УДК 004.02

Стецяк Т.Б., аспірант кафедри захисту інформації
Національний університет "Львівська політехніка"
Логвиненко В.М., канд. філос. наук, доцент
Львівський державний університет безпеки життєдіяльності, м.Львів

ВДОСКОНАЛЕННЯ МОДЕЛЮВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЙНИХ АКТИВІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ НЕПЕРЕРВНОСТІ БІЗНЕСУ

Проведено аналіз моделей інформаційної безпеки, що базуються на принципах процесного моделювання. Встановлені та описані недоліки цих моделей стосовно виявлення якнайбільшої множини факторів, на етапі ідентифікації ризиків, які впливають на ефективність систем захисту інформації та систем управління інформаційними ризиками. Обґрунтовано необхідність вдосконалення існуючих моделей та запропоновано доповнити їх побудовою імітаційних моделей подій, процесів, поведінки або здійснити імплементацію цих моделей в корпоративну архітектуру безпеки. Встановлено, що найдоцільнішим способом вдосконалення цих моделей на предмет управління ризиками є їхня імплементація в корпоративну архітектуру безпеки.

Ключові слова: інформаційна безпека, моделі інформаційної безпеки, система захисту інформації, система управління інформаційними ризиками, корпоративна архітектура безпеки.

Проведен анализ моделей информационной безопасности, основанных на принципах процессного моделирования. Установлены и описаны недостатки этих моделей по выявлению наиболее полного перечня факторов, на этапе идентификации рисков, влияющих на эффективность систем защиты информации и систем управления информационными рисками. Обоснована необходимость совершенствования существующих моделей и предложено дополнить их построением имитационных моделей событий, процессов, поведения или осуществить имплементацию этих моделей в корпоративную архитектуру безопасности. Установлено, что наиболее целесообразным способом совершенствования этих моделей на предмет управления рисками является их имплементация в корпоративную архитектуру безопасности.

Ключевые слова: информационная безопасность, модели информационной безопасности, система защиты информации, система управления информационными рисками, корпоративная архитектура безопасности.

The analysis of information security models based on the principles of process modeling has been made. Established and described the shortcomings of these models to identify most possible variety of factors regarding the stage of risk identification that affect the effectiveness of information security and information risk management systems. The urgency of improving existing models has been described and relevant solutions proposed: to complement their development with simulating models of events, processes, behavior, or to implement these models in corporate security architecture. The conclusion has been found, that the most appropriate way to improve these models in terms of risk management is implementing an enterprise architecture framework.

Key words: information security, information security model, information security system, information risk management system, enterprise architecture framework.

Ускладнення інформаційних систем, їх архітектури, а також архітектури та інфраструктури самих підприємств, поява нових процесів, станів системи та поведінки її елементів призводить до невизначеностей [1]. Невизначеності зумовлені ймовірнісним характером ризиків та пов'язаних з ними інцидентами, оскільки останні прямо залежать від факторів, які впливають на ризик – активів, загроз, уразливостей та механізмів контролю. Звідси, в процесі проектування систем захисту інформації (СЗІ), виникає проблема зростання множини факторів, які впливають на інформаційну безпеку [2]. Тому одним із важливих завдань моделювання в інформаційній безпеці є побудова моделей, котрі братимуть в розрахунок якомога більше факторів, що зменшить діапазон ймовірнісного розподілу ризику та дасть змогу максимально об'єктивно визначити ефективність системи захисту та системи управління інформаційними ризиками (СУІР), які планується впровадити чи модернізувати.

На сучасному етапі розвитку інформаційної безпеки фахівцями розроблено багато моделей для системи управління інформаційними ризиками. Проте жодна існуюча модель не є, і не може бути, у зв’язку з унікальністю та специфічністю потреб, бізнес-цілей та інформаційних середовищ кожного конкретного підприємства, універсальною, а декотрі з них мають ряд недоліків. Тому, проблема вдосконалення існуючих моделей є колом наукових пошуків багатьох вчених. Так, Є.С. Родін, виходячи з процесних підходів до моделювання, розробляє побудову більш функціональних та математично обґрунтованих моделей управління ризиками інформаційної безпекою; В.Г. Кононович, Ю.В. Копитін – розробляють моделі оцінки ризиків інформаційної безпеки на основі розфарбованої мережі Петрі, багатошарових графів, гіперграфів та ін. Проте, розроблення моделі, котра б враховувала найбільшу кількість факторів, з метою якнайточнішого подальшого розрахунку цінності активів, ймовірності використання уразливостей та реалізації загроз,

обчислення часу, необхідного для реалізації загрози, часу відновлення ресурсу після виникнення інциденту та, зрештою, розрахунок коефіцієнта повернення інвестицій в інформаційну безпеку та забезпечення безперервності бізнесу залишається актуальним завданням в сфері інформаційної безпеки. Відповідно для цього, в процесі управління ризиками потрібно розробити таку модель на етапі ідентифікації ризику, щоб максимально врахувати фактори, що впливають на ефективність СЗІ та СУІР. Тому метою цієї статті є аналіз моделей, побудованих на базі процесного моделювання, на предмет ідентифікації факторів та визначення можливих варіантів вдосконалення цих моделей з метою зменшення впливу суб'єктивних експертних оцінок та невизначеності (оскільки захист не може бути абсолютним і тому можливість реалізації загроз мають ймовірнісний характер) при здійсненні оцінювання ефективності як уже розробленої СЗІ на етапі її аудиту, так і СЗІ, які планується впровадити.

