# Модель системи моніторингу захищеності інформації в автоматизованій системі керування підприємством

Сугоняк І. І., Молодецька К. В.
Житомирський військовий інститут Національного авіаційного університету, katerina_mk@ukr.net

***Using a systematic approach described formalization of the problem of monitoring information security incidents to determine in an automated system organization. Implementation of the subsystem monitoring incidents sold in accordance with the constructed model allows for the following benefits: improved monitoring, which is a measure of system performance, improved information quality management services, excluding losses and incorrect accounting incidents and inquiries.***

## Вступ

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. Задачами системи управління інформаційною безпекою є систематизація процесів забезпечення захисту інформації, розташування пріоритетів організації в галузі захисту інформації, забезпечення адекватності системи існуючим ризикам тощо.

В роботі сучасних систем моніторингу інцидентів в [1, 2] 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. Основною метою є розробка системної моделі моніторингу інцидентів.

Згідно з переліком функції системи управління інцидентами її можна віднести до систем моніторингового типу [3], отже для розробки математичної моделі її функціонування можна використати методи ідентифікації систем відповідного класу.

1) 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 доступні в мережі тощо);

– дії користувачів корпоративної мережі.

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 і 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. У випадку моніторингу інцидентів система результати наступні:

– в системі визначено один інцидент інформаційної безпеки якщо 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 $\mu_{ik}$ що розраховані для інциденту. Якщо інтегральна оцінка множини ознак має відхилення, що не перевищує певне значення $\varepsilon$ від еталонної множини ознак інциденту, що наявні в базі знань, тобто

$$\left|F_i^c - F_i^{ek}\right| \le \varepsilon; \qquad (1)$$

– в автоматизованій системі одночасно відбуваються декілька інцидентів, якщо 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 (2):

$$D^c \in \bigcup_{i=1}^{k} D_i; \qquad (2)$$

– для кожного типу інцидентів розраховується інтегральна оцінка підмножини ознак $D_k^C$, що наявні у системі і відповідають певному типу інформаційних погроз з визначеної сукупності і, відхилення від еталонної множини ознак, що наявні в базі знань окремих інцидентів такому випадку не перевищує певне значення $\varepsilon$ для всіх інцидентів

$$\left|F_i^c - F_i^{ek}\right| \le \varepsilon. \qquad (3)$$

1) Автоматизована 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, 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.

2) Знайдено декілька взаємовиключних інцидентів, або декілька можливих множин потенційних інформаційних погроз - тоді найбільш ймовірним є інцидент з найменшим $\varepsilon$, за необхідності можна провести додаткове тестування системи у відповідності до протоколів дій для визначеного переліку інцидентів.

## Висновки

Впровадження підсистеми моніторингу інцидентів реалізованої у відповідності до побудованої моделі дозволяє отримати наступні переваги: вдосконалений моніторинг, який дозволяє виміряти 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.И3-06 // [ел.ресурс]. Режим доступу до ресурсу: www.isofts.kiev.ua/c/document_library/

[2] ISO 17799: 2005 – Міжнародний стандарт управління інформаційною безпекою як управлінська складова в галузі менеджменту інформаційної безпеки.

[3] Сугоняк І.І. Модель системи підтримки прийняття рішень з оптимального керування життєвим циклом інноваційних проектів підприємств / Сугоняк І.І. // Вісник ЖДТУ – Серія: технічні науки. – 2007. – № 43 (4). – С. 91–99.