УДК 004.621.3

ВИКОРИСТАННЯ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ У ПРОЦЕСІ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Алєксєєва К.І., Толюпа С.В.
Київський національний університет імені Тараса Шевченка, м. Київ, Україна
E-mail: Karinaalekseeva@ukr.net

Analysis of computer incidents in modern information and communication systems is conducted. The main aspects and elements of information security incident management are examined. Based on a detailed analysis of incident monitoring process index performance of incident management are defined. In order to improve efficiency of incident management implementing of intellectual technology is proposed. The algorithm of intellectual system of decision-making process to improve security by optimal incident management is described.

Система управління інцидентами інформаційної безпеки є базовою частиною загальної системи управління інформаційною безпекою (СУІБ) і дозволяє виявляти, враховувати, реагувати й аналізувати події та інциденти інформаційної безпеки. Без реалізації цих процесів неможливо забезпечити рівень захищеності, що адекватний сучасним стандартам і галузевим нормам.

Управління комп'ютерними інцидентами – процес або набір процесів, на вхід яких подаються дані, отримані у результаті збору і протоколювання даних про події, що зачіпають інформаційні системи, а на виході цих процесів одержують інформацію про причини інциденту, що відбувся, про збиток, нанесений організації, і заходах, які необхідно прийняти для того, щоб інцидент не повторився. Управління комп'ютерними інцидентами спрямовано на вдосконалення системи забезпечення безпеки організації.

Реагування на інцидент - сукупність дій, спрямованих на виявлення комп'ютерної інформації, що має відношення до інциденту, і збереження її цілісності та юридичної значущості, а також на збір інших відомостей, що мають відношення до інциденту.

В останні роки істотно підвищився інтерес до дослідження, розробки й впровадження прикладних інтелектуальних систем управління. Аналіз існуючих систем управління сучасними інформаційними мережами показав, що їх рівень не відповідає повною мірою сучасним вимогам до управління мережами нового покоління, не дає змоги отримувати інформацію потрібної якості для оперативного прийняття обґрунтованих рішень щодо управління об’єктами, обміну інформацією між суб’єктами системи управління, а також не дає можливості оперативно управляти ситуаціями на мережах в автоматизованому режимі [1].

Інциденти інформаційної безпеки (ІБ) є окремим підкласом кризових і надзвичайних ситуацій, що можуть відбутися в інфо-соціо-технічній інфраструктурі та інфокомунікаційних мережах, впливаючи на стан інформаційних ресурсів і безпеки.

Основна задача управління інцидентами – якомога швидше відновити нормальну роботу служб і звести до мінімуму негативний вплив інциденту на

роботу організації для підтримки якості і доступності служб на максимально можливому рівні [2].

Специфічні питання управління інцидентами інформаційної безпеки розглядаються у наступних документах: ISO/IEC 27001:2005 Information security management system Requirements; ISO/IEC TR 18044 Information security incident management; CMU/SEI-2004-TR-015 Defining incident management processes for CISRT та ін. [3].

З кожним днем стає все складніше зберегти монополію на інформацію. Зловмисник завжди має перевагу, тому для організації дуже важливо мати змогу вдало налагодити СУІБ задля якнайшвидшого виявлення та найскорішого реагування на інциденти будь-якого роду, аби мінімізувати витрати та ліквідувати негативні наслідки. Матимемо на увазі:

- Аналіз загроз безпеки є важливою та невід'ємною складовою побудови та супроводження ІТ систем.
- Побудова моделі загроз необхідна, так як різні види інформації потрібно захищати по-різному і від різних типів загроз.
- Модель безпеки, ефективна 5-10 років тому, більше не може вважатися прийнятною для вирішення сучасних задач, оскільки на зміну відносно необразливому хуліганству в мережі Інтернет прийшла організована кіберзлочинність.

Моніторинг ІБ — один з найважливіших процесів інформаційної безпеки в організації. Програма моніторингу налаштована на миттєве реагування на будь-які відхилення показників стану безпеки кожного комп’ютера від стану безпеки, заміряному при його нормальному функціонуванні.

У разі виникнення інциденту, компоненти безпеки, призначені для виявлення аномальної поведінки, подачі сигналів тривоги, реакції на загрози і криміналістичного аналізу порушень безпеки, сповіщають про порушення адміністратора, визначають інцидент, аналізують його та надають свій журнал реєстрації подій. Ознаки інциденту діляться на дві основні категорії: повідомлення про те, що інцидент відбувається зараз, і повідомлення про те, що інцидент, можливо, відбудеться в недалекому майбутньому.

Щоб підвищити ефективність процесу управління інцидентами, необхідно визначити показники ефективності, що залежить від:

- координації і узгодженості дій всіх залучених у процес осіб;
- наявних можливостей з отримання і аналізу інформації, пов'язаної з інцидентом;
- оперативності і коректності отриманих результатів.

Застосування інтелектуальних технологій в управлінні інцидентами ІБ повинно дати поштовх до ефективності управління цим процесом. В якості базових можна виділити чотири інтелектуальні технології: технологія експертних систем, технологія нечіткої логіки, технологія нейромережних структур, технологія асоціативної пам’яті [4]. Саме технологія підтримки прийняття рішень у поєднанні з технологією експертних систем є найбільш актуальними у сфері ІБ завдяки своїй здатності допомагати адміністратору приймати рішення відповідно до інциденту.

Якщо після аналізу виявилося, що інцидент впливає на систему, наступним кроком буде звернення до інтелектуальної системи. На цьому етапі сигнатури вхідного інциденту будуть порівнюватися з сигнатурами вже наявних інцидентів у базі знань, кожному з яких однозначно відповідає певна гіпотеза з поясненнями наступних дій адміністратора.

В якості інтелектуальної системи пропонується інформаційна система підтримки прийняття рішень (ІСППР), яка може працювати за наступним алгоритмом:

1. Оперативні дані сенсорів безпеки аналізуються та оцінюються на предмет наявності сигнатур відомих інцидентів за допомогою бази знань ІСППР.

2. ІСППР на підставі аналізу надає інструкцію щодо усунення причин і наслідків інциденту ІБ, якщо його сигнатура наявна у базі знань.

3. Якщо виник інцидент, сигнатури якого немає у базі знань, то ІСППР дає декілька гіпотез відносно подальших дій адміністратора ІБ.

4. Необхідно виконати дії щодо запобігання повторного виникнення інциденту ІБ. Доцільно, щоб алгоритм роботи інтелектуальної системи щодо керування інцидентами ІБ вписувався в цикл моделі безперервного поліпшення управління процесами PDCA.

Отже, було представлено у якості інтелектуальної системи – ІСППР у сфері інцидентів ІБ в організаційно-технічних системах. При використанні процесного підходу, визначеного у відповідних міжнародних стандартах ISO/IEC, дана схема цілком вписується в модель PDCA.

Таким чином, питання підтримки прийняття рішень є досить важливим в контексті прийняття рішень у сфері інцидентів ІБ, його можна розглядати як частину більш загальної проблеми підтримки прийняття управлінських рішень у кризових ситуаціях. Визначено головні чинники, критерії і показники автоматизованих процедур підтримки прийняття рішень у сфері управління інцидентами ІБ. За вдалого налаштування ІСППР, особа, що уповноважена приймати рішення щодо інцидентів ІБ, буде мати у своєму розпорядженні декілька гіпотез, до яких будуть відноситися певні дії на етапі реагування, а також фундаментальну теоретичну основу для прийняття оптимальних рішень, аби якнайшвидше ліквідувати наслідки та максимально мінімізувати втрати, тому дослідження даного наукового напрямку вважаємо актуальним та перспективним.

Література

1. Толюпа С.В. Проектирование систем поддержки принятия решений в процессе восстановления и обеспечения комплексной защиты в информационных системах. // Науково-технічний журнал “Сучасний захист інформації”.– 2012. - №4. – С. 69-74.
2. Куканова Н. Управление инцидентами информационной безопасности // Открытые системы. — 2006. — № 10. — Електронний ресурс.
3. Стандарт ISO/IEC TR 18044:2004 "Менеджмент інцидентів інформаційної безпеки"
4. Гладиш С.В. Підтримка прийняття рішень щодо керування інцидентами інформаційної безпеки в організаційно-технічних системах. Експертні системи та підтримка прийняття рішень. с. 116-124.