сотрудников, выдвижении на должность, организация контроля, увольнение. Поскольку методика изучения и оценки психологии личности – прерогатива специалистов соответствующего профиля, в основу этой работы должна быть положена деятельность профессиональных психологов при обязательном участии сотрудников кадрового аппарата, службы безопасности, руководителей подразделений. Затем, на основе сопоставления психологических портретов пользователей, участвующих в информационном обмене, с учетом характера их взаимодействия следует оценить риски возникновения межличностных конфликтов, способных негативно повлиять на состояние ИБ. Построенная таким образом работа с персоналом позволяет:

- предотвратить межличностные конфликты;
- своевременно выявить признаки назревающих конфликтов;
- принимать адекватные меры, направленные на решение конфликтов и устранение условий, способствующих их созреванию;
- минимизировать риски в области ИБ, определяемые человеческим фактором.

Изучение вопросов, рассмотренных в настоящей работе в рамках указанной выше дисциплины, обеспечивает необходимую разноплановость в подготовке специалистов и магистров в области защиты информации и позволяет дать им практические рекомендации, реализация которых в их будущей деятельности положительно скажется на уровне обеспечения ИБ объекта информационной деятельности.

Литература: ***1.*** *Духов В. Е. Экономическая разведка и безопасность бизнеса. - Киев: ИМСО МО Украины, НВФ "Студцентр", 1997. – 175с.* ***2.*** *Пюкке С. М. Конфликтное социальное взаимодействие в информационной сфере // Сб. научн. тр. "Інформаційні технології та безпека". Вип. 5, Институт проблем регистрации информации НАН Украины, Киев, 2003. С. 58-69.* ***3.*** *Нюстром Джон В., Дэвис К. Организационное поведение: поведение человека на рабочем месте. - Сп.Б., 2000.* ***4.*** *Гаврюшин Е. И. Человеческий фактор в обеспечении безопасности конфиденциальной информации: http//www.it2b.ru/it2b3.view1.page3.html.* ***5.*** *Прасолов В. И. Технологии обеспечения лояльности персонала в структуре политики безопасности фирмы. Материалы конференции: "Создание системы корпоративной безопасности. Практические подходы", Москва, 2005: http://www.it2b.ru/it2b2.view6.page32.html*

УДК 681.3.06

КОНЦЕПЦІЯ ВИЗНАЧЕННЯ ОПТИМАЛЬНОГО РЕЖИМУ КОНТРОЛЮ ЗАХИЩЕНОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ КОМП'ЮТЕРНИХ СИСТЕМ

Ігор Терейковський
Державний університет інформаційно-комунікаційних технологій

Анотація: **Запропонована концепція визначення оптимального режиму контролю атак на комп'ютерні системи. Основою концепції є використання параметрів, що визначають технічний стан об'єкта захисту та модель оптимізації режиму контролю, адаптована до захисту від атак на відмову в обслуговуванні. Використання даної концепції доцільне при формуванні систем аналізу захищеності та систем виявлення атак.**

Summary: **The concept of definition of an optimum verification mode of attacks on computer systems is offered. By a basis the concept is use of parameters, which define a technical status of object of protection and model of optimization of a verification mode adapted to protection against attacks on failure in service. Use of the given concept is expedient at formation of systems of the analysis of security and systems of definition of attacks.**

Ключові слова: **Атака на відмову в обслуговуванні, оптимальний режим контролю, об'єкт захисту, система виявлення атак, система аналізу захищеності.**

I Вступ

Для більшості вітчизняних та закордонних організацій ефективність функціонування багато в чому залежить від надійної та ефективної роботи їхніх комп'ютерних систем. При цьому однією із досить давніх та основних проблем забезпечення надійної та ефективної роботи корпоративних комп'ютерних систем є проблема безпеки інформації, що циркулює та зберігається в цих системах. Відзначимо, що з поширенням використання локальних комп'ютерних мереж та глобальної мережі Інтернет вказана проблема набуває все більшої актуальності, адже комп'ютер, підключений до мережі, може бути

атакований по цій мережі з віддаленого комп'ютера. Практично в усіх випадках така атака полягає в передачі мережею на комп'ютер, що атакується, деякої програми або запиту, виконання яких викликає певні негативні наслідки. Як показує практичний досвід, в деяких випадках наслідком атаки може бути повне блокування роботи та втрата ефективності комп'ютерної системи. Проблема загострюється тим, що особливості мережі Інтернет та використання доступних програмних засобів дозволяють зловмиснику проводити атаку інкогніто, без загрози покарання. Внаслідок того, що кількість комп'ютерів, підключених до мережі Інтернет, продовжує збільшуватись, небезпека таких атак постійно зростає.

