УДК 65.012.8

ВНУТРІШНІ ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ЗАХОДИ ПО ЇХ МІНІМІЗАЦІЇ

Будник Марина Миколаївна,Тимофєєв Дмитро Сергійович
Державний ВНЗ «Національний гірничий університет», www.nmu.org.ua, Marina-Dnepr17@mail.ru

В статті розглянуті внутрішні загрози інформаційної безпеки. Проведений аналіз їх утворення, класифікації, запропоновано заходи щодо мінімізації загроз.

Ключові слова – інформаційна безпека, внутрішні загрози інформації, зовнішні загрози інформації, класифікація внутрішніх порушників, нейтралізація, мінімізація внутрішніх загроз .

ВСТУП

Створення ефективної системи управління інформаційною безпекою є неможливим без чіткого визначення загроз інформації, що охороняється. Під загрозами інформації прийнято розуміти потенційні або реально можливі дії стосовно інформаційних ресурсів, що призводять до неправомірного володіння інформацією.[1]

УТВОРЕННЯ ТА КЛАСИФІКАЦІ ВНУТРІШНІХ ЗАГРОЗ

За джерелом походження загрози інформаційній безпеці можуть поділятися на внутрішні та зовнішні.

Проаналізувавши можливості утворення внутрішніх та зовнішніх загроз, можна перерахувати їх в порядку зменшення імовірності реалізації:

- внутрішні загроз;
- зовнішні загрози;
- загрози, які створюють випадкові особи.

До внутрішніх загроз відносять дії чи бездіяльність (навмисні чи не навмисні) співробітників, що протидіють інтересам діяльності підприємства, наслідком яких може бути нанесення економічних збитків компанії, втрата інформаційних ресурсів, підрив ділового іміджу компанії, виникнення проблем у відносинах з реальними чи потенційними партнерами тощо. [3]

Враховуючи, що значна частина внутрішніх загроз реалізується за участі або сприяння персоналу, можна вважати, що основним джерелом таких загроз є працівники даної організації.

Виходячи з цього внутрішні загрози можуть утворюватися внаслідок:

- Непрофесійних дій працівників;
- Низького стану виховної та профілактичної роботи в організації;
- Недосконалої системи заробітної плати та стимулювання праці персоналу;
- Порушень правил кадрової роботи, невідповідності кадрової політики умовам роботи в організації;
- Психологічних та комунікаційних особливостей працівників;
- Відсутності нормативної бази організації, яка б установлювала режими їх діяльності та правила поведінки персоналу;
- Низького стану трудової та виробничої дисципліни, слабкої вимогливості керівного складу;

Існує декілька підходів класифікації внутрішніх порушників. На мій погляд, одною з найкращих класифікацій можна назвати екосистему внутрішніх порушників компанії InfoWatch таблиця 1 [3].Фахівці компанії фокусують увагу виключно на захисті даних від витоку, модифікації та знищення, і тому їх погляди відрізняються великою глибиною аналізу.

Таблиця 1. Екосистема внутрішніх порушників

Тип	Навмисність	Користь	Постановка задачі	Дії при неможливості
Халатний	Ні	Ні	Ні	Повідомлення
Маніпульований	Ні	Ні	Ні	Повідомлення
Скривджений	Так	Ні	Сам	Відмова
Нелояльний	Так	Ні	Сам	Імітація
Підробляючий	Так	Так	Сам/ Ззовні	Відмова/ Імітація/ Злом
Впроваджений	Так	Так	Ззовні	Злом

ЗАХОДИ ЩОДО МІНІМІЗАЦІЇ ВНУТРІШНІХ ЗАГРОЗ

Отже, для нейтралізації та мінімізації внутрішніх загроз потрібно вжити наступних заходів:

- Організаційні заходи з захисту інформації(комплекс адміністративних та обмежувальних заходів);
- Контрольно-правові заходи (контроль за виконанням персоналом вимог відповідних інструкцій, розпоряджень, наказів, нормативних документів);
- Профілактичні заходи (спрямовані на формування у персоналу мотивів поведінки, які спонукають їх до безумовного виконання у повному обсязі вимог режиму, правил проведення робіт та ін., а також на формування відповідного морально-етичного стану в колективі);
- Інженерно-технічні заходи;
- Робота з кадрами (підбір персоналу, інструктажі, навчання персоналу з питань забезпечення захисту інформації, виховання пильності співробітників, підвищення їхньої кваліфікації);
- Психологічні заходи (встановлення відео спостереження, оприлюднення інцидентів із спробою винесення забороненої інформації за межі організації).

ВИСНОВОК

Внутрішні загрози безпеки є постійними і не залежать від ролі, місця, значення організації або наявності зовнішніх загроз.

Тому креівництву організації слід вкрай серйозно підходити до проблеми захисту інформації від внутрішніх загроз, адже для цього існують всі необхідні засоби як технічні так і організаційні.

ПЕРЕЛІК ВИКОРАСТАНИХ ДЖЕРЕЛ

1. Ткачук Т.,Інформація з обмеженим доступом на підприємстві: проблеми безпеки та захисту, Право України № 3, 2011. – 366с.

2. Об'єднання професіоналів конкурентної розвідки Росії (Електрон. ресурс) / Спосіб доступу : URL : http://ww.rscip.ru.

3. Скиба В., Курбатов В. Керівництво по захисту від внутрішніх загроз інформаційної безпеки М.: видавництво Пітер, 2008. – 320с.

4. Скляренко А. Загрози конфіденційності інформації, пов'язані з персоналом,Бізнес и безпека №1,2010 .– 92с.