УДК 621.3.019.3

Н.В. СЕСПЕДЕС ГАРСІЯ*

ОЦІНКА РІВНЯ КОНФІДЕНЦІЙНОСТІ ГАРАНТОЗДАТНИХ КОМП'ЮТЕРНИХ СИСТЕМ

*Інститут проблем математичних машин і систем НАН України, Київ, Україна

Анотація. *У статті розглянуті основні аспекти конфіденційності гарантоздатних комп'ютерних систем (ГКС), описано механізми та методи забезпечення конфіденційності ГКС, запропонований метод кількісної оцінки рівня конфіденційності систем.*
Ключові слова: *конфіденційність, порушення конфіденційності, методи забезпечення конфіденційності, оцінка конфіденційності.*

Аннотация. *В статье рассмотрены основные аспекты конфиденциальности гарантоспособных компьютерных систем (ГКС), описаны механизмы и методы обеспечения конфиденциальности ГКС, предложен метод количественной оценки уровня конфиденциальности систем.*
Ключевые слова: *конфиденциальность, нарушение конфиденциальности, методы обеспечения конфиденциальности, оценка конфиденциальности.*

Abstract. *The main aspects of confidentiality of dependable computer systems (DCS) were considered in the article. The mechanisms and methods of ensuring confidentiality of DCS were described. Method of quantitative evaluation of the level of privacy systems was proposed.*
Keywords: *confidentiality, breach of confidentiality, ensuring confidentiality methods, confidentiality assessment.*

1. Вступ

Однією із складових гарантоздатності комп'ютерних систем (ГКС) є їх конфіденційність. Конфіденційність ГКС зводиться до того, щоб закрита або інша конфіденційна інформація була захищена, так як її несанкціоноване розкриття може призводити до значних матеріальних втрат. Мається на увазі, що гарантоздатна комп'ютерна система повинна забезпечити захист від несанкціонованого використання інформації, підміни інформації та пошкодження інформації. Також в ГКС має бути забезпечений захист від несанкціонованого використання, підміни або пошкодження технічного засобу (системи).

З розвитком інформаційних технологій проблема конфіденційності та конфіденційної інформації набуває більшої значущості. І в різних областях і різних країнах конфіденційність і інформація, що відноситься до конфіденційної, визначається по-різному.

У країнах Європейського союзу, наприклад, конфіденційність інформації регулюється за допомогою низки угод і директив, таких як директива ЕС 95/46/ЕС, 2002/58/ЕС и ETS 108, ETS 181, ETS 185, ETS 189.

Так, конвенція «Про злочинність у сфері комп'ютерної інформації» (ETS N 185) спрямована на стримування, в тому числі дій, спрямованих проти конфіденційності комп'ютерних даних і комп'ютерних мереж, систем. Згідно з даною конвенцією для протидії злочинам проти конфіденційності, доступності та цілісності комп'ютерних даних і систем, кожна сторона вживає законодавчі та інші заходи, необхідні для того, щоб кваліфікувати як кримінальний злочин згідно з її внутрішнім законодавством:

- протизаконний доступ;
- неправомірне перехоплення;
- вплив на дані;
- вплив на функціонування системи;
- протизаконне використання пристроїв [1].

Часто конфіденційність виявляється залежною від часу. Інформація, яка вимагає спочатку величезних зусиль для свого захисту, поступово втрачає цінність і це слід брати до уваги при аналізі. У якій би області не використовувалися комп'ютерні системи (КС) – теплоенергетика, авіація, космос, транспортне управління, фінансова сфера і т.д і навіть в органах держуправління – завжди необхідно оцінювати розміри збитку, які можуть виникнути через витік конфіденційної інформації. Конфіденційність є важливим атрибутом для відкритих і розподілених систем, в основі яких лежить мережева ідеологія, а також для систем критичного застосування.

Конфіденційність є однією і найбільш важливою із складових у галузі забезпечення інформаційної безпеки, особливо для систем у критичних областях. На сьогоднішній момент не існує чітких методик визначення кількісної оцінки конфіденційності різних систем. У роботі проаналізовано існуючі методи забезпечення конфіденційності та запропоновано метод кількісної оцінки атрибута «конфіденційність» в ГКС.

2. Визначення поняття конфіденційність

Для проведення аналізу алгоритмів і методів забезпечення конфіденційності необхідно привести саме визначення поняття конфіденційності ГКС.

Під конфіденційністю ГКС слід розуміти властивість системи (об'єкта) забезпечувати захист від несанкціонованого використання інформації або технічних засобів, підміни інформації або технічних засобів, пошкодження інформації або технічних засобів з боку внутрішнього та / або зовнішнього впливу.

