МАТЕМАТИЧНІ МЕТОДИ, МОДЕЛІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ

Савчик А.Г.
студентка,
Науковий керівник: **Кириченко В.В.**
кандидат фізико-математичних наук, доцент,
Донецький державний університет управління

ЗАХИСТ ІНФОРМАЦІЇ У КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Інформатизація суспільства змінила відношення до інформації. Зараз інформація стоїть на одному рівні з матеріальними, фінансовими ресурсами, а також персоналом. Конкурентні позиції організації залежать від того наскільки якісною, достовірною, повною та актуальною інформацією організація володіє. Однак в сучасних умовах господарювання мало просто володіти інформацією, потрібно також мати ефективні засоби її захисту. Саме від ступеня захисту конфіденційної інформації залежить конкурентоспроможність організації. Адже наявність такої інформації дає змогу організації першій вийти на нові ринки і завоювати великі його сегменти.

Метою дослідження є визначення загроз захисту інформації, а також засобів захисту цієї інформації у корпоративних інформаційних системах.

Для задоволення життєво важливих інтересів будь-якої організації необхідно забезпечити інформаційну безпеку. Створення та функціонування розвиненого та захищеного інформаційного середовища є важливою умовою розвитку організації в сучасних економічних умовах.

Серед основних ризиків бізнесу ризик втрати конфіденційної інформації посідає друге місце. І це є свідченням того, що на сьогоднішній день система захисту інформації на підприємствах є недосконалою. Через цю недосконаліть підприємства можуть зазнати значних збитків в процесі здійснення своєї діяльності.

Актуальність проблеми забезпечення захисту інформації у корпоративних інформаційних системах (КІС) визначається наступними чинниками [3, с. 1]:

1. Позитивною динамікою зростання кількості ЕОМ, які використовуються у роботі.

2. Багатоманітністю напрямків використання ЕОМ.

3. Великою кількістю інформації, яка обробляється на ЕОМ.

4. Вдосконаленням роботи користувача з різними ресурсами ЕОМ.

5. Ускладненням обчислюваних процедур на ЕОМ.

В залежності від структури КІС, програмних та технічних засобів, які використовуються в процесі обробки інформації, можна виділити наступні загрози інформаційної безпеки [2, с. 310]:

1. Загрози пов’язані з перехватом даних у каналах передачі інформації.

2. Загрози пов’язані з неправомірним доступом до інформації КІС.

3. Загрози пов’язані з неправомірним розповсюдженням даних мережевими каналами.

4. Загрози пов’язані з втратою інформації через недосконаліть засобів її обробки та збереження.

В даний час проводиться багато досліджень, пов’язаних з інформаційною безпекою підприємств. Одним з таких досліджень було дослідження наукового інституту Computer Security Institute (Сан-Франциско, штат Каліфорнія, США), згідно якого порушення захисту інформації на підприємствах, що використовують КІС, відбувається з таких причин (рис. 1) [1, с. 123]:

