

Іванченко Н.О.

канд.екон.наук, доцент,
доцент кафедри статистики, інформаційно-аналітичних систем і демографії
Київський національний університет імені Тараса Шевченка, Україна

Подскребко О.С.

доцент, доцент кафедри економічної кібернетики
Київський національний університет імені Тараса Шевченка, Україна

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Управління інформаційною безпекою – це невід’ємна складова загальної системи управління, що базується на аналізі ризиків і призначена для проектування, реалізації, контролю, супроводу і вдосконалення заходів в області інформаційної безпеки. До цієї системи входять організаційні структури, інформаційна політика, дії з планування, обов'язки, процедури, процеси і ресурси.

Головною метою більшості систем інформаційної безпеки є захист бізнес інтересів і знань компанії від знищення або витоку. Також однією з основних цілей системи інформаційної безпеки є гарантія майнових прав та інтересів клієнтів. У той же час заходи з інформаційної безпеки не повинні обмежувати або ускладнювати процеси обміну знаннями в компанії, оскільки це може поставити під загрозу розвиток організації.

Система управління інформаційною безпекою повинна забезпечувати гарантію досягнення таких цілей як забезпечення конфіденційності критичної інформації, забезпечення неможливості несанкціонованого доступу до критичної інформації, цілісності інформації та пов'язаних з нею процесів (створення, введення, обробки і виведення) і ряду інших цілей.

Досягнення заданих цілей можливо в ході вирішення наступних основних завдань, таких як визначення відповідальних за інформаційну безпеку, розробка спектра ризиків інформаційної безпеки і проведення їх експертних оцінок, розробка політик і правил доступу до інформаційних ресурсів, розробка системи управління ризиками інформаційної безпеки, в тому числі методи їх оцінки, контроль інформаційної безпеки на підприємстві/по виду економічної діяльності/ у державі.

Виділяється чотири стадії реалізації системи управління інформаційною безпекою рис.1:

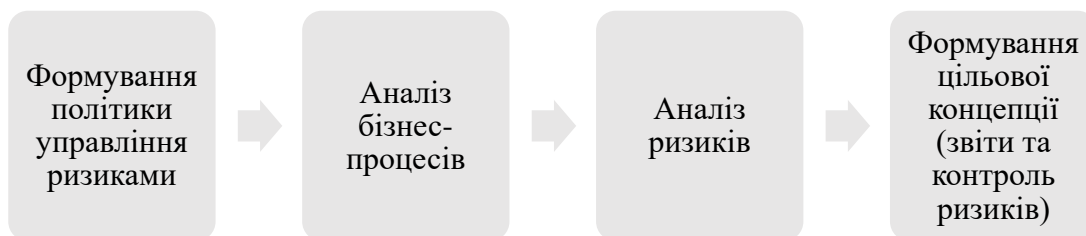


Рис. 1. Стадії реалізації системи управління інформаційною безпекою

Основна мета формування системи управління інформаційною безпекою – сформувати і забезпечити виконання програми робіт у галузі інформаційної безпеки, виділяючи необхідні ресурси і контролюючи кожний етап. Основою даної програми є політика безпеки, що відображає підхід організації до захисту своїх інформаційних інтересів.

Політика безпеки – це сукупність документованих рішень, що приймаються керівництвом організації і спрямовані на захист інформації та асоційованих з нею ресурсів. З практичної точки зору політику безпеки доцільно розглядати на трьох рівнях деталізації.

До верхнього рівня належать рішення, що стосуються організації в цілому. Вони мають загальний характер і, як правило, виходять від керівництва організації. Список подібних рішень може складатися з таких елементів:

1. рішення про формування або перегляд комплексної програми забезпечення інформаційної безпеки, призначення відповідальних за реалізацію програми;
2. формулювання цілей, до яких прагне організація у сфері забезпечення інформаційної безпеки, визначення загальних напрямків досягнення цих цілей;
3. забезпечення бази для дотримання законів і правил;
4. формулювання адміністративних рішень з тих питань реалізації програми безпеки, які повинні розглядатися на рівні організації в цілому.

До середнього рівня відносять питання, що стосуються окремих аспектів інформаційної безпеки, але важливі для різних експлуатованих організацією систем. Приклади таких питань – ставлення до передових (але, можливо, недостатньо перевірених) технологій, доступ до Internet, використання домашніх комп'ютерів, застосування користувачами неліцензійного програмного забезпечення і т.д.

Політика безпеки нижнього рівня стосується конкретних інформаційних сервісів. Вона включає два аспекти – цілі і правила їх досягнення, тому її інколи важко відокремити від питань реалізації. На відміну від двох верхніх рівнів, дана політика повинна бути визначена детальніше.

