформаційної безпеки для порушення безпеки інформації, отримання незаконної вигоди (заподіяння шкоди власнику, користувачу інформації). Крім того, можливі незловмисні дії джерел загроз щодо активізації тих чи інших недоліків моделі, що здатні заподіяти шкоду.

Кожній загрозі можуть бути зіставлені різні недоліки безпеки інформації. Усунення або істотне ослаблення недоліків впливає на можливість реалізації загроз моделі інформаційної безпеки підприємства.

Для зручності аналізу та пізнання всі недоліки можуть поділятися на класи, групи і підгрупи. Недоліки безпеки інформації за своєю природою можуть бути:

- об'єктивними;
- суб'єктивними;
- випадковими.

Об'єктивні недоліки залежать від особливостей побудови і технічних характеристик обладнання, що застосовується на підприємстві, тобто на об'єкті, який захищається. Повне усунення цих недоліків неможливе, але вони можуть істотно послаблюватися технічними та інженерно-технічними методами протидії загрозам інформаційної безпеки. До них можна віднести:

Супутні технічним засобам випромінювання:

- електромагнітні (побічні випромінювання елементів технічних засобів, кабельних ліній технічних засобів, випромінювання на частотах роботи генераторів, на частотах самозбудження підсилювачів);
- електричні (наведення електромагнітних випромінювань на лінії і провідники, просочування сигналів у ланцюзі електроживлення, в ланцюзі заземлення, нерівномірність споживання струму електроживлення);
- звукові (акустичні, вібро-акустичні).

Активізуючі:

- апаратні закладки (встановлюються як у телефонні лінії, мережі електроживлення, так і безпосередньо в приміщеннях та технічних засобах);
- програмні закладки (віруси, в тому числі програми-шпигуни, технологічні виходи з програм, нелегальні копії ПЗ).

Визначені особливостями елементів:

- елементи, що володіють електроакустичними перетвореннями (телефонні апарати, гучномовці та мікрофони, котушки індуктивності, дроселі, трансформатори та ін.);
- елементи, схильні до дії електромагнітного поля (магнітні носії, мікросхеми, нелінійні елементи, повалені ВЧ нав'язуванню).

Визначаються особливостями об'єкта, що захищається:

- місцем розташування об'єкта (відсутність контрольованої зони, наявність прямої видимості об'єктів, віддалених і мобільних елементів об'єкта, вібруючих віддзеркалювальних поверхонь);

- організацією каналів обміну інформацією (використання радіоканалів, глобальних інформаційних мереж, каналів, що орендуються) [13, *173*].

Суб'єктивні недоліки залежать від дій співробітників підприємства та знешкоджуються організаційними і програмно-апаратними методами. До них можна віднести такі категорії, як "помилки" і "порушення". Розглянемо детальніше кожну з них.

Першу групу складають помилки, які виникають:

- у процесі підготовки і використання програмного забезпечення (в тому числі як у процесі розроблення алгоритмів і програмного забезпечення, так і безпосередньо інсталяції та завантаження готового програмного забезпечення, його експлуатації, введення даних);
- під час управління складними системами (у випадках використання можливостей самонавчання систем, налаштування сервісів універсальних систем, організації управління потоками обміну інформацією);
- у процесі експлуатації технічних засобів (при увімкненні/вимкненні технічних засобів, використанні технічних засобів охорони та засобів обміну інформацією).

До другої групи можна віднести порушення (детально розглянуті О. А. Кириченко) [13, *175*]:

- режиму охорони і захисту (доступу на об'єкт і до технічних засобів);
- режиму експлуатації технічних засобів (енергозабезпечення, життєзабезпечення);
- режиму використання інформації (оброблення та обміну інформацією, зберігання і знищення носіїв інформації, знищення виробничих відходів і браку);
- режиму конфіденційності (співробітниками в неробочий час, звільненими співробітниками)".

Випадкові недоліки залежать від особливостей навколишнього середовища об'єкта інформаційної безпеки і непередбачених обставин. Ці фактори, як правило, мало передбачувані і їх усунення можливо тільки при проведенні комплексу організаційних та інженерно-технічних заходів з протидії загрозам інформаційної безпеки підприємства. До таких взагалі відносять:

Збої і відмови:

- відмови і несправності технічних засобів (що обробляють інформацію, забезпечують працездатність засобів оброблення інформації, забезпечують охорону і контроль доступу);
- старіння і розмагнічування носіїв інформації (дискет і знімних носіїв, жорстких дисків, елементів мікросхем, кабелів і сполучних ліній);
- збої програмного забезпечення (операційних систем, прикладних, сервісних і антивірусних програм);
- збої електропостачання (обладнання, що обробляє інформацію, забезпечуюче і допоміжне обладнання).

Ушкодження:

- життєзабезпечуючих комунікацій (електро-, водо-, газо-, теплопостачання, каналізації, кондиціонування і вентиляції);

- огороджувальних конструкцій (зовнішніх огороджень територій, стін і перекриттів будинків, корпусів технологічного обладнання) [12].