На сучасному етапі одним із найбільш популярних шляхів забезпечення безпеки інформації є використання в комп'ютерних системах та мережах комплексної системи захисту інформації (КСЗІ), яка є сукупністю організаційних і інженерно-технічних заходів, програмно-апаратних засобів, спрямованих на забезпечення захисту інформації під час функціонування [1]. Практичний досвід та висновки [2 – 4] вказують на те, що підвищити ефективність КСЗІ можливо завдяки вдосконаленню математичного забезпечення програмних засобів, що входять до складу комплексу засобів захисту (КЗЗ). Під КЗЗ будемо розуміти сукупність програмно-апаратних засобів КСЗІ, які реалізують політику безпеки інформації [1, 5].

Метою статті є вдосконалення математичного забезпечення програмних засобів, що входять до складу КЗЗ комп'ютерних систем та мереж. Проблема безпосередньо пов'язана з важливим науково-практичним завданням забезпечення інформаційної безпеки розподілених комп'ютерних систем та мереж.

II Аналіз останніх досягнень та публікацій

Для забезпечення безпеки інформації в комп'ютерній системі, відповідно до наявних загроз зі сторони зловмисників та за рахунок випадкових причин, необхідно вирішити задачі забезпечення конфіденційності, цілісності та доступності даних. В [2, 3] відзначається, що існує досить багато моделей та технологій, за допомогою яких вирішуються задачі забезпечення конфіденційності та цілісності даних. Вирішити задачу забезпечення доступності комп'ютерної системи виявилось набагато важче. В останній час ця задача стає все більш актуальною, бо з поширенням локальних мереж та глобальної мережі Інтернет дії зловмисників з метою виведення з ладу комп'ютерної системи фіксуються все частіше. Ці дії зловмисників класифікують як атаку на відмову в обслуговуванні. Прикладом такої атаки може бути відправка великої кількості запитів комп'ютеру – серверу Інтернет. Сервер може виходити з ладу через те, що весь його процесорний час витрачається на виконання вхідних запитів, або через переповнення черги цих запитів. Як правило, сучасний КЗЗ повинен хоча б частково забезпечувати вирішення всіх перерахованих задач. Для цього до складу КЗЗ включають такі засоби захисту як брандмауери, системи виявлення атак, антивірусні пакети, системи аналізу захищеності, системи контролю цілісності, різноманітні криптографічні системи, сервери автенфікації, тощо.

В [3, 4] відзначено, що донедавна першочергова увага приділялась питанням післядії, тобто розкриттю комп'ютерних злочинів після їхнього здійснення та ліквідація наслідків. Однак у сучасних умовах ріст величини збитку робить зусилля ліквідації наслідків неефективними в порівнянні з мірами попередження. Тому досить актуальними є задачі:

контролю за якістю настроювання програмного забезпечення КЗЗ;

контролю за здійсненням атаки.

На даний час ці задачі вирішується за допомогою систем аналізу захищеності (САЗ) та систем виявлення атак (СВА). САЗ проводять всебічне дослідження контрольованих ресурсів з метою виявлення "слабких місць". Процес аналізу захищеності закінчується узагальненням отриманих результатів і складанням звіту. Результати, отримані від засобів аналізу захищеності, є миттєвим знімком стану захищеності в даний момент часу. Ці системи не виявляють атаку під час її виконання, однак вони дозволяють визначити потенційну можливість її виконання. Очевидно, що сигналом про потенційну можливість атаки є досягнення контрольованими параметрами деяких граничних величин. Після виявлення такої можливості необхідно реалізувати заходи для того, щоб зробити атаку не можливою. В [6] відзначено, що САЗ, що використовуються в даний час, мають низку недоліків. Одним із основних недоліків є те, що контроль програмного забезпечення, який проводиться даними системами, досить часто носить реактивний, запізнілий характер. Цей факт різко зменшує оперативність прийняття рішення щодо підвищення рівня захищеності. Тому, пропонується концепція здійснення постійного контролю (в режимі реального часу) за станом захищеності ресурсів комп'ютерної мережі. Основою даної концепції є розробка автоматизованої САЗ комп'ютерної мережі з метою автоматизації процесу збору та аналізу стану захищеності і настроювання програмного та апаратного забезпечення локальної мережі. Автоматизація для САЗ має особливе значення, оскільки ефективність застосування таких систем залежить від періодичності запуску. Основними засадами реалізації автоматизованої системи для контролю за станом захищеності комп'ютерної мережі є адаптація під конкретні умови експлуатації комп'ютерної мережі, врахування

завантаженості як окремих апаратних засобів, так і сегментів мережі в цілому, а також врахування можливих дій з боку зловмисника. На наш погляд запропонована концепція потребує деякого уточнення. Проведення постійного контролю може призвести до значного використання обчислювальних ресурсів комп'ютерної системи, що не завжди можливо з економічних та технічних причин. Крім того, додаткове використання обчислювальних ресурсів послаблює захищеність комп'ютерної системи від атаки на відмову в обслуговуванні. Тому на наш погляд необхідно розглядати доцільність не тільки постійного, але й періодичного контролю за станом контрольованих ресурсів. Ще одним доповненням може бути встановлення взаємозв'язку між періодом контролю та граничною величиною контрольованих параметрів. Відзначимо, що такий взаємозв'язок встановлюється за допомогою режиму контролю [7, 8]. Важливим висновком [4] є те, що в теперішній час відсутні підходи і наукове обґрунтування щодо розробки відповідної системи. В зв'язку з цим особливий інтерес викликає розробка методів та засобів контролю контрольованих ресурсів комп'ютерних систем на основі моделювання та оптимізації.

