УДК 004.621.3

МОДЕЛЬ СИСТЕМИ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Юрій Тичина, Валентина Ящук, Орест Полотай
Львівський державний університет безпеки життєдіяльності, Львів Україна

Розглянуто теоретичні, науково-методичні та організаційно-функціональні основи моделювання системи управління інцидентами інформаційної безпеки. Визначено сучасні підходи до управління інцидентами інформаційної безпеки. Наведено методичні підходи до формування концепції та структури автоматизованої системи управління інцидентами інформаційної безпеки. Запропоновано модель управління інцидентами інформаційної безпеки та наведено методику розслідування інцидентів інформаційної безпеки.

Ключові слова: інформаційна безпека, інцидент інформаційної безпеки, система управління інцидентами інформаційної безпеки, модель системи управління інцидентами.

The theoretical, scientific-methodical, and organizational-functional bases of modeling the information security incident management system are considered. Modern approaches to information security incident management are defined. Methodical approaches to the formation of the concept and structure of the automated information security incident management system are given. The information security incident management model is proposed and the method of investigation of information security incidents is given.

Key words: information security, information security incident, information security incident management system, incident management system model.

Управління інцидентами є однією з найважливіших процедур управління інформаційною безпекою (ІБ). Основною метою створення системи інформаційної безпеки (ІБ) організації є зниження ризиків щодо інформаційних активів і зменшення негативних наслідків від можливих інцидентів ІБ. Процес управління інцидентами інформаційної безпеки (УІІБ) – ключовий процес у системі інформаційної безпеки. Саме цим зумовлені теоретична значущість, практична спрямованість та новизна теми кваліфікаційної роботи, його мета і сукупність завдань.

Для управління ІІБ необхідно організувати комплекс методів та засобів управління інцидентами (УІ), забезпечити його належними ресурсами, відповідною нормативно-розпорядчою і робочою документацією, технічними засобами забезпечення механізмів контролю.

Управління інцидентами інформаційної безпеки (УІІБ) є важливим процесом, який забезпечує організацію можливістю своєчасного виявлення інциденту та якомога швидшого реагування на нього за допомогою адекватних засобів підтримки. Для опису процесу формування СМІІБ в роботі використовується класична модель безперервного удосконалення процесів (рисунок на слайді), що отримала назву від циклу Шухарта-Демінга - модель PDCA (Плануй, Plan - Виконуй, Do - Перевіряй, Check - Дій, Act).

Проблеми інформаційної безпеки істотно залежать від типу інформаційних систем і сфери їх застосування. У локальних системах малого масштабу систему захисту побудувати набагато простіше, ніж в системах розподіленого типу, що пояснюється особливостями цих систем. Саме тому запропонована структурна модель інформаційної безпеки систем розподіленого типу (рис.1). Структурна модель передбачає, що рішення проблеми безпеки в інформаційних системах розподіленого типу полягає в аналізі таких основних компонентів: визначення основних завдань захисту інформації, визначенні суб’єктів інформаційних процесів, класифікації основних можливих загроз безпеки, визначенні рівнів вразливості інформаційних систем, визначенні джерел інформації,

ознайомленні з особливостями джерел загроз, дослідженні способів та напрямів захисту та звичайно цілей захисту.

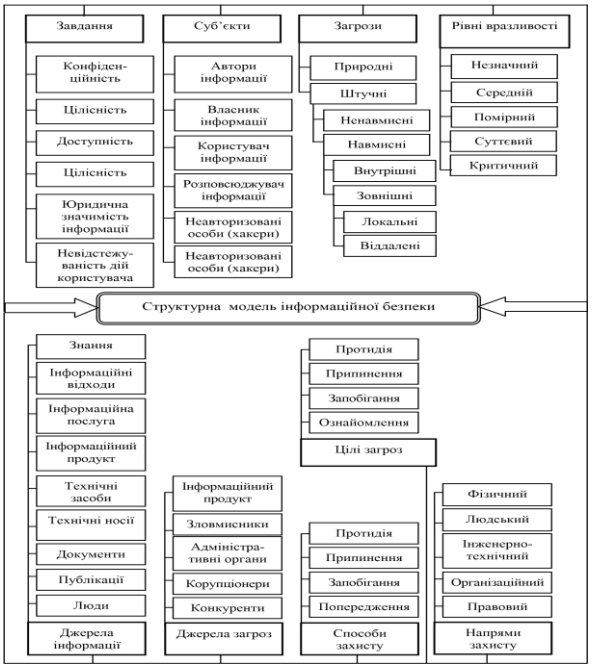

Рис. 1. Структурна модель інформаційної безпеки систем розподіленого типу

Формалізуючи модель системи інцидентів інформаційної безпеки у математичному вигляді, доцільно визначити її функціональну залежність від завдань захисту інформації, суб'єктів інформаційних процесів, загроз безпеки, рівнів вразливості інформаційних систем, джерел інформації, джерел загроз, способів захисту, напрямів захисту, цілей захисту:

Роботи із впровадження СУІБ нами пропонується проводити у декілька етапів: обстеження об'єкту; розробка процедур та процесів системи управління, написання відповідних документів; впровадження СУІБ; впровадження АС моніторингу й управління інцидентами ІБ.

Проведений аналіз вітчизняного ринку програмних продуктів для оброблення подій дозволив визначити один із кращих СУІБ – netForensics nFX Open Security Platform. Система netForensics призначена для роботи з гетерогенним середовищем продуктів забезпечення ІБ і реалізує безперервний збір, обробку та відображення подій безпеки. Система може працювати на платформах Windows, Linux або Solaris, використовуючи в якості сховища даних повнофункціональну СУБД Oracle.

Отже, запропонована вдосконалена структурна та математична модель управління інцидентами інформаційної безпеки надала можливість побудувати ефективну систему захисту інформації, застосувати адекватні засоби і методи безпеки на всіх рівнях інформаційних процесів. Розроблені та обґрунтовані практичні рекомендації з побудови та функціонування систем управління інцидентами інформаційної безпеки сприятимуть підвищенню ефективності управління інцидентами інформаційної безпеки підприємств.

Література

1. Драб Ю. Основні підходи до побудови системи управління інформаційною безпекою / Ю.Драб, В. Ящук // Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с. (С.29-32).

2. Малькевич Р. Проблеми забезпечення безпеки інформації підприємства в умовах пандемії / Р. Малькевич, В. Ящук // Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с. (С.69-72).

3. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD) ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. — [Чинний від 2010-07-01]. — К.: Національний банк України 2010. — 163 с. — (Галузевий стандарт України).