Перш ніж пропонувати будь-які рішення з усунення дисфункцій моделі інформаційної безпеки підприємства, слід встановити для нього конкретні інтереси та цілі. Власне, такий підхід забезпечує порядок реалізації інформаційної безпеки на підприємстві.

Модель інформаційної безпеки підприємництва ефективна тоді, коли вона органічно вписується в інтереси підприємницької діяльності, і навпаки. Напрямами визначення дисфункцій моделі інформаційної безпеки є: внесення до опису об'єкта структури інтересів і проведення аналізу ризиків; визначення правил будь-якого процесу користування інформацією, що мають певний ступінь цінності [14, *322*]. Організаційно-правові напрями забезпечення інформаційної безпеки підприємства оформлюють у вигляді документа, який узгоджують та затверджують із засновниками.

Деталізований опис загальної побудови моделі інформаційної безпеки підприємства забезпечується сукупністю чинників або критеріїв, які уточнюють мету діяльності підприємства. Сукупність чинників є основою визначення вимог до моделі інформаційної безпеки підприємства. Принципи розподілу чинників безпеки запропоновані вище. Зазначимо, що модель інформаційної безпеки покликана забезпечити безперешкодне досягнення підприємством своїх інтересів та мети. Тому модель невід'ємно пов'язана з інтересами підприємства і прямо залежить від їхнього рівня розвитку та розвитку всього підприємства [15, *82*].

Функціональні вимоги до організаційно-правових напрямів визначення дисфункцій моделі інформаційної безпеки підприємства визначають з добре відомими, відпрацьованими і узгодженими функціональними вимогами до інтересів підприємства. Потрібно правильно визначити вичерпний перелік інтересів об'єкта, мету цих інтересів та шляхи її досягнення. Визначення інтересів описує об'єктивний набір вимог до концептуальної моделі безпеки. Між суб'єктами забезпечення інформаційної безпеки встановлюються певні права та обов'язки, визначається регламент відносин.

Таким чином, структура організаційно-правових напрямів забезпечення інформаційної безпеки підприємств охоплює компоненти й елементи гарантій досягнення інтересів та цілей. Гарантування відображають в робочій документації, алгоритмі етапів життєвого циклу підприємства, аналізі, оцінці вразливості моделі тощо.

Отже, визначення можливих дисфункцій моделі інформаційної безпеки підприємства виявляються оцінкою діяльності служби інформаційної безпеки та аналізом вразливостей. Такий аналіз реалізують на рівні окремого механізму захисту, що дає змогу визначити здатність відповідної моделі безпеки протистояти ідентифікованим загрозам. Залежно від встановленого потенціалу загрози визначається і сила функції захисту та протидії.

Основою для визначення потенціалу загрози має бути аналіз її можливостей, ресурсів і мотивів. Тому до загальних організаційно-правових напрямів визначення та нейтралізації дисфункцій моделі інформаційної безпеки під-

приємництва слід віднести впровадження певних процедур, які необхідно застосовувати в тій чи іншій ситуації виникнення загрози. Регламентація дій суб'єктів даних процедур повинна визначатися в адміністративно-правових документах підприємства.

Джерела

1. Про доктрину інформаційної безпеки України: Указ Президента України від 25.02.2017 р. № 47/2017 [Електронний ресурс] // Президент України Петро Порошенко. Офіційне інтернет-представництво. URL: http://www.president.gov.ua/documents/472017-21374
2. *Адизес И.* Управляя изменениями / Ицхак Адизес. СПб.: Питер, 2008. 224 с.
3. *Барановський О. І.* Філософія безпеки [монографія] / У 2-х т. К.: УБС НБУ, 2014. Т. 1. 831 с.
4. *Волощук Л. О.* Теоретико-методологічні засади безпекоорієнтованого управління інноваційним розвитком промислового підприємства : дис. ... д-ра екон. наук : спец. 08.00.04 / Л. О. Волощук. Одеса, 2016. 605 с.
5. Загальна теорія держави і права / М. В. Цвік, О. В. Петришин, Л. В. Авраменко та ін. ; за ред. М. В. Цвіка, О. В. Петришина. Х.: Право, 2009. 584 с.
6. *Лафта Дж. К.* Теория организации [учеб. пособ.]. М.: ТК "Велби"; Изд-во "Проспект", 2006. 416 с.
7. Економічна безпека: навч. посіб. [Електронний ресурс] / О. Є. Користін [та ін.] ; за ред. О. М. Джужі. К.: Всеукраїнська асоціація видавців "Правова єдність"; Алерта; КНТ ; Центр учбової літератури, 2010. 368 с. // Бібліотека українських підручників. URL: http://westudents.com.ua/glavy/16506--1-ponyattya-bezpeki-pdprimnitsko-dyalnost-ekonomchna-bezpeka-pdprimstva-pravove-zabezpechennya-ekonomchno-bezpeki-pdprimstva.html
8. *Гордєєв О.* Концептуальні підходи до сутності інституційного механізму [Електронний ресурс] // Публічне управління: теорія та практика : зб. наук. праць Асоціації докторів наук з державного управління. 2012. № 3 (11). URL: http://www.kbuapa.kharkov.ua/e- book/putp/2012-3/doc/1/07.pdf
9. *Сафонов Лука.* Ризики інформаційної безпеки веб-додатків [Електронний ресурс] // IT українською. URL: http://it-ua.info/news/2016/03/15/riziki-nformacyno-bezpeki-veb-dodatkv.html
10. *Ілляшенко О. В.* Інституційний та правовий механізми системи економічної безпеки підприємства // European cooperation (Європейське співробітництво). 2016. № 3 (10). С. 48–58.
11. Модели и механизмы управления безопасностью [монография] / В. Н. Бурков, Е. В. Грацианский, С. И. Дзюбко, А. В. Щепкин. М.: Синтег, 2001. 140 с.
12. *Присяжнюк А. Й.* Адміністративно-правовий механізм забезпечення економічної безпеки держави [Електронний ресурс] // Глобалтека. URL: http://globalteka.ru/books/doc_view/15006-a--------.raw?tmpl=component
13. Проблеми управління економічною безпекою суб'єктів господарювання [монографія] / О. А. Кириченко та ін. К.: ІМБ Ун-ту економіки та права "КРОК", 2010. 412 с.
14. Проблемы теории государства и права [учеб. пособ.] / под ред. М. Н. Марченко. М.: Юристь, 2001. 656 с.
15. Термины и определения в области информационной безопасности / И. С. Школьник, С. А. Комов, В. В. Ракитин, С. Л. Родионов. М.: АС-ТРАСТ, 2010. 304 с.