Як і САЗ, СВА є однією з складових КЗЗ. Досить часто СВА об'єднують с системою реакції на атаку. В базовий склад СВА, як правило, входять наступні компоненти: підсистема збору даних, підсистема аналізу даних, інтерфейс взаємодії з користувачем, база конфігураційних даних, база даних аудиту [6]. Основна задача СВА полягає в генерації рішень про здійснення чи відсутність атаки на об'єкти захисту в той чи інший момент часу. В деяких СВА висновок про здійснення атаки може бути доповнений відображенням доказів, що підтверджують висновки аналізатора, а також переліком можливих наслідків атаки. Для аналізу даних і прийняття рішень СВА використовуються два основних методи – визначення аномалій та визначення зловживань. Класифікація відбувається залежно від того, які контрольовані параметри сприймаються у вказаних методах як еталонні для прийняття рішення. Прийняття рішення про здійснення захисних заходів відбувається після досягнення контрольованими параметрами деяких граничних величин. В більшості СВА використовується постійний контроль програмного забезпечення. На наш погляд, як і для САЗ, проведення постійного контролю не завжди доцільне. Тому слід розглянути можливість проведення періодичного контролю даних, що вказують на реалізацію атаки. Доцільно розглянути можливість взаємозв'язку між періодом контролю та граничною величиною контрольованих параметрів. Розгляд таких можливостей необхідно проводити з позицій забезпечення ефективного рівня захисту при розумних витратах на їх досягнення [9]. З цієї причини задачу визначення періоду контролю та граничних величин контрольованих параметрів слід вирішувати як задачу оптимізації технічних систем. Крім того, це дозволить використати добре апробований та надійний математичний апарат. Таким чином, до основних недоліків КЗЗ програмного забезпечення комп'ютерних систем можливо віднести:

- відсутність концепції визначення оптимального режиму контролю в САЗ та СВА;
- існуючі методики захисту програмного забезпечення комп'ютерних систем не достатньо адаптовані від атак на відмову в обслуговуванні.

Постановка задачі: розробка концепції визначення оптимального режиму контролю в САЗ та СВА. Дана концепція повинна базуватись на моделюванні контролю комп'ютерних систем, та враховувати актуальність захисту від атак на відмову в обслуговуванні.

III Формування концепції визначення оптимального режиму контролю

На наш погляд реалізація контролю в системах аналізу захищеності та СВА означає проведення контролю технічного стану (ТС) об'єкту комп'ютерної системи, що підлягає захисту. Контроль ТС об'єкту захисту включає в себе операції з перевірки працездатності, локалізації відмов та визначення прогнозованого ТС. Розрізняють декілька видів контролю ТС: функціональний, параметричний, контроль працездатності тощо. При визначенні оптимального періоду контролю в першу чергу слід звернути увагу на параметричний контроль ТС об'єкту захисту. Під ТС об'єкту захисту будемо розуміти сукупність властивостей об'єкту захисту, які характеризуються в визначений момент часу параметрами, встановленими в нормативно–технічній документації та можуть змінюватись в процесі експлуатації. Через те, що для багатьох об'єктів захисту такі параметри в нормативно–технічній документації не встановлені, то як параметри можливо використати ті якісні та кількісні характеристики об'єктів захисту, або об'єктів тісно з ними пов'язаних, для яких можливо встановити допустимі області існування. Надалі параметр, за допомогою якого можливо визначити ТС об'єкту захисту, будемо називати визначаючим параметром (ВП). В багатьох випадках ТС програмного забезпечення комп'ютерних систем та мереж доцільно визначати не тільки за допомогою параметрів, що стосуються безпосередньо самого програмного забезпечення та підлягають безпосередній реєстрації. Доцільно використовувати ще й ті характеристики комп'ютерної системи та мережі, які безпосередньо залежать від функціонування програмного забезпечення. Крім того, ВП можуть бути розраховані на основі декількох параметрів, що підлягають безпосередній реєстрації. Наприклад, ВП може бути відношення величини завантаження центрального

процесора комп'ютера – сервера Інтернет до кількості запитів. Відзначимо, що задача визначення номенклатури ВП та параметрів, що підлягають безпосередній реєстрації в САЗ та СВА, є досить складною та залежить від особливостей об'єкту захисту. Основою для її вирішення можуть стати математичні вирази, наведені в [1, 2].