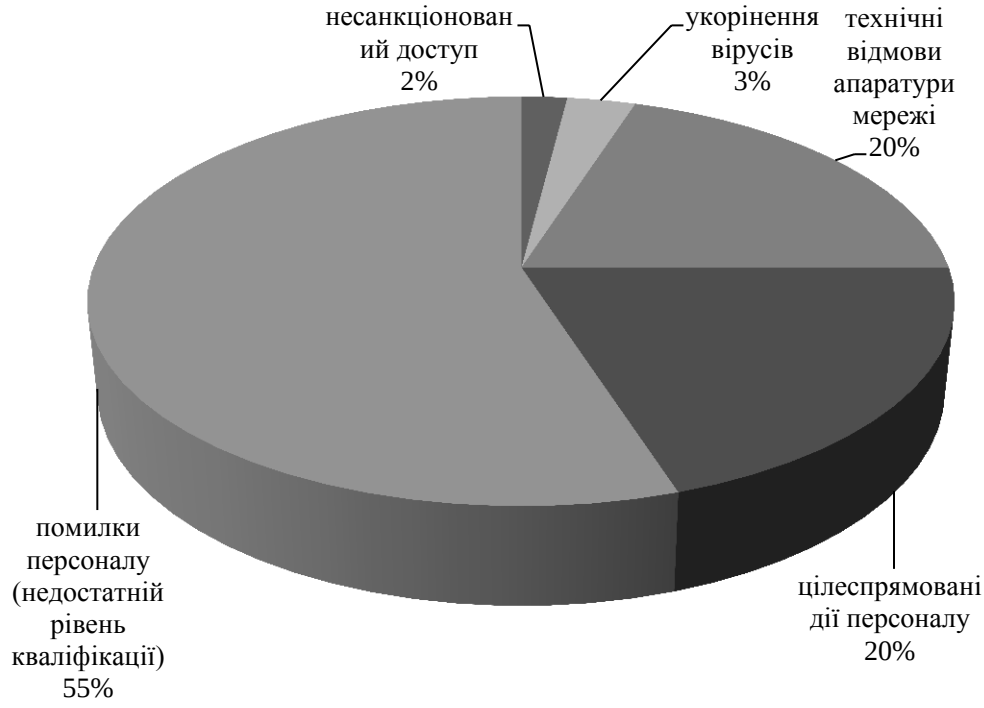

Рис. 1. Причини порушення захисту інформації у КІС

Отже, найвагомішою загрозою для інформації в КІС є цілеспрямовані або випадкові дії персоналу, які становлять 75 % від загальної суми усіх загроз. Тобто можна сказати, що захищеність інформації у КІС більшою мірою залежить від людського фактору.

Реалізація тієї або іншої загрози захисту інформації може переслідувати наступні цілі [3, с. 2]:

1. Порушення конфіденційності інформації. Дуже часто інформація, яка обертається у КІС є дуже цінною для підприємства. Її викриття сторонніми особами може нанести дуже значних збитків підприємству, аж до банкрутства.

2. Порушення цілісності інформації. Втрата цілісності інформації (повна або часткова компрометація, дезінформація) – загроза близька до її розкриття. Інформація може знецінитись шляхом її викривлення. Такі дії можуть завдати ще більших збитків, ніж порушення конфіденційності.

3. Порушення (часткове або повне) працездатності корпоративної системи (порушення доступності). Вивід з ладу або некоректна зміна режимів роботи компонентів КІС, їх модифікація або підміна можуть привести до отримання невірних результатів, відмови КІС від потоку інформації або відмова при обслуговуванні.

Забезпечення надійності роботи КІС, а також розробка ефективних засобів захисту інформації є одним з важливіших напрямків розвитку інформаційних технологій. Це обумовлюється

тим, що втрата конфіденційної інформації здатна нанести значних фінансових збитків для суб'єктів господарювання, а іноді навіть і призвести до банкрутства.

Система захисту інформації у КІС повинна спиратись на засадах комплексного підходу, який довів свою ефективність і надійність. На основі цього підходу доцільно застосовувати такі методи забезпечення інформаційної безпеки КІС [2, с. 311-312]:

Адміністративно-правові:

розробка та вдосконалення політики інформаційної безпеки, а також розробка та корегування документів, які її супроводжують;

визначення порядку реалізації процесів обробки інформації;

визначення персональної відповідальності за порушення норм та правил безпечної обробки інформації;

призначення та підготовка відповідальних осіб за організацію та реалізацію процесів обробки інформації;

здійснення контролю за дотриманням персоналу норм та правил безпечної обробки інформації;

проведення аналізу ефективності застосування заходів щодо інформаційної безпеки та надання рекомендацій щодо їх вдосконалення.

Організаційно-технічні:

попередження несанкціонованого поширення інформації технічними каналами;

своєчасне виявлення фактів несанкціонованого втручання в роботу КІС;

проведення обліку ресурсів, що підлягають захисту та контролю за дотриманням рівня захищеності інформації.

Економічні методи інформаційної безпеки КІС передбачають розробку системи фінансових стягнень та заохочень за дотримання правил інформаційного захисту на підприємстві. Причому система фінансових стягнень повинна бути дуже жорсткою. Адже, від халатного відношення до роботи деяких працівників, майбутній стан підприємства може дуже сильно погіршитись в результаті втрати цінної інформації.

Для надійного захисту інформації у корпоративних системах необхідно застосовувати ці методи у комплексі, створивши єдину систему захисту інформації. Ці методи дозволять підвищити захист конфіденційної інформації організацій, тим самим ліквідувавши збитки від втрати такої інформації.

Таким чином захист інформації у КІС має дуже важливе значення для ефективності роботи та розвитку організації. Адже, інформація на сьогоднішній день є одним з головних ресурсів організації, який визначає її конкурентоспроможність серед конкурентів. Нерозвинена система захисту інформації може призвести до дуже поганих наслідків, тому необхідно постійно вдосконалювати систему інформаційної безпеки організації.

Список використаних джерел:

1. Волик О.Ф., Кащеєва О.В., Дорда І.В., Пашко П.В. Митні інформаційні технології : навч. посіб.. – К.: 2011. – 391 с.

2. Філоненко С., Швець В., Мужик І. Захист інформації в системах обробки персональних данних / С. Філоненко, В. Швець, І. Мужик // Захист інформації. – 2013. – № 4. – С. 307-315.

3. Франко В.М. Проблеми безпеки сучасних корпоративних мереж / В.М. Франко // Collection of Scientific Papers of Applied Math and Computer Technologies Faculty of Khmelnytskyy National University. – 2012. – № 1. – С. 1-4.