РАЗВИТИЕ РЕГИОНАЛЬНЫХ СЛОЖНО–ПРЕДПРИНИМАТЕЛЬСКИХ СТРУКТУР: СОВРЕМЕННЫЕ ПРОБЛЕМЫ И РЕШЕНИЯ

УДК 354:330.341:62

ФОРМУВАННЯ ПОЛІТИКИ БЕЗПЕКИ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ

А.О. Ващишин
Національний університет водного господарства та природокористування, Україна,
a.o.vashchyshyn@nuwm.edu.ua

Для досягнення економічної безпеки своїх підприємств більшість країн із стабільною економікою інвестують інноваційні проекти та сприяють розвитку науково-технічного забезпечення [1]. Значна кількість компаній в розвинутих країнах керуються наступними принципами: наукові знання виступають ключем в забезпечене майбутнє; сучасні технології створюють основу розвитку соціально-економічної безпеки підприємств; керівництво підприємств повинно стимулювати розвиток науки і технічного прогресу.

В економічно розвинених країнах нормативно-правова база визначає об'єктивну реальність ризиків, які пов'язані із посиленням конкуренції і загостренням проблем ринкового середовища в різних сферах діяльності на зовнішньому та внутрішньому ринках. Для цього необхідно застосувати організаційні та структурні заходи підтримки та забезпечення стійкості підприємств, виділяючи сектори малого і середнього бізнесу в сучасних складних умовах [2].

Стрімкий розвиток ІТ-технологій перетворив їх в надто ризиковану сферу людської діяльності. Вартісне вираження ймовірної події, що веде до втрат, називають ризиком. Процес оцінювання ступеня ризику за спеціальними методиками у випадку здійснення того чи іншого варіанта загроз називають аналізом ризику. У процесі аналізу ризику вивчають компоненти інформаційної системи, що можуть зазнати посягань на їх безпеку, визначають уразливі місця системи, оцінюють можливість реалізації для кожної конкретної загрози та очікувані розміри відповідних втрат, вибирають ймовірні методи захисту й обчислюють їхню вартість. На заключному етапі оцінюється зиск від застосування пропонованих заходів захисту. Цей зиск може мати як позитивний, так і негативний знак: у першому випадку – йдеться про очевидний виграш, а у другому – про додаткові витрати для гарантування власної безпеки.

Виходячи з результатів цього аналізу, приймають рішення про доцільність тих або інших заходів захисту. В остаточному підсумку складається план захисту, формується політика безпеки.

План захисту містить такі розділи:

– поточний стан системи;
– рекомендації щодо реалізації системи захисту;
– відповідальність персоналу;
– порядок запровадження засобів захисту;
– порядок перегляду плану засобів захисту та їх складу.

Політика безпеки – це комплекс законів, правил і практичних рекомендацій, на основі яких будується управління, захист і розподіл критичної інформації в системі.

Управляти інформаційними ресурсами компанії не можна без запобіжних заходів безпеки. На етапі розробки можливе комплексне використання таких видів захисту, як правові, морально-етичні, адміністративні, фізичні та технічні правила.

До правових заходів належать чинні в країні закони, укази, положення міжнародних організацій, нормативні акти, що регламентують правила взаємодії з інформацією обмеженого використання і відповідальність за їх порушення. Ці заходи відіграють роль стримуючого чинника для потенційних порушень.

До морально-етичних заходів протидії належать всілякі норми поведінки, що традиційно склалися раніше, виникають або спеціально розробляються в міру поширення ЕОМ та інформаційних систем.

Адміністративні заходи захисту – це заходи організаційного характеру, що регламентують процеси функціонування інформаційної системи, використання її ресурсів, діяльність персоналу і т. ін. Мета цих заходів – найбільшою мірою виключити можливість реалізації загроз безпеці. До переліку адміністративних заходів можна віднести такі:

– розробка правил обробки інформації в інформаційній системі;

– організація захисту від установки апаратури прослухування в приміщеннях обчислювального центру або розташування АРМ;

– ретельний відбір персоналу;

– організація обліку, збереження, використання і знищення документів та носіїв із конфіденційною інформацією;

– розподіл реквізитів розмежування доступу (паролів, профілів повноважень);

– організація прихованого контролю за роботою користувачів і персоналу інформаційної системи;

– інші заходи.

Фізичні заходи захисту – це різного роду механічні, електро- або електронно-механічні пристрої і будови, призначені для створення фізичних перешкод на можливих шляхах проникнення й доступу потенційних порушників до компонентів захисту інформації.

Технічними (апаратно-програмними) засобами захисту називаються різноманітні електронні й спеціальні програми, що виконують функції захисту. Серед цих функцій відзначимо такі: ідентифікація й аутентифікация (відповідність вимогам) користувачів або процесів, розмежування і контроль доступу до ресурсів, реєстрація й аналіз подій, криптографічний захист інформації (шифрування даних), резервування ресурсів і компонентів інформаційної системи.

До апаратно-програмних заходів належать антивірусні програми [3].

Проблема управління ІТ-ризиками, оцінка інвестиційних ІТ-проектів – найважливіша складова будь-якого процесу автоматизації. Ймовірність того, що проект завершиться у плановий термін і буде відповідати плановому бюджету, а також будуть реалізовані очікувані функції, представляє великий інтерес для розробників і для організацій [4].

За даними The Standish Group [5] з більш, ніж 9000 розглянутих проектів впровадження інформаційних систем, успіху домоглися лише 16,2 %, в категорію «спірні проекти» попали 52,7 %, в категорії провальних проектів (від реалізації яких відмовились) залишились 31,1 %. В середньому бюджети ІТ-проектів завищені в 1,5−2 рази, а час на їх реалізацію – в 2–3 рази. При цьому факторів, що визначають успіх та проблеми реалізації ІТ-проектів, достатньо багато.

Заслуговуючими на увагу є напрацювання Ткалич Т.А., яка в результаті проведених розрахунків прийшла до висновків:

1) В систематизації ризиків знайшли відображення ризики зниження якості та споживчої цінності ІТ-послуг;

2) Показники якості, цінності і узгодженості ІТ-послуг можуть бути факторами визначення ризиків втрати споживчих властивостей інформаційної системи;

3) Використання прогнозних моделей розповсюдження ІТ-послуг дозволяє уточнити очікувані рівні ризиків сприйняття результативності ІТ-послуг [4].

Таким чином можна констатувати, що всі галузі критичної інфраструктури можуть наражатися на суттєву небезпеку. Тільки при правильному підході до запобігання її можна досягнути певного прогресу у розвитку країни.

Список використаних джерел:

1. Корчевська Л.О. Міжнародний досвід формування інституціонально-правової основи безпекознавства [Електронний ресурс]. – Режим доступу: http: // iepjournal.com / journals / 24 /2016_4_Korchevska.pdf]

2. Денисенко М. П. Зарубіжний досвід регулювання економічної безпеки / М. П. Денисенко, П.Т. Колісніченко // Інвестиції: практика та досвід. – 2017. − № 6. С. 15-19.

3. Сазонець О.М. Розвиток світового господарства та глобальні інформаційні системи / О.М. Сазонець. – Донецьк: Юго-Восток, 2010. – 289 с.

4. Ткалич Т.А. Прогнозирование рисков инвестиционных ИТ-проектов / Т.А. Ткалич // Інвестиції: практика та досвід. – 2017. − № 6. – С. 9-14

5. The Standish Group (2017), “Report Chaos” [Електронний ресурс]. – Режим доступу: https: // projectsmart.co.uk / white-papers / chaos-report.pdf (Accessed 05 March 2017)