УДК 519.81

Т.М. Мужанова

ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА: ОСНОВНІ ЗАСАДИ

Стаття присвячена дослідженню основних засад організаційного забезпечення інформаційної безпеки підприємства, зокрема розглянуто й узагальнено існуючі наукові підходи до визначення сутності, функцій, напрямів та принципів організаційного забезпечення інформаційної безпеки фірми.

Ключові слова: інформаційна безпека, забезпечення інформаційної безпеки, організаційне забезпечення інформаційної безпеки підприємства.

Постановка проблеми

В умовах бурхливого розвитку інформаційних технологій та появи наростаючого числа інформаційних загроз основною цінністю для підприємства поступово стають інформаційні ресурси та інфраструктура для їх створення, обробки, передачі, а забезпечення інформаційної безпеки (ЗІБ) набуває першочергового значення для успішної діяльності бізнесу. З огляду на зазначені обставини дослідження основних засад організаційного забезпечення ІБ (ОЗІБ) організації є актуальним і створює наукові передумови для вирішення практичних завдань у сфері ІБ.

Аналіз останніх досліджень і публікацій

Дослідження ґрунтується на вивченні публікацій вітчизняних та закордонних дослідників з організаційних аспектів ЗІБ підприємства [1-2, 4-6], положень Стандарту ISO/IEC 27001:2005 «Система управління інформаційною безпекою. Вимоги», а також аналітичних матеріалів Європейського Агентства з питань мережевої та інформаційної безпеки [7].

Метою дослідження є огляд і узагальнення вітчизняних та зарубіжних підходів до визначення основних засад ОЗІБ організації та представлення власного бачення, що визначає наукову новизну роботи.

Викладення основного матеріалу

Очевидно, що сьогодні для досягнення стану захищеності підприємства від внутрішніх та зовнішніх інформаційних загроз необхідним є створення системи ЗІБ, що включає створення і підтримання в дієвому стані організаційної структури (підрозділів, посадових осіб), здійснення активної, цілеспрямованої і послідовної діяльності, що передбачає впровадження комплексу нормативних, організаційних, програмно-технічних та інших заходів і використання різноманітних засобів ЗІБ (рис1.).

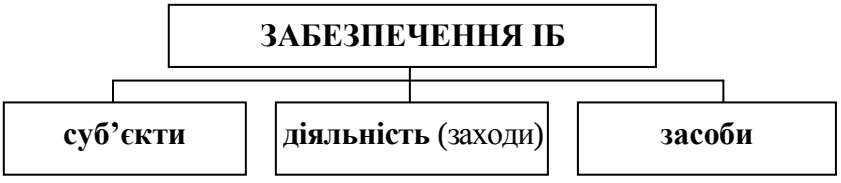

Рис. 1. Структура ЗІБ

ОЗІБ є однією з найважливіших складових загальної системи ЗІБ організації і має на меті досягнення таких цілей як забезпечення конфіденційності, цілісності та уникнення

несанкціонованого доступу до критичної інформації і пов'язаних з нею процесів та інших цілей.

У рамках ОЗІБ здійснюється організаційна діяльність у сфері нормативного, програмно-технічного, фізичного та інших забезпечення ІБ і регламентуються процеси функціонування інформаційних систем; використання інформаційних ресурсів; діяльність персоналу служби ІБ і працівників підприємства загалом; порядок взаємодії користувачів із системою.

Організаційна діяльність передбачає використання засобів планування, інструктування, координації, контролю, вироблення управлінських рішень, надання допомоги, забезпечення своєчасного виконання завдань, сприяння проведенню відповідних заходів за зазначеними вище напрямами.

У загальному вигляді ОЗІБ виконує такі функції: інформаційну (збирання, обробка і використання всіх наявних видів інформації, яка впливає на досягнення цілей організації), міжперсональну (забезпечення взаємодії між керівництвом, персоналом, зовнішніми організаціями, споживачами та всіма зацікавленими сторонами), прийняття рішення (вибір оптимальної альтернативи, вирішення конфліктів, запобігання виникненню проблем) [6].

Розглянемо різні наукові підходи до визначення структури ОЗІБ.

Відповідно до процесного підходу ОЗІБ можна розглядати як замкнутий цикл процесів управління і представити у вигляді моделі «Плануй – Виконуй – Перевіряй - Дій» («Plan-Do-Check-Act») [3] (рис 2.).

