СОЦІАЛЬНА ІНЖЕНЕРІЯ В КОНТЕКСТІ РОЗУМІННЯ МЕТОДОЛОГІЇ ЩОДО АНАЛІЗУ ОЦІНКИ РИЗИКІВ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Василенко М. Д.

доктор фізико-математичних наук, професор кафедри кібербезпеки Національного університету «Одеська юридична академія»

Слатвінська В. М.

аспірантка кафедри господарського права та процесу Національного університету «Одеська юридична академія»

Інформаційне суспільство охоплює всі області людського та національного життя. Однак людство, яке стало широко використовувати телекомунікації і глобальні комп'ютерні мережі, не може передбачити можливості використання цих технологій. Соціальну інженерію можна представляти як метод керування діями індивіда без використання технічних засобів, що ґрунтується на використанні слабкостей людського фактору [1]. Соціальна інженерія побудована на використанні некомпетентності, непрофесіоналізму або недбалості персоналу для отримання доступу до інформації, доводячи, що найслабкішою ланкою системи «безпеки – людина» залишається людина. З іншого боку, соціальну інженерію часто розглядають як незаконний метод отримання інформації, тому сьогодні її активно використовують в Інтернеті для отримання закритої інформації або інформації, що має достатню цінність. Тоді методи несанкціонованого доступу до інформації можна умовно поділити на категорії, коли використовують методи соціальної інженерії та ті, що, в певній мірі, існують без них. Тому створення політики безпеки захисту інформації від несанкціонованого доступу стало необхідною складовою загальної справи безпеки підприємства в контексті використання аналізу та управління ризиками. Аналіз ризику відноситься до процедури виявлення факторів ризику та оцінки їх значущості. Таким чином, ризик - це ймовірність настання певних небажаних подій, які негативно вплинуть на досягнення цілей конкретного бізнес-процесу. Аналіз ризику включає оцінку ризику і методи зниження ризику або пов'язаних з ним несприятливих наслідків. Існує два види аналізу ризику - якісний і кількісний, які доповнюють один одного. Якісний аналіз спрямований на визначення (ідентифікацію) факторів, секторів і видів ризику. Кількісний аналіз ризику повинен дозволяти визначити величину окремих ризиків і загальну величину ризику в цілому. Кінцевий результат якісного аналізу ризику, в свою чергу, забезпечує вихідну інформацію для кількісного аналізу. Однак кількісна оцінка ризику також є найбільш складною, оскільки потребує відповідної вихідної інформації та чіткої шкали оцінки ризику. Тематика застосування різних методів аналізу ризику в інформаційній безпеці розглядається в рамках курсу «Аналіз і управління ризиками», який читається на

факультеті кібербезпеки та інформаційних технологій НУ «Одеська юридична академія». Суть управління ризиками полягає в аналізі факторів ризику та прийнятті відповідних рішень щодо усунення ризиків. Фактори ризику використовуються при оцінці ризику і пов'язані з основними параметрами, зазначеними в міжнародних стандартах. Залежно від методології оцінки ризику, що використовується організацією, визначається метод аналізу та оцінки поданих параметрів. Загальний процес аналізу ризику складається з трьох етапів: підготовка до аналізу ризику, аналіз можливих сценаріїв аварії, визначення ступеня ризику і вибір рекомендацій з управління ризиком. Існує експертний метод оцінки ризику, який являє собою сукупність логічних і математико-статистичних методів і процедур обробки висновків групи експертів, при цьому висновки є єдиним джерелом інформації. І тут виникає можливість використання інтуїції, життєвого та професійного досвіду учасників опитування. Методи використовуються тоді, коли недолік або повна відсутність інформації не дає змоги використовувати інші можливості. Найбільш відомим серед цих методів став метод Делфі. Перевага цього підходу в тому, що якісний підхід дозволяє конкретно оцінити кожну ситуацію. У деяких випадках може бути важливіше ретельно розглянути різні фактори, що визначають ситуацію, ніж проводити систематичну кількісну оцінку. Такий підхід заохочує незалежне мислення членів комісії і дозволяє збалансовано оцінити питання.

До недоліків можна зарахувати надмірну суб'єктивність оцінок. При прийнятті рішень будь-які риси або переваги експертів можуть істотно впливати на підсумкові оцінки. Все ж таки основним обмеженням у використанні методу Делфі стає складність у підборі великої групи експертів, які мають необхідну компетенцію у досліджуваному питанні. Існують також статистичні методи оцінки ризику (наприклад, метрика ризику з використанням VaR), які визначають ймовірність втрат на основі статистичних даних за попередній період і встановлюють області (зони) ризику, фактори ризику та інші параметри ризику. Основна перевага статистичних методів полягає в тому, що можна аналізувати і оцінювати різні сценарії і розглядати різні фактори ризику в рамках одного підходу з урахуванням накопичених статистичних даних. Основні переваги методології метрики ризику полягають у тому, що ризик може бути виміряний універсально в різних умовах навколишнього середовища, оскільки ризик може бути виміряний в термінах ймовірності втрат, і що ризики окремих компонентів можуть бути об'єднані в одне значення для всього досліджуваного об'єкта з урахуванням різних факторів, що впливають на об'єкт. Позитивним аспектом є те, що втрати і пов'язані з ними ризики можна аналітично порівняти. Інформаційні методи оцінки ризиків, основним завданням яких можна виділити визначення ризиків, найбільш актуальних для конкретної інформаційної системи.

Розгляньмо новітні і найбільш поширені методи, включаючи CRAMM, RiskWatch і CORAS.