Лисенко С. О. Організаційно-правові шляхи визначення основних дисфункцій концептуальної моделі інформаційної безпеки підприємництва. *Ідентифікація джерел загроз інформаційної безпеки підприємництва показує, що такі загрози реалізуються не самі по собі, а через дисфункції (недоліки) на підприємстві, що призводять до порушення цілісності моделі інформаційної безпеки конкретного підприємства. Можливі дисфункції моделі інформаційної безпеки підприємства визначаються і конкретизуються під час процедури оцінювання діяльності служби інформаційної безпеки та аналізу вразливостей. Такий аналіз реалізують на рівні окремого механізму захисту, що дає змогу визначити здатність відповідної моделі безпеки протистояти ідентифікованим загрозам. Залежно від встановленого потенціалу загрози визначається і сила функції захисту та протидії. Основою для визначення потенціалу загрози має бути аналіз її можливостей, ресурсів і мотивів. Тому до загальних організаційно-правових напрямів визначення та нейтралізації дисфункцій моделі інформаційної безпеки підприємництва слід віднести впровадження певних процедур, які необхідно застосовувати в тій чи іншій ситуації виникнення загрози. Регламентація дій суб'єктів даних процедур повинна визначатися в адміністративно-правових документах підприємства.*

Lysenko S. O. Organizational and legal ways of determining the main dysfunctions of the conceptual model of information security of entrepreneurship. *The identification of the sources of threats to enterprise security information shows that such threats are not realized on their own, but through dysfunctions (disadvantages) in the enterprise, which leads to a breach of the integrity of the information security model of a particular enterprise. Possible dysfunctions of the information security model of an enterprise are defined and specified during the procedure for evaluating the activity of the information security and vulnerability analysis. Such an analysis is implemented at the level of a separate mechanism of protection, which enables one to determine the ability of the appropriate security model to withstand identified threats. Depending on the potential threat, the strength of the protection and response functions is also determined. The basis for determining the threat potential should be an analysis of its capabilities, resources and motives. Therefore, the general organizational and legal directions of defining and neutralizing dysfunctions of the model of information security of entrepreneurship should include the introduction of certain procedures that need to be applied in one or another threat situation. Regulation of actions of subjects of these procedures should be defined in the administrative-legal documents of the enterprise.*

Лысенко С. А. Организационно-правовые пути определения основных дисфункций концептуальной модели информационной безопасности предприни-

мательства. *Идентификация источников угроз информационной безопасности предпринимательства показывает, что такие угрозы реализуются не сами по себе, а через дисфункции (недостатки) на предприятии, приводящие к нарушению целостности модели информационной безопасности конкретного предприятия. Возможные дисфункции модели информационной безопасности предприятия определяются и конкретизируются во время процедуры оценки деятельности службы информационной безопасности и анализа уязвимостей. Такой анализ реализуют на уровне отдельного механизма защиты, позволяет определить способность соответствующей модели безопасности противостоять идентифицированным угрозам. В зависимости от установленного потенциала угрозы определяется и сила функции защиты и противодействия. Основой для определения потенциала угрозы должен быть анализ ее возможностей, ресурсов и мотивов. Поэтому к общим организационно-правовым направлениям определения и нейтрализации дисфункций модели информационной безопасности предпринимательства следует отнести внедрение определенных процедур, которые необходимо применять в той или иной ситуации возникновения угрозы. Регламентация действий субъектов данных процедур должна определяться в административно-правовых документах предприятия.*

Надійшла 15 грудня 2017 р.