Відповідно визначенню ТС, ВП може змінюватись в процесі експлуатації об'єкта захисту. Тобто для кожного ВП існує функція:

$$g_i = f_i(t), \tag{1}$$

де g_i – величина і-го ВП, t – час експлуатації об'єкту захисту.

Відповідно для всіх контрольованих параметрів:

$$\{g_i\} = \{f_i(t)\}. \tag{2}$$

Для багатьох випадків справедливе твердження, що перебування всіх ВП в певних межах означає працездатний стан об'єкту захисту. Приймемо припущення, що величини ВП не корелюються. Область величин і–го ВП, в межах яких об'єкт захисту є працездатним, будемо називати областю працездатності (ОП) R_i для цього ВП. Також, будемо вважати, що метою атаки є викид ВП із меж ОП. Надалі атаку на відмову в обслуговуванні, метою якої є викид і–го ВП за межі його ОП, будемо називати атакою на і–й ВП. Необхідною умовою працездатного стану об'єкту захисту є:

$$\begin{cases} g_i \in R_i \\ R_i \in R \end{cases}, \tag{3}$$

де R_i – область працездатності для і–го ВП, R – множина областей працездатності всіх ВП.

Якщо позначити верхню межу ОП і–го ВП – $G_i^{\max}$, а нижню межу – $G_i^{\min}$, то необхідною умовою працездатного стану об'єкту захисту буде:

$$g_i \in [G_i^{\min}, G_i^{\max}]. \tag{4}$$

При цьому достатньою умовою працездатного стану об'єкту захисту буде:

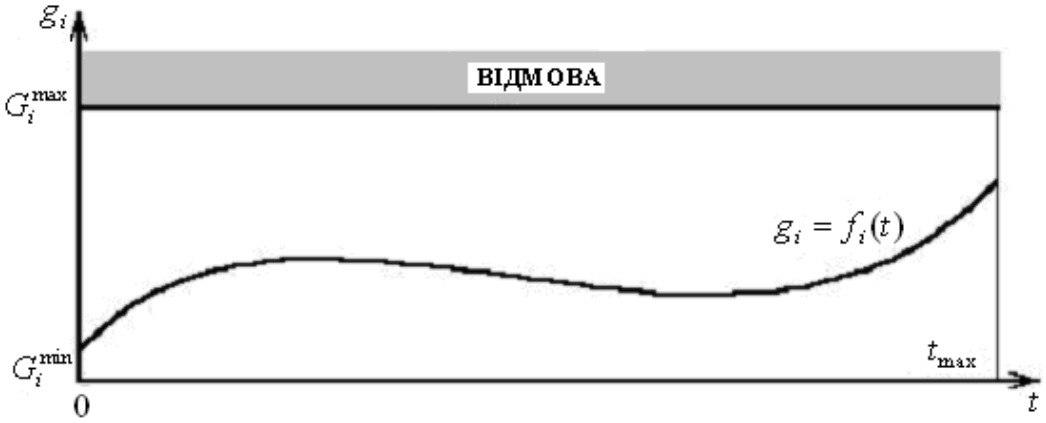
$$\{g_i\} \in R. \tag{5}$$

Достатньою умовою відмови об'єкту захисту є вихід будь–якого ВП за межі своєї області працездатності:

$$g_i \notin [G_i^{\min}, G_i^{\max}]. \tag{6}$$

Розрізняють односторонню та двосторонню ОП. При двосторонній ОП можливий вихід ВП за будь–яку межу. При односторонній ОП можливий вихід ВП тільки за верхню, або тільки за нижню межу. В [7, 8] показаний можливий механізм адаптації моделі з ОП з верхнею межею до ОП з нижньою межею та до двосторонньої ОП. Тому для спрощення моделювання будемо використовувати модель зміни ТС об'єкта захисту з односторонньою ОП з можливим виходом і–го ВП тільки за верхню межу. Графічною ілюстрацією такої моделі є рис. 1.

Запропонована модель зміни ТС дозволяє перейти до формування оптимізаційної моделі режиму контролю об'єкту захисту. Ця модель повинна встановити оптимальний взаємозв'язок між періодом контролю ВП та тією величиною ВП, досягнення якої сигналізує про необхідність проведення деяких захисних заходів (ЗЗ). Стосовно нашої моделі зміни ТС, проведення ЗЗ полягає в поверненні ВП у свою ОП. Для САЗ ці заходи будуть спрямовані на зменшення потенційної можливості атаки. Для СВА ЗЗ будуть реалізувати захист від здійснення атаки. Під періодом контролю ВП будемо розуміти термін між двома сусідніми контролями. Відзначимо, якщо період контролю менший певної величини, то це означає проведення постійного контролю. Визначення цієї величини залежить від характеристик комп'ютерної системи. Наприклад, можна вважати постійним контроль прикладного програмного забезпечення, що працює під управлінням операційної системи Windows в режимі користувача, якщо період контролю менший ніж 20 нс.



