Гуманітарні аспекти підготовки фацівця з інформаційної безпеки

Дудатьєва В.М.[1], Літушко О.А.[2]
[1]Асистент кафедри захисту інформації, Вінницький національний технічний університет,
вул. Хмельницьке шосе, 95 м. Вінниця, Україна, andreysaf60@mail.ru
[2]Студент кафедри кафедри захисту інформації, Вінницький національний технічний університет,
вул. Хмельницьке шосе, 95 м. Вінниця, Україна, andreysaf60@mail.ru

***Анотація* — Розглянуто питання комплексної інформаційної безпеки підприємства. Обгруновано важливість гуманітарної складової фахової підготовки загалом і етичної культури зокрема фахівця з інформаційної безпеки підприємства. Зачначено, що сучасні підприємства, як об'єкти комплексного інформаційного захисту, працюють у конкурентному середовищі, яке характеризується проведенням спеціальних інформаційно-психологічних операцій з боку конкурентів. Запропоновано "ситуаційний план поведінки" або так звані правила поведінки фацівця з інформаційної безпеки, виконання яких зменшує ризики для підприємства.**

Ключові слова: *комплексна інформаційна безпека підприємства, етичні аспекти підготовки фахівця з інформаційної безпеки, правила поведінки фахівця з інформаційної безпеки .*

Humanitarian aspects of professional training in information security

Dudatieva V.M.[1], Litushko O.A.[2]
[1]**Asist., Department *of information security, Vinnytsia National Technical University***
st. Khmelnytsky Highway, 95 m. Vinnitsa, Ukraine, andreysaf60@mail.ru
[2]***Student the chair of the department of information security Vinnitsa National Technical University***
st. Khmelnytsky Highway, 95 m. Vinnitsa, Ukraine, andreysaf60@mail.ru

***Abstract* — The problems of integrated information security. Importance of the humanitarian component of training in general and ethical culture in particular specialist in information security. Noted that modern enterprises, as objects of complex information security, operating in a competitive environment, characterized by carrying out specific information and psychological operations from competitors. Suggested "situational plan of conduct" or so-called rules of conduct for information security professionals, the implementation of which reduces the risks for the enterprise.**

Keywords: ***comprehensive enterprise information security, ethical aspects of training specialist information security professional rules of conduct for information security.***

I. Вступ

Одним з ресурсів сучасного підприємства, що обов'язково підпадає під комплексний захист, є його персонал. З точки зору комплексної інформаційної безпеки персонал підприємства є одним з потенційних джерел витоку конфіденційної інформації. Питома вага факторів, які пов'язані з людиною у забезпеченні інформаційної безпеки доволі великий, в окремих випадках він досягає 80%, до того ж з часом критерії етичної поведінки можуть змінюватись [1]. Тому відповідний відбір, підготовка і навчання персоналу є однією з ключових комплексних задач, рішення якої зменшить ризики підприємства як об'єкта захисту.

Сучасне підприємство функціонує у конкурентному середовищі, яке характеризується можливістю проведення спеціальних інформаційних операцій з боку конкурентів. У даному випадку комплексний захист формується 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. Складність задачі виконання своїх службових обов'язків ускладнюється тим, що існує достатньо велика кількість середовищ, механізмів і засобів для передавання інформації. Очевидно, що є специфічні особливості безпекової приватності і етики поведінки у середовищі Internet, реклами на телебаченні, друкованих ЗМІ, під час особистих зустрічей, проведення приватних перемовин тощо Принцип будь-якої професійної етики – "Ні нашкодити"!. Ствердження основ професійної етики сприяють розвитку підприємства і суспільства в цілому, оскільки дозволяє вирішити питання щодо відповідальності і надійності людини. Проведений аналіз показує, що у західних країнах, зокрема США, вже в середині 1980-х рр. сформувалася так звана "комп'ютерна етика" як навчальна дисципліна, яка викладалася при підготовці відповідних фахівців. У навчальному процесі використовувалисьі підходи:

1) введення окремої дисципліни «безпекової» етики;
2) включення окремих модулей питань професійної етики у відповідні дисципліни.