Провідною моделлю для розробки СУІР, є процесна модель [3]. Саме вона використовується в стандартах щодо систем управління інформаційною безпекою, та, зокрема, знайшла своє відображення в стандарті ISO/IEC 27005. Ця модель не є математичною, проте вона передбачає послідовний перелік етапів, які потрібні для управління ризиками інформаційної безпеки: планування, реалізація, перевірка та дія. Перший етап – планування, якраз і передбачає ідентифікацію активів та складання профілів загроз і уразливостей, виявлення існуючої нормативної бази та механізмів контролю.

Процесна модель реалізується через такі популярні методики як CRAMM, RiskWatch, OCTAVE, NIST та інші. Зупинимося на розгляді методик CRAMM та RiskWatch.

CRAMM, як основний спосіб оцінювання ризиків, використовує метод опитування. Опитування ретельно планується і передбачає детальні листи-опитувальники. Даний метод, при його запровадженні, враховує усі складові підприємства, в тому числі технічні, фахові тощо. В основі методики CRAMM поєднуються кількісні та якісні методи аналізу при оцінюванні ризиків. У методі CRAMM будується модель активів інформаційної системи, яка описує

взаємозв’язки між інформаційними, програмними та технічними активами. Проте цей метод має ряд недоліків. Так, в цій методиці оцінюються так звані «чисті» ризики, безвідносно до реалізованих у системі механізмів контролю. На етапі оцінювання ризиків передбачається, що контрзаходи взагалі не використовуються. Методика CRAMM для кожного етапу визначає набір вихідних даних, послідовність заходів, зміст опитувальника для проведення інтерв’ю, списки перевірки і набір звітних документів [4]. Окрім того в цій методиці нівелюється комплексний підхід; область застосування має обмежений характер, експертне опитування посадових осіб підприємства містить суб'єктивні оцінки, які до того ж часто використовують статистичні дані минулих періодів, які вже не відповідають дійсності, особливо у випадку частих оновлень та заміни програмного і апаратного забезпечення, введення нових послуг тощо.

Методика RiskWatch допомагає провести аналіз ризиків і зробити обґрунтований вибір заходів і засобів захисту. Використовувана в програмі методика включає в себе 3 фази. Перша фаза – визначення предмету дослідження. На даному етапі описуються параметри підприємства – тип підприємства, склад досліджуваної системи. Опис формалізується у ряді підпунктів. Далі кожен з обраних пунктів описується детально. Для полегшення роботи аналітика в шаблонах даються списки категорій захищених ресурсів, втрат, загроз, уразливих місць і заходів захисту. З них потрібно вибрати ті, що реально присутні на підприємстві. Друга фаза – введення даних, що описують конкретні характеристики системи. На цьому етапі детально описуються ресурси, втрати та класи інцидентів. Третя фаза – оцінка ризиків. Спочатку встановлюється зв’язок між ресурсами, втратами, загрозами і вразливими місцями, виділеними на попередніх етапах. Методика RiskWatch робить аналіз ризиків на програмно-технічному рівні захисту, без врахування організаційних та адміністративних чинників та не бере до уваги комплексний підхід до інформаційної безпеки. Крім того, RiskWatch розглядає ризики як математичне очікування втрат. Ця методика не враховує багатьох факторів, які впливають на

безпеку інформації та має обмежену область застосування. Використовуючи метод опитування так само як і CRAMM, RiskWatch не позбавлена суб'єктивності оцінок при опитуванні, використанні респондентами застарілої інформації тощо.

Існуючі методології та відповідні моделі, які на них ґрунтуються, часто не враховують всієї комплексності системи безпеки, яка має орієнтуватися передусім на бізнес. Використання процесної моделі з опитувальною схемою, як ми з'ясували, має ряд недоліків, проте вона залишається достатньо популярною та дієвою. Очевидно, доцільно не відмовлятись від неї, а спробувати її вдосконалити та доповнити, наприклад, шляхом побудови імітаційних моделей подій, процесів та поведінки, або ж здійснити імплементацію вищезгаданих методик в корпоративну архітектуру безпеки.

