В роботі з використанням системного підходу викладено формалізацію проблеми моніторингу системи безпеки інформації для визначення інцидентів в інформаційній системі організації

Ключові слова: інформаційні системи, модель моніторингу інцидентів

В работе с использованием системного подхода изложена формализация проблемы мониторинга системы безопасности информации для определения инцидентов в информационной системе организации

Ключевые слова: информационные системы, модель мониторинга инцидентов

A formalization of the problem of monitoring the information security system to identify the incidents in the information system of organization using a systematic approach is presented in this work

Keywords: information systems, model of monitoring incidents

УДК 004.891.3

МОДЕЛЬ ПІДСИСТЕМИ МОНІТОРИНГУ ІНЦИДЕНТІВ БЕЗПЕКИ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ОРГАНІЗАЦІЙ

І.А. Пількевич
Доктор технічних наук, професор, завідувач кафедри*
Контактний тел.: (0412) 415-686, 067-39-787-39
E-mail: igor.pilkevich@mail.ru
В.І. Котков
Кандидат технічних наук, доцент*
Контактний тел.: (0412) 22-94-08
E-mail: eko_univer@i.ua
*Кафедра моніторингу навколишнього природного середовища
Житомирський національний агроекологічний університет
бул. Старий, 7, м. Житомир, Україна, 10008
Н.М. Лобанчикова
Кандидат технічних наук, доцент**
Контактний тел.: 093-652-61-64
E-mail: lobanchikovanm@rambler.ru
І.І. Сугоняк
Кандидат технічних наук, доцент**
Контактний тел.: 050-463-17-37
E-mail: isygon@mail.ru
**Кафедра безпеки інформаційних і комунікаційних систем
Житомирський військовий інститут імені С.П. Корольова Національного авіаційного університету
пр. Миру, 23, м. Житомир, Україна, 10004

Вступ

Однією з найбільших проблем експлуатації інформаційних систем в сучасному світі є проблема забезпечення достатнього рівня інформаційної безпеки. В сучасних умовах жоден комплекс програмно-технічних засобів, що підтримується відповідним штатом фахівців з інформаційної безпеки, не здатний забезпечити ефективне функціонування системи захисту інформації. Дане питання вимагає системного підходу та розробки комплексних систем управління безпекою, в яких мають брати безпосередню участь всі співробітники організації. Згідно з [1, 2] метою системи управління безпекою є створення високоефективної інфраструктури, що дозволяє забезпечити безперебійність бізнес-процесів, які підтримуються цими інформаційними системами, та унеможливити інформаційні втрати. Отже, задачами системи управління інформаційною безпекою є систематизація процесів забезпечення захисту інформації, розташування пріоритетів організації в галузі захисту інформації, забезпечення адекватності системи існуючим ризикам тощо. Слід звернути увагу, що забезпечення інформаційної безпеки компанії пов'язано не тільки із захистом інформаційних систем і бізнес-процесів, які підтримуються цими інформаційними системами. В [3] визначено, що основною проблемою організації систем управління інформаційною безпекою є відсутність налагодженої системи моніторингу інцидентів, так як часто відсутність інцидентів не вказує на те, що система управління безпекою працює правильно, а означає тільки те, що інциденти не фіксуються або не визначаються.

Мета дослідження

Як відомо [1], в роботі сучасних систем моніторингу інцидентів виділяються наступні етапи: визначення інциденту; сповіщення про виникнення інциденту; реєстрація інциденту; усунення наслідків і причин

інциденту; розслідування інциденту; реалізація дій, що застерігають повторне виникнення інциденту. За даними аналізу сучасних систем, для забезпечення управління інцидентами система повинна виконувати наступні функції:

1. Контроль зовнішніх пристроїв, що підключаються, зокрема можливість в режимі online контролювати клієнтські комп'ютери, контроль роботи агента, контроль політик агента, можливість налаштування реагування на події, захист агента від видалення або виключення, наявність засобів контролю цілісності.

2. Моніторинг агентів і їх захист, зокрема можливість в режимі online контролювати клієнтські комп'ютери, контроль роботи агента, контроль політик агента, можливість налаштування реагування на події, захист агента від видалення або виключення, контроль цілісності.

