УДК 342.9 (043.2)

Юринець Ю. Л., д.ю.н., доцент,
Вова В. М., студентка,
Юридичний факультет,
Національний авіаційний університет, м. Київ, Україна

ЛЮДСЬКИЙ ФАКТОР ТА ЙОГО ВПЛИВ НА ОРГАНІЗАЦІЮ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сучасний етап розвитку суспільства неможливо розглядати відокремлено від технічного прогресу і зокрема від інформаційних систем. Інформаційні системи використовуються практично в усіх сферах життя суспільства. Вони надають зручне середовище для роботи, навчання, розміщення та обміну інформації; вони дозволяють спілкуватися, забезпечують зручні сервіси для банківської, комерційної діяльності тощо.

Кожен нещасний випадок, порушення охорони праці чи інформаційні помилки мають одну спільну причину – людський фактор. Основна, ключова роль в безпеці належить не техніці чи технології, а людині. Сам людський фактор є непередбачуваним. Саме йому належить адаптація до тієї чи іншої небезпеки в залежності від середовища та умов, де він перебуває. Тобто відбувається поступова адаптація не лише до небезпеки, але і до порушень.

Людський фактор у загальному визначається як сукупність основних соціальних якостей людини, які історично склалися в суспільстві. До них відносяться ціннісні орієнтири, моральні принципи, норми поведінки, життєві плани, рівень знань та інформованості, характер трудових та соціальних навичок, установки та уявлення про особисто значимі елементи соціального життя – соціальну справедливість, про права і свободи людини, про громадянський обов'язок [1].

На практиці цей фактор розглядається при прийнятті людиною неправильного (алогічного) рішення в конкретній ситуації або як сукупність певних якостей особистості. Єдиного визначення поняття «людського фактора» немає, у багатьох галузях знань та сферах професійної діяльності є своя інтерпретація [2].

Найбільш вразливою ланкою в системі інформаційної безпеки будь-якого підприємства, насамперед, є люди, їх слабкості. Яскравим прикладом є Німеччина часів Другої світової війни, коли оператори машини Enigma, для полегшення своєї роботи, використовували стандартні скорочення, що дало можливість дешифровки закодованої інформації. Тобто шифрувальники були недостатньо вмотивовані виконувати трудомістку працю з найвищим рівнем захисту і це полегшення їх роботи (виникла вразливість) відкрило шлях для створення

загрози витоку інформації, що і сталося в реальності [3].

Людський фактор має значний вплив на інформаційну безпеку, зокрема на загрози інформаційній безпеці. Вчені виділяють багато загроз інформаційній безпеці, проте основну увагу слід приділити так званій “загрозі конфіденційності”. Загроза порушення конфіденційності полягає в тому, що інформація стає відомою тому, хто не володіє повноваженнями доступу до неї. Вона має місце, коли отримано доступ до деякої інформації обмеженого доступу, що зберігається в комп’ютерній системі або передається від однієї системи до іншої. У зв’язку з загрозою порушення конфіденційності, використовується термін «витік». Подібні загрози можуть виникати внаслідок «людського фактора» (наприклад, випадкове делегування тому або іншому користувачеві привілеїв іншого користувача), збоїв роботи програмних та апаратних засобів. До інформації обмеженого доступу належить державна таємниця (комерційна таємниця, персональні дані, професійні види таємниці: лікарська, адвокатська, банківська, службова, нотаріальна таємниця страхування, слідства й судочинства, листування, телефонних переговорів, поштових відправлень, телеграфних або інших повідомлень (таємниця), відомості про сутність винаходу, корисної моделі або промислового зразка до офіційної публікації (ноу-хау) та ін.) [4].

Підсумовуючи усе вищесказане можна зробити висновок, що одне з найважливіших місць у безпеці інформаційних систем посідає людський фактор. І нехтування ним може становити загрозу не лише окремій особистості а й цілим організаціям. Тому слід проводити регулярну роботу з користувачами інформаційних систем як у навчальних закладах так і в організаціях.

Література

1. Загуменна Н. В. Людський фактор та специфіка його активізації у соціально-філософських дослідженнях. К.: Альманах. Філософські проблеми гуманітарних наук, 2010. № 16. С. 68-72.

2. Коцюк Ю. А. Роль людського чинника у питаннях захисту інформаційних систем. URL: https://psj.oa.edu.ua/articles/2012/n20/%D0%9A%D0%BE%D1%86%D1 %8E%D0%BA.pdf (date of access: 20.04.2019).

3. Нікіфорова Л. О. Використання мотиваційних важелів для підвищення інформаційної безпеки підприємства. URL: https://webcache. googleusercontent. com/search?q=cache:USluz6A-Mm8J:https://conferences.vntu.edu.ua /index.php/all-fm/all-fm-017/paper/download/2343/2735+&cd=2&hl=uk&ct=clnk&gl=ua (date of access: 20.04.2019).

4. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. К.: КНТ, 2006. 280 с. (Серія: Національна і міжнародна безпека).