УДК 331.108

Іванчук Т. С.
курсант,
Львівський державний університет безпеки життєдіяльності
Кухарська Н. П.
кандидат фізико-математичних наук, доцент
Львівський державний університет безпеки життєдіяльності

АНАЛІЗ ЗАГРОЗ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА З БОКУ ЙОГО ПЕРСОНАЛУ

В сучасних умовах господарювання, коли ситуація в країні в цілому та в економіці зокрема характеризується значною нестабільністю, підприємства піддаються постійним впливам різноманітних загроз. За статистикою зовнішні і внутрішні загрози економічній безпеці підприємства співвідносяться як 20 до 80. Тобто 4/5 усіх проблем породжуються внутрішнім середовищем компанії.

Розглянемо внутрішні загрози підприємства, джерелом яких є персонал.

1. Розкрадання майна підприємства (корпоративне шахрайство). Може проявлятися в трьох варіантах: дрібні разові розкрадання; постійні розкрадання у невеликих та середніх розмірах, які розглядаються крадієм як своєрідна “надбавка до зарплати”; розкрадання в особливо великих розмірах – організація “бізнесу в бізнесі”.

2. Використання ресурсів підприємства (матеріальних, фінансових, технічних, транспортних та ін.) в особистих цілях. Найчастіше це явище має місце на підприємствах, де погано налагоджений контроль з боку керівників лінійних підрозділів за використанням їхніми підлеглими робочого часу.

3. Умисне псування і нищення майна підприємства (диверсія). Як показали дослідження CERT (Computer Emergency Response Team) серед корпоративних диверсантів є велика частка фахівців, які тим чи іншим чином пов'язані з інформаційними технологіями (IT). На технічно підкованих

диверсантів припадає 87 % інцидентів, а саме: до 38 % таких інцидентів причетні системні адміністратори, до 21 % – програмісти, до 14 % – інженери і ще до 14 % – фахівці з ІТ. Аналітики також підрахували, що у 31 % випадку про плани та (або) діяльність диверсанта знали інші (колеги – у 64 % випадків, друзі – у 21 %, члени сім'ї – у 14 %). У 14 % диверсантів були спільники [1].

4. Отримання заробітної плати за невиконану роботу (саботаж). У класичному визначенні саботаж – це свідоме невиконання або недбале виконання своїх обов'язків, прихована протидія здійсненню чого-небудь.

За цілями саботажу інциденти можуть бути класифіковані таким чином:

- Зниження репутації організації, наприклад, шляхом компрометації якості послуг, що надаються організацією, або інші способи нанесення збитків відносинам організації з клієнтами з метою заволодіння клієнтською базою організації.
- Саботаж діяльності контрагентів організації.
- Зрив, перешкоджання, маніпулювання і піддавання іншим впливам управління, ведення, результату деякої бізнес-діяльності, допоміжної діяльності або окремого проекту організації. Наприклад, для отримання конкурентами організації чи іншими суб'єктами ринкових відносин певних переваг, зловмисником створюються умови, що перешкоджають забезпеченню організацією її законних прав.
- Саботаж здійснюваних підприємством заходів безпеки і створення вразливостей з метою зниження захищеності інформаційних активів організації перед зовнішніми і внутрішніми загрозами.
- Приховування доказів, створення хибних версій та інших перешкод для розслідування протиправної діяльності на підприємстві.
- Маніпулювання ринками цінних паперів шляхом створення “негативу” через розповсюдження інформації про надзвичайні події в організації.
- Помста організації або окремим її працівникам.
- Екстремістські, терористичні, політичні та інші схожі їм цілі.

За відомостями аналітиків, 92 % випадкам саботажу передує неприємний інцидент на роботі або ціла серія таких інцидентів. Так, 47 % випадків пов’язані із звільненням з роботи, 20 % спровоковані суперечкою з нинішніми або колишніми колегами, причиною 13 % випадків саботажу є пониження в посаді або переведення на іншу роботу [1].

5. Шантаж компетентністю (“я – незамінний працівник”). Суть цього явища полягає у вимозі працівником деяких пільг і преференцій за його реальні або надумані унікальні виробничі знання та вміння.

6. Шантаж повноваженнями (концентрація в одних руках повноважень за кількома посадами) призводить до створення сприятливих умов для крадіжок. Особливо це небезпечно, коли компетенції однієї людини в рамках одного бізнес-процесу акумулюють в собі компетенції кількох посадових осіб.

7. Торгівля секретами (продаж “на сторону” комерційних секретів підприємства). Для попередження цього явища на підприємстві слід запровадити режим комерційної таємниці. Без встановлення такого режиму будь-які розписки, зобов'язання та додатки до трудової угоди з працівником стосовно збереження в секреті комерційної інформації підприємства будуть безпідставними.

8. Порушення дисципліни. Загальний стан дисципліни є показником готовності і можливостей колективу вирішувати виробничі завдання. Високий рівень дисципліни досягається шляхом дотримання розумного співвідношення між заходами заохочення та покарання, заснованому на понятті “справедливість”.

9. Створення в колективі нестерпного морально-психологічного клімату (“мобінг”). Буває, що у колективі виникає ситуація, коли “виживають” неугодного. Причин тому може бути багато і, як правило, цим питанням займається служба управління персоналом, HR-менеджери та інші профільні фахівці. З точки зору безпеки, це явище має бути своєчасно виявлене та викоренене, так як працівник, що піддається “виживанню” з боку колег, стає потенційним “диверсантом”, “саботажником” і “продавцем секретів”.

10. Схильність працівників до різних адитивних залежностей. Адитивна поведінка характеризується прагненням відійти від реальності за допомогою зміни свого психічного стану. Виокремлюють хімічні та нехімічні форми адикцій. До нехімічних відносять: азартні ігри (гемблінг), сексуальну адикцію, любовну адикцію, адикцію відносин, трудову адикцію, адикцію до витрати грошей, ургентні адикції, Інтернет та комп'ютерну адикцію. Проміжне місце між хімічними та нехімічними адикціями займає адикція від їжі (булімія, анорексія). При цій формі адикції безпосередньо задіяні біохімічні механізми. До хімічних форм залежності відносять алкогольну залежність і наркотичну. Є очевидним, що працівники схильні до будь-якого виду залежності – "слабка ланка" підприємства. Боротися з залежностями – не є завданням системи безпеки. Залежності необхідно виявляти і враховувати в повсякденній роботі. Якщо ж залежність співробітника завдає шкоди підприємству, то вихід тільки один – звільнення.

Вищі перелічені загрози, джерелом яких є персонал, здатні порушити стійкість, розвиток і навіть привести до зупинки діяльності організації. У зв'язку з цим, основним завданням діяльності служби управління персоналом має бути забезпечення своєчасності виявлення, аналізу, запобігання і прогнозування потенційних загроз економічній безпеці організації з боку її працівників.

Література:

1. Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors [Electronic resource]. – Access mode : https://resources.sei.cmu.edu/asset_files/SpecialReport/2005_003_001_51946.pdf