Кожний із можливих підходів має свої переваги і недоліки, які пов'язані як із кваліфікацією викладачів, так і з сприйняттям інформації студентами.

II. ПРАВИЛА ПОВЕДІНКИ ФАХІВЦЯ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Дотримання положень професійної етики, передусім, підвищує довіру до фахівців і організацій в області інформаційної безпеки. Інший аспект позитивного полягає в створенні базових рекомендацій фахівцям, що пройшли процедуру навчання з дотримання принципів професійної етики. Принципи професійної етики є базовими положеннями, якими керуються фахівці при виконанні робіт по організації і забезпеченню комплексної інформаційної безпеки підприємства. Основні положення для фахівця з інформаційної безпеки:

1) пріоритет інтересів підприємства;
2) професійна честь;
3) сумлінність;
4) відповідальність;
5) заборона нерекомендованих методів роботи з джерелами інформації;
6) збереження комерційної таємниці;
7) професійна солідарність тощо.

Відповідно до вищенаведених базових принципів фахівцеві з безпеки підприємства забороняється виконувати будь-які дії, які можуть завдати збитків безпеці підприємства. Цими діями можуть бути такі [2-4]:

1) записувати потай на диктофон і відеоносій без дозволу учасника переговорів;
2) отримувати від конкурентів і передавати їм цінну конфіденційну інформацію;
3) поширювати дезінформацію;
4) використовувати методи "чорного" PR;
5) використовувати промислові секрети;
6) проникати в інформаційні мережі без отримання санкції на доступ до них від їх власників;
7) перекручувати або видаляти інформацію в мережах;
8) копіювати і поширювати програмне забезпечення;
9) видавати себе за іншу особу тощо.

Такі правила виникають через існуючі труднощі або відсутність ефективної нормативно-правової бази, посадових інструкціях для всіх складних випадків, що можуть виникнути під час діяльності фахівців. Ці правила професійної поведінки є загальними для всього підприємства або конкретними для співробітників та фокусують увагу на розумінні службового обов'язка і власної відповідальності за свої дії у будь-якій ситуації. Існують міжнародні професійні організації, які стимулюють законотворчу діяльність і створення різноманітних кодексів і хартій, що відносятьс та відповідних професіоналів. Найбільш відомі з них такі:

1) International Confederation of FreeTrade Unions (ICFTU);
2) communications International (PTTI);
3) international Union of Food, Agricultural, Hotel, Restaurant,Catering, Tobacco and Allied Workers' Associations (IUF)
4) international Federation of Commercial, Clerical, Professional and Technical Employees (FIET);
5) media and Entertainment International (MEI).

Окремим блоком є вимоги до поведінки фахівця з інформаційної безпеки за межами підприємства. Наприклад, неетичною буде вважатися згода на проведення приватної зустрічі, під час якої обговорюються питання, що відносяться до підприємства, особливостей його продукції і технологій, обговорення слабких і сильних рис характеру керівника підприємства або провідних фахівців з метою складання так званого портрету людини-фацівця і подальшого його використання у корисних цілях. 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.

III. ВИСНОВКИ

Запропоновані правила професійної етики фахівця в області комплексної інформаційної безпеки підприємства дозволяють досить чітко визначити межі професійної поведінки фахівця і механізми професійної атестації і контролю його діяльності. Розглянуті правила мають бути адаптовані до конкретних підприємств з урахуванням умов їх функціонування та їх задач.

[1] Ю.Ю. Петрунин, В.К. Борисов, Этика бизнеса.– Издательство М.: Дело, 2000 г., - 177 с.
[2] Nissenbaum H. Should I Copy My Neighbor's Software? // Computer Ethics and Social Values / Ed. by D.Johnson and H.Nissenbaum. Prentice Hall, 1995.
[3] Johnson D.G. Computer Ethics. Prentice Hall, 3rd Edition, 2001.
[4] Reynolds G. Ethics in Information Technology. Thomson Course Technology, Boston, 2003.