УДК 338:658.5
Р.Ю.Клим
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ПОЛІТИКА БЕЗПЕКИ ЯК СКЛАДОВА ЧАСТИНА КОМПЛЕКСНОГО ЗАХИСТУ ІНФОРМАЦІЇ ПІДПРИЄМСТВА

R.Y. Klym

SAFETY POLICY AS A COMPOSITE PART COMPLEX PROTECTION OF THE INFORMATION OF THE ENTERPRISE

Виробничі, технологічні, комерційні дані, які використовують підприємства, мають високу вартістю, а їх втрата або витік може привести до серйозних фінансових втрат. Тому однією з цілей для підприємств є створення надійної системи захисту інформації.

Система захисту інформації і - це комплекс організаційних і технічних заходів, спрямованих на забезпечення інформаційної безпеки підприємства. Головним об'єктом захисту є дані, які обробляються в автоматизованій системі управління і задіяні при виконанні виробничих-процесів [1].

Процес створення системи захисту інформації можна розділити на три етапи:

- формування політики підприємства в області інформаційної безпеки;
- вибір і впровадження технічних і програмних засобів захисту;
- розробка і проведення ряду організаційних заходів.

Фундаментом для створення системи захисту інформації є документ, в якому формулюються принципи і основні положення політики підприємства в області інформаційної безпеки. Політика інформаційної безпеки визначає стратегію і тактику побудови корпоративної системи захисту інформації. Політика безпеки компанії є основою для розробки цілого ряду документів безпеки: стандартів, інструкцій, процедур, практик, регламентів, посадових інструкцій та інше [2].

Загальний життєвий цикл політики інформаційної безпеки включає в себе ряд основних кроків:

- проведення попереднього дослідження стану інформаційної безпеки;
- розробку політики безпеки;
- впровадження розроблених політик безпеки.

Політика безпеки стосується практично кожного співробітника компанії. Досвід створення політик безпеки показує, що впровадження політики безпеки часто призводить до виникнення напруженості у взаєминах між співробітниками компанії. Якщо це можливо, про те що розробляють нову політику інформаційної безпеки компанії необхідно повідомити співробітників заздалегідь. До початку впровадження нової політики безпеки бажано надати співробітникам текст політики на один-два тижні для ознайомлення і внесення поправок і коментарів. Політика безпеки повинна бути реалістичною і здійсненною, бути короткою і зрозумілою, а також не приводити до істотного зниження загальної продуктивності виробничих підрозділів компанії. Політика безпеки повинна містити основні цілі та завдання організації режиму інформаційної безпеки, чітко містити опис області дії, а також вказувати на контактні особи та їх обов'язки [2].

Література

1. Скрипник Д.А. Забезпечення безпеки персональних даних. М., 2014.

2. Політики безпеки компанії при роботі в Internet [Електронний ресурс]. - Режим доступу http: / / citforum. ru / security / intemet / security_pol / . Дата доступу01.11.2017.