УДК 004.921

Л.Є.Шведова

УПРАВЛІННЯ ЗАХИСТОМ ДОСТУПУ ДО ІНФОРМАЦІЙНИХ СИСТЕМ

Процеси управління захистом доступу до інформаційних систем в кожному окремому випадку повинні відображати особливості кожної конкретної інформаційної системи. Відповідні особливості дозволяють визначитися з такими параметрами, які можуть використовуватися для оцінки рівня безпеки та оцінки величини ризику використання тієї чи іншої послуги з тих, що надає інформаційна система та визначатися з цілим рядом інших вимог до системи захисту. Будь-яке управління системою захисту потребує певних критеріїв, завдяки яким можна сформувати цілі управління таким чином, щоб їх опис дозволив формувати конструктивні алгоритми забезпечення необхідного рівня безпеки. Це означає, що формування цілі управління безпеки, що полягає у забезпеченні максимальної безпеки інформаційної системи не доцільно. Тому розглянемо ряд критеріїв та вимог до системи захисту на основі яких визначимося з факторами, що впливають на зміни значень відповідного рівня безпеки інформаційної системи. До таких критеріїв, вимог та факторів можна віднести:

- шкалу вимірювання рівня захисту, що визначається реальними потребами прикладних задач, або прикладної системи, яка реалізується в середовищі відповідної інформаційної системи (IS);
- інтерпретацію поняття про ризик того, що система не забезпечить необхідного рівня захисту прикладній системі, реалізованій в середовищі IS;
- необхідно окреслити клас типів небезпек та загроз, найбільш характерних для відповідних прикладних систем (PS);
- вимоги до методів реалізації процесу управління захисту доступом до PS;
- вимоги до просторової організації PS в рамках засобів захисту доступу до відповідного інформаційного середовища у якому функціонує PS;
- критерії розвитку системи засобів захисту, що зумовлюються розвитком PS, яка обслуговується відповідною системою захисту (SZ) в середовищі IS;
- можливістю реалізації процесів адаптації SZ, до зміни умов функціонування PS і відповідно SZ, що зумовлюються факторами, які не передбачувались проектами PS та SZ і плановими модифікаціями, що виникають у зв’язку із зміною вимог до PS.

Наведені фактори можуть бути розширеними, але кожний з них має досить широку інтерпретацію як у рамках PS і PZ, так і в рамках IS. Завдяки цьому, можна обмежитися даними факторами, оскільки можливі аспекти, що

носять менш загальний характер, які могли б виникнути у процесі дослідження методів управління системою захисту доступу (SZD), було би можна враховувати у рамках вищенаведених факторів.

Розглянемо детально кожний з наведених факторів та проаналізуємо історичний стан розв'язку задач, визначених відповідними факторами. Вимірювання рівня захисту, який повинна забезпечувати відповідна прикладна система є досить складною задачею. На сьогодні для її розв'язку використовується ряд моделей прикладом яких можуть бути такі моделі: модель Bella-Lapaduli, модель Biby [1]. Для оцінки рівня захисту в моделях такого типу використовуються оцінки, які за своєю природою є дискретними і запозичені з системи охорони таємниць, яка використовувалась без участі інформаційних комп'ютерних систем. Прикладом оцінок рівня захисту у таких системах є декларовані значення величин, що позначалися як рівень персональної таємниці, рівень таємниці, рівень надзвичайної таємниці, що відповідає відомим способам позначення: ДСК – для службового використання, Т – таємна інформація, НТ – надзвичайно таємно. Інтерпретація оцінок визначає природнім чином ієрархію міри захисту, яку кожна з цих оцінок вимагає і може бути представлена співвідношенням: ДСК<Т<НТ.

