УДК 004.056.52

О.А.Суліма, Київ

АНАЛІЗ МЕТОДІВ ОЦІНОК РІВНЯ БЕЗПЕКИ ДОСТУПУ ДО ДАНИХ

Abstract. Analysis of assessment methods safety. One of the widespread estimates is estimate using idea of reduce the risk of system security. Also widely methods used based on the use of expert opinion.

Актуальність

В роботах [1 – 3] обґрунтовано актуальність, поставлено та розв'язано задачу, розроблення технології адаптивного захисту систем доступу до мережевих інформаційних ресурсів. Основу технології складають модельні описи поточної поведінки споживачів послуг комп'ютерної мережі та методи динамічного налаштування параметрів систем захисту інформаційних ресурсів для підтримки бажаного рівня їх захищеності від шкідливих дій споживачів.

Актуальною є задача розширення функціональних можливостей даної технології за рахунок аналізу методів оцінок рівня безпеки доступу до даних**.**

Постановка задачі

Системи захисту доступу до баз даних, чи до інформаційних систем завжди забезпечують певний рівень захисту, який є достатнім для окремої системи. Не існує, в даному випадку розподілу на системи захищені, або не захищені. Це обумовлюється наступними факторами та особливостями:

- різні системи даних, інформаційні системи можуть вміщати дані, які мають різні міри значимості або різні міри їх важливості по відношенню до заданого критерію такої значимості;
- засоби захисту доступу до системи в залежності від міри захисту, яку вони забезпечують, мають різну вартість, яка вимірюється, що найменше, величиною обчислювальних ресурсів, які є необхідні для реалізації того, чи іншого рівня захисту;
- захист, крім забезпечення санкціонованого доступу до даних, забезпечує можливість довготривалого зберігання відповідних даних, що в більшості випадків не приймається до уваги, при дослідженні систем захисту доступу.

Здійснимо аналіз методів оцінок рівня безпеки доступу до даних.

Вирішення задачі

Будь-яка інформаційна система має певний рівень захисту навіть у тому випадку, коли, при проектуванні системи не розглядалась задача формування окремих засобів захисту.

Така ситуація має місце завдяки тому, що базові засоби, з яких складається система, наприклад, операційна система, чи стандартна система бази даних, мають засоби захисту, що закладаються, при їх проектуванні,

незалежно від того, чи потенціальний користувач потребує, чи не потребує захисту, у відповідності з поданою ним декларацією про необхідні параметри системи [1].

Кожна система, як деякий продукт, повинна забезпечувати задану міру надійності [2]. В рамках цього параметру не виділяються причини, через які система перестала працювати. Серед можливих причин відмови системи, важливе місце займає причина, що полягає у вразливості системи на зовнішні атаки. Виявлення і протидія таким атакам є безпосередньою задачею системи захисту, яка в тій, або іншій мірі повинна бути реалізована в рамках довільної інформаційної системи.

Приведений аналіз ілюструє необхідність розв'язана наступних задач при проектуванні державної інформаційної системи (*DIS*):

- визначення рівня безпеки функціонування системи, або здійснення оцінки рівня безпеки системи
- створення в рамках системи, або у вигляді незалежної компоненти системи захисту
- прогнозування зміни рівня безпеки системи з ціллю упередження можливої відмови системи
- створення засобів управління рівнем захищеності системи в процесі її функціонування.

В даному випадку більш детально зупинимося на методиці оцінки величини безпеки системи. У зв'язку з використанням уявлень про надійність системи та ряд інших понять та характеристик, зміна значень, яких проявляється таким чином, які є подібним до прояву зниження рівня безпеки системи, необхідно мати можливість виявляти причини проявів тих чи інших відхилень. Тому, приймемо, що рівень безпеки зменшується в результаті успішної дії зовнішніх атак на систему. Це означає, що система повинна в своєму складі мати засоби для виявлення таких атак. Завдяки таким засобам, є можливим інтерпретувати зміну стану системи, як зниження текучого рівня безпеки системи. Оскільки прояв дії атак на систему не обов'язково полягає у відмові останньої, а може полягати у негативній зміні параметрів функціонування системи, то доцільно зниження рівня безпеки оцінювати в одиницях, які характеризували б вплив змін в системі на параметри, що характеризують зменшення показників якості функціонування.

