замещение – М.6 Радио и связь. 1981 – 560 с.
15. *Крикавський Є.* Логістичне управління – Львів НУ «Львівська політехніка» 2005 – 604 с.
16. *Лямець В. И., Тевяшев А. Д.* Системний аналіз – Харків. ХНУРЕ. 2004 – 448 с.
17. *Василенко В. А.* Теорія та практика розробки управлінських рішень – К.: ЦУЛ 2003 – 420 с.
18. *Кузьмін О. Є. Подольчак Н. Ю., Подольчак Н. І.* Управління ризиками в іноваційній діяльності – Львів НУ «Львівська політехніка» 2009 – 176 с.
19. *Трахатуров В. М., Шевчук О. Б.* Ризики підприємницької діяльності: Проблеми аналізу – К.: Зв'язок. 2000 – 152 с.
20. *Машина Н. І.* Економічний ризик та методи його вимірювання – К. ЦНЛ. 2003 – 188 с.
21. *Жарковська Е. П., Бродский Б. Е.* Антикризисное управление – М.: Омега-1. 2007 – 356 с.
22. *Коротков Є. М.* Антикризисное управление – М.: Цифра-М. 2000 – 432 с.
23. *Пригожин А. И.* Организации: системы и люди – М.: Политиздат. 1983 – 176 с.
24. *Танаєв В., Карнаух Н.* Практическая психология управлення – М.: АСТ-ПРЕСС КНИГА, 2003 – 2004 с.
25. *Ларичев О. Н.* Теория и методи принятия решения – Москва, ЛОГОС, 2000 – 246 с.
26. *Глушков Р. М.* Введения в АСУ – К.: Техніка 1974 – 317 с.

Поступила 28.01.2011р.

УДК 004.921

Л. Є. Шведова

РОЗШИРЕННЯ МОДЕЛІ УПРАВЛІННЯ ПОВНОВАЖЕННЯМИ

Одним з основних призначень системи управління повноваженнями (*SUP*) є забезпечення певного рівня безпеки системи у вигляді функцій надання повноважень різним компонентам та системи що розв'язує прикладну задачу (*SPZ*) в рамках інформаційної системи (*IS*). Тому коротко зупинимося на відповідних аспектах уявлень про безпеку системи.

Поняття безпеки інформаційної системи є досить загальним. Тому розглянемо деякі аспекти уявлення про безпеку *IS*, що дозволить звузити дане поняття, знайти більш конструктивні підходи до визначення рівня безпеки та сформувати механізми управління рівнем безпеки. В даному випадку аналіз уявлень про безпеку буде стосуватися виключно систем, що пов'язані з управлінням повноваженнями.

В загальному уявлення про безпеку поруч з іншими підходами дозволяє розглядати її як таку, що може мати наступні форми свого прояву:

— абсолютна безпека;
— відносна безпека;

— об’єктивна безпека.

Під абсолютною безпекою слід розуміти таку безпеку, яка створюється для деякої системи незалежно від того чи діють на неї різноманітні види атак. Така безпека досягається за рахунок наступних факторів:

— повної системи контролю процесу функціонування всіх систем та компонент, що розв’язують певну прикладну задачу в деякому цифровому інформаційному середовищі або в *IS*;
— використання засобів виявлення та протидії всім відомим атакам, що можуть здійснюватися відносно системи, що захищається;
— використанням системи аналізу існуючих небезпек, які можуть виникнути в системі, що захищається, або у її відповідному оточенні.

Розв’язок вищенаведених задач в повній мірі є неможливим, оскільки за визначенням неможливо передбачити чи виявити в оточенні системи, що захищається, виникнення всіх можливих небезпек. Спроба розв’язати цю задачу в максимально можливій мірі призводить до великих затрат ресурсів *IS* та інших матеріальних затрат. Відносна безпека має місце в тому випадку, коли вибрано певний клас небезпек, які можуть уже існувати, або можуть бути створені. На основі аналізу таких небезпек формуються необхідні засоби захисту та інші підсистеми, функціонально орієнтовані на розв’язок задач захисту відповідних об’єктів. До таких підсистем, в якості прикладу, можна віднести:

— підсистему виявлення загроз в об’єкті, який захищається, оскільки загроза в даному випадку розглядається як певна властивість об’єкту захисту (*WZ*);
— підсистему виявлення атак, ініційованих небезпеками та активізованих в рамках системи, що захищається системою безпеки (*WA*);
— підсистему протидії атакам, які виявлені в системі, що захищається та елімінації загроз, які використовувались відповідними атаками (*PAZ*),
— систему управління засобами захисту, яка включає компоненти, що розв’язують цілий ряд задач пов’язаних із створенням безпеки системи, основними з яких є:
    — прогнозування ініціації атаки окремими небезпеками (*OPA*);
    — моніторинг системи, який здійснюється у відповідності з даними прогнозування про час виникнення атаки (*OMZ*);
    — задачі збільшення, або зменшення рівня безпеки системи яка захищається (*ZRB*).