g_i, – величина і-го ВП, G_i^{min}, G_i^{max} – межі ОП для і-го ВП, t – термін експлуатації об'єкта захисту, t_{max} – максимальний термін експлуатації об'єкта захисту

Рисунок 1 – Модель зміни ТС об'єкта захисту з верхнею межею ОП

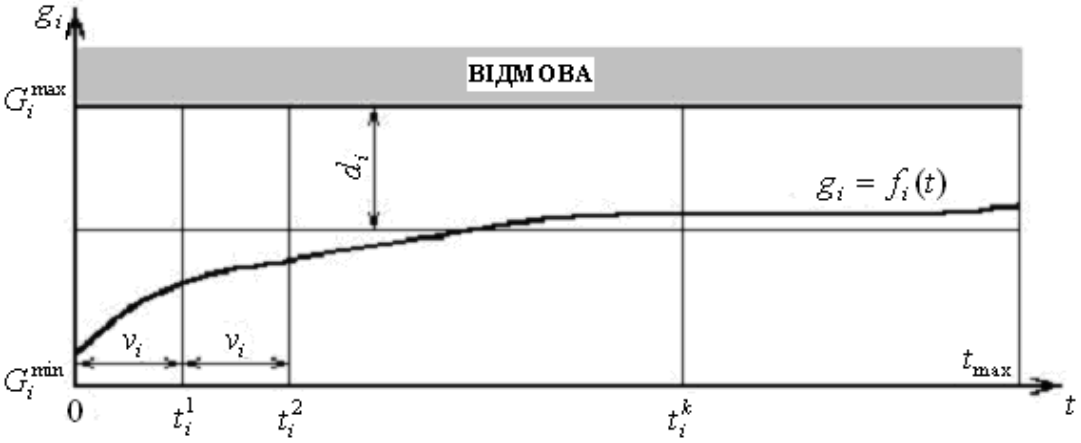
Досягнення і–м ВП граничної величини, що вказує на необхідність ЗЗ, можна записати у вигляді:

$$\begin{cases} g_i < G_i^{max} \\ g_i > G_i^{max} - d_i \\ t = t_i^j \\ t \le t_{max} \end{cases}, \tag{7}$$

де d_i – попереджувальний допуск на і–й ВП, t – термін експлуатації об'єкту захисту, t_i^j – j–й момент контролю і–го ВП, t_{max} – максимальний термін експлуатації об'єкту захисту.

Для спрощення розрахунків будемо вважати, що величини періоду контролю та попереджувального допуску не змінюються в процесі експлуатації. Відзначимо, що таке спрощення досить часто використовується при оптимізації режиму контролю реальних технічних систем [6].

Графічної ілюстрацією запропонованої моделі режиму контролю є рис. 2.



v_i – період контролю і–го ВП, d_i – величина попереджувального допуску для і–го ВП, t_i^1, $t_{i,}^2$, t_i^k – 1, 2, *k* моменти контролю і–го ВП.

Рисунок 2 – Модель режиму контролю об'єкту захисту

В представленій моделі період контролю і–го ВП можна розрахувати таким чином:

$$v_i = t_i^{j-1} - t_i^j = const\,, \tag{8}$$

де t_i^{j-1}, t_i^j – (j –1) та j моменти контролю і–го ВП.

Визначення оптимального режиму контролю означає вирішення задачі встановлення оптимального співвідношення між величинами періоду контролю та попереджувального допуску. В наслідок того, що для багатьох об'єктів захисту нормативні величини показників надійності не встановлені, доцільно вирішувати цю задачу як обернену задачу оптимізації технічних систем. Характерною особливістю оберненої задачі оптимізації є мінімізація втрат, що залежать від характеристик технічної системи, тому що як критерії оптимізації можливо вибрати приведені сумарні втрати при експлуатації об'єкту захисту (S_Σ), що залежать від величин періоду контролю та попереджувального допуску:

$$S_\Sigma(V, D) \to \min\,, \tag{9}$$

де V – множина періодів контролю ВП, D – множина попереджувальних допусків ВП.

Для визначення оптимальних величин періодичності контролю та попереджувального допуску необхідно вирішити систему рівнянь:

$$\begin{cases} \partial S_\Sigma(V, D)/\partial V = 0, \\ \partial S_\Sigma(V, D)/\partial D = 0. \end{cases} \tag{10}$$

В свою чергу:

$$S_\Sigma(V, D) = C_\Sigma(V, D)/t_{\max}\,, \tag{11}$$

де $C_\Sigma(V, D)$ – абсолютні сумарні вартісні втрати при експлуатації об'єкту захисту, що залежать від величин періоду контролю та попереджувального допуску, $t_{\max}$–максимальний термін експлуатації об'єкту захисту.