Очевидно, що для оцінок необхідного рівня захисту PS чи певних даних в IS також можуть бути запропоновані інші інтерпретації. Якщо прийняти до уваги, що бізнесові структури потребують значно більше зберігати таємниці, пов'язані з їх діяльністю, то можна прийняти наступне:

— шкала для вимірювання необхідного рівня захисту може бути значно детальнішою, ніж шкала у вищенаведеному прикладі;
— інтерпретація окремих, дискретних величин необхідного рівня захисту може бути зведена до величини втрат, до яких може призвести порушення відповідного рівня захисту PS;
— вимоги до контролю реального рівня безпеки PS, можуть визначатися у залежності від характеру задач, які розв'язуються у PS.

Один із способів реалізації такої шкали може полягати у наступному. Будемо вважати, що у рамках PS можна диференціювати витрати втрати з дискретністю в ΔV і для зручності будемо їх обчислювати у величині коштів відповідних втрат. Такий підхід досить поширений у сфері бізнесу. Якщо максимальна величина втрат власника PS становить $V\max$ коштів, то масштаб вимірювання можливих втрат є ΔV, а шкала для вимірювання рівня безпеки PS в одиницях коштів може бути представлена у вигляді:

$$SR = \left[V\min \to \left(v\min + \Delta V \right) \to ... \to V_i \to ... \to V\max \right]. \qquad (1.1)$$

Очевидно, що така шкала може бути лінійною чи ні, або може описуватися тією чи іншою дискретною функцією.

Важливим аспектом введення шкали рівня захищеності є встановлення зв'язку між шкалою необхідного рівня захисту в інтерпретації PS з відповідними можливостями SZ. Відомо, що можливості SZ визначаються засобами захисту, що формують відповідну SZ. Приймемо, що використання

засобу Z_i в SZ потребує реалізувати затрати w_i. Відомо також, що різні засоби захисту потребують різних затрат w_j. Якщо відповідні затрати визначати у вигляді *i*-коштів, то можна встановити деяку шкалу вартостей окремих елементів засобів захисту, з яких компонується SZ. У більшості випадків існує ситуація, коли величина w_i пов'язана з певною величиною або певними можливостями окремого z_i. Різні типи також орієнтовані на різні класи небезпек. Тому доцільно величини w_i розділити на множини або класи, які відповідають різним z_i. Така класифікація не може бути абсолютно точною, оскільки, на практиці використання засобів захисту одного класу, може реалізовуватися відносно небезпек, які в більшій мірі можна віднести до класу інших засобів захисту, орієнтованих на протидію відповідним небезпекам. У рамках даної роботи не враховуватимемо цю особливість і приймемо, що кожен клас небезпек відповідає окремому класу засобів захисту. Тоді шкали SK із співвідношення (1.1) можна сформувати для кожного класу z^j, який включає окремі засоби z_i^j. Такий підхід дозволяє встановити певні зв'язки між рівнем захисту від небезпек певного типу та засобами захисту, які у першу чергу орієнтовані на протидію відповідному класу засобів захисту. Такий зв'язок ґрунтується на співставленні чи порівнянні вартостей v_i та w_i з різних шкал. Зрозуміло, що коли $v_i < w_i$, то відповідний засіб захисту $z_i\left(w_i\right)$ використовувати недоцільно. Якщо виявиться, що $v_i > w_i$ то необхідно провести аналіз чи вистачить можливостей $z_i\left(w_i\right)$ для забезпечення рівня захисту V_i. На основі такого аналізу реалізуються управляючі дії відносно SZ. Якщо відповідні z_i^j допускають параметричне регулювання то така управляюча дія носить неперервний характер. Коли ж z_i^j не допускає параметричного управління, то відповідна управляюча дія носить дискретний характер і може полягати у заміні одного екземпляра z_i^j на інший. Очевидно, що відповідне управління не може бути реалізоване у момент виявлення необхідності здійснення відповідного управління. У зв'язку з цим, виникає необхідність визначати величину ризику процесу функціонування PS в умовах, коли рівень захисту понизився і не відповідає необхідному рівню захисту PS, а система управління не може оперативно прореагувати або реалізувати відновлення захисту вхідного рівня. Задачі визначення величини ризику виникають не тільки у випадку вищенаведеної ситуації, але й в інших випадках і у кожному із них виникає необхідність формувати індивідуальну інтерпретацію всіх можливих ситуацій та особливостей. Результатом такого підходу є те, що методи моделювання величини ризику вибираються таким чином, щоб вони були універсальними. Це, в свою чергу, призводить до неефективності використання