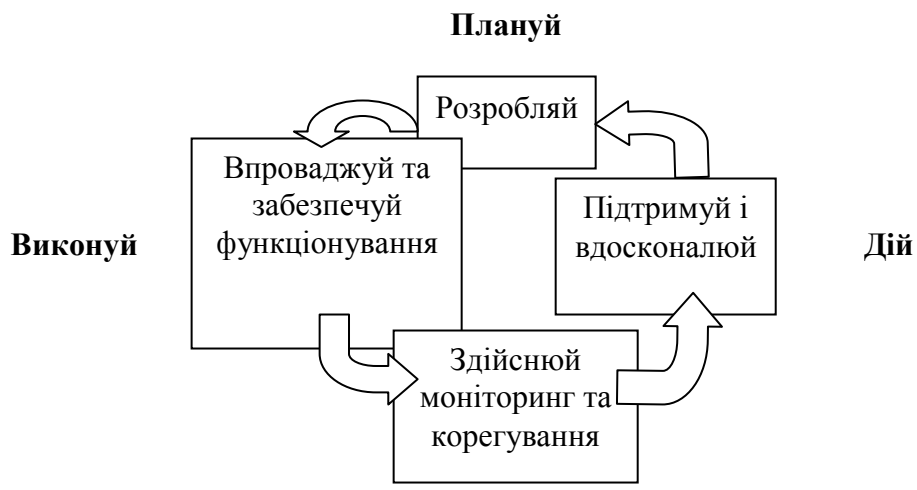

Рис. 2. Етапи ОЗІБ

Складові системи забезпечення ІБ у руслі системного підходу розділяють на три множини: основи (з чого складається: база, структура, заходи, засоби), напрямки (для чого призначені: захист об’єктів ІС, процесів та каналів зв’язку, управління і контроль системи ІБ), етапи (як працює: визначення критичних ресурсів, виявлення загроз та вразливостей, формування вимог до системи ІБ, здійснення заходів, вибір засобів і контроль) [2].

У контексті ситуаційного підходу ОЗІБ підприємства має ґрунтуватися на аналізі ситуації, тобто конкретного складу внутрішніх і зовнішніх чинників, які впливають на організацію в конкретний момент.

До внутрішніх відносять такі чинники: мета й завдання підприємства у сфері ІБ, його структура, технології, які використовуються, і люди (поведінка окремих осіб, членів груп, керівника). Зовнішні фактори можуть змінюватися в залежності від ситуації, але основні з них такі: фактори прямого впливу (політика держави, нормативне забезпечення, позиції споживачів, партнерів, конкурентів) і фактори опосередкованого впливу (стан економіки, розвиток науково-технічного прогресу, політичні та міжнародні події тощо).

Цікавим є бачення західних вчених, згідно з яким ОЗІБ як складова загальної системи ЗІБ має здійснюватися за схемою «шість «Р»:

– планування (*Planning*) - діяльність, необхідна для підтримки проектування, створення і реалізації стратегій ІБ;

– політика (*Policy*) - сукупність організаційних засад, які встановлюють певну поведінку в межах організації;

– програми (*Programs*) ІБ, які спеціально управляються як окремі об'єкти;

– захист (*Protection*) - діяльність з управління ризиками, включаючи оцінку і контроль ризиків, механізмів захисту, технологій та інструментів;

– люди (*People*) - включає в себе забезпечення безпеки персоналу і власне персонал, задіяний у системі ІБ;

– управління проектами (*Project Management*) - визначення та контроль ресурсів, залучених для реалізації проектів із ЗІБ, вимірювання результатів та корегування заходів [6].

На думку фахівців, організаційну структуру системи забезпечення ІБ підприємства можна представити у вигляді сукупності таких рівнів:

- рівень 1 - керівництво організації;
- рівень 2 - підрозділ ОІБ;
- рівень 3 - адміністратори штатних і додаткових засобів захисту;
- рівень 4 - відповідальні за ОІБ в підрозділах (на технологічних ділянках);
- рівень 5 - кінцеві користувачі і обслуговуючий персонал [1].

Крім того, на інформаційну безпеку організації можуть впливати сторонні особи і сторонні організації, як партнерські, так і такі, що мають за мету втручання в процес функціонування системи ІБ або несанкціонований доступ до інформації як локально, так і віддалено.

Розглянемо представлені в науці підходи до визначення напрямів ОЗІБ. Через призму структурно-функціонального підходу виділяють такі напрями ОЗІБ підприємства:

– формування та практична реалізація комплексної багаторівневої політики ІБ організації і системи внутрішніх вимог, норм і правил;

– організація підрозділу (департаменту, служби, відділу) ІБ;

– управління інцидентами;

– проведення аудитів стану ІБ в організації [3].

За сферами діяльності щодо ЗІБ фірми окреслюють такі напрями ОЗІБ:

– організація режиму і охорони;

– робота з носіями конфіденційної інформації;

– робота з персоналом;

– організація аналітичної роботи і контролю;

– комплексне планування робіт з ОЗІБ [5].

Відповідно до іншого підходу, діяльність у межах напрямів ОЗІБ підприємства включає і виконання завдань з циклу управління (планування, організація, контроль, коригування), і завдань за сферами ЗІБ (обмеження та розмежування доступу, сертифікація і ліцензування, робота з персоналом) [4]. Детальніше показано на рис. 3.

Рис. 3. Завдання ОЗІБ підприємства

Узагальнивши різні наукові підходи [1-7], можна виділити такі основні принципи ОЗІБ:

– комплексності, тобто ефективне використання сил, засобів, способів і методів ЗІБ для вирішення поставлених завдань залежно від конкретної ситуації;

– адаптивності, що означає пристосовуваність системи ЗІБ до швидко змінних оточуючих підприємство умов та загроз;

– оперативності ухвалення управлінських рішень;

– ефективності, що передбачає дотримання оптимального балансу між можливостями, продуктивністю і витратами системи ЗІБ;

– економічної доцільності, відповідно до якого обсяги витрат на ЗІБ не можуть перевищувати розміру збитків у випадку реалізації потенційних загроз.

Крім того ОЗІБ має бути складовою системи управління організацією, бути узгодженим із її бізнес-завданнями і стратегією, здійснюватися централізовано за умов однозначної підтримки і зобов'язань з боку керівництва організації, гарантувати повне дотримання керівництвом і персоналом встановлених норм та правил ЗІБ, а також здійснення обліку й контролю за діяльністю у системі ЗІБ із використанням зворотного зв'язку.

З метою протидії негативним проявам т.зв. «людського фактора» ОЗІБ має здійснюватися на засадах персональної відповідальності, розподілу обов'язків та мінімізації привілеїв; постійного навчання й обізнаності персоналу; формування організаційної прихильності та уникнення дисциплінарних методів.

Важливими умовами успішного ОЗІБ є створення системи багаторівневого захисту, різноманіття захисних засобів та посилення найслабшої ланки [2].

Висновки

Дослідження показало, що в закордонній та вітчизняній науковій думці активно вивчалися питання щодо сутності, напрямів, етапів та принципів ОЗІБ підприємства, що створює наукове підгрунтя для вдосконалення засад забезпечення ІБ в бізнес-діяльності на практиці.

Література

1. Безопасность информационных технологий: материалы курса. [Електронний ресурс]. Режим доступу: http://asher.ru/security/book/its/08

2. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты / В.В. Домарев - К.: ООО ТИД «ДС», 2002. – 688 с.

3. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, MOD). ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. – К.: Національний банк України, 2010. – 49 с.

4. Романов О.А. Организационное обеспечение информационной безопасности Учебник для студ. высш. учеб. заведений / О.А. Романов, С.А. Бабин, С.Г. Жданов. - М.: Академия, 2008. - 192 с.

5. Управление информационной безопасностью. [Електронний ресурс]. – Режим доступу: http://www.arinteg.ru/articles/upravlenie-informatsionnoy-bezopasnostyu-26728.html

6. M. E. Whitman, H. J. Mattord. Management of Information Security. [Електронний ресурс]. Режим доступу: https://ru.scribd.com/doc/102088851/Management-of-Information-Security

7. Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools. [Електронний ресурс]. Режим доступу: https://www.enisa.europa.eu.

Надійшла 19.05.2016 р. Рецензент: д.т.н., с.н.с. Наконечний В.С.