УДК 004.5

**М. Г. Кузнєцова**
Інститут проблем реєстрації інформації НАН України
вул. М. Шпака, 2, 03113 Київ, Україна

# Застосування механізмів підвищення живучості для забезпечення захищеності інформаційного ресурсу в розподілених системах

*Розглянуто особливості забезпечення захищеності інформаційних ресурсів у розподілених інформаційних системах (РІС). Проаналізовано притаманні РІС механізми підвищення живучості й показано можливість їхнього застосування при побудові сучасних систем захисту.*

***Ключові слова:*** *живучість, захищеність, інформаційні ресурси, розподілені інформаційні системи.*

Широке впровадження розподілених інформаційних систем (РІС) є характерним сьогодні майже для всіх галузей людської діяльності, де на них покладається вирішення все важливіших задач. Вони відповідають за виконання технологічних процесів на виробництві, за зв'язок і телекомунікації, енергетичне постачання й транспортне обслуговування, виконання соціальних і медичних програм, за підтримку державної, оборонної, наукової діяльності. Від якості функціонування РІС суттєво залежить якість напрацювання та прийняття рішень й ефективність функціонування багатьох соціальних, економічних, військових, політичних структур тощо.

РІС складаються з технічних, програмних та інших засобів, поєднаних структурно й функціонально для забезпечення одного чи декількох видів інформаційних процесів та надання інформаційних послуг. Сучасним РІС притаманні ієрархічність, функціональна розподіленість, високий ступінь розпаралелювання ресурсів (обслуговування, логіки, програмного та апаратного забезпечення, телекомунікацій), і практично повна відсутність централізованого управління.

З точки зору системного аналізу, РІС — це складні технічні системи, які функціонують в умовах дії випадкових факторів, при активній взаємодії із зовнішнім середовищем, при наявності негативних впливів різної природи та при високій вартості наслідків можливих порушень чи помилок у роботі системи [1, 2]. РІС мають свою ціль функціонування, велику кількість взаємодіючих елементів, блоків, підсистем, складну ієрархічну систему управління. Вони характеризуються

також складністю поведінки та функцій, що ними виконуються, постійним зростанням кількості користувачів та підключеного обладнання, постійною модифікацією складових, що призводить до неможливості побудови адекватної математичної моделі для вичерпного опису функціонування системи. Зростання складності структури й функціонування РІС обумовлює появу таких властивостей як природна надмірність, адаптивність, надійність, стійкість до відмов, стійкість до зовнішніх впливів, живучість.

Інтенсифікація процесів інформаційної взаємодії, підсилений розвиток територіально розподілених систем, широке використання ресурсів мережі Інтернет висуває нові вимоги до технологій роботи в РІС, технологій розробки таких систем, забезпечення безпеки їхнього функціонування, потребує розвитку безпечних технологій роботи з інформаційними ресурсами, впровадження методів і засобів підвищення живучості РІС.

Організація роботи з інформаційним ресурсом (ІР) у розподілених системах передбачає вирішення комплексу задач забезпечення зручного та швидкого доступу до інформації для тих, хто має на це право, і найширшого, на всіх шляхах передачі й при всіх видах обробки та перетворення, захисту інформації від тих, хто не має відповідного права доступу. Це призводить до необхідності вирішувати додаткові проблеми безпеки, пов'язані із захистом каналів зв'язку, авторизації віддалених користувачів і програм, захисту віддалених вузлів системи, захисту всієї розподіленої системи як цілого, керування нею. Саме вимоги щодо системності й комплексності засобів захисту викликають сьогодні найбільші проблеми, а успішне створення систем забезпечення інформаційної безпеки відстає від розвитку технологій передачі й обробки інформації.

Захищеність інформаційних ресурсів та інформаційного середовища традиційно розглядають як [6, 7]:

— сукупність засобів і технологічних прийомів, що забезпечують захист компонентів інформаційного середовища;

— мінімізацію ризику для компонентів і ресурсів інформаційного середовища;

— комплекс процедурних, логічних і фізичних заходів, які спрямовані на протидію загрозам інформаційному ресурсу і компонентам інформаційного середовища.