Основним недоліком цього підходу є необхідність аналізу небезпек, які визначенні як такі, що можуть діяти на систему захисту шляхом активізації відповідних атак. Ця трудність зумовлена тим, що небезпеки в більшості випадків пов’язані з участю зацікавлених в атаках фахівців, а спосіб реалізації тих чи інших атак може не мати явно вираженого характеру [2].

Об’єктивна безпека має місце в тому випадку, коли система захисту функціонує у відповідності до атак, що ініціюються відносно об’єкту захисту.

В цьому випадку система захисту із вищенаведених задач, розв'язує задачі виявлення атак та задачі протидії відповідним атакам. Перевагою такого підходу є те, що не розв'язуються задачі, пов'язані з аналізом небезпек, які існують відносно самої системи. Це суттєво здешевлює проблему створення системи захисту. Основною проблемою, яку при цьому необхідно розв'язувати, є проблема забезпечення оперативної реакції на можливе виникнення атаки, оскільки остання може бути виявлено лише у випадку коли вона ініційована відповідною небезпекою і активізована в об'єкті захисту.

Для того, щоб можна було управляти рівнем безпеки необхідно мати можливість оцінювати величину безпеки. На сьогодні відомі оцінки рівня безпеки що ґрунтуються на таких підходах:

— за можливою величиною втрат, до яких може призвести відсутність певного захисту, або недостатній рівень захисту;
— за кількістю засобів захисту, що використовуються для забезпечення безпеки;
— за складністю структури системи захисту, яка забезпечує певний рівень безпеки;
— на основі використання різних оцінок рівня безпеки, що ґрунтуються на тих чи інших методиках.

Перш ніж детальніше аналізувати різні підходи оцінки рівня безпеки, розглянемо методи синтезу *SUP* і відповідно *MUP*, оскільки в останню входить цілий ряд окремих компонент. Перша компонента, що входить в склад системи управління повноваженнями, являє собою систему аналізу параметрів суб'єкта і об'єкта. Формально цю компоненту подамо у вигляді системи співвідношень, що являють собою розширення логічних функцій функціями порівняння. В цьому випадку повна система функції являє собою таку множину $\{\&, \vee, \rightarrow, \neg, \geq, >, \leq, <\}$:

$$\begin{cases} L_1\left\{C_1\left[y_1\left(W_i\right)\right], k_1\left(x_1\right)\right\} \rightarrow \left(y_1 \rightarrow x_1\right) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ L_n\left\{C_n\left[y_n\left(W_j\right)\right], k_m\left(x_m\right)\right\} \rightarrow \left(y_n \rightarrow x_m\right). \end{cases}$$

Наступною компонентою системи *SUP* є система виявлення аномалій в *SUP*. Розглянемо більш детально аномалії, що можуть виникнути в результаті здійснення операцій в рамках *SUP*. першим типом аномалій є така взаємодія між суб'єктом і об'єктом, в результаті якої дані з об'єкту з вищою категорією попадають у об'єкт з нижчою категорією, що записується у вигляді:

$$\begin{aligned} & C_i\left\{y_t\left[W^i\left(x_i\right)\right] \& \, y_i\left[W^j\left(x_j\right)\right]\right\} \rightarrow \\ & \rightarrow \left\{\left[k_i\left[x_i\left(d_j\right)\right] \rightarrow k_j\left[x_j\left(d_j\right)\right]\right] \& \left(k_i > k_j\right) \& \left(c_i \geq k_i\right)\right\}. \end{aligned} \qquad (1)$$

Другим типом аномалій є така взаємодія суб'єкта з об'єктом, коли об'єкт являє собою деяку програмну компоненту, яка ініціюється програм-

ною компонентою y_i, що являє собою суб'єкт, а в результаті функціонування x_i змінюється величина значущості суб'єкта, який ініціював відповідну взаємодію, або величину значення своєї категорії.

Будь-яка аномалія, що може виникнути в рамках *SUP*, в основному інтерпретується засобами предметної області прикладної задачі, що розв'язується в той чи іншій момент часу. Тому більш детально зупинимося на описі відповідних аномалій не доцільно.