Розглянемо складові частини $C_\Sigma(V, D)$. Проведення контролю та ЗЗ за його результатами спрямовані на зменшення втрат, пов'язаних з успішною реалізацією атаки. Проте реалізація контролю та ЗЗ також призводить до втрат. Таким чином:

$$C_\Sigma = C_K + C_Z + C_A\,, \tag{12}$$

де C_K – втрати при проведенні контролю, C_Z – втрати, пов'язані з реалізацією ЗЗ, C_A – втрати на ліквідацію наслідків відмов, пов'язаних з успішними атаками.

Розрахунок втрат є досить складною економіко–технічною задачею, при вирішенні якої слід враховувати специфіку об'єкту захисту та тип атаки, від якої проводиться захист. На першому етапі розрахунку необхідно визначити тип втрат. Найбільш інформативними та узагальнюючими є економічні втрати. Доцільність їх використання в задачах забезпечення конфіденційності та цілісності даних не викликає сумніву. Проте розрахунок економічних втрат при захисті комп'ютерних систем загального призначення від атак на відмову досить складний. Наприклад, визначення економічних втрат при реалізації програмними засобами контролю та ЗЗ комп'ютера–сервера Інтернет залежить від багатьох факторів. На наш погляд, при захисті від атаки на відмову в обслуговуванні можливо використовувати зменшення коефіцієнта технічної готовності K_Σ комп'ютерної системи. В багатьох випадках зменшення K_Σ відбувається за рахунок зменшення обчислювальних потужностей комп'ютерної системи при проведенні контролю K_K, ЗЗ K_Z та при відмові внаслідок успішної атаки K_A. При цьому, зменшення обчислювальних потужностей комп'ютерної системи можна оцінити за допомогою не багатьох параметрів, реєстрація яких не викликає труднощів. Наприклад, для комп'ютера–сервера Інтернет цими параметрами є: завантаження центрального процесора, використання оперативної пам'яті, величина черги мережевих запитів, використання постійної пам'яті. Адаптована до задачі захисту від атаки на відмову в обслуговуванні формула розрахунку втрат (12) виглядає наступним чином:

$$K_\Sigma = K_K + K_Z + K_A \tag{13}$$

Відзначимо, що K_K, K_Z, K_A є узагальнюючі величини, розрахунок яких можливо провести так:

$$\begin{cases} K_K = \sum_{i=1}^{N} K_K^i \\ K_Z = \sum_{i=1}^{N} K_Z^i \\ K_A = \sum_{i=1}^{N} K_A^i \end{cases}, \tag{14}$$

де N–кількість ВП, K_K^i, K_Z^i, K_A^i – зменшення коефіцієнта готовності комп'ютерної системи внаслідок контролю і–го ВП, проведення ЗЗ за результатами контролю і–го ВП та відмови системи, пов'язаної з виходом і–го ВП за межі ОП (атакою на і–й ВП).

Аналіз [1 – 3, 7] вказує на те, що реалізація ВП при штатних умовах експлуатації, а також процес здійснення атак в більшості випадків має випадковий характер. Тому розрахунок K_K^i, K_Z^i, K_A^i можливо провести таким чином:

$$\begin{cases} K_K^i = k_K^i \times P_K^i \\ K_Z^i = k_Z^i \times P_Z^i \\ K_A^i = k_A^i \times P_A^i \end{cases}, \tag{15}$$

де k_K^i, k_Z^i, k_A^i – зменшення коефіцієнта готовності комп'ютерної системи внаслідок одного контролю і–го ВП, проведення одного ЗЗ по результатам контролю і–го ВП та однієї відмови об'єкту захисту, яка пов'язана з атакою на і–й ВП, P_K^i, P_Z^i, P_A^i – ймовірності здійснення контролю і–го ВП, проведення ЗЗ по результатам контролю і–го ВП та реалізації відмови системи, пов'язаної з атакою на і–й ВП за максимальний термін експлуатації об'єкту захисту.

Надалі k_K^i, k_Z^i, k_A^i будемо називати одиничними втратами при проведенні контролю, ЗЗ та при відмові, пов'язаної з атакою на і–й ВП.

Використання (13) – (15), (11), (9) дозволяє записати вираз для розрахунку основного критерію оптимізації так:

$$\sum_{i=1}^{N} \frac{k_K^i \times P_K^i + k_Z^i \times P_Z^i + k_A^i \times P_A^i}{t_{\max} \times P_{\max}} \to \min, \tag{16}$$

де $P_{\max}$ – ймовірність працездатного стану об'єкту захисту за встановлений максимальний термін експлуатації.