Таким чином можна виділити два типи конфіденційності: технічна та інформаційна.

Основними метриками конфіденційності є ймовірність загроз, доступність і секретність.

Ймовірність загроз – ймовірність виникнення порушення конфіденційності технічних засобів та (або) інформації. Допустима ймовірність загроз забезпечується наявністю комплексної системи захисту технічних засобів та інформаційних ресурсів.

Доступність – властивість технічного засобу або інформації, що забезпечує фізичну можливість зміни заданих параметрів певними засобами в заданих точках за кінцевий час. Доступність забезпечується наявністю у певних осіб паролів доступу до технічного засобу або інформації.

Секретність – сукупність взаємопов'язаних засобів і заходів, спрямованих на збереження секретності технічних та (або) інформаційних ресурсів. Секретність забезпечується засобами засекречування конфіденційних даних і наявністю технічних засобів захисту інформації.

Багато компаній, наприклад, такі як Hewlett Packard, Google та ін., надають можливість вибору налаштувань конфіденційності. Для запобігання несанкціонованого доступу до особистої інформації або її розголошення, забезпечення її точності та належного використання ці компанії використовують відповідні фізичні, технічні та адміністративні процедури.

3. Причини порушення конфіденційності ГКС і можливі загрози

Щоб сформулювати деякі більш конкретні цілі в питаннях конфіденційності, необхідно визначити причини її порушення, а саме:

- прорахунки в розробці системи;
- нечітка робота програмних засобів щодо забезпечення конфіденційності;
- непрофесійні дії персоналу при взаємодії з КС (зловмисні / випадкові);
- недотримання адміністративних процедур щодо забезпечення конфіденційності;
- вплив, завданий несанкціонованими користувачами або програмами.

4. Методи забезпечення конфіденційності ГКС

Конфіденційність інформації в ГКС забезпечується програмно-апаратними засобами захисту інформації. Такі засоби сприяють досягненню більш високих показників ефективності, якщо застосовувати їх комплексно. До таких засобів відносять обладнання для криптографічного захисту мовної інформації, програми для криптографічного захисту текстової чи іншої інформації, програми для забезпечення аутентифікації поштових повідомлень за допомогою електронного цифрового підпису, програми забезпечення антивірусного захисту, програми захисту від мережевих вторгнень, програми виявлення вторгнень, програми для приховування зворотної адреси відправника електронного листа. В обов'язковому порядку в корпоративну мережу повинні бути включені служби інформаційної безпеки, високої готовності, централізованого моніторингу та адміністрування [2].

Подібний перелік програмно-апаратних засобів, як правило, розробляється фахівцями в області захисту інформації з урахуванням багатьох факторів, наприклад, характеристик ГКС, кількості користувачів у цій системі, відмінності рівня доступу цих користувачів та ін.

Деякі системи можуть мати вихід в Internet, тому сьогодні на першому плані виникає проблема забезпечення безпеки КС з боку мережевого впливу. Цей сегмент не стоїть на місці і постійно розвивається, причому дуже динамічно. Основними засобами захисту КС були, є і залишаються міжмережеві екрани. У літературі можна зустріти їх синоніми, такі як брандмауер (firewall), фільтруючий маршрутизатор та ін. [3].

Забезпечення конфіденційності в ГКС здійснюється системою забезпечення конфіденційності (СЗК) за допомогою ідентифікації та встановлення повноважень користувача [4]. У СЗК повинні встановлюватися вимоги до користувачів щодо доступу до ресурсів. Ці вимоги включають не тільки встановлення необхідної ідентичності користувача, але і підтвердження того, що користувач є дійсно заявленим користувачем. Для цього користувач повинен надати системі деяку інформацію, яка закладена в систему і пов'язана з даним користувачем. При цьому повинні включатися функції, призначені для установки і перевірки необхідної ідентичності.

СЗК повинні включати функції, які дають можливість додавати нових користувачів і видаляти або позбавляти законної сили старих користувачів. Точно так само повинні включатися функції для дозволу прийому, зміни або перевірки користувачами розпізнавальної інформації, необхідної для перевірки ідентичності даного користувача. Повинні також включатися функції, які гарантують цілісність або запобігають неуповноваженого використання розпізнавальної інформації, а також функції для обмеження можливості повторних спроб встановити помилкову ідентичність.

У багатьох СЗК повинні встановлюватися вимоги для захисту даних під час передачі по каналах зв'язку. Такий захист зазвичай згадується як захист зв'язку на відміну від комп'ютерного захисту.