3. Управління системою та обробка інцидентів, зокрема наявність власної консолі, розподіл ролей адміністратора і спеціалістів з безпеки, налаштування сповіщень, можливості реагування на інциденти, аналіз подій, зафіксованих системою, збереження історії інцидентів для наступного аналізу, заборона на пропуск затриманого повідомлення або дозвіл із записом про інцидент.

4. Формування системи звітності про роботу системи управління інцидентами, зокрема можливість побудови звітів про порушення, наявність варіантів отримання звітів про порушення, тимчасовий запис звіту в локальне сховище у разі недоступності сервера, експорт звітів, запис в журнал реєстрації дій адміністраторів системи.

Основним завданням даної статті є розробка системної моделі моніторингу інцидентів. Згідно з переліком функції системи управління інцидентами її можна віднести до систем моніторингового типу [4]. Отже для розробки математичної моделі її функціонування можна використати методи ідентифікації систем відповідного класу. В дослідженні обмежимося формалізацією процесу моніторингу інформаційної системи та визначення типу інциденту.

Основна частина

Розглянемо узагальнену схему системи моніторингових спостережень, що включає (рис. 1):

1. Кінцеву групу об'єктів моніторингових спостережень системи $V_1,...,V_N$ в абстрактному обмеженому просторі W. Такими об'єктами системи моніторингу інцидентів є:

• апаратні засоби (комутатори, маршрутизатори, сканери, UTM пристрої);

• програмні комплекси (операційні системи, антивірусні шлюзи, персональні антивірусні системи, підсистеми обробки даних, доступні служби та сервіси);

• інформаційні ресурси (бази даних, файли користувачів, що доступні в мережі, тощо);

• дії користувачів корпоративної мережі.

2. Кінцеву групу зовнішніх об'єктів спостережень системи $U_1,..,U_M$ в обмеженому просторі Ω. Такими об'єктами є: мережні потоки даних, зовнішні повідомлення тощо.

3. Підсистему S_1 спостережень над об'єктами $U_1,..,U_M$, збору і представлення зовнішніх (некерованих) параметрів системи. До некерованих параметрів системи відносяться запити на доступ від користувачів, що не пройшли встановлену процедуру авторизації, кількість запитів в одиницю часу, заявки на обслуговування певних типів, несанкціонований доступ до інформаційних ресурсів, деструктивні дії резидентних програм та користувачів тощо.

4. Підсистему S_2 спостережень над об'єктами $O_1,..,O_N$, збору і представлення внутрішніх (керованих) параметрів системи. До керованих параметрів відносяться інформація про роботу комутаційних пристроїв та інформація щодо доступності служб і додатків.

5. Підсистему S_0 аналізу і прогнозування стану системи, в якій ухвалюється рішення про управляючі дії на об'єкти моніторингу.

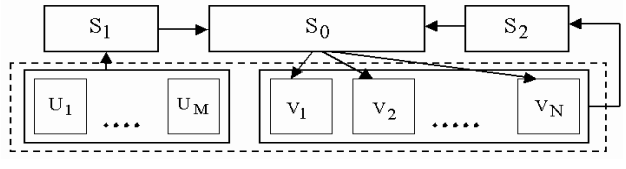

Рис.1. Формальна схема системи управління інцидентами інформаційної безпеки

Для подальшого аналізу введемо наступні позначення:

а) для програмних комплексів (O_1): доступність служби – O_{11}; наявність помилки в роботі додатків – O_{12}; дисковий простір вичерпано – O_{13};

б) для устаткування (O_2): збій системи – O_{21}; внутрішній сигнал тривоги – O_{22}; відмова мережевого пристрою – O_{23};

в) для зовнішніх повідомлень (O_3): надходження заявки на отримання додаткової інформації, поради, документації – O_{31}; забутий пароль – O_{32};

г) для інформаційних ресурсів (O_4): спроба несанкціонованого доступу – O_{41}; знищення інформації – O_{42}; зміна інформації – O_{43}.