CRAMM (Метод аналізу та управління ризиками ССТА) був розроблений компанією Insight Consulting у відповідь на запит Центрального агентства з

комп'ютерів і комунікацій у Великобританії. Через деякий час була впроваджена версія CRAMM для громадянського суспільства, фінансових і комерційних організацій.

Аналіз ризику в CRAMM полягає у виявленні та визначенні рівня ризику на основі оцінки активів, загроз і вразливості активів; CRAMM забезпечує аналіз і документування вимог, пов'язаних з безпекою, обґрунтування витрат, пов'язаних зі створенням інформаційних систем, надмірні заходи захисту, що всі можливі ризики були визначені, що вразливості ресурсів були визначені і оцінений їх рівень, що загрози були визначені і оцінений їх рівень, і що заходи захисту засновані на формальному підході для забезпечення їх ефективності.

CRAMM ділить процедуру аналізу ризиків на три етапи: ідентифікація та оцінка активів. Оцінка ризиків (включаючи оцінку загроз і вразливості). Вибір і рекомендація захисних заходів. CRAMM має велику бібліотеку захисних заходів.

Переваги CRAMM включають комплексний підхід до оцінки ризиків, застосування методів оцінки загроз та вразливостей щодо довіреності, систему моделювання інформаційної системи, зручну для застосування в галузі інформаційної безпеки, багату базу знань про захисні заходи, універсальність та адаптованість до різних організаційних профілів, а також проведення аудиту відповідно до

Недоліком методу CRAMM є те, що для його використання потрібна спеціальна підготовка і висока кваліфікація аудиторів; CRAMM краще підходить для аудиту вже працюючих інформаційних систем, ніж систем, що знаходяться в стадії розробки; аудити CRAMM досить трудомісткі і можуть вимагати від аудиторів безперервної роботи протягом декількох місяців. Програмний інструментарій CRAMM створює велику кількість паперової документації, яка не завжди корисна на практиці; CRAMM не дозволяє користувачам створювати власні шаблони звітів або змінювати існуючі; база знань CRAMM не може бути доповнена користувачами не може бути доповнена користувачем, що створює деякі проблеми при адаптації її до потреб конкретної організації [1].

Метод RiskWatch був розроблений компанією RiskWatch Inc. у США за участю NIST, Міністерства оборони США і Міністерства національної оборони Канади. Вона підтримує програмні продукти для різних видів аудиту, включаючи відповідність ряду стандартів і керівних документів, класифікованих по областях застосування, таких як охорона здоров'я, банківський і фінансовий сектор і корпоративна безпека (за винятком стандарту PCI DSS, актуальність якого сумнівна за межами США).

Усі продукти RiskWatch використовують як базову платформу загальну для цього типу продуктів архітектуру. У спрощеному вигляді ця архітектура може бути виражена наступним чином: Велика база знань, що містить інформацію про активи, загрози, вразливості, види шкоди, засоби захисту та анкети для оцінки факторів ризику. Програмний інтерфейс для маніпулювання базою знань та оцінки ризиків на основі даних бази знань і результатів анкетування. Інтерфейсний

додаток для створення і заповнення анкет користувачів і генерації звітів за результатами оцінки ризиків.

У методі RiskWatch як показники для оцінки та управління ризиками використовуються прогнозовані середньорічні втрати (Annualized Loss of Expectancy, ALE) та оцінка повернення від інвестицій (Return on Investment, ROI).

Отже, можна зробити висновок, що можуть застосовувати комбінований підхід як найкращий підхід до оцінки ризиків інформаційної безпеки. Цей підхід включає в себе використання набору методів аналізу ризиків, що складається з методів, які найкраще підходять для конкретних областей конкретної організації. Наприклад, метод Дельфі добре підходить для CRAMM, оскільки він дозволяє враховувати специфіку конкретного об'єкта. Це дозволяє підвищити точність оцінки ризиків інформаційної безпеки за рахунок обліку всіх характеристик інформаційної системи. Тому розглянуті загальні методи аналізу ризиків можуть бути успішно застосовані до інформаційної безпеки, якщо їх адаптувати і вдосконалити.

Список використаних джерел:

1. Соціальна інженерія // Вікі-знання/Тернопіл. нац. техн. ун-т ім. Івана Пулюя. URL: http://wiki.tstu.edu.ua/Соціальна_інженерія.

СПОСОБИ ВИЯВЛЕННЯ SQL-ІН'ЄКЦІЙ

Васильєв Б. Г.

студент 1-го курсу магістратури
факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»

Перші відомості про SQL-ін'єкцію з'явилися у відкритому доступі в статті «Вразливості вебтехнологій NT», опублікованій ще в 1998 році. З 2000 року дану техніку почали широко застосовувати кіберзлочинці для взлому інтернет-сайтів. Сьогодні є багато технік експлуатації SQL-ін'єкцій для різних СКБД та застосунків на їх основі. За минулі кілька років, атаки, які були спрямовані на різні Web застосунки вимагали особливої уваги з боку захисного персоналу [1]. Все це відбувається через те, що наскільки б сильним не був між мережний захист або наскільки старанно б не латали "дірки" в існуючих програмах, все одно може статися, що розробники ПЗ не досить добре захистили свої програми, і зловмисники можуть використовувати це для злому порту. Існує два найбільш частовикористовуваних методів для нападів: SQL ін'єкція і міжсайтовий скріптніг.

SQL ін'єкція належить до методики вставки мета-симолів і SQL команд в поля введення на Web сторінках, у результаті чого відбуваються зміни виконання кінцевих SQL запитів [2, 27]. Такі напади в основному спрямовані на Web-сервера. Принцип дії міжсайтового скриптингу полягає у використанні