Конфіденційність ГКС можна оцінити кількістю і якістю засобів, призначених для забезпечення конфіденційності.

СЗК ГКС можуть будуватися з багатьох компонентів. Деякі компоненти не сприяють задоволенню цілей безпеки, інші компоненти націлені на забезпечення безпеки. Ці компоненти вважаються такими, що забезпечують безпеку. Нарешті можуть бути деякі компоненти, які не забезпечують безпеку, але все ж таки повинні працювати правильно для забезпечення безпеки. Вони вважаються такими, що мають відношення до безпеки. Поєднання компонентів, що забезпечують безпеку і які мають відношення до безпеки, часто називають Trusted Computing Base (TCB).

На підставі визначення функцій ГКС, які в тій чи іншій мірі забезпечують правильну роботу системи, може бути оцінена критичність цих функцій. Така класифікація функцій є похідною від аналізу відмов та їх наслідків. Класифікація функцій за рівнями крити-

чності (іноді званими рівнями цілісності), разом з максимально допустимою тривалістю переривання обслуговування, дозволяє в процесі розробки системи вибрати відповідні механізми обробки помилок і, особливо, вибрати принципи реконфігурації для обробки несправності.

Рішення задач конфіденційності покладається на послуги безпеки. Послуги, залежно від того, на вирішення яких завдань вони спрямовані, можна віднести до одного з трьох класів.

• Опорні послуги безпеки. До даного класу відносяться послуги, які є загальними і лежать в основі реалізації більшості інших послуг безпеки. Іншими словами, вони виступають в ролі базису для надбудови, до якої входять послуги двох інших класів.

• Послуги запобігання – це послуги безпеки, в основному орієнтовані на запобігання різного роду порушень безпеки.

• Послуги виявлення порушень і відновлення безпеки спрямовані, насамперед, на вирішення завдань виявлення порушень безпеки (до або після їх здійснення) і відновлення системи в безпечний стан.

Опорні послуги безпеки виступають в ролі базису для побудови всіх інших послуг безпеки. До даного класу відносяться такі послуги безпеки.

Ідентифікація (привласнення імен). Однозначно ідентифікований об'єкт та суб'єкти інформаційних взаємин є необхідною умовою для реалізації більшості послуг безпеки. Ідентифікація забезпечує можливість присвоєння унікального ідентифікатора користувачам, процесам, інформаційним та іншим ресурсам.

Управління криптографічними ключами. Дана послуга обов'язкова у разі застосування криптографічних функцій у будь-яких послугах безпеки. Під управлінням ключами розуміють сукупність методів і процедур, що здійснюють безпечне встановлення та управління ключовими взаємовідносинами між авторизованими об'єктами.

Управління безпекою і адміністрування. Під управлінням безпекою розуміють поширення і управління інформацією, необхідною для роботи послуг і механізмів безпеки. Під адмініструванням розуміють процеси налаштування параметрів інсталяції і експлуатації програмного і апаратного забезпечення послуг безпеки, а також облік внесених змін до експлуатованого обладнання.

Захищеність системи являє собою сукупність властивостей системи, які дозволяють довіряти технічній реалізації системи. Розглядається не тільки якість реалізованих засобів захисту, а й процедури їх розробки, способи досягнення та вирішення технічних завдань.

Прикладами засобів захищеності системи є захист залишкової інформації (або захист від повторного використання), мінімізація повноважень, поділ процесів, модульність та рівні розробки, мінімізація кола обізнаних осіб і т.д.

Залишкова інформація – інформація на пристрої пам'яті, що залишилася від формально віддалених операційною системою даних. Інформація може залишитися через формальне видалення файлу або через фізичні властивості запам'ятовуючих пристроїв. Залишкова інформація може призвести до випадкового розповсюдження конфіденційної інформації, якщо сховище даних опиниться поза зоною контролю (наприклад, буде видалено або передано третій стороні). В даний час, щоб уникнути появи залишкової інформації, застосовується безліч методів. Залежно від ефективності і призначення вони підрозділяються на «очищення» і «знищення» такої інформації. Конкретні методики використовують перезаписування, розмагнічування, шифрування та фізичне знищення.

