УДК 004.6

ВПЛИВ ЛЮДСЬКОГО ФАКТОРУ НА СИСТЕМИ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Заник О., Ткачук Р.
Львівський державний університет безпеки життєдіяльнсті, м. Львів

В роботі зазначений вплив людського фактору на корпоративну безпеку. Виділені основні проблеми та ризики у збереженні інформаційної безпеки, які модуть виникати при наявності негативної мотивації, непрофесіоналізму, свідомих чи несвідомих помилок.

***Ключові слова**: людський фактор, персонал, корпоративна мережа, інформаційна безпека, захист.*

The paper mentions the impact of the human factor on corporate security. The main problems and risks in maintaining information security, which may arise in the presence of negative motivation, unprofessionalism, conscious or unconscious mistakes.

***Key words:** human factor, personnel, corporate network, information security, protection.*

За характером організації захист інформації є багатокомпонентний та має складну ієрархічну структуру. У рамках теорії організації інформаційної безпеки чітко визначено постулат, що організація інформаційної безпеки повинна враховувати не тільки складність техніко-технологічних складових системи, а й людський фактор. І відповідно, до цього вже на етапі проектування систем технічного та програмного захисту, необхідно враховувати не тільки технічний аспект а й кількісні та якісні індивідуальні характерологічні особливості персоналу, який буде брати участь у системі захисту інформації [1].

Наявність людського фактора має першорядне значення в теорії інформаційної безпеки. Головна, ключова роль у безпеці належить не машинам чи технологіям, а людині. Людський фактор, як такий залежить від багатьох, як внутрішніх так і зовнішніх, змінних а іноді може проявлятися у «ніби» нелогічних діях. Хоча при детальнішому аналізі прослідковується певна закономірність та послідовність подій.

Людський фактор завжди був і є одним із найважливіших ризиків будь-якої сфери діяльності, оскільки більшість інцидентів відбувається з вини працівників. Навмисний відтік часто важко відрізнити від ненавмисного, але це не завжди необхідно, оскільки наслідки для підприємства в будь-якому з цих варіантів можуть бути катастрофічними [2].

Люди, які контролюють і використовують корпоративну мережу, є найбільш вразливою складовою цієї системи. Захист усієї системи часто перебуває в руках системного адміністратора. Якщо адміністратор не має достатнього рівня кваліфікації або вирішить стати на шлях злочину, то така система знаходиться в серйозній небезпеці [3].

Звичайних користувачів корпоративних мереж, операторів та інший персонал також можуть підкупити або змусити вчинити протиправні дії (видати паролі, логіни, іншу конфіденційну інформацію), що створює небезпечне середовище для захисту системи.

Окремо можна виокремити так званих «ображених» працівників, які досить часто, виношують плани помсти, а іноді при певному збігу обставин її реалізують. І в результаті така категорія працівників може завдати значної шкоди, оскільки вони володіють службовою інформацією про організацію та мають певні навики [4].

Основним захистом від внутрішніх ворогів є підтримка трудової дисципліни в колективі та встановлення особистого контакту між керівником та його підлеглими для подальшого вирішення проблем, а саме особистих конфліктів.

Категорія працівників, звільнених або понижених у посаді, особливо небезпечна. В комп'ютерній інформаційній діяльності ці працівники повинні перебувати під безпосереднім наглядом керівництва, особливо якщо персонал має право доступу до активного цінного інформаційного ресурсу. А у разі звільнення слід подбати, щоб особа більше не мала доступу до корпоративної інформації.

Тобто належне адміністрування є основою безпеки організації. В інформаційній діяльності це управління відоме як політика інформаційної безпеки.

Найпоширенішими та найнебезпечнішими загрозами доступності є ненавмисні помилки звичайних користувачів, операторів, системних адміністраторів та інших, які користуються інформаційними системами чи їх обслуговують. Такі помилки зазвичай стають загрозами (неправильно введені дані або помилка в програмі, що призвела до збоїв системи), іноді вони створюють вразливості, якими можуть скористатися зловмисники. Виходячи з цього, найрадикальнішим способом боротьби з ненавмисними помилками є максимальна автоматизація та суворий контроль [1, 2].

Отже, ми можемо зробити висновок, що для зменшення навмисних та ненавмисних загроз ключовим елементом є належне управління людським фактором. В якому важливу роль відіграє політика безпеки, а також правильний підбір персоналу, логічний алгоритм доступу до інформаційних ресурсів, якісне обладнання та програмне забезпечення. А для підтримання порядку повинна бути сформована корпоративна етика, яка регулюватиме правила безпечної поведінки як в самій організації так і за її межами.

Інформаційні джерела

1. Ромака В.А. Дудикевич В.Б., Гарасим Ю.Р. Системи менеджменту інформаціної безпеки: НУ«ЛП» 2012, 256 с.

2. http://uk.wikipedia.org/wiki/Політика_інформаційної_безпеки

3. https://uk.wikipedia.org/wiki/Система_управління_інформаційною_безпекою

4. http://www.info-library.com.ua/books-text-11433.html Філософські проблеми гуманітарних наук (Збірка наукових праць)