УДК 004.056.53; 378
І. Фартушок
(Дрогобицький державний педагогічний університет імені Івана Франка)

ІНФОРМАЦІЙНА БЕЗПЕКА: ВИРОБНИЧІ РИЗИКИ ТА ОСВІТНІ ЗАВДАННЯ

Інформація, яка завжди мала реальну ціну, сьогодні стає дедалі дорожчою. А витік конфіденційних даних завдає не менших збитків, ніж, скажімо, крадіжка чи пожежа. Так, за статистикою Лабораторії Касперського, кожна друга компанія втрачає дані під час вірусних інцидентів. А за результатами досліджень компаній SearchInform [1] та PGP Innovative Consulting [2], основним масивом інформації, що зазнає витоку, є персональні дані клієнтів. Їхня частка, за різними даними, становить від 40 до 90%, що пояснюється високою зацікавленістю з боку шахраїв. Найпопулярнішими персональними даними є інформація про користувачів (e-mail, вік, особисті уподобання) та дані їхніх банківських карт.

Закон України «Про персональні дані» був прийнятий 1 червня 2010 року й набув чинності 1 січня 2011-го. Проте, щоб одержати позитивні результати, потрібні не лише закони, але й люди, які цих законів дотримуються, розуміють, для чого потрібні засоби захисту від витоку інформації, й уміють фахово з ними працювати.

Відповідно до статистики Лабораторії Касперського, 36% вищого керівництва компаній не вважає кіберзагрози серйозним ризиком для бізнесу. Більше того, чверть ІТ-фахівців ніколи не чули про такі найвідоміші кіберзагрози, як Zeu, SpyEye, Stuxnet, Operation Aurora, Duqu, Koobface чи Heartbleed. До топ-факторів, які заважають ефективній боротьбі із кіберзагрозами також належать недостатнє розуміння питань ІТ-безпеки керівництвом структурних підрозділів компанії, жорсткі бюджетні обмеження та брак фахівців з інформаційної безпеки.

Проте не лише фахівці з ІТ-безпеки, а й звичайні офісні чи банківські працівники повинні володіти основами знань з інформаційної безпеки. Основні їхні професійні компетенції мають полягати у вміннях:

1) адекватно оцінювати ІТ-ризики, визначати потенційні загрози, вразливості та їх можливі наслідки;

2) визначати пріоритети не лише у своїй безпосередній професійній діяльності, але й у галузі інформаційної безпеки та захисту персональних даних клієнтів;

3) налагоджувати ефективне співробітництво між відділами та структурними підрозділами компанії щодо попередження ІТ-загроз та підвищення кібербезпеки;

4) підвищувати особисті ІТ-знання задля зменшення ризиків і кіберзагроз;

5) удосконалювати власні навички реагування на цільові кібератаки та події. в ІТ-просторі, які мають ознаки кібершахрайства.

Такі професійні компетенції слід формувати ще під час навчання у вищому навчальному закладі. Це не потребує введення додаткової навчальної дисципліни чи збільшення кількості годин. Достатньо у нормативній навчальній дисципліні «Безпека життєдіяльності» передбачити вивчення розділу «Інформаційна безпека».

Список використаних джерел

1. Идов Р. Как защитить свои персональные данные от кражи / Роман Идов. – 16 декабря 2013. [Режим доступу: http://delo.ua/tech/kak-zaschitit-svoi-personalnye-dannye-ot-krazhi-222183/]
2. Почему в Украине игнорируют IT-безопасность – 05 февраля 2013. [Режим доступу: http://delo.ua/tech/pochemu-v-ukraine-ignorirujut-it-bezopasnost-196499/]