Для якісного забезпечення конфіденційності необхідно слідувати політиці конфіденційності (ПК), яка має на увазі під собою кінцеву безліч умов, при виконанні яких санкціоновані користувачі системи отримують певний доступ до інформації та ресурсів ГКС. Необхідні умови задаються у вигляді вимог і повинні бути передбачені й реалізовані в СОК ГКС. Функціонування конкретної ПК базується на відповідних механізмах конфіден-

ційності: організація ідентифікації і аутентифікації, розподіл ресурсів, забезпечення відмовостійкості і т.д. У більшості випадків механізми конфіденційності можуть складатися з автоматизованих і організаційних компонентів. Автоматизовані компоненти часто є частиною основного обчислювального оточення, включаючи відповідну безліч процедур користувача та адміністратора.

5. Оцінка рівня конфіденційності ГКС

Спільним для моделей забезпечення конфіденційності є те, що всі вони спрямовані на введення певних обов'язкових процедур аналізу конфіденційності, програм, засобів, ресурсів і користувачів, які взаємодіють з ГКС.

Пропонується найбільш загальний підхід до оцінки конфіденційності системи. Кожній метриці конфіденційності відповідає набір критеріїв, за якими відбувається оцінка конфіденційності ГКС (табл. 1). Набір критеріїв може мінятися залежно від призначення і специфіки функціонування конкретної ГКС.

Таблиця 1. Основні метрики і критерії оцінки конфіденційності

Метрики конфіденційності	Найменування критерію
Ймовірність загроз P_D – ймовірність порушень конфіденційності технічних засобів та (або) інформації	Наявність функцій ідентифікації і аутентифікації
	Наявність функцій перевірки збереження конфіденційних даних
	Наявність функцій контролю дотримання конфіденційності
	Наявність функцій відновлення конфіденційності
	Наявність функцій моніторингу та оповіщення порушень конфіденційності
Рівень доступності L_A – здатність системи забезпечувати фізичний захист від можливості зміни заданих параметрів технічних і (або) інформаційних ресурсів у заданих точках за кінцевий час	Наявність паролів доступу до інформаційних ресурсів
	Наявність розподілу зон (рівнів) доступу між користувачами
	Наявність стійкості функціонування при помилках користувача, пов'язаних з конфіденційністю
Рівень секретності L_S – характеристика здатності системи зберігати секретність технічних і (або) інформаційних ресурсів	Наявність технічних засобів захисту інформації
	Наявність захисту від несанкціонованого доступу
	Наявність криптографічних засобів захисту інформації

Для визначення комплексної кількісної оцінки рівня гарантоздатності системи в цілому визначаються комплексні оцінки її основних атрибутів. Комплексну оцінку конфіденційності визначимо за допомогою середнього арифметичного, яке визначається за формулою [5]:

$$A_{конф} = \sum_{j=1}^{m} g_j L_j, \qquad (1)$$

де L_j – численне значення j-тої метрики конфіденційності;

g_j – ваговий коефіцієнт j-тої метрики конфіденційності;

m – кількість метрик конфіденційності.

Вагові коефіцієнти g_j враховують важливість кожної метрики серед інших і визначаються експертним методом $(\sum_{j=1}^{m} g_j = 1)$.

Метрики конфіденційності мають якісний вид представлення, тому для визначення їх комплексної оцінки використовується експертний метод з ранжируванням за трирівневою шкалою.

Конфіденційність характеризується трьома метриками: вірогідність загроз P_D, рівень доступності L_A, рівень секретності L_S.

Як приклад визначимо комплексну оцінку ймовірності загроз P_D.

Експертним методом визначаємо рівень критеріїв оцінки ймовірності загроз. При цьому позначимо: В – високий рівень; С – середній рівень; Н – низький рівень. Комплексна оцінка ймовірності загроз визначається формулою [5]:

$$P_D = 1 - \sum_{j=1}^{m_H} g_{H_j} - 0{,}5\sum_{j=1}^{m_C} g_{C_j}, \qquad (2)$$

де m_H – число показників низького рівня;

m_c – число показників середнього рівня;

g_{H_j} – нормований критерій низького рівня;

g_{C_j} – нормований критерій середнього рівня.

Вимоги нормування зводяться до того, щоб сума ваг усіх критеріїв дорівнювала одиниці. Критерії оцінки ймовірності загроз позначимо таким чином:

K_1 – наявність функцій ідентифікації і аутентифікації;

K_2 – наявність функцій перевірки збереження конфіденційних даних;

K_3 – наявність функцій контролю дотримання конфіденційності;

K_4 – наявність функцій відновлення конфіденційності;

K_5 – наявність функцій моніторингу та оповіщення порушень конфіденційності.

