

СТВОРЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ АВТОМАТИЗОВАНОЇ СИСТЕМИ ІНТЕРНЕТ ПРОВАЙДЕРА

Створення системи захисту інформації для організацій, що займаються наданням телематичних послуг, є обов'язковою складовою діяльності організації Інтернет-провайдера. Дана необхідність зумовлена тим, що подібні організації обробляють великий обсяг конфіденційних відомостей, у тому числі персональні дані, захист яких обов'язкова за вимогам законодавства. Жорстка конкуренція на ринку призводить до того, що конфіденційна інформація, якою володіє організація, може дати значну конкурентну перевагу. Також комплексна система захисту інформації дозволить забезпечити безперебійне функціонування сервісів, запобігти прямі матеріальні втрати від витоку або втрати конфіденційної інформації, а також запобігти можливому збитку репутації компанії.

Для того, щоб визначити доцільність створення КСЗІ, зону і глибину її охоплення слід провести детальний аналіз організації, що включає: аналіз діяльності підприємства. Положення організації на ринку. Виявлення конфіденційної інформації та захищаються. Аналіз загроз, вразливостей і потенційного збитку від реалізації загрози.

На основі отриманої інформації про діяльність організації та вразливі місця у діючій системі захисту необхідно скласти технічне завдання на створення комплексної системи захисту інформації.

Та частина ризиків, якої часто приділяється занадто мало уваги. Суть даної групи ризиків полягає в тому, що по-перше поточний стан інформаційної системи організації має задовольняти вимоги впроваджуваних заходів, по-друге впроваджені технічні заходи повинні перебувати в гармонії з організаційними та програмно-апаратними заходами. Можливі ризики: Конфлікт встановлюваного програмного і апаратного забезпечення зі встановленою операційною системою і апаратною частиною. Складність в експлуатації технічних і програмних засобів. Наявність закладних пристроїв в встановлюваних апаратних засобів. Наявність декларованих можливостей в інсталиються програмних засобах. Основні заходи запобігання даної групи ризиків: Перевірка всіх поставляються програмних і апаратних засобів. Вибір надійних постачальників. Ретельний вибір необхідних програмних та апаратних засобів.

За допомогою складеної структури організації була розрахована матриця відповідальності, яка дозволяє виявити відповідальних за той чи інший захід. Завдяки детальному плану заходів можна оцінити загальну підсумкову вартість побудови комплексної системи захисту інформації. Незважаючи на досить високу вартість створення комплексної системи захисту інформації, дані заходи повністю окупають себе з причини високої вартості інформації, що захищається.

Науковий керівник – к.т.н., доц., Швець В.А.