В рамках першого підходу, основою, для оцінки рівня безпеки, являється оцінка втрат до яких зведена повна втрата даних, їх модифікація чи втрата відповідної міри конфіденційності відповідних даних. Отже такий підхід передбачає у першу чергу досить детальний аналіз предметної області до якої відноситься задача, що розв'язується в рамках вказаними засобами. Відомою предметною областю, в якій досліджуються різні аномалії, в якості прикладу може бути область страхової діяльності [3]. Оскільки поява аномальних подій не може описуватися детермінованими методами, то для розв'язку задач в цій області використовуються апарат теорії ймовірності та статичний аналіз [4]. Для оцінки рівня безпеки часто використовується обернена величина рівня безпеки, яка називається ризиком. Справа у тому, що рівень безпеки у відповідності з його інтерпретацією відображає в певному сенсі позитивні аспекти функціонування системи захисту, які повинні домінувати в системі. Ризик навпаки характеризує можливість виникнення негативних факторів, які можуть порушувати необхідний процес функціонування системи. Загальноприйнятим підходом до визначення величини ризику є підхід, у відповідності з яким оцінюється ймовірності або функції розподілу ймовірностей виникнення негативних факторів. При цьому приймається, що величини втрат від дії таких факторів на об'єкт захисту знаходиться в детермінованій залежності від типу негативного фактору. Тому величина ризику може вимірюватися величиною втрат до яких призводять відповідні негативні фактори. У випадку технічних систем існує тісний зв'язок між окремими негативними факторами, незалежно від моменту, в який такий фактор починає діяти та результатом такої дії. У випадку систем, що надають послуги, у нашому випадку, величина втрат та характер негативних наслідків дії відповідних факторів, наприклад, на систему *SUP* залежить від характеру прикладної задачі, яка в цей момент користується послугою. Таким чином, для визнання величини ризику, необхідно оцінити не тільки ймовірність виникнення певного негативного фактора, а й оцінити час його виникнення.

Другий підхід ґрунтується на положенні про те, що негативні фактори будуть виникати. Серед цих факторів завжди існують фактори, які з точки зору можливих втрат відносяться до виділеної категорії. Таке виділення можна позначити наприклад, як катастрофічні фактори, які призводять до втрат, що розцінюються як критичні для можливості функціонування певної системи. Інша категорія втрат може бути віднесена до значних втрат. Введемо третю категорію втрат, як технічні втрати або втрати, що швидко

можуть бути усунені. Якісній поділ деякої множини на групи, окрім того що є недостатньо точним не може мати кількість складових більшою ніж 3, чи 7. Досить часто такий поділ обмежується чотирма оцінками, наприклад, в моделі Белла – Ла Радули оцінкам рівня необхідного захисту надаються такі градації: «відкритій доступ», «службовий доступ», «таємні дані» і «надтаємні данні», відповідно *J*, *F*, *T* і *S* [5]. Це в першу чергу обумовлюється відсутністю загальної формалізованої методики визначення тих чи інших оцінок для даних різного типу, а також досить неоднозначною інтерпретацією відповідальних даних в різних предметних областях. В цьому випадку необхідний рівень безпеки забезпечується вимогами стандартів безпеки інформаційних систем [6]. Здійснюється це таким чином:

— визначається характер, прикладної задачі, яку необхідно розв'язувати в рамках відповідної системи *IS*;
— на основі аналізу прикладної задачі, з використанням стандартів, формується профіль безпеки *IS*, який визначає, що необхідно в системі захищати;
— у відповідності з профілем безпеки здійснюється вибір необхідних засобів захисту, що інсталюються у відповідній системі *IS*,
— у відповідності з вибраним профілем безпеки в процесі експлуатації реалізуються всі технологічні заходи з технічного обслуговування системи, що передбачені відповідними нормами стандартів.

З вищенаведеного опису зрозуміло, що така система захисту є стандартною і не може вирішувати задач оперативного захисту прикладних систем. Очевидно, що засоби захисту в рамках однієї *IS* об'єднаються в деяку структуру. Необхідність функціональних зв'язків між окремими засобами обумовлюються тим, що прояви однієї атаки можуть існувати в різних засобах захисту, тому для успішного виявлення атак, в рамках системи захисту *IS*, необхідно використовувати відповідну систему програмного забезпечення, яке співпрацює з усіма засобами захисту та здійснює цими засобами захисту відповідне управління. В цьому випадку у рамках розв'язку задач управління доступом та наданням повноважень такою системою є система *SUP*, що будується на основі моделі *MUP*. Складність такої системи обумовлюється наступними факторами:

— наявністю зв'язків між системою та засобами захисту, що використовуються;
— можливостями системи захисту при управлінні відповідними засобами захисту;
— наявністю в рамках системи захисту засобів аналізу інформації, яку отримує система від засобів захисту;
— наявністю розвинутих зовнішніх інтерфейсів, які забезпечують зв'язок системи з оточенням та з користувачами, які обслуговують систему захисту;
— можливістю розширювати функції захисту окремих засобів в автоматичному режимі за рахунок переналаштування їх локальних систем управління, та за рахунок підвантаження систем захисту додатковими

даними чи додатковими функціями.

