УДОСКОНАЛЕННЯ МЕТОДІВ УПРАВЛІННЯ ПРОЦЕСАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Андрій ІВАНУСА, Ростислав ТКАЧУК, Тарас БРИЧ

Процес інформаційної безпеки компанії базується на принципах захисту даних. Він вимагає постійне вдосконалення захисних функцій. Це пов'язано з тим, що область захисту інформації постійно розвивається та удосконалюється. Захисні системи, створені лише кілька років тому, швидко стають неефективними. З кожним роком підвищується ризик того, що зловмисники зламають їх.

Ключове рішення при розробці ефективного підходу для вирішення цих проблем – це розробка політики інформаційної безпеки організації, оскільки вона вирішує ключове завдання, використовуючи комплексний підхід. Тому необхідно постійно покращувати та оновлювати цю політику. Коригування, які були внесені, важливо постійно порівнювати із засобами захисту, що вже застосовуються. Крім того, необхідно розробити систему захисту даних, яка включає сукупність технічних, програмних, криптографічних та організаційних засобів, що дозволяють забезпечити безпеку мережі у будь-який момент часу від випадкового чи навмисного впливу, а також несанкціонованого використання.

Вибір правильних елементів керування та їх реалізація спочатку допоможуть організації знизити ризик інформаційної безпеки до прийнятних рівнів. Тому вибір контролю повинен слідувати і ґрунтуватися на оцінці ризику.

Організації можуть здійснювати додаткові заходи контролю відповідно до вимог організації. «Адміністративний контроль (також його інколи називають процедурним контролем) складається із затверджених письмових політик, процедур, стандартів та керівних принципів». Адміністративний контроль формує рамки для ведення бізнесу та управління людьми. Вони інформують людей про те, як вести бізнес та як проводити щоденні операції.

Також необхідно налагодити процес своєчасного виявлення та нейтралізації загроз інформаційній безпеці, яка могла б запобігти можливим

збиткам. Оцінка можливих загроз безпеці проводиться шляхом формування експертної групи, що проводить аналіз вразливостей. Завдяки якісному формуванню експертної групи можна знизити рівень суб'єктивності в оцінці загроз.

Систематичний метод виявлення загроз інформаційної безпека передбачає безперервний процес, спрямований на виявлення та визначення загроз, подальшу ідентифікацію джерела загрози та оцінку можливої шкоди у разі її реалізації. На регулярній основі повинен проводитись огляд та переоцінка загроз інформаційній безпеці. Забезпечення автоматизованого моніторингу може здійснюватися як керівництвом підприємства, так і адміністратором безпеки. Моніторинг та контроль дій персоналу також відноситься до систематичного методу виявлення загроз.

Для удосконалення цього методу необхідно, щоб у процесі експлуатації інформаційної системи, певний співробітник мав можливість змінювати її базову конфігурацію таким чином, щоб забезпечити зміну пріоритетів значущості інформації, що обробляється, відповідно до появи нових загроз або нових вимог на законодавчому рівні.

Отже, для удосконалення методів управління інформаційною безпекою необхідно зробити цей процес циклічним, який повинен включати: усвідомлення працівниками організації ступеня необхідності захисту інформації та постановку завдань, збір та аналіз даних про стан інформаційної безпеки в організації, оцінку інформаційних ризиків, планування заходів щодо обробки ризиків, реалізацію та впровадження відповідних механізмів контролю, розподіл ролей та відповідальності, навчання та мотивацію персоналу, оперативну роботу щодо здійснення захисних заходів, моніторинг функціонування механізмів контролю, оцінку їх ефективності та відповідні коригувальні впливи.

Також для удосконалення методів захисту інформації необхідно, щоб система захисту інформації охоплювала сукупність засобів контролю інформаційних потоків, спостереження за локальними мережами та даними, які організація отримує з глобальних мереж.