УДК 621.32

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ НАДІЙНОСТІ АСУ

к.т.н. М.І. Гіневський, к.в.н. І.М. Майборода, С.Ю. Гайдаров
(подав проф. А.В. Корольов)

Розглянуто підходи до забезпечення захисту інформації в АСУ від викривлень. Запропоновано рекомендації з застосування комплексу мір активного програмного захисту від викривлень.

Надійність – це одна з центральних проблем АСУ. Правильний підхід до неї та її рішення забезпечать життєдіяльність АСУ. Надійність в АСУ – проблема комплексна. Тому що всі частини АСУ взаємозалежні одна з одною, низька надійність будь-якого елемента АСУ позначається на надійності всієї системи. При проектуванні системи завжди прагнуть забезпечити високу ефективність її застосування, однак при низькій надійності ця висока ефективність не буде реалізована.

Прагнення до підвищення надійності системи спрямоване на те, щоб одержати вірну інформацію про управляємий об'єкт і про середовище, у якому він знаходиться. Викривлення інформації може з'явитися в самому джерелі ще до введення інформації. Джерелом може бути як автоматичний пристрій, так і людина, що готує інформацію для введення. Можуть з'явитися викривлення й у каналі зв'язку, включаючи кінцеве устаткування, при передачі інформації. Викривлення може виникнути також у результаті систематичних чи випадкових збоїв при програмній обробці інформації. Порушення порядку надходження повідомлень у систему в порівнянні з технологічним порядком виконання операцій, про які сповіщається, також є причиною, що викликає викривлення інформації. Це може порушити відповідність між інформацією, що міститься в базах даних, і фактичним станом об'єкта.

Міри захисту частин АСУ від викривлення інформації за способами здійснення поділяють на самостійні і сполучені з іншими функціями; за призначенням – на міри для виявлення власних викривлень і міри для виявлення викривлень, що виникли в попередніх частинах АСУ [1]. Перші передбачаються в кожній частині системи, щоб не допустити появи викривлень, а також виявити і виключити ті, що з'явилися в цій же частині викривлення і визначити причини їхнього виникнення. Природно, що першою мірою в цьому випадку є високоякісна побудова самої частини (технічної чи програмної) таким чином, щоб вона сама не виявилася джерелом викривлень.

Міри захисту другої групи служать для виявлення викривлень інформації, що з'явилися в попередніх частинах системи, і причини їхнього виникнення. Вони можуть бути самостійними чи мірами сполученими з функціями,

які реалізують будь-які інші задачі.

Широко застосовуються міри для захисту окремих частин АСУ [2]. Серед них виділяється група мір, спрямована на забезпечення ймовірності в самому каналі зв'язку. До них можна віднести міри, пов'язані з утворенням надлишкових (захищених) несущих кодів та із спеціальною їх обробкою при передачі і прийомі. Це можуть бути коди для перевірки слів на парність, коди Хеммінга та багато інших. Крім того, звичайно застосовується використання і перевірка контрольних сум усього переданого інформаційного матеріалу; дубльована передача з використанням тих же контрольних сум; метод посимвольного порівняння для більш щільного використання каналу зв'язку й ін.

Однак перерахованих мір недостатньо, тому що викривлення може виникнути в самому джерелі, і в цьому випадку надійний канал зв'язку буде ймовірно передавати викривлену інформацію.

Якщо виключити застосування коригувальних надлишкових захисних кодів, то описані міри захисту системи від викривлень можуть бути охарактеризовані як пасивні. Якщо викривленням тільки перепиняти шлях до пам'яті, то ми не позбудемося від них. Це зумовлено тим, що відсутність інформації про подію, яка відбулася, на об'єкті також є викривленням правильного відображення, що містилося в пам'яті. Тому необхідно, щоб захист був активний, тобто щоб він не тільки виявляв викривлену інформацію та перепиняв їй шлях у пам'ять, але і сприяв появі достовірної. Нижче перелічуються й узагальнюються деякі підходи до комплексного застосування активного програмного захисту.

Повторення викривлення. При застосуванні цього виду активного захисту після виявлення в повідомленні викривлення необхідно, щоб система видала вимогу на повторення тієї частини повідомлення, що була викривлена.

У випадку, коли джерелом є автоматичний датчик без пристрою пам'яті, вимога повторної передачі нездійсненна. Якщо ж датчик буде мати таку пам'ять, то повторна передача можлива. Очищення пам'яті в цьому випадку буде здійснюватися за сигналами з керуючої ЕОМ, яка збільшить завантаження каналів зв'язку. Помітимо, що якщо викривлення мало місце при прийомі повідомлення датчиком, то воно буде й у його пам'яті. Питання про доцільність застосування датчиків з пам'яттю повинне бути вивченим у кожному випадку окремо.

Ця міра вимагає зайвого завантаження каналів зв'язку і пам'яті та може вповільнити рух вхідного інформаційного потоку, якщо поряд з нею не будуть застосовані й інші, більш ефективні заходи.

Повне відновлення інформації. Ця міра застосовна, коли програмно, за супутніми факторами і даними, можна безпомилково встановити вірогідність заміни виявленого викривлення (наприклад, відновлення правильної літери або букви у слові відповідно до інших букв, що може бути виконане за допомогою зіставлення із словником - довідником під час пошуку цифрових кодів при обробці повідомлення по прийому і при перевірках типу пошуку семан-

тичних помилок і ін.).

Ймовірне виправлення. Цей підхід, зокрема, подібний попередньому. Його відмінність полягає в ступені впевненості у вірогідності виправлення, яка може бути оцінена програмно. Така міра застосовна в тому випадку, коли очікується надходження іншого, технологічно зв'язаного повідомлення слідом за прийнятим з викривленням. По цьому другому повідомленню виявляється можливим зробити остаточний висновок про коректність зробленого ймовірного виправлення. При застосуванні ймовірного виправлення виробляється оцінка виправленого, котра зберігається до надходження другого повідомлення і переходу його з категорії ймовірного до категорії абсолютного виправлення.

Повторення з виправленням. Можливий випадок, коли викривлення виявляється на одній з останніх подій технологічного ланцюжка. Тоді частини бази даних, де накопичуються дані про фактично виконану роботу, будуть викривлені. У цьому випадку після уточнення запитами типу «вимога повторення» необхідно виправити масив на значення алгебраїчної різниці, отриманої при використанні викривленої інформації та достовірної.

Облік викривлень. В АСУ не повинні автоматизуватися тільки «чужі» стосовно системи праці. Автоматизації підлягає й власна діяльність системи. Одним з аспектів цього є ведення обліку викривлень у спеціальній частині БД. Найважливішою активною мірою для постійного захисту системи є автоматичне виконання в самій системі обліку й аналізу викривлень, які з'явилися та виявилися, по класах пристроїв і операторах. Це повинен бути науково обґрунтований облік