У табл. 2 як приклад наведено рівні критеріїв ймовірності загроз, проставлених сьома експертами. Визначимо комплексну оцінку ймовірності загроз P_D при значеннях вагових коефіцієнтів, які також визначаються експертами, для вищеозначених критеріїв:

$$g_1 = 0{,}25; \quad g_2 = 0{,}12; \quad g_3 = 0{,}13; \quad g_4 = 0{,}25; \quad g_5 = 0{,}25.$$

Таблиця 2. Експертна таблиця ранжирування критеріїв оцінки ймовірності загроз

Експерти	K_1	K_2	K_3	K_4	K_5
1	В	Н	С	В	В
2	С	Н	Н	В	С
3	В	С	Н	С	В
4	С	С	С	В	С
5	В	С	Н	С	В
6	В	Н	С	С	В
7	В	С	Н	В	В

Кількість критеріїв низького рівня дорівнює $n_н = 7$. Пронормуємо ваги критеріїв низького рівня:

$$g_{2,н} = \frac{0{,}12 \cdot 3}{7} = 0{,}051;\ g_{3,н} = \frac{0{,}13 \cdot 4}{7} = 0{,}074.$$

Кількість критеріїв середнього рівня дорівнює $n_c = 14$. Пронормуємо ваги критеріїв середнього рівня:

$$g_{1,c} = \frac{0{,}25 \cdot 2}{7} = 0{,}071;\ g_{2,c} = \frac{0{,}12 \cdot 4}{7} = 0{,}069;\ g_{3,c} = \frac{0{,}13 \cdot 3}{7} = 0{,}056;$$

$$g_{4,c} = \frac{0{,}25 \cdot 3}{7} = 0{,}11;\ g_{5,c} = \frac{0{,}25 \cdot 2}{7} = 0{,}071\cdot$$

Підставивши пронормовані ваги критеріїв у формулу (2), отримаємо комплексну оцінку ймовірності загроз P_D.

$$P_D = 1 - (0{,}051 + 0{,}074) - 0{,}5(0{,}071 + 0{,}069 + 0{,}056 + 0{,}11 + 0{,}071) = 0{,}6865.$$

Аналогічно визначаються комплексні оцінки рівня доступності L_A та рівня секретності L_S. Комплексна оцінка рівня конфіденційності визначається за формулою (1).

6. Висновки

Конфіденційність гарантоздатних КС зводиться до розробки заходів, спрямованих на забезпечення збереження і строго регламентованої доступності технічних та інформаційних ресурсів. Всі умови і параметри конфіденційності встановлюються на етапах розробки і проектування ГКС і, в основному, зводяться до встановлення різного рівня доступу персоналу до інформації з різним ступенем секретності і використання програмно-апаратних засобів захисту інформації. Для кожної ГКС розробляється політика конфіденційності, яка базується на певних методах і механізмах забезпечення конфіденційності. У роботі вперше запропоновано підхід до кількісної оцінки рівня конфіденційності ГКС, який може застосовуватися для систем найрізноманітнішого призначення, включаючи системи критичного використання. Отримана таким чином кількісна оцінка конфіденційності дозволить надалі здійснити кількісну оцінку рівня гарантоздатності системи в цілому.

СПИСОК ЛІТЕРАТУРИ

1. Совет Европы. Конвенция о преступности в сфере компьютерной информации (ETS N 185). Будапешт [Електронний ресурс]. – Будапешт, 2001. – Режим доступу: http://www.alppp.ru/law/pravosudie /46/konvencija-o-prestupnosti-v-sfere-kompyuternoj-informacii---185-rus--angl-.html.
2. Галицкий А.В. Защита информации в сети. Анализ технологий и синтез решений / А.В. Галицкий, С.Д. Рябко, В.Ф. Шаньгин. – М.: ДМК Пресс, 2004. – 616 с.
3. Норткатт С. Защита сетевого периметра / Норткатт С.; пер. с англ. – К.: ООО «ТИД «ДС», 2004. – 672 с.
4. ITSEC. Information Technology Security Evaluation Criteria (ITSEC): Preliminary Harmonised Criteria. Document COM (90) 314, Version 1.2. Commission of the European.Communities [Електронний ресурс]. – 1991. – June. – Режим доступу: http://www.ssi. gouv.fr/ site documents/ITSEC/ITSEC-uk.pdf. Retrieved 2006-06-02.
5. Хамханова Д.Н. Основы квалиметрии: учебн. пособ. для студентов специальности 190800 «Метрология и метрологическое обеспечение» / Хамханова Д.Н. – Улан-Удэ, Россия: Изд-во ВСГТУ, 2003. – 76 с.

Стаття надійшла до редакції 27.05.2014