С позицій спрощення розрахунків доцільно розглядати об'єкти захисту як не відновлювальні. Тому:

$$\sum_{i=1}^{N} P_Z^i + \sum_{i=1}^{N} P_A^i + P_{\max} = 1. \tag{17}$$

Після підстановки (16) в (10) та відповідних спрощень отримуємо остаточний вираз для розрахунку основного критерію оптимізації:

$$\begin{cases} \sum_{i=1}^{N} \frac{\partial\left(\frac{k_K^i \times P_K^i + k_Z^i \times P_Z^i + k_A^i \times P_A^i}{t_{\max} \times P_{\max}}\right)}{\partial v_i} = 0, \\ \sum_{i=1}^{N} \frac{\partial\left(\frac{k_K^i \times P_K^i + k_Z^i \times P_Z^i + k_A^i \times P_A^i}{t_{\max} \times P_{\max}}\right)}{\partial d_i} = 0. \end{cases} \tag{18}$$

Розв'язати (18) можливо чисельним способом, при цьому період контролю та попереджувальний допуск необхідно уточнювати після реалізації поточного контролю. Відзначимо, що ймовірності P_K^i, P_Z^i, P_A^i залежать не тільки від періоду контролю та попереджувального допуску, але й від динаміки ВП.

Таким чином, (19) слід доповнити моделлю динаміки ВП. Відзначимо, що модель має враховувати залежність динаміки ВП від реалізації поточного етапу атаки. Практичний досвід свідчить, що в загальному випадку залежність динаміки ВП від реалізації поточного етапу атаки може мати досить складний характер. Крім того, залежності, що є інформативними в САЗ, можуть суттєво відрізнятися від тих, що мають використовуватись в СВА. З цієї причини розробка єдиної, універсальної моделі динаміки ВП викликає значні труднощі. Вирішенням проблеми може стати використання моделей, адаптованих для захисту від атак певного типу та призначених для використання в СВА, або/та в САЗ.

Розглянемо можливу модель динаміки ВП, пристосовану до використання в СВА, з метою визначення та захисту від атаки на відмову в обслуговуванні, що реалізується методом відправки на сервер великої кількості запитів. Метою такою атаки є вичерпання обчислювальних потужностей сервера [3]. За цих обставин як ВП визначимо кількість запитів до серверу за одиницю часу. Відзначимо, що на сьогодні подібні атаки на локальні комп'ютерні мережі, з'єднані з Інтернет, є поширеними. Разом з тим в багатьох випадках велика кількість запитів за одиницю часу пояснюється і об'єктивними причинами. Таким чином, в першому наближенні, реалізацію ВП визначимо як послідовність випадкових подій, що узгоджується з [6]. Це припущення дозволяє провести розрахунок динаміки ВП на основі марківської моделі. Вибір марківської моделі пояснюється її надійністю та апробованістю в задачах експлуатації та захисту різноманітних, в тому числі і комп'ютерних, технічних систем [6 – 8]. Ймовірну залежність інтенсивностей переходів марківського процесу від того, яким шляхом контрольований об'єкт опинився в певному стані, можливо компенсувати за рахунок використання псевдостанів [8]. Таким чином можна врахувати результати попередніх етапів атаки.

Ще одним випадком застосування марківської моделі в СВА може бути захист від поширеної атаки з метою несанкціонованого доступу до ресурсів комп'ютерної мережі, що реалізується шляхом підбору імені та паролю санкціонованого користувача. Як ВП можливо визначити кількість запитів "ім'я користувача – пароль" за одиницю часу, а динаміку ВП моделювати на основі апарату марківської апроксимації. Отже марківська модель, хоча і не є універсальною, може знайти досить широке застосування для визначення динаміки ВП. Її використання полягатиме в розрахунку P_K^i, P_Z^i, P_A^i при фіксованих параметрах режиму контролю.

Таким чином, концепція визначення оптимального режиму контролю передбачає:

- визначення номенклатури ВП об'єкта захисту;
- визначення номенклатури параметрів, що безпосередньо реєструються в САЗ та СВА;
- формування ОП для кожного із ВП;
- формування моделі апроксимації ВП;
- розрахунок одиничних втрат при проведенні контролю, ЗЗ та при відмові, пов'язаної з атакою на кожний із ВП;
- розрахунок за допомогою оптимізаційної моделі (17), (18) та марківської моделі апроксимації ВП оптимальних показників режиму контролю.

IV Висновки

Запропонована концепція визначення оптимального режиму контролю атак на комп'ютерні системи. Основою запропонованої концепції є використання параметрів, що визначають ТС об'єкта захисту та оригінальна модель оптимізації режиму контролю, адаптована до захисту від атак на відмову в обслуговуванні. Використання даної концепції при формуванні САЗ та СВА дозволить підвищити ефективність КСЗІ.

Перспективи подальшого розвитку в даному напрямку:

- адаптація запропонованої концепції для вдосконалення КСЗІ реальних комп'ютерних систем та мереж;
- формування методики визначення номенклатури ВП та параметрів, що підлягають безпосередній реєстрації в САЗ та СВА;
- розробка моделей динаміки ВП, адаптованих до різних типів атак та застосування в САЗ та СВА;
- доопрацювання запропонованої оптимізаційної моделі з точки зору обґрунтування та визначення обмежуючих критеріїв;
- дослідження оптимального режиму контролю захищених об'єктів комп'ютерних систем та мереж.