Прикладом імітаційних моделей є модель поведінки порушника; модель роботи технічних засобів; модель роботи програмного забезпечення; модель атаки на відмову в обслуговуванні; модель роботи СЗІ; модель роботи користувача [3]. Таким чином, в кожному конкретному випадку розробки моделі СУІР, необхідно вибрати таку модель чи комбінацію моделей, яка бере до уваги якомога більше результуючих факторів, притаманних даній системі, та найбільш достовірно визначає ймовірність реалізації найгіршого сценарію для кожної події з дерева подій, сформованого за результатами інжинірингу системи. При цьому така модель повинна динамічно змінювати вихідні результати при зміні факторів. Імітаційні моделі, хоча і виправляють недоліки процесних моделей, усе ж їх застосування подібне «латанню дірок» чи боротьбі з окремими «осередками пожежі».

Корпоративна архітектура безпеки проникає глибше, ніж засоби та методики управління ризиками, і надає більше деталей. Наприклад, якщо політика безпеки вимагає, щоб мережне управління доступом було реалізовано і впроваджено, архітектура може розглядати схему мережі, окремі зони мережі на основі рівня довіри та бізнес-потреб, зовнішні підключення, механізми безпеки, інструменти та ролі, які беруть участь на кожному рівні. Архітектура

працює від рівня політики до рівня компонентів, покриваючи всі аспекти діяльності підприємства.

Сьогодні існує багато методологій побудови корпоративної архітектури безпеки. Більшість з них працюють з структурами заданими моделями Дж. А. Захмана та TOGAF. Коротко охарактеризуємо кожну з них.

Модель Захмана була розроблена ще в 1980-х роках та розширена в 90-х і ґрунтується на принципах класичної архітектури бізнесу, що містять правила, які керують і впорядковують безліч відносин. Ця модель є двовимірна, вона використовує шість основних запитань (communicaions interrogatives): Що (вихідні дані)?, Як (функції)?, Де (дислокація)?, Хто (особи та підприємства)?, Коли (час)?, і Чому(мотивація)?, які перетинаються з різними рівнями (Планувальник, Власник, Конструктор (архітектор), Проектувальник, Розробник (і співробітник)). [4]. Такий підхід є легким для розуміння будь-яким спеціалістом і дає цілісне уявлення про організацію. Загалом, ця модель не орієнтована на безпеку, проте її застосування в цій сфері є вельми перспективним, оскільки вона вказує, як зрозуміти реальне підприємство модульним способом.

Модель TOGAF (The Open Group Architecture Framework) – створена як «засіб для розробки архітектур інформаційних систем» й покликана їх інтенсифікувати. Вона пропонує підходи для розробки, впровадження, і управління корпоративною інформаційною архітектурою. TOGAF дає змогу розробникам та особам, залученим до створення СУІР, зрозуміти організацію з різних точок зору (див рис.1).

Рисунок 1. Типи архітектур в TOGAF

Таким чином, проведений аналіз моделей інформаційної безпеки, що базуються на принципах процесного моделювання показав, що ці моделі є

недосконалими стосовно виявлення факторів на етапі ідентифікації ризиків, які впливають на ефективність систем захисту інформації та систем управління інформаційними ризиками. Тому буде доцільним здійснити імплементацію цих моделей в корпоративну архітектуру безпеки. Завдяки тому, що в моделях Захмана та TOGAF розглядають організацію у більш широкому масштабі та з різних точок зору, це дає можливість уникнути суб'єктивного чинника, який характерний для процесної моделі та дозволить врахувати та ідентифікувати більшу кількість факторів ризику, що зробить ідентифікацію об'єктивнішою.

Подальші дослідження з цього напряму можуть бути присвячені розробці корпоративних архітектур безпеки, які, окрім вирішення проблем, описаних у цій статті, також враховують фактор часу – старіння, втрата актуальності та первісного значення інформації, як необхідної для швидкого та ефективного прийняття управлінських рішень, так і інформаційного активу підприємства, що підлягає захисту. Також в наступних дослідженнях доцільно проаналізувати перспективи та необхідність імплементації системи управління інформаційною безпекою в загальну систему управління підприємством.

Література

1. Кононович В. Г. Моделювання процесів управління ризиками інформаційної безпеки / В. Г. Кононович, Ю. В. Копитін // Управління розвитком складних систем. – 2013. – Вип. 16. – С. 100-109.
2. Гарасимчук О.І., Костів Ю.М. Оцінка ефективності систем захисту інформації // Вісник КНУ імені Михайла Остроградського. – 2010. - Вип 1. - С. 16 – 20.
3. Родін Є.С. Процесні підходи до моделювання у сфері управління ризиками інформаційної безпеки / В. Г. Кононович, Ю. В. Копитін // Математичні машини і системи. – 2012. – №4. – С. 142-148.
4. Астахов А. М. Искусство управления информационными рисками. – М.: ДМК Пресс. – 2010. – 312 с.
5. Shon Harris CISSP Cerified Information Systems Security Professional : All-in-One Exam Guide Sixth Edition / Shon Harris. - McGrawHill. - 2013. - 1430 p. - ISBN 978-0-07-178173-2