Результатами роботи даної підсистеми є визначення ймовірності інциденту, його документування та вибір дій щодо усунення.

Для визначення її ефективності необхідною є оцінка функціонування системи за визначеними нижче параметрами: своєчасна реєстрація (аудит) подій різних типів (U_1), що оцінюється за множиною типів подій (показники (U_{1i})); визначення рівня достовірності каналів (U_2), що оцінюється за множиною каналів (показники (U_{2i})); цілісність комплексу засобів захисту, що оцінюється за множиною засобів захисту (показники (U_{3i})); можливість самотестування (U_4), що оцінюється за множиною перевірочних тестів, які наявні в системі (U_{4i}); можливість ідентифікації та автентифікації користувачів при обміні, автентифікації відправника, автентифікації отримувача (U_5), що оцінюється за множиною параметрів оцінки ефективності системи аутентифікації користувачів (U_{5i}).

В схемі моніторингу, що розглядається (див. рис. 1), припустимо наявність динамічних зв'язків між її елементами. Сучасна концепція представлення знань в системах штучного інтелекту передбачає наявність

змішаної інформації структурованого і неструктурованого типів. На початковому (нульовому) етапі для запропонованої схеми моніторингу формується структура знань системи підтримки прийняття рішень (СППР), що надається підсистемі S_0 підсистемами S_1, S_2.

Розглянемо теперішній момент часу t_0, що відповідає моменту ухвалення рішення та поточному стану системи. Тоді система знань буде включати:

1. Статичні структуровані знання (дані) $D_0(U_i^*,t)$, де $U_i^* \in U^*$ – множина граничних значень контрольованих параметрів інформаційної системи; $t \le t_0$. $D_0(U_i^*,t)$ містить кількісні накопичені знання (дані), які не підлягають подальшій зміні. До таких знань відносяться знання про можливі інциденти системи та стан параметрів системи, що їм відповідає і дозволяє їх визначення.

Така система знань формується на основі метода експертного оцінювання, коли кожному з експертів пропонується визначити характерні для інциденту ознаки в роботі системи та ймовірність їх прояву в окремих випадках. Кожному інциденту відповідає нечітка множина оцінок параметрів, що визначається наступним чином $D_{oi} = \{\mu_{ik} / O_{ik}\}$, де μ_{ik} – визначає ймовірність (можливо нечітку) прояву даної ознаки інциденту O_{ik}.

2. Динамічні структуровані знання (дані) $D_S(t,O_i)$, де $O_i \in W$; $t > t_0$. $D_S(t,O_i)$ містить кількісні прогностичні знання (дані), які можуть коректуватися в процесі роботи. Якщо показники стану об'єктів моніторингу при інциденті не є бінарними, то можливим є наявність якісно різних значень параметра, а його ймовірність розраховується за спрощеною формулою Байєса:

$$\mu_{ik} = p(N_{ir}|N_i) * p(N_i),$$

де $p(N_{ir}|N_i)$ – ймовірність присутності даної ознаки інциденту із r-статусом серед всіх випадків прояву інциденту; $p(N_i)$ – загальна ймовірність прояву ознак відповідного інциденту.

Далі можливим є використання декартового добутку станів системи, що забезпечить наявність декількох альтернативних нечітких множин характеристик прояву інциденту на об'єктах моніторингу інформаційної безпеки. При формуванні нечіткої множини ознак інциденту, для визначення інцидентів інформаційної системи, включається тільки одне значення, що якісно відповідає поточним параметрам системи.

3. Статичні неструктуровані знання (дані) $D_C(U_i^*,t)$, де $U_i^* \in U^*$; $t \le t_0$. $D_C(U_i^*,t)$ містить базові шкали по різних групах фізичних параметрів, що оцінюються в процесі ухвалення рішень на різних рівнях, спільно із значеннями лінгвістичних змінних, а також накопичені знання (дані), які не підлягають подальшій зміні. Ймовірності прояву ознаки при інциденті визначаються наступним чином: якщо параметри, за якими відбувається моніторинг, мають бінарну оцінку (True або False), то для визначення ваги використовується класичне визначення ймовірності $j_{ik} = \frac{N_i}{N}$; якщо параметри характеризуються діапазоном можливих значень, то $\mu_{ik} = \frac{\sum_{i=1}^{n} p_i \nu_i}{\sum_{i=1}^{n} \nu_i}$, де ν_i – ваговий коефіцієнт, що відображує ранг експерта.