Література: ***1.*** *Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.// НД ТЗІ 2.5-008-2002, ДСТСЗІ СБ України Київ, 2002, 30 с.* ***2.*** *Э. Таненбаум Соверменные операционне системы // СПб.:Питер, 2002. – 1036 с.* ***3.*** *Терейковський*

І. А. Дослідження стійкості серверних технологій Java від атак на відмову // Захист інформації. – 2004. – №4, с.11 – 18. ***4.*** *Шохін Б. П., Юдін О. М., Мазулевський О. Є.Вдосконалення контролю за станом захищеності ком'ютерної мережі на основі адаптивного моніторингу // Зб. н. п. військового інституту телекомунікацій та інформатизації національного технічного університету України "КПІ". – 2004. – Випуск №4, с.208 – 217.* ***5.*** *Богуш В. М., Кривуца В. Г., Кудін А. М. Інформаційна безпека: Термінологічний навчальний довідник. // К.: ООО „Д.В.К", 2004. – 508 с.* ***6.*** *Кузнецов Г. В., Иванов А. М. Методы анализа данных для обнаружения атак в компьютерных системах и сетях банковских структур. Защита информации. Сб. н. тр. НАУ, Киев – 2004, С.34-42.* ***7.*** *Воробьев В. Г., Глухов В. В., Козлов Ю. В. Диагностирование и прогнозирование технического состояния авиационного оборудовани.– М.: Транспорт, 1984.-191 с.* ***8.*** *Игнатов В. А., Маньшин Г. Г., Трайнев В. А. Статистическая оптимизация качества функционирования электронных систем. М.: Энергия, 1974,-264 с.* ***9.*** *Хорошко В. О., Кудінов В. А. Методичний підхід до формалізації задачі оцінювання ефективності системи захисту інформаційної системи ОВС України. Захист інформації. – 2004. – №4, с.11 – 18.*

УДК 681.3

ЕКСПЕРТНА ОЦІНКА БЕЗПЕКИ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ЗА КРИТЕРІЄМ "РИЗИК БЕЗПЕКИ-ГАРАНТІЯ БЕЗПЕКИ"

Вячеслав Шорошев
Державний науково-дослідний інститут МВС України

Анотація: **Надаються узагальнені критерії експертної оцінки стану безпеки інформації в комп'ютерних системах за критерієм "ризик безпеки-гарантія безпеки".**
*Summary:***The generalized yardsticks of an expert estimation of safety of the information in computer systems by yardstick « of risk the safety - safe conduct » are esteemed.**
Ключові слова: **Ризик безпеки, гарантія безпеки, послуга безпеки, стандартний профіль захищеності інформації.**

Вступ

Складність проблеми полягає в тому, що стан безпеки інформації в комп'ютерних системах України необхідно оцінювати за умови її обробки, захисту та поширення з широким використанням сучасних інформаційних технологій. На цей час їх основою є комп'ютерні дані та системи, а також суворе дотримання вимог чинних нормативних документів Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України щодо забезпечення конфіденційності, цілісності та доступності оброблюваної інформації. Це вже висвітлювалось у роботах [1 – 6].

Це не така проста проблема. Провідними країнами світу вона вирішувалась понад 14 років (1983 – 1997 роки), поки на було розроблено міжнародні критерії і стандарти щодо експертної оцінки стану захищеності інформації в комп'ютерних системах від загроз несанкціонованого доступу. Було інвестовано і успішно реалізовано дослідження щодо розробки міжнародних критеріїв і стандартів комп'ютерної безпеки в США, Канаді, Франції, Англії, Німеччині, Нідерландах, Російській Федерації. Аналогічна проблема протягом 9 років (1991 – 1999 роки) кардинально вирішувалась і в Україні. З 1999 р. в Україні було введено в дію вітчизняні критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

При розробці критеріїв у провідних країнах світу в основу було покладено велику сукупність критеріїв – від 6 – 10 простих універсальних критеріїв (1983 – 1991 р. р.) до 70 – 160 (1992 – 1999 р. р.) складних часткових критеріїв [6]. Користуватись такими критеріями і робити експертну оцінку стану безпеки інформації в комп'ютерних системах за такими підходами дуже непросто. Така проблема стояла і при використанні вітчизняних критеріїв щодо експертної оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Треба було знайти якийсь вихід.

Але для цього треба перейти від сукупності 110 часткових критеріїв оцінки стану захищеності (безпеки) інформації в комп'ютерних системах згідно з вимогами НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-005-99 до двох-трьох узагальнених критеріїв, які треба розробити та реалізувати. Це обумовлено тим, що прийняття рішення за багатьма критеріям саме по собі теоретично проблемне і поки що фундаментально розроблено ще не до кінця. Так, на цей час в теорії прийняття рішень за багатьма критеріями обмежуються золотим