Для визначення рівня безпеки, який забезпечує відповідна система в цьому випадку, необхідно оцінити такі компоненти та її функціональні можливості:

— можливості кожного окремого засобу захисту, які відображають функції захисту;
— здатність кожного засобу захисту модифікуватися при відповідних управляючих діях, що ініціюються системою захисту;
— функціональними можливостями зв'язків між окремими засобами захисту та системою управління цими засобами в рамках всієї *IS*.

Чисто формально описати можливі способи оцінки величин відповідних можливостей досить складно, оскільки різні засоби захисту мають власну специфіку не тільки процесів їх функціонування, а й способів їх реалізації. Тому оцінка складності структури системи захисту і відповідна оцінка рівня безпеки, яка завдяки такій структурі забезпечується, може носити суб'єктивний характер.

Зазвичай, під оцінкою рівня безпеки розуміється певна інтегральна характеристика відповідного об'єкту, основна інтерпретація якої полягає у тому, що прикладна задача, яка розв'язується засобами системи, буде у найближчому майбутньому розв'язана, а система при цьому буде функціонувати у відповідності з технічними вимогами. Це означає, що визначення рівня безпеки системи стосується деякого майбутнього часу її функціонування. Виходячи з цього оцінка рівня безпеки базується на таких підходах:

— розв'язку задач прогнозування виникнення визначених факторів, що впливають на систему і можуть призвести до зміни її стану, що заблокує виконання задач, які розв'язуються з її використанням;
— розв'язку задачі визначення зміни поточного стану системи на основі аналізу змін, що відбувались на деякому минулому інтервалі процесу її функціонування, який включає і поточний момент часу, з цілю виявлення можливих змін в деякому майбутньому інтервалі часу, що також являє собою процес прогнозування;
— розв'язку задачі оцінки величини можливої зміни поточного рівня безпеки, що дозволяє прийняти рішення про можливість використання системи для розв'язку певної задачі з допомогою її засобів;
— відносно системи стосовної якої проводиться аналіз її безпеки, можуть діяти певні зовнішні чинники, які по визначенню орієнтовані на зниження рівня безпеки, а система володіє засобами виявлення відповідних чинників та такого впливу на систему, який унеможливлює успішне повторення такої дії. В цьому випадку система, внаслідок відповідних модифікацій своїх компонент, буде постійно підвищувати свій рівень безпеки. Рівень безпеки можна оцінювати на основі аналізу інтенсивності процесів модифікації системи, що обумовлюється процесами, які ініціюються в результаті протидії негативним зовнішнім факторам.

Як зазначалось вище для здійснення в системі процесів управління рівнем безпеки, необхідно, крім формального опису самої системи, здійснювати оцінку поточного значення величини безпеки системи. Наведенні та проаналізовані вище підходи та методи ілюструють всю складність процесу розвитку цієї задачі у повній мірі. В цьому випадку під мірою повноти розв'язку вказаної задачі розуміється певна точність визначення значення величини безпеки. Точність визначення величини рівня безпеки системи визначається наступними факторами:

— рівнем точності опису, або мірою адекватності моделі системи реальній системі;
— точністю вибраного способу обчислення величини рівня безпеки системи;
— адекватністю початкових даних що використовуються в обчисленнях, відносно значень, які відповідні дані мають в реальній системі;
— додатковими умовами та вимогами, що формуються по відношенню до процесів обчислення та способів опису моделі відповідної системи;
— параметрами, що характеризують процеси використання отриманих значень рівня безпеки системи.

Вибір рівня адекватності моделі, що описує система обумовлюється такими умовами чи обставинами:

— міра наявної інформації про об'єкт чи систему, для якої передбачається формувати модель;
— ціль, з якою така модель будується, може визначати необхідну точність відображення останнього об'єкта або системи;
— можливості теоретичних засобів, що використовуються для моделювання.