4. Динамічні неструктуровані знання $D_L(t,O_i)$, де $O_i \in O$; $t \ge t_0$. $D_L(t,O_i)$ включає прогностичні дані значень лінгвістичних змінних, які можуть коректуватися в процесі роботи. Уточнення коефіцієнту μ_{ik} в процесі роботи системи відбувається шляхом врахування результатів поточного аналізу стану інформаційної системи і визначення інцидентів, як думки окремого експерту, ранг якого підвищується із збільшенням кількості даних [5]. На етапі тестування роботи системи в базу даних системи управління інцидентами записуються логі із значеннями всіх параметрів, що підлягають моніторингу. Далі за наявності необхідних даних проводиться аналіз проявів інциденту та призначається додаткове тестування. Після визначення наявності інциденту та його типу визначаються дії з усунення його проявів.

Процес відображення початкової множини знань про інциденти на простір можливих рішень щодо усунення їх проявів і генерацію допустимого рішення здійснюється в підсистемі S_0. Інтегральна оцінка ймовірності інциденту визначається наступним чином [6]:

$$F_i^k = \sum_{i=1}^{n} M_i D_{oi} + \sum_{j=1, i \ne j}^{B} M_j D_{uj}, \quad (1)$$

де $M = \{\mu_i\}$ – вектор ймовірності прояву ознак при інциденті.

Інтегральна оцінка наявних інформаційній системі ознак інциденту визначається аналогічним чином [6]:

$$F_i^c = M^* D^c, \quad (2)$$

де $M^* = \{\mu_i^*\}$ – розширений вектор ймовірності прояву ознак при інцидентах, в яких за умови наявності в системі ознак, що не належать до ознак даного інциденту, приймаються нульові значення для коефіцієнтів.

Таким чином, в системі враховується можливість одночасного настання двох або більшої кількості інцидентів.

Для розрахунку допустимого значення відхилення (ε) з множини еталонних інцидентів необхідно розрахувати граничні інтегральні оцінки за всіма ознаками інцидентів у випадку наявності для кожного інциденту однієї множини ознак або мінімальні та максимальні інтегральні оцінки у випадку наявності альтернативних множин ознак.

Граничними інтегральними оцінками інциденту у випадку наявності для кожного порушення однієї множини ознак інциденту вважається оцінка співвідношення (1), та оцінка, що розраховується за співвідношенням (1) лише для підмножини ознак $\mu_{ik}(C_j e_k) \ge \mu^*$ (для достатньої достовірності приймається $\mu^* = 25\%$).

В обох випадках відхилення ε визначається як $\varepsilon = (F_{max} + F_{min}) / 2$.

У загальному вигляді система моніторингу має декілька рівнів прийняття рішень. На нульовому рівні здійснюються спостереження, збір, первинна обробка даних, формування системи знань. На першому, другому та третьому рівнях послідовно здійснюється обробка даних з проходженням всіх етапів, передбачених моделлю. Виконання робіт на даних етапах здійснюється системним аналітиком з метою отримання експертної оцінки поточного і прогнозованих станів об'єктів моніторингу. На цих етапах поповнюються динамічні знання системи. На четвертому рівні особа, що приймає рішення, на основі оцінок стану системи, генерує рішення по управляючій дії на об'єкти моніторингу і системи спостереження. Крім того, на даному етапі поповнюється база знань (даних) СППР, вносяться корективи в існуючі знання та відбувається перетворення частини динамічних знань в статичні. Весь процес управління розглядається в динамічній взаємодії підсистем.