відповідних моделей і отримані результати можуть не відповідати реальній ситуації. Тому формування різних інтерпретацій величини ризику і, відповідно, використання різних моделей визначення його величини є більш доцільним. Розглянемо можливі типи інтерпретації ризику, які можна сформувати в рамках задач захисту інформаційних систем.

Перший тип інтерпретації ризику описує випадок, коли певні засоби захисту, що орієнтовані на визначені загрози та небезпеки знижують, або втрачають свої можливості із забезпечення початкового рівня безпеки. Таке зниження рівня безпеки може виникнути в тому випадку, коли певний рівень через різні причини був задекларований і поки ситуація, що формується в мережі і безпосередньо стосується відповідного z_i не вимагає від z_i виявлення задекларованого рівня, більшого від β_i на попередньому інтервалі часу, або $\beta_i < \beta_j \le \beta \max$. У цьому випадку величину ризику доцільно моделювати таким чином, щоб у відповідній моделі враховувались не тільки наслідки зміни β_i для PS, або окремої її компоненти, а й фактори, що призвели до виникнення такої ситуації. До вказаних факторів слід віднести:

— причини виникнення змін рівня безпеки в мережі, які в першу чергу можуть являти собою небезпеки відносно PS або PSi;
— зміна умов розв'язку задачі, яку необхідно розв'язати чи яка розв'язується в PS, що призводить до зміни вимог, які ставляться до рівня безпеки.

Другий тип інтерпретації ризику розв'язку задач в PS описує випадки, коли не існує однозначного алгоритму розв'язку задачі і тому не існує гарантії, що результат розв'язку буде адекватний очікуваним результатам. Це пов'язано з тим, що в процесі розв'язку можуть появитися додаткові дані, які треба було врахувати перед початком процесу розв'язку задачі. Відсутність достатньо повних і об'єктивних даних про задачі, які передбачається розв'язувати є досить поширеною причиною існування ризику. Ця причина безпосередньо не пов'язана з проблемами захисту від факторів, що по своїй природі не мають відношення до предметної області задачі. Тому їх не будемо більш детально розглядати.

Третій тип інтерпретації ризику, що може виникнути в процесі розв'язку задач описує коректність алгоритмів їх розв'язку, достовірність методів, що використовуються для побудови алгоритмів розв'язку. Це особливо актуально в тому випадку, коли засобами розв'язку задач є не тільки універсальні засоби, прикладом яких може бути IS, але й цілий ряд спеціалізованих засобів, якими можуть бути ті чи інші фізичні об'єкти.

Всі наведені типи інтерпретації ризику описують причини виникнення факторів, що його зумовлюють. У багатьох випадках наслідком виникнення ризиків є збитки, яких зазнає автор чи замовник задачі, яку передбачається розв'язати. Але це не єдина можлива інтерпретація втрат до яких може призвести існування ризику. Втрат від виникнення недопустимо високого