Для випадку, коли об'єктом небезпеки є *DIS*, приймаємо, що експерти, які працюють з системою, можуть встановити шкалу зниження рівня якості їх функціонування, а фахівці з питань безпеки реалізують співставлення, в рамках шкали якості, різним значенням якості різні рівні безпеки, якщо таке зниження рівня якості обумовлюються зовнішніми атаками.

Існуючі методи оцінки рівня безпеки орієнтовані на можливість їх використання для широкого класу інформаційних систем. Тому, в таких підходах закладаються деякі загальні ознаки змін в процесі функціонування і на основі таких загальних ознак формуються моделі оцінки рівня безпеки.

Досить поширеним підходом до визначенні оцінки рівня безпеки є

підхід, в якому приймаються наступні тези. Перша теза полягає у тому, що зовнішня атака на *DIS* , виникає у випадкові моменти, а характер діючих атак змінюється в залежності від успішності, чи не успішності дії попередньо ступеня атак. Це означає, що на початку процесу функціонування *DIS* , рівень безпеки *RB* (*DIS*) приймає значення 100%.

В залежності від кількості успішних атак, *RB* може знижуватися. Якщо значення величини *RB* пов'язувати зі зниженням якості функціонування *DIS* , то такі дані задають фахівці, що експлуатують *DIS*. У відповідності з оцінкою фахівців, встановлюються відповідні величини текучого рівня безпеки в процентах. Наприклад, зниження рівня безпеки на 30% приведе до того, що текучий рівень безпеки стає рівним 70%. Таким чином, одна з моделей оцінки рівня безпеки може полягати у прогнозуванні кількості випадків успішних зовнішніх атак по відношенню до *DIS*. В такому підході, умовно приймається, що кількість атак впливає на величенну зміни рівня безпеки. Досить поширеною оцінкою величини зміни рівня безпеки функціонування *DIS* є величина ризику того, що система відмовить у обслуговуванні користувачам [3]. В залежності від інтерпретації всіх факторів, що входять в склад моделі, в даному випадку моделі ризику, який прийнято позначати *R* , стає можливим визначити деяку величину, яка допускає інтерпретацію зниження рівня безпеки *R* для системи *DIS*. В рамках такого підходу, зміна величини *R* залежить від параметрів потоку атак $A\{z_i\}$, що подаються на *DIS*. Для того, щоб зміну величини *R* можна було інтерпретувати відповідними змінами в *DIS*, необхідно реалізувати моделювання дії різних атак на систему, що є досить громіздким та потребує значних затрат. Для вирішення цієї проблеми на рівні експертних оцінок встановлюються різні рівні зниження рівня безпеки у процентних величинах. Наприклад, може бути прийнято, що коли рівень безпеки *RB* знизився на 50%, то необхідно переходити до рівня моделювання дії атак на об'єкт, щоб можна було активізувати необхідні функції протидії атакам.

Оскільки, в даному випадку, мають місце дискретні процеси, то прикладом дискретної динамічної моделі визначення величини ризику може служити наступне співвідношення [4] $R(t) = r + ct - \sum_{i=1}^{N(t)} y_i$, де $R(t)$ величина текучого значення ризику, *r* -величина, що відображає початковий потенціал можливостей засобів захисту, *c* - коефіцієнт, що відображає інтенсивність виявлення атак, *N(t)* - точковий процес, що визначає моменти успішних дій атак, *y* - величини їх ефективності, що визначають ефект негативного впливу на систему захисту. Всі приведені інтерпретації змінних, що використовуються в приведеній моделі, потребують досить детального узгодження з конкретною реалізацією інформаційної системи, стосовно якої може використовуватися приведена модель. Оскільки формула вище використовує дані, які накопичуються в процесі функціонування об'єкту захисту і, по суті, представляють собою статистичні дані відповідного типу, то для практичного використання цієї моделі, необхідно зібрати статистичні

дані, на основі яких можна було б сформувати величини значень компонент, що входять у приведену модель.

Крім того, необхідно обґрунтувати характер розподілу випадкових величин, що особливо стосується точкового процесу виникнення зовнішніх атак *N(t)* та величин y_i, які визначають ефективність дії кожної окремої атаки з процесу *N(t)*.

Структура приведеної моделі відображає прийняту спрощену інтерпретацію процесу реакції, або взаємодії *DIS* з зовнішніми атаками, яка може в окремих випадках відрізнятися від реальних залежностей, які використовуються в моделі.

Таким чином, приведена модель, для її використання, потребує суттєвих досліджень, в результаті яких можуть бути отримані дані, які необхідні для практичного обчислення оцінки величини ризику зміни рівня безпеки в результаті дії на *DIS* деяких зовнішніх атак.

Існують інші підходи до визначення величини ризику зміни рівня безпеки, або для визначення текучого значення величини безпеки системи. Один з таких підходів ґрунтується на експертних даних, які практично є деяким узагальненням статистичних даних про вплив різних параметрів на величину того ризику, який відповідає тому, чи іншому рівню безпеки. На відміну від ймовірнісних моделей, модель, що ґрунтується на експертних даних є більш проста з точки зору її використання, а використання експертних даних виключає необхідність проводити додаткові дослідження для виявлення елементів, що входять в склад ймовірнісної моделі.

Підходом, який ґрунтується виключно на експертних даних, є метод, що передбачає декларування областей значень всіх параметрів, що використовується для визначення величини ризику. При цьому, сама величина ризику також декларується по відношенню до встановлених діапазонів значень параметрів, що його визначають. Прикладом такого підходу може служити наступне [5].

Приймаються наступні параметри та їх значення:

параметр вартості засобів, що оцінюються в масштабі умовно вибраних числових значень від 0 до 4,

встановлено три рівні загроз, які визначаються як низький рівень загроз, середній рівень загроз, та високий рівень загроз;

визначена, або прийнята шкала міри піддатності засобів, яка визначається для кожного рівня загроз окремо шкалою, що складається з трьох діапазонів «низька піддатність», «середня піддтаність та висока піддатність» засобів по відношенню до можливих атак, або негативних зовнішніх впливів;

кожній можливій позиції піддатності засобів, для відповідного рівня загроз, окремо для кожного рівня ціни засобів захисту, приймається певна величина ризику, яка задається на множині цілих чисел.

При визначенні рівня загроз експертами, приймаються до уваги наступні

фактори.

1. При здійсненні цільової атаки, яка реалізується несанкціонованою особою, аналізується наступне:

- оригінальність засобу, який наражається на атаку;
- легкість заміни отриманого засобу на очікувану вигоду від реалізації такого втручання;
- технічний рівень, що визначає можливість несанкціонованої особи успішно реалізувати своє втручання в роботу системи з ціллю отримання відповідного засобу або інформації.

2. Можливість виникнення загрози (з точки зору ймовірності такої події).

3. Вразливості або піддатності окремих засобів на несанкціоноване технічне і нетехнічне використання засобів системи та інші.

Перший і другий фактори є очевидними. Третій фактор полягає в наступному. Під вразливістю, в даному випадку, розуміється можлива міра втрат від несанкціонованого втручання. Під піддатністю розуміється міра складності реалізації послідовності дій зі сторони несанкціонованих факторів, які необхідно реалізувати, для успішного здійснення атаки на систему.

Якщо атака здійснюється з цілю отримання з системи даних, то міра піддатності відповідних компонентів системи може бути така, що досить виявити ключ доступу до даних, щоб їх можна було не санкціоновано отримати. Це ілюструє одну міру піддатності. Може мати місце ситуація, коли, для того, щоб отримати можливість доступу до даних, необхідно, спочатку впровадити в систему «троянського коня», в якому можуть розміщатися інтрузи, які, при виникненні певних умов в системі, можуть активізуватися і, наприклад, зчитати відповідну інформацію і тільки після того несанкціонований користувач, або атака зможе отримати відповідні дані.

Очевидно, що другий випадок ілюструє нижчу піддатність системи на спроби несанкціонованого доступу до даних системи.

Величина ризику також задається у вибраному діапазоні чисел, наприклад, в діапазоні [0,8].

В рамках такого підходу, для кожного засобу оцінюється зв'язана з ним піддатність та відповідна загроза. На основі приведених даних будується таблиця в першому рядку якої записується рівень загрози. В другому рядку таблиці записується рівень піддатності, для кожного рівня загрози. Таким чином, якщо рівнів піддатності є *K*, то, для кожного рівня загрози, вказуються всі *K* рівнів піддатності. Таким чином, в таблиці отримуємо $n = k \cdot m$ стовпців, де m- кількість рівнів загрози. В рядках цієї таблиці розміщаються рівні вартостей засобів, до яких може отримати доступ інтруз, під яким розуміється несанкціонований користувач чи атака. Наприклад, якщо вартість засобу є найвища, рівень загрози є найвищим, і рівень піддатності відповідних засобів, є найвищим, то і величина ризику є найвища. Цей факт

відображається шляхом запису відповідної величини ризику в клітині таблиці, яка знаходиться на перетині рядка і стовпця, що вибираються по приведених вище ознаках. Це означає, що найвищий ризик може існувати лише при визначених умовах. Всі інші величини ризиків, що розміщаються в інших клітинах таблиці визнаються на основі значень вартості інших засобів міри загрози та міри піддатності відповідний засобів.

Очевидно, що ці величини вибираються експертними методами. Слід відмітити, що найменша величина ризику, наприклад, рівна нулю також може бути тільки в одній клітині відповідної таблиці.

Методи аналізу ризику повинні давати відповіді на цілий ряд питань, які безпосередньо пов'язані з безпекою інформаційної системи. Прикладом таких питань може служити питання [6], які загрози є найбільш небезпечними для зниження рівня безпеки та значимість втрат від таких загроз.

Для відповіді на це питання досить просто сформувати відповідну таблицю, якщо користуватися експертними даними, оскільки вони є найбільш повні, по визначенню, з точки зору інформації, яку вони можуть надавати. В цьому випадку, можна побудувати таблицю, в кожному рядку якої описується небезпека, що буде складати перший стовпчик таблиці. В другому стовпчику таблиці описується вартість наслідків дії загрози, які визначаються експертним способом.

В третьому стовпчику записується величина загрози, або рівень загрози, який обумовлюється відповідною небезпекою. Ці величини також визначаються експертним способом. Тоді, величину ризику по відношенню до типу небезпеки, можна визначати, як результат множення величини втратна величину загрози. Оскільки величини загрози є безрозмірна, то величина ризику буде вимірюватися в коштах, в яких вимірюється величина втрат від успішної дії окремої небезпеки. По величині ризику можна встановити ранг різних небезпек, з точки зору їх дії на систему.

При проектуванні інформаційних систем, важливим є врахування всіх аспектів виникнення ризику по відношенню до окремої системи. Оскільки приймається, що будь яка інформаційна система може піддаватися тим, чи іншим атакам, то доцільно встановити величину ризику, яка уже існує в середовищі незалежно від того, чи певна інформаційна система уже реалізована чи ні.

Це означає, що слід розділити ризики, що найменше на дві категорії: уже відомі можливі ризики, які обумовлюються атаками, що активізуються по відношенню до цих систем і з великою ймовірністю будуть активізуватися по відношенню до системи, що створюється, та ризики, які можуть повстати в процесі функціонування окремої системи, що обумовлюються особливостями самої системи та характером даних, які передбачається розміщати в системі. Необхідність в такому розподілі типів ризику обумовлюється тим, що будь-яка інформаційна система повинна мати певний рівень захисту від самого початку свого функціонування. Це обумовлюються тим, що будь яка інформаційна система, що проектується, є орієнтована на певний клас задач,

розв'язок яких система повинна забезпечувати.

Результат розв'язку довільної задачі може представляти собою продукт, який має певну вартість, більше того, коли системи використовуються для задач, що орієнтовані на обслуговування соціального середовища, то існують відповідні закони, що до інформації соціального характеру, які необхідно враховувати, при побудові інформаційних систем. Прикладом такого закону може служити закон про захист персональних даних.

Крім приведених аргументів, при побудові інформаційних систем, необхідно приймати до уваги міжнародні стандарти, які визначають вимоги по захисту інформації та вимоги по безпеці відповідної інформаційної системи. Такі вимоги є обов'язковими до врахування, оскільки вони сформовані у вигляді стандартів по безпеці інформаційних систем [7].

Стандарти, що орієнтовані на розв'язок задач захисту інформаційних систем, в першу чергу, регулюють термінологію, яка використовується в галузі захисту інформації. Крім того, в стандарті визначаються базові елементи, які означають компоненти, що повинні формуватися для того, щоб забезпечувати відображення всіх вимог стандарту до інформаційної системи. До таких компонентів відносяться наступні:

- задачі захисту;
- профілі захисту;
- проект захисту.

Профіль захисту представляє собою нормативний документ, який описує сукупність задач, які необхідно вирішувати в рамках інформаційної системи.

Профіль захисту досить часто називають профілем безпеки системи. В ньому, крім самих задач захисту, приводяться вимоги безпеки по відношенню до визначеної категорії інформаційного продукту або інформаційної технології. Але в цьому документі не приводяться засоби реалізації необхідного захисту.

Проект захисту вміщає опис засобів захисту та обґрунтування їх використання [8]. Структура профілю безпеки вміщує цілий ряд вимог, яким повинна відповідати система захисту. Профіль безпеки системи, як правило, орієнтований на конкретний тип системи. Тому немає необхідності кожний раз проектувати новий профіль.

Висновки

Проведений аналіз методів оцінки рівня безпеки до даних, завдяки чому з'явилась можливість кількісно оцінювати небезпеку і відповідно необхідний рівень безпеки, які забезпечуються певними засобами захисту системи.

Однією з поширених оцінок є оцінка, що використовує уявлення про ризик зниження рівня безпеки системи. Також широко використовуються методи, що ґрунтуються на використанні експертних оцінок. В більшості з них, в якості експертів використовуються фахівці, які можуть оцінити рівень вразливості окремих засобів, можливість виникнення загрози та інші фактори.

1. *Davydenko A.* Formalization level of abstraction of state information resourses access systems / A. Davydenko // Scientific letters of academic society of Michel Baludansky, ISSN 1338-9432. Volume 4, 1 2016, p.35-38.
2. *Давыденко А.Н.* Расширение теоретических возможностей математических моделей нейронных сетей обуславливаемых их использованием для решения задач защиты систем доступа / А.Н. Давыденко // Збірник наукових праць Інститут проблем моделювання в енергетиці НАН України : Зб. наук. праць вип. 45.. – К., 2008,– С. 112-115.
3. *Давыденко А.Н.* Анализ основных информационных компонент систем доступа / А.Н. Давыденко // Моделювання та інформаційні технології: Зб. наук. праць вип. 59. – К., 2011, – С.11-20
4. *Ильинская Е.В.* Теория риска и перестрахование. Часть 1. Упорядочение рисков / *Е.В Ильинская* – М.: МГУ, 2001.
5. *Бенинг В.Е.* Введение в математическую теорию риска / *В.Е. Бенинг, В.Ю. Королев* – М.: МАКС-Пресс, 2000.
6. *Морозов А.Д.* Введение в теорию фракталов / А.Д. Морозов. – М.: Ижевск, 2002.
7. *Лейбин В.М.* Информатизация и системне исследования / В.М. Лейбин. – М.: Книжный дом «ЛИБРОКОМ», 2009.
8. *Столинг В.* Основы защиты сетей. Положения и стандарты / *В. Столинг* – М.: Издательский Дом «Вильямс», 2002.

Поступила 20.04.2017р.

УДК 004.94

О.С.Гайденко, Г.М.Голуб, Київ

ХАРАКТЕРНІ ОСОБЛИВОСТІ МОДЕЛЮВАННЯ СИСТЕМИ ТА ПРОЦЕСІВ ТЯГОВОГО ЕЛЕКТРОПОСТАЧАННЯ ЗАЛІЗНИЦЬ ЯК ОБ'ЄКТА МОНІТОРИНГУ І КЕРУВАННЯ

Abstract. The role of monitoring in modeling and its features are considered. The paper analyzes the factors that have a direct or indirect impact on the system of the traction power supply load is conducted. Taking into account these influences and relationships between the factors useful in modeling power consumption as the main process of the system.

Постановка проблеми

Автоматизовані процеси, що складають ланцюг «моніторинг – аналіз – управління» обумовлені широким розповсюдженням мікропроцесорної техніки в системі електропостачання. Згідно тенденцій останнього часу вони використовуються для найрізноманітніших функцій: діагностики та прогнозування відмов обладнання, прогнозування виникнення аварійних ситуацій та електроспоживання, оптимізації процесу прийняття рішень та інших функцій управління, тощо.