У випадку моніторингу інцидентів система може отримати наступні результати:

1. В системі визначено один інцидент інформаційної безпеки, якщо:

а) нечітка множина значень параметрів спостереження в системі відповідає нечіткій множині параметрів спостереження інцидентів і-го типу, $E^c = E_i$ або $E^c \in E_i$. Для порівняння множині ознак D_j^c присвоюються значення μ_{ik}, що розраховані для інциденту;

б) інтегральна оцінка множини ознак має відхилення, яке не перевищує певне значення ε, від еталонної множини ознак інциденту, що наявні в базі знань: $\left|F_i^c - F_i^{ek}\right| \le \varepsilon$.

2. В інформаційній системі одночасно відбуваються декілька інцидентів, якщо:

а) нечітка множина ознак системи перетинається з нечіткою множиною ознак інформаційних погроз $D^c \cap D$. У такому випадку проводиться пошук сукупності з k інцидентів, що задовольняють умові: $D^c \in \bigcup_{i=1}^{k} D_i$;

б) для кожного типу інцидентів розраховується інтегральна оцінка підмножини ознак D_k^c, що наявні у системі та відповідають певному типу інформаційних погроз з визначеної сукупності, і відхилення від еталонної множини ознак, що наявні в базі знань окремих інцидентів у випадку, коли вони не перевищують певне значення ε для всіх інцидентів: $\left|F_i^c - F_i^{ek}\right| \le \varepsilon$.

3. Інформаційна система потребує додаткового тестування та моніторингу у випадках, якщо:

а) $E^c \notin E_i$ або $E^c \subseteq \sum_{i=1}^{k} E_i$ та немає можливості змінити масив ознак, виключивши незначні з точки зору інформаційної безпеки або додавши інші. Тестування визначається у напрямку, що відповідає масиву ймовірних інформаційних загроз: $\inf\{ E^c - E_i \}$;

б) $E^c = E_i$ або $E^c = \sum_{i=1}^{k} E_i$, але $\left|F_i^c - F_i^{ek}\right| > \varepsilon$. В такому випадку крім тестування можна визначати дії щодо запобігання або перешкоджання, так як відхилення може бути обумовлене особливостями конкретного інциденту.

4. Знайдено декілька взаємовиключних інцидентів або декілька можливих множин потенційних інформаційних погроз. Тоді найбільш ймовірним є інцидент з найменшим ε. В цьому випадку, за необхідності, можна провести додаткове тестування системи у відповідності до протоколів дій для визначеного переліку інцидентів.

Висновок

Впровадження підсистеми моніторингу інцидентів реалізованої у відповідності до побудованої моделі дозволяє отримати наступні переваги: вдосконалений моніторинг, що підвищує продуктивність системи; поліпшена інформація для управління якістю обслуговування; виключення втрат і некоректного обліку інцидентів і запитів.

Література

1. Проект „Розробка та впровадження типових рішень щодо комплексної системи захисту інформації в АІС НАНУ". Система управління інцидентами інформаційної безпеки. Керівництво адміністратора. 05540149.90000.043.ИЗ-06 // [Електронний ресурс]. – Режим доступу до ресурсу: http: www.isofts.kiev.ua/c/document_library/.
2. Information technology. Security techniques. Code of practice for information security management: ISO 17799: 2005. – London: The International Standards Glossary, 2005. – 34 p. – (Міжнародний стандарт).
3. Юдін О.К. Захист інформації в мережах передачі даних [Текст] / О.К. Юдін, О.Г. Корченко, Г.Ф. Конахович. – К.: Вид-во ТОВ „НВП „Інтерсервіс", 2009. – 716 с.
4. Сугоняк І.І. Модель системи підтримки прийняття рішень з оптимального керування життєвим циклом інноваційних проектів підприємств / І.І. Сугоняк // Вісник ЖДТУ. – Серія: технічні науки. – 2007. – № 43 (4). – С. 91-99.
5. Система функционального активного мониторинга FLAME / В.А. Васенин, В.В. Корнеев, М.Ю. Ландина, В.А. Роганов // Программирование. – 2003. – №3. – С. 161-173.
6. Пількевич І.А. Моделі та методи побудови системи підтримки прийняття рішень автоматизованої системи ідентифікації особи / І.А. Пількевич, Н.М. Лобанчикова // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем: збірник наукових праць. Вип. 5. – Житомир: ЖВІ нау, 2011. – С. 69-76.