результату дії ризику, може зазнати не тільки власник чи замовник задачі, розв'язок якої зумовив виникнення таких втрат, але й інші представники оточення в рамках якого відповідна задача розв'язувалась. Така інтерпретація ризику потребує уявлення про підсилювання значимості небезпеки, що може зумовлюватися задачею, розв'язок якої може призвести до виникнення втрат, що визначаються величиною ризику. В цьому випадку приймається, що фрагмент середовища, в якому знаходиться замовник задачі, включає все оточення, а елементи, що в це оточення входять є між собою рівноправними з точки зору втрат, яких вони можуть зазнати. Таким чином, відповідне оточення являється підсилювачем наслідків дії відповідних факторів і величина ризику не залежить від відповідних факторів і величина ризику не залежить від інших причин , підсилюється в m разів, де m-кількість членів відповідного оточення. Ця обставина є досить важливою, оскільки при визначенні величини ризику у класичних підходах у більшості випадків обмежуються втратами, що можуть понести лише замовники задач, або об'єкти відносно яких розв'язується та чи інша задача. Це є досить важливим аспектом і для задач захисту інформації в системах типу IS він вказує на необхідність не тільки визначати втрати безпосередньо власника відповідної інформації, але й втрати тих учасників, які також є власниками втраченої інформації, які довірили її третій стороні. Важливість цього аспекту для SZ полягає у тому, що методи протидії атакам ґрунтуються на основі аналізу таких обставин:

— типу атаки та способу її реалізації;
— на основі аналізу величини ризику успішної дії атаки;
— на основі прогнозування можливих атак, які ініціюють відомі небезпеки.

Аналіз типу атаки та способу її реалізації дозволяє SZ виявити атаку та протидіяти її в штатному режимі, у якому не передбачається переривання процесу функціонування PS [3]. Розрахунок величини ризику ініціюється тільки в тому випадку, якщо в системі відбуваються події, які зумовлюють можливість порушення штатного режиму роботи PS. Прикладами таких подій можуть бути події, пов'язані з реєстрацією успішних атак на систему, виявленням загроз в системі та плановим контролем інформації та об'єктів PS, в результаті якого виявились факти недопустимих змін у них. Моделі обчислення ризику, що повинні використовуватися в SZ складаються з таких компонент:

— формування значення величини ризику на основі аналізу причин виникнення ризикованих ситуацій в IS;
— виявлення підсилювачів ризику у предметній області, до якої відносяться втрати, що обчислюються як величина ризику;
— формування, або виявлення, додаткових типів інтерпретації факторів, що зумовлюють виникнення ризикованої ситуації.

Управління захистом залежно від величини ризику та характеру його причин, може полягати не тільки у модифікації існуючих засобів захисту, а й

у впровадженні нових z_i. У випадку, коли величина ризику R перевищує певний поріг D_R, то SZ може перервати процес функціонування PS, або його заборонити в цілому. Для оцінки величини R важливою обставиною є виявлення міри розповсюдження ризику в IS в результаті його активізації при локальному проявленні. Ця проблема потребує окремого дослідження і тому її в рамках цієї роботи розглядати не будемо.

При дослідженні систем захисту та засобів захисту, в більшості випадків приймається, що небезпеки, існуючі відносно об'єктів,які необхідно захищати, є універсальними і можуть ініціювати довільного типу атаки [4]. При більш детальному аналізі небезпек виявляється не все виглядає саме так. Це зумовлюється такими причинами:

— будь-який об'єкт, що може бути атакованим, має певні особливості, які визначають відповідний характер атак, що можуть ініціюватися небезпеками;
— небезпеки не являють собою деякі абсолютно універсальні фактори, які не мають окремих зацікавлень відносно PS;
— небезпеки в основному формують ті чи інші фахівці, які мають певну інформацію про PS і відповідні SZ, тоді IS, які використовуються певним типом PS та володіють необхідним програмно-апаратним інструментарієм, за допомогою якого можна реалізовувати послідовність дій відносно PS;
— кожна небезпека активізує певну атаку на PS тільки в тому випадку, якщо вона може сформувати відповідну ціль для такої атаки тощо.