Переважно всі наведені умови узгоджуються між собою, оскільки всі вони в основному в однаковій мірі впливають на точність отриманого результату досліджень, що проводяться на моделі. В цьому випадку, виходячи з рівня представлення процесів надання повноважень суб'єктам, можна зупинитися на використанні засобів математичної логіки для формування моделі. Необхідно визначити, що відповідає одній з ключових компонент моделі, описаній співвідношенням (1) [7]. У цій роботі не будемо детально оцінювати міру адекватності моделі *MUP* системі *SUP*.

Рівень безпеки системи прийнятого оцінювати величиною ризику R, на який наражається кінцевий користувач, або процес, який ініціює відповідний користувач в даній системі. З точки зору системи *SUP*, ризик проявляється у відмові системи у наданні повноважень одному із суб'єктів системи, що реалізує, або представляє собою реалізацію прикладної системи користувача. В цьому аспекті стає очевидним необхідність надання різним суб'єктам системи прикладної задачі, різних значимостей різним суб'єктам. Прикладним є призначення більш високих значимостей суб'єктам, що мають більшу значущість для прикладної задачі. В цьому випадку величина ризику безпосе-

редньо залежить від кількості суб'єктів з великою значущістю та здатністю системи забезпечити їм надання повноважень. В даному випадку можна ускладнювати *SUP*, наприклад, моделями масового обслуговування, для оптимізації задач управління чергами на надання повноважень, які можуть виникати в *SUP* та іншими компонентами. Цей приклад ілюструє можливість зменшувати величину ризику функціонування прикладної системи за рахунок підвищення складності структури *SUP*, що призводить до підвищення безпеки системи. Наведений приклад ілюструє підвищення функціональної безпеки *SUP*. Очевидно, що розширення *SUP* системою аналізу коректності повноважень суб'єктів та категорій об'єктів підвищує рівень безпеки системи по відношенню до зовнішніх факторів, для яких ключовим елементом для реалізації атаки є несанкціонована зміна цих значень у суб'єкта чи об'єкта.

Точність початкових даних, що використовуються для обчислення величини ризику, найбільш значиму роль відіграє в тих випадках, коли в якості способів обчислення *R* приймаються числові способи. Прикладом таких способів можуть бути способи, що ґрунтуються на використані ймовірнісних уявлень, про можливість виникнення факторів, які призводять до збільшення величини *R*, ймовірнісних уявлень про вплив відповідних факторів на ті чи інші процеси розв'язку відповідної задачі та ін.

Крім функцій оцінки рівня безпеки, або оберненої величини *R*, для реалізації управління рівнем безпеки необхідно у склад *SUP* включити засоби, які такі управляючі дії реалізують. Очевидно, що управління, в цьому випадку, суттєво відрізняється від уявлень про управління в системах автоматичного регулювання. В даному випадку управління носить характер окремих дій, що реалізуються на основі виявлених причин, які являють собою реалізацію дискретних змін, що відбуваються в системі, яка захищається. Засоби, що реалізують відповідні управляючі дії, здійснюють розширення структури відповідної системи захисту, модифікацію фрагментів самого об'єкта, що захищається і після цього їх дія припиняється на період часу поки не виявляться фактори, що призводять до необхідності повторення всього циклу процесу реалізації захисту об'єкта. Такий цикл складається з наступних етапів:

— обчислення рівня безпеки, або величини ризику;
— виявлення причин збільшення ризику;
— протидія факторам, що причинили збільшення *R*;
— встановлення періоду затримки процесів вимірювання ризику у відповідності з встановленою величиною інертності системи захисту.

1. *Зегпеда Д. П.* Как построить защищенную информационную систему / *Д. П. Зегпеда, А. М. Ивашко* // Технология создания безопасных систем. – СПб. : Мир и семья – 95, 1998.
2. Атака через Интернет. – М. : Мир и семья. 1997.
3. *Бенинч В.Е.* Введение в математическую теорию актуальных расчетов / *В.Е. Бенинч, В.Ю. Королев, С.Я. Шоргин*. – М. : МАКС-Пресс, 2002.

4. *Королев В.Ю.* Теория вероятности и математическая статистика / *В.Ю. Королев.* – М. : Проспект, 2005.
5. *Зегпеда Д. П.* Теория и практика обеспечения информационной безопасности / *Ред. Д.П. Зегпеда.* – М. : Агенство «Яхтсмен», 1996.
6. *Зегпеда Д. П.* Как построить защищенную информационную систему / *Д.П. Зегпеда, А.М. Ивашко*. – СПб. : Мир и семья – 95, 1997.
7. *Акимов О. Е.* Дискретная математика / *О. Е. Акимов.* – М. : Изд. Акимова, 2005.

Поступила 7.02.2011р.