

Бандоріна Л. М.
к.е.н., доцент
Климкович Т. О.
старший викладач
Удачина К. О.
к.е.н., асистент

Національна металургійна академія України, м. Дніпро

УДОСКОНАЛЕННЯ ПОЛІТИКИ БЕЗПЕКИ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІЙ СИСТЕМІ ПІДПРИЄМСТВА

Нові інформаційно-інтелектуальні технології можуть бути не тільки корисними, але й небезпечними для інформаційних систем та мереж підприємства, оскільки спостерігається тенденція зростання випадків несанкціонованого доступу та контролю над віддаленою інформаційною системою, копіювання конфіденційної інформації та її зловмисне використання третіми особами. Тому проблема удосконалення політики безпеки інформації в інформаційно-телекомунікаційній системі підприємства (ІТС) є актуальною.

Фрагмент обстеження об'єкта інформаційної діяльності наведено на прикладі аутсорсінгового контакт-центру, який є провідною компанією в сфері управління відносинами з клієнтами та надання послуг контакт-центрів країн Європи, Азії та Близького Сходу.

Аутсорсінг (від англ. Outsourcing: використання зовнішнього джерела/ресурсу) – це передача організацією на підставі договору певних бізнес-процесів або виробничих функцій на обслуговування іншій компанії, що спеціалізується у відповідній області. ІТС даного підприємства являє собою локальну мережу, до складу якої входять 47 персональних комп'ютерів, сервер баз даних, який відповідає за обробку та зберігання інформації, мережеве і друкарське обладнання. За сукупністю характеристик автоматизована система (АС) компанії відноситься до третього класу: розподілений багатомашинний комплекс, який обробляє інформацію різних ступенів обмеження доступу і розрахований на багато користувачів. Особливістю класу є необхідність передачі інформації

ції через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки [1].

Політика безпеки може розроблятися для такого ІТС в цілому або для окремої компоненти, окремої функціональної задачі, окремої технології обробки інформації та ін. згідно із НД ТЗІ 3.7-003-05 [2]. Виходячи з цього, а також з того, що в компанії відбулося різке збільшення проектів, і це призвело до збільшення обсягів інформації та її видів, керівництво прийняло рішення щодо додаткового обстеження відповідних департаментів з метою удосконалення комплексної системи захисту інформації, яка вже існує в даній компанії. Тому процес обстеження необхідно виконувати з урахуванням вимог вже існуючої в компанії політики інформаційної безпеки, а саме: політики класифікації інформаційних активів, політики безпеки персоналу, політики захисту від шкідливого і мобільного коду, політики використання корпоративної електронної пошти, політики управління інцидентами інформаційної безпеки тощо.

Для проведення обстеження об'єкта інформаційної діяльності необхідно:

- провести аналіз умов функціонування департаментів, їх розташування (ситуаційного плану) для визначення можливих джерел загроз;
- дослідити засоби забезпечення інформаційної діяльності, які мають вихід за межі контрольованої території;
- вивчити схеми систем життєзабезпечення даних департаментів, а також інженерних комунікацій;
- дослідити інформаційні потоки, технологічні процеси передачі, одержання, використання, розповсюдження і зберігання інформації;
- визначити наявність та технічний стан засобів забезпечення технічного захисту інформації;
- перевірити наявність нормативних документів, які забезпечують функціонування системи захисту інформації, а також нормативної та експлуатаційної документації, яка забезпечує інформаційну діяльність;
- визначити технічні засоби і системи, застосування яких не обґрунтовано службовою необхідністю і які підлягають демонтажу;

– визначити технічні засоби, що потребують переобладнання та реалізації технічного захисту інформації.

При обстеженні інформаційного середовища аналізу повинні підлягати усі дані, що використовуються і зберігаються в ІТС, а також програмне забезпечення. Таємна інформація, інформація, яка є власністю держави, а також відомості, що становлять державну таємницю, в автоматизованій системі аутсорсінгового контакт-центру не циркулюють. За режимом доступу інформація, що обробляється в АС компанії, поділяється на відкриту і з обмеженим доступом. За правовим режимом до інформації з обмеженим доступом належить конфіденційна інформація [2]. Отже, збереження і захист інформації даної компанії повинні забезпечуватися відповідно до Цивільного і Господарського кодексів, а також законів України: «Про захист персональних даних», «Про інформацію», «Про захист від недобросовісної конкуренції».

Виконання аналізу технології обробки інформації дозволить визначити і описати інформаційні потоки, виявити особливості використання електронних документів в департаментах компанії, виявити джерела виникнення інформаційних потоків і місця їх призначення; зафіксувати різновиди носіїв інформації та умови їх використання під час роботи ІТС.

При обстеженні середовища користувачів ІТС необхідно провести аналіз наступних складових частин:

- функціонального і кількісного складу користувачів ІТС;
- повноважень визначеного кола користувачів стосовно доступу до ІТС та її компонентів, допуску до відомостей, що проходять через ІТС;
- ступеня можливостей різних категорій користувачів вживати послуги ІТС.

Результатом такого обстеження можуть стати відповідні матриці доступу працівників до інформації.

Щоб визначити найцінніший ресурс в ІТС департаментів компанії можна застосувати модель оцінювання, в основі якої лежить класифікація інформації за основними властивостями, а саме: за розголошенням чи конфіденційністю; за цілісністю або несанкціонованою модифікацією; за доступністю або наявністю тощо (рис. 1).

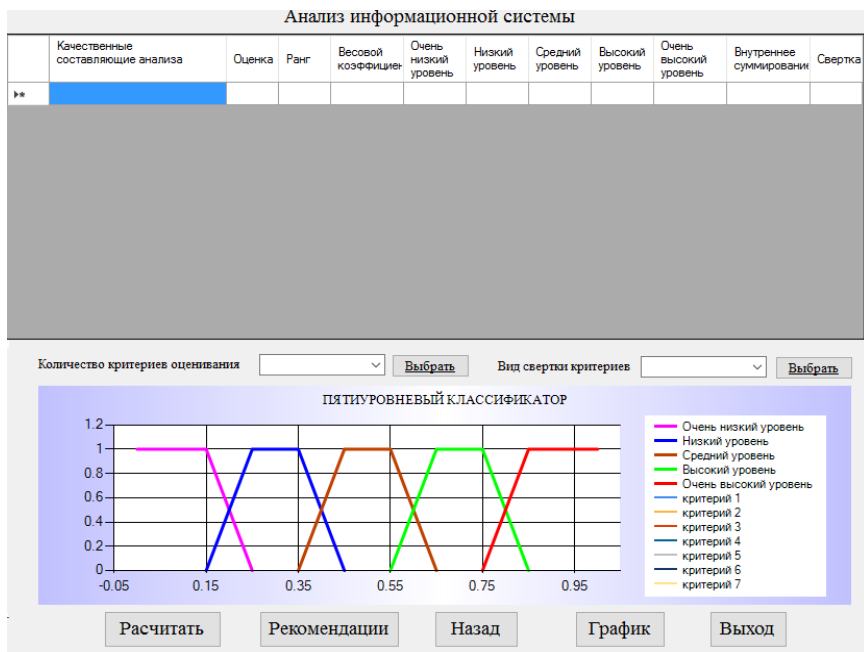


Рис. 1. Интерфейс програмної реалізації моделі оцінювання інформації

За результатами роботи такої моделі можна буде зробити висновки про найважливішу інформацію компанії, яка повинна бути забезпечена найбільшим рівнем захисту.

Список використаних джерел

1. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99. — [Чинний від 1999.04.28]. — К. : ДСТСЗІ СБУ, 1999. — № 22. — (Нормативний документ системи технічного захисту інформації).
2. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі: НД ТЗІ 3.7-003-05. — [Чинний від 2005.08.11]. — К. : ДСТСЗІ СБУ, 2005. — № 125. — (Нормативний документ системи технічного захисту інформації).