Оскільки захищеність інформаційного ресурсу передбачає ще й неможливість його втрати внаслідок відмов компонентів інформаційного середовища, проблему забезпечення безпечної роботи з інформаційним ресурсом, звичайно, декомпозують на проблему забезпечення високонадійної обчислювальної бази (ТСВ — Trusted Computing Base), яка має гарантувати безперервність функціонування інформаційного середовища, і на проблему створення системи протидії та запобігання загрозам ІР.

Вимоги щодо безпеки функціонування розподілених інформаційних систем мають бути формально визначені. Виконання цих вимог гарантує, що при виникненні передбачених проблемних ситуацій від небажаних впливів різної природи, включаючи відмови складових РІС, система буде здатна виконувати свою цільову функцію в повному обсязі. При чіткому визначенні технічних умов функціону-

вання безпека системи оцінюється та забезпечується в процесі проектування, шляхом ретельного формування архітектури системи, впровадження спеціальних засобів і процесів, і не може бути порушена незалежно від будь-яких передбачених обставин. Реалізація надійної обчислювальної бази можлива за рахунок використання якісних програмно-технічних компонентів, прийняття обґрунтованих рішень щодо підвищення надійності та відмовостійкості, впровадження засобів безперервного живлення, резервування критичних компонентів, застосування механізмів динамічної реконфігурації, спеціальних засобів підвищення живучості.

Для забезпечення захищеності ІР у розподілених системах набуває розвитку підхід, пов'язаний зі створенням технологій безпечної роботи з інформаційним ресурсом на весь його життєвий цикл, на основі аналізу можливих ризиків, особливостей зберігання, обробки й передачі.

Рішення щодо побудови технологій безпечної роботи з ІР базуються на виборі стратегії боротьби за інформаційну безпеку [6]. Оборонна стратегія спрямована на автономне протистояння відомим загрозам, які є найбільш вірогідними для даної системи. Наступальна стратегія передбачає використання активних засобів боротьби проти всієї множини очікуваних загроз, використовуючи й можливості самого інформаційного середовища. Для випереджуючої стратегії характерним є створення такого інформаційного середовища, у якому загрози взагалі не мають умов для свого проявлення.

Зрозуміло, що технологія безпечної роботи з інформаційним ресурсом суттєво залежить від ретельності дослідження інформаційної моделі, передбаченої множини загроз, якості прийнятих рішень щодо технічного та програмного забезпечення РІС. На сьогодні, нажаль, не формалізовані й кількісно не визначені такі суттєві поняття, як рівень захищеності та необхідний рівень захищеності ІР у розподілених системах.

Разом із тим, напрацьовані й впроваджуються стандартні засоби підтримки безпечних технологій роботи з інформаційним ресурсом: набули широкого розвитку засоби захисту ІР у базах даних (наприклад, Informix — DCE/Net, операційні системи з багаторівневим захистом від несанкціонованого доступу), використовуються нові технології створення засобів обробки й передачі даних, які дозволяють захистити їх від витоку технічними каналами (оптоволокно, смарткарти, жетони SecurID, карточки для формування цифрового підпису), розроблені технології захищеної передачі даних відкритими мережами (VPN-технології), запропонована технологія периметру, який охороняється (ТПО), що передбачає всебічний захист корпоративних інформаційних активів від загроз безпеці [4, 7, 9–11].

ТПО взагалі передбачає побудову навкруги корпоративної мережі периметру, через який весь Internet-трафік пропускається тільки після ретельної перевірки [11]. Ця технологія потребує інтеграції засобів захисту різних типів, об'єднання їх у єдину структуру з багаторівневою організацією, що забезпечує підвищення загального рівня захищеності й ефективності контролю над інформацією. Необхідними компонентами технології є брандмауер, служба каталогів, маршрутизатор, програмне забезпечення фільтрації інформаційного наповнення (від вірусів, від шкідливого коду, фільтри електронної пошти, web-ресурси управління каналами web-доступу).

Одним із технологічних рішень, які дозволяють забезпечити заданий рівень захищеності для, наприклад, розподіленої корпоративної мережі, є використання віртуальних приватних мереж (Virtual Private Networks — VPN) [7, 12]. Як мережі передачі даних використовуються мережі загального призначення (наприклад, Internet), а захищеність інформації досягається за допомогою криптографічних засобів та механізму електронного цифрового підпису. Така технологія дозволяє забезпечити виконання вимог щодо конфіденційності, автентичності (достовірності) та цілісності інформації, що передається каналами зв'язку, підтвердити одержання та авторство повідомлень, забезпечити захист IP від несанкціонованого доступу з боку мереж і каналів передачі даних

При побудові та впровадженні VPN-технологій для розподілених систем сьогодні використовуються такі стандартні рішення: VPN на базі мережних операційних систем, VPN на базі маршрутизаторів (CISCO), VPN на базі міжмережевих екранів (Firewall, Check Point), VPN на базі спеціалізованого програмного забезпечення, VPN на базі спеціалізованих апаратних засобів тощо.

Для підвищення захищеності інформаційних ресурсів нещодавно був запропонований новий підхід — створення адаптивних систем захисту, які орієнтовані на активне протистояння загрозам безпеці [8, 13]. Реалізація такого підходу потребує проведення аналізу ризиків, розробки політики безпеки, використання традиційних засобів захисту, а також впровадження контрзасобів для протистояння загрозам, постійного аудиту безпеки та моніторингу стану системи, що має дозволити оперативно реагувати на ризики безпеки. Основними засобами, які використовуються при реалізації адаптивних систем захисту, є пасивні — фільтри, екрани, і активні — датчики виявлення вторгнень, алгоритми розпізнавання аномальної поведінки, адаптивні алгоритми відновлення.

На практиці умови функціонування більшості розподілених інформаційних систем досить важко визначити формально, вичерпно, вони можуть порушуватися через негативний вплив як людських, так і технічних факторів, тому можливе виникнення непередбачених проблемних ситуацій, які потребують адекватної реакції системи. Для прогнозування, встановлення, уникнення, подолання таких ситуацій використовуються механізми та засоби підвищення живучості систем, незважаючи на всі складності їхньої реалізації.

Живучість як властивість РІС характеризує її здатність обирати оптимальний режим функціонування за рахунок власних внутрішніх ресурсів, перебудови структури, зміни функцій та поведінки окремих підсистем у зв'язку зі зміною зовнішніх умов та відповідно до цілі її функціонування [1, 2].

Для забезпечення живучості в РІС передбачається наявність механізмів:

— моніторингу стану системи та впливів середовища;

— адаптації при незначній зміні умов для оптимізації функціонування системи відповідно до заданих критеріїв;

— відновлення функціонування після збоїв, відмов, помилок;

— перерозподілу ресурсів системи для виконання цілі її функціонування в нових умовах.

Задачі, які вирішуються за допомогою цих механізмів у РІС, дуже схожі на ті задачі, які мають вирішуватися для створення захищеного інформаційного сере-

довища при використанні адаптивних систем захисту. Розглянемо докладніше ті механізми підвищення живучості, які реалізуються зараз у РІС і які можуть бути використані для підвищення захищеності інформаційного середовища та інформаційних ресурсів РІС.

Серед механізмів підвищення живучості зазвичай виділяють механізми реконструкції, реорганізації, реконфігурації, розпізнавання, протидії, відновлення, адаптації [1–3, 5, 14, 15].

Механізми розпізнавання в РІС дозволяють на основі даних моніторингу системи й середовища виявляти потенційно небезпечні стани й незабаром адекватно на них реагувати (фіксувати структурні зміни в системі внаслідок відмов її компонентів, підвищення ризику виходу з ладу критичних компонентів систем, виявляти атаки, успішні вторгнення, ризики втрати чи викривлення інформації тощо).

Механізми протидії в РІС спрямовані на підтримку визначених умов функціонування й мінімізацію збитків, які можливі в зв'язку з виникненням нових умов функціонування та непередбачених впливів. Ці механізми базуються на класичних методах забезпечення безпеки, надійності та відмовостійкості інформаційних систем, включаючи резервування критичних компонентів, контроль доступу та використання ресурсів системи, відвернення вірусних атак тощо.

Механізми адаптації дають можливість пристосовуватися до зовнішніх змін середовища функціонування РІС, компенсуючи небажані впливи й дозволяючи системі оптимізувати свою роботу відповідно до встановлених критеріїв, і навіть змінити ціль функціонування, якщо цього вимагають нові умови.

Механізми відновлення в РІС забезпечують відновлення функціональності та працездатності компонентів системи й РІС у цілому при небажаних впливах, а також після припинення впливів. Механізми відновлення мають виконувати ідентифікацію й локалізацію несправностей, виправлення помилок у програмах і даних, встановлення затримки в часі, перерозподіл ресурсів між процесами, заміну й відключення несправних елементів, ремонт, реєстрацію спостережень і виконаних дій, власно відновлення роботи (повне чи часткове) або завершення послідовності операцій безпечного останову.

Механізми реорганізації забезпечують перерозподіл функцій компонентів РІС, які вийшли з ладу, між працездатними компонентами системи або, у разі неможливості перерозподілу, — перехід системи до нової цілі функціонування.

Механізми реконфігурації реалізують автоматичну перебудову структури мережі обміну інформацією для досягнення найбільшої ефективності виконання цілі функціонування на наявних працездатних ресурсах РІС.

Механізми реконструкції виконують редукцію цілі функціонування та ресурсів системи до визначених базових рівнів, коли система може виконувати чітко окреслену множину функцій, або забезпечити плавність деградації визначених параметрів (безпечний останов).

Конкретна реалізація цих механізмів передбачає використання як відомих технічних та технологічних рішень та засобів, так і розробку нових, відповідно до специфіки задач системи. Впровадження механізмів підвищення живучості в розподілені інформаційні системи потребує проведення аналізу ризиків, урахування особливостей і цілей функціонування кожної конкретної системи, оцінки економічної доцільності.

Сьогодні суттєвим є використання наявних системних засобів та можливостей розподіленої інформаційної системи для забезпечення безпечної роботи з інформаційними ресурсами. Для вирішення цієї проблеми окрім уже згаданих вище спеціальних засобів та технологій захисту можуть бути використані притаманні РІС механізми підвищення живучості, розвинуті для вирішення задач безпеки, наприклад, при створенні адаптивних систем захисту, що орієнтовані на активне протистояння загрозам безпеці.

Особливістю використання механізмів та засобів забезпечення живучості є те, що вони дозволяють відреагувати на небажаний вплив, і забезпечити перехід системи в безпечний для неї стан ще до проведення аналізу причин події (наприклад, порушення безпеки). Отже, спираючись на механізми забезпечення живучості, системи захисту інформаційного середовища та інформаційного ресурсу можна будувати на схемах «що, якщо», а не на класичних схемах «захист від».

Уже сьогодні механізми підвищення живучості можуть бути застосовані для цілеспрямованої зміни конфігурації програмно-апаратних засобів РІС із метою покращення захисту системи та її інформаційних ресурсів, ускладнення реалізації атак на систему, відвернення атак, протидії виникненню нештатних ситуацій, продовження чи подовження функціонування системи в нештатних ситуаціях, «безпечного останову», повного чи часткового відновлення функціонування системи тощо. Використання системних засобів та механізмів підвищення живучості можливе після проведення досліджень з аналізу ризиків, виявлення критичних функцій і ресурсів системи, розробки політики безпеки, вибору традиційних засобів захисту, реалізації засобів для протидії визначеним загрозам.

Так, аудит безпеки й моніторинг стану системи механізмами розпізнавання та протидії дозволять розпізнавати та оперативно реагувати на ризики безпеки, виконуючи, наприклад, такі функції, необхідні для підвищення захищеності інформаційного ресурсу в розподілених системах:

— викриття несанкціонованої діяльності (навмисної чи випадкової) та відвертання можливих наслідків у реальному масштабі часу;

— відвертання хакерських атак на критичні додатки та системні сервіси;

— виконання заданої послідовності відповідних дій при виявленні спроб вторгнення в систему (з метою припинення з'єднання з порушником, зміни конфігурації вузлів мережі, повідомлення адміністратору тощо);

— реєстрація діяльності користувачів системи й аналіз одержаних даних із метою відвернення подальших спроб порушення політики безпеки за вже відомими схемами;

— аналіз існуючої конфігурації системи з метою виявлення та усунення вразливостей.

Завдяки застосуванню механізмів реконфігурації можуть бути виконані:

— автоматична реконфігурація міжмережевих екранів, маршрутизаторів, комутаторів та інших засобів для відбиття атаки на РІС у реальному масштабі часу;

— створення кордону й відвернення подальшого проникнення порушника в мережу;

— динамічне формування надійної конфігурації систем захисту для різних груп користувачів відповідно до їхніх повноважень.

Прийняття своєчасних і ефективних рішень щодо захисту інформаційних ресурсів РІС можливе при використанні механізмів реконструкції та реорганізації, механізми протидії та відновлення дозволять зберегти критичні інформаційні ресурси системи, механізми адаптації дозволять компенсувати небажані впливи на інформаційні ресурси РІС.

Таким чином, сучасною задачею забезпечення захищеності інформаційних ресурсів РІС є не стільки обмеження доступу до тих чи інших програм та даних, скільки визначення та делегування їхніх повноважень у корпоративному вирішенні задач, виявлення спроб аномального використання ресурсів, прогнозування аварійних ситуацій та ліквідація їхніх наслідків за рахунок гнучкої адаптації структури системи при виникненні відмов, частковій утраті чи тривалому блокуванні ресурсів. Нагальною потребою подальших досліджень є розробка та створення наскрізних системних рішень, які дозволяли б ефективно використовувати наявні засоби й механізми забезпечення живучості, інтегровані в різні програмно-апаратні платформи та прикладні застосування.

1. *Додонов А.Г., Кузнецова М.Г., Горбачик Е.С.* Введение в теорию живучести вычислительных систем. — К.: Наук. думка, 1990. — 184 с.

2. *Додонов А.Г., Кузнецова М.Г., Горбачик Е.С.* Живучесть и надежность сложных систем. Методическое пособие. — Международный научно-учебный центр ЮНЕСКО/МПИ информационных технологий и систем. — 2001. — 163 с.

3. *Додонов А.Г., Горбачик Е.С., Кузнецова М.Г.* Живучесть информационно-аналитических систем в аспекте информационной безопасности: Сб. науч. тр. «Информационные технологии и безопасность». Вып. 4. — К.: ИПРИ НАНУ, 2003. — С. 27–30.

4. *Кузнєцова М.Г.* Забезпечення захищеності інформаційних ресурсів у розподілених системах: Сб. науч. тр. «Информационные технологии и безопасность». Вып. 7. — К.: ИПРИ НАНУ, 2004. — С. 38–40.

5. *Кузнєцова М.Г.* Використання механізмів підвищення живучості у розподілених інформаційних системах: Сб. науч. тр. «Информационные технологии и безопасность». Вып. 8. — К.: ИПРИ НАНУ, 2005. — С. 63–65.

6. *Домарев В.В.* Защита информации и безопасность компьютерных систем. — К.: Изд-во «ДиаСофт», 1999. — 480 с .

7. *Домарев В.В.* Безопасность информационных технологий. Методология создания систем защиты. — К.: ООО «ТИД «ДС», 2001. — 688 с.

8. *Ильин В.Е., Комарович В.Ф., Осадчий А.И.* Анализ проблемы адаптивной защиты ИВС в условиях информационного противоборства // Защита информации. Конфидент. — 2002— № 4-5. — С. 99–107.

9. *Шнейер Б.* Сетевой контроль и безопасность // Защита информации. Конфидент. — 2004. — № 4. — С. 75–81.

10. Новая концепция надежного хранения данных // Банковские технологии. — 2004. — № 6. — С. 25–30.

11. Будущее информационной безопасности: интегрированная система охраны периметра // Защита информации. Конфидент. — 2001. — № 2. — С. 56–59; оконч. — 2001. — № 3. — С. 86–90.

12. *Лукин В.* Первый кирпич в стене VPN // Сети и телекоммуникации. — 2002. — № 4. — С. 51–55.

13. *Левитт К.Н., Роу Д., Балепин И.В., Мальцев С.В.* Системы быстрого реагирования // Защита информации. Конфидент. — 2003. — № 5. — С. 47–50.

14. *Robert J. Ellison, David A. Fisher, Richard C. Linger, Howard F. Lipson, Thomas A. Longstaff, Nancy R. Mead.* Survivable Network Systems: An Emerging Discipline. http://www.cert.org/research/97tr013.pdf

15. *Robert J. Ellison, David A. Fisher, Richard C. Linger, Howard F. Lipson, Thomas A. Longstaff, Nancy R. Mead.* Survivability: Protecting Your Critical Systems. http://www.cert.org/archive/html/protect-critical-systems.html

Надійшла до редакції 18.08.2006