Згідно вищевказаного можна стверджувати, що засоби захисту, відомі на сьогодні, і які можна спроектувати, можуть бути класифікованими таким чином, що класи засобів захисту будуть відповідати певним класам атак, а через них відповідним небезпекам. При цьому, посередниками в цьому зв'язку є в першу чергу загрози різних класів, а в другу – різні типи атак. Це дозволяє сформувати методику для кожної PS з врахуванням особливостей IS і таку систему захисту SZ_i, яка б повністю відповідала вимогам до відповідних Z_i і SZ в цілому. Виходячи з цих положень, являється більш оптимальним не використовувати як можна більш загальні за своєю суттю Z_i, а використовувати функціонально орієнтовані Z_i, які є більш простими у випадку коли необхідно шляхом змін їх параметрів перебудовувати їх під ті чи інші особливості певного типу атак. Це дозволяє реалізовувати ефективне управління системою захисту в процесі функціонування PS в середовищі IS.

Оскільки SZ і PS є за своєю суттю дискретними системами, то доцільно формувати систему управління SZ, як дискретну. З цього випливає, що всі управляючі дії, здійснені на SZ формуються на основі аналізу певної сукупності подій. Прикладом таких подій можуть бути події, виявлення певного типу атак, реєстрації факту успішної протидії виявленій атаці, захист PS від атаки на неї тощо. Це означає, що певний синтез системи прийняття рішень та системи

реалізації тих чи інших дій, що відповідають прийнятим в першій частині системи управління (SUZ) рішенням. В загальному вигляді можна записати співвідношення: SUZ=F[SPR,SRR], кожне з рішень з управлінням SZ може являти собою певний дискретний процес, що формується системою реалізації рішень (SRR). Прикладами відповідних рішень можуть бути рішення з визначення величини ризику роботи PS з передачею управління системі прийняття рішень (SPR), рішення про призупинення процесу функціонування PS тощо. Таким чином SUZ здійснює управління не тільки SZ а й PS та IS, якщо прийняті рішення передбачають необхідність втручання у процес функціонування IS чи PS. В основному SRR орієнтована на управління SZ, яке полягає у зміні параметрів окремих Z_i у заміні одних Z_i на інші, розширенні їхнього асортименту в SZ і т.д.

Оскільки IS і в певній мірі SZ є універсальними а PS_i, що використовуються в їхньому середовищі можуть заміщуватися іншими, чи PS_i може в процесі її експлуатації модифікуватися в періоди, коли з PS_i проводяться планові профілактичні роботи, то відповідні зміни можуть бути необхідними в рамках SZ та IS. Наприклад, зміни в SZ можуть бути зумовлені змінами в PS, які призводять до змін характеру даних окремних програмних засобів чи інших компонент, які змінюють необхідний рівень їхнього захисту чи вимагають забезпечення захисту від певного типу небезпек і відповідно атак тощо. Тому система SUZ на основі аналізу таких змін повинна сформувати ті чи інші рішення про модифікацію SZ та, у випадку необхідності, про модифікацію IS. Справа в тому, що IS являє стандартне програмне забезпечення, основним елементом якого є операційна система. Різного типу операційні системи володіють різними за своїми можливостями стандартними засобами захисту, що природно використовувати у рамках всієї SZ. Тому при модифікації PS може виявитися необхідність модифікування чи заміни компоненти з IS, що приводить до необхідності інсталяції та налаштування відповідного програмного забезпечення компонент IS.

Важливою властивістю системи SUZ є її здатність реалізовувати процеси адаптації. На відміну від процесів розвитку системи, які в основному реалізуються фахівцями, вони повинні реалізовуватися автоматично на фоні процесів функціонування PS в IS. Очевидно, що адаптація в даному випадку стосується виключно системи SZ. Проблеми адаптації є досить складними і потребують окремого дослідження.

1. Теория и практика обеспечения информационной безопасности. — М. : «Агенство «Яхтемен», 1996.
2. *Мак Т.* Математика рискового страхования. — М. : Олимп-Бизнес, 2005.
3. *Столлинг В.* Основы защиты сетей. Приложения и стандарты. — М. : Изд. дом «Вильямс», 2002.
4. Атака через Internet. — СПб. : «Мир и семья», 1997.

Поступила 20.09.2010р.