Є багато речей, специфічних для окремих видів послуг, які не можна однаково регламентувати. В той же час, ці речі настільки важливі для забезпечення режиму безпеки, що рішення, які їх стосуються, повинні ухвалюватися на управлінському, а не технічному рівні. Наведемо декілька прикладів питань, на які слід дати відповідь у забезпеченні політики безпеки нижнього рівня.

1. Хто має право доступу до об'єктів, підтримуваних сервісом?
2. За яких умов можна читати і модифікувати дані?
3. Яким чином організовано віддалений доступ до сервісу?

Принципова особливість такого аналізу, як аналіз бізнес-процесів, полягає в тому, що він дозволяє побачити всю сукупність операцій. Формалізація бізнес-процесів дозволяє відносно чітко розмежувати функції управління і департаментів, виділити основні зони відповідальності, описати зв'язки між підрозділами, формалізувати інформаційні потоки всередині підприємства, визначити основні зони контролю і т. ін.

Аналіз та оцінка ризику – це процес, який використовується для присвоєння значень наслідків, ймовірності виникнення та рівня ризику. Він включає в себе:

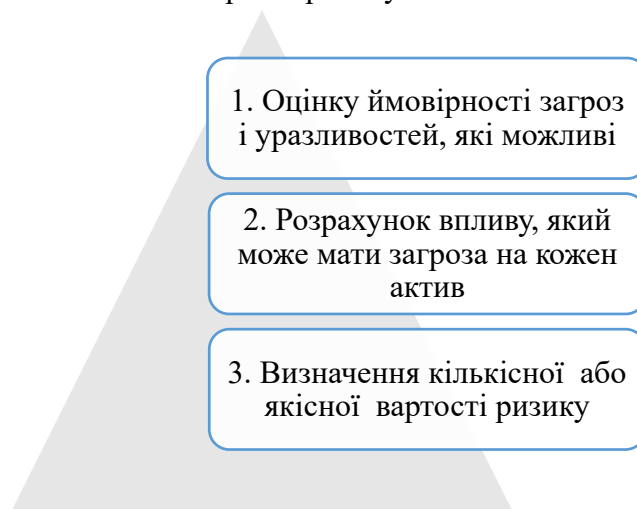


Рис. 2. Етапи аналізу та оцінки ризику

Для досягнення цілей забезпечення інформаційної безпеки економіки важливо правильно визначити об'єкти інформаційної безпеки. До таких об'єктів належать:

- інформаційні ресурси держави, підприємств, установ та організацій, що містять конфіденційну інформацію (секретну, обмеженого доступу або ж комерційну таємницю), а також загальнодоступну відкриту інформацію та наукові знання, які мають пряме відношення до економіки держави;
- інформаційна інфраструктура (мережі зв'язку та інформаційних комунікацій, центри аналізу та обробки даних, системи і засоби захисту інформації);
- система формування, поширення і використання інформаційних ресурсів в країні;
- система управління інформацією підприємства конкретного сектору економіки;
- результати наукової та інноваційної діяльності.

Функції інформаційної безпеки економіки полягають у ефективному управлінні системою забезпечення інформаційної безпеки, використанні ефективних механізмів управління.

До основних факторів, що впливають на рівень інформаційної безпеки економіки є:

1. Декларування пріоритетів науково-технічної політики.
2. Систематичний моніторинг і оперативний розвиток законодавчої бази.
3. Послідовне і постійне здійснення структурних перетворень.
4. Пошук шляхів комерціалізації науково-виробничої діяльності.
5. Міжнародне співробітництво у сфері розробки та впровадження інновацій.
6. Захист внутрішнього ринку, цілеспрямовані активні дії по завоюванню вітчизняними товаровиробниками частки світового ринку.
7. Створення сприятливих умов для поширення і впровадження інновацій.
8. Створення науково-технічних та інвестиційних центрів в новітніх галузях досліджень і розробок.

Список використаних джерел:

1. Іванченко Н.О. Інформаційна складова економічної безпеки підприємства та її значення для забезпечення стійкого розвитку національної економіки. / Стратегія розвитку України (економіка, соціологія, право). – 2011. – №3. – С. 124-128.
2. Харченко Л.С. Інформаційна безпека України: Глосарій / Л.С. Харченко, В.А. Ліпкан, О.В. Логінов. – К.: Текст, 2004. – 136 с
3. Діброва О.В. Аналіз головних складників інформаційної безпеки наукоємного сектора національної економіки України / Східна Європа: економіка, бізнес та управління. Випуск 4 (04) –2016. – С. 77 –79.