УДК 007:304

ПРОФЕСІЙНА ЕТИКА СПЕЦІАЛІСТА У ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В. М. Дудатьєва, асистент
В. В. Гаврилишен, студент
Вінницький національний технічний університет
andreysaf@mail.com

Сучасне підприємство функціонує у конкурентному середовищі, тому воно потребує комплексного захисту власних інформаційних ресурсів. У даному випадку комплексний захист складається з двох складових: захисту власних інформаційних ресурсів та захисту від інформаційного впливу ймовірних конкурентів. Тому важливою складовою забезпечення комплексної інформаційної безпеки підприємства є наявність на підприємстві спеціаліста з інформаційної безпеки, який виконує свої професійні обов'язки в межах етичних норм.

Спеціалісти з інформаційної безпеки стикаються з чималим числом етичних проблем, особливо, коли кількість інформаційних ресурсів підприємства дуже велика. Підґрунтям таких проблем можуть стати дуже багато факторів, зокрема неактуальність політики безпеки підприємства або повна її відсутність. В першому випадку спеціаліст з інформаційної безпеки (або інший працівник), отримавши доступ до конфіденційної інформації, сам може стати загрозою для інформаційної безпеки та нанести непоправні збитки. У другому випадку відсутність політики безпеки може спричинити репресивні дії щодо підприємства або навіть повне припинення його діяльності.

Саме тому професійна етика відіграє дуже значну роль в забезпеченні нормального функціонування підприємства. Спеціаліст з інформаційної безпеки в будь-яких умовах повинен залишатися професіоналом та діяти, дотримуючись кодексу професійної етики.

Дотримання положень професійної етики, передусім, підвищує довіру до фахівців і організацій в області інформаційної безпеки. Інший позитивний аспект полягає в створенні інституту рекомендацій фахівцям, що пройшли процедуру суспільної атестації і сертифікації на дотримання принципів професійної етики. Принципи професійної етики є базовими положеннями, якими керуються фахівці при виконанні робіт по організації і забезпеченню безпеки підприємства. Основні положення для фахівця з інформаційної безпеки: пріоритет інтересів підприємства; професійна честь; толерантність; сумлінність; відповідальність; недопустимість використання заборонених прийомів збору інформації; обмеження не рекомендованих методів роботи з джерелами інформації; збереження комерційної таємниці; професійна солідарність.

Фахівцеві з безпеки підприємства забороняється: виконувати будь-які дії, які можуть завдати збитків безпеці підприємства; записувати потай на диктофон і відеоносій без дозволу учасника переговорів; встановлювати підслуховуючі пристрої та інші пристрої спостереження за конкурентами; отримувати від конкурентів і передавати їм цінну конфіденційну інформацію; поширювати дезінформацію, використовувати методи "чорного" PR; використовувати промислові секрети; проникати в інформаційні мережі без отримання санкції на доступ до них від їх власників; перекручувати або видаляти інформацію в мережах, не створену ним; копіювати і

поширювати не створене ним програмне забезпечення; видавати себе за іншу особу, тощо.

Також має бути чітко визначена відповідальність за збереження комерційної таємниці партнера підприємства. Фахівець несе повну відповідальність за збереження комерційної таємниці партнера, що стала доступною йому при виконанні доручених робіт. Якщо час збереження комерційної таємниці не вказаний у договорі (контракті), то її зміст може бути розголошений тільки з відома партнера.

Крім того, фахівцеві з інформаційної безпеки забороняється: перевищувати свої повноваження пов'язані з можливістю його доступу до даних інших користувачів інформаційної системи; маніпулювати ким-небудь з співробітників, опираючись на можливість втручання в конфіденційність його особистих даних; переоцінювати вартість забезпечення безпеки підприємства, з метою власного збагачення; маніпулювати даними підприємства, щоб забезпечити собі додаткові матеріальні блага, покращити власне становище, нашкодити кому-небудь із персоналу через особисту неприязнь. Не рекомендується без необхідності слідкувати за діями користувачів інформаційної системи, що жодним чином не стосуються інформаційної безпеки.

Розглянуті принципи розробки кодексу професійної етики фахівця в області безпеки дозволяють досить чітко визначити межі професійної поведінки фахівця в області безпеки підприємства і механізми суспільної атестації і контролю. Розглянуті підходи мають бути адаптовані до конкретних підприємств з урахуванням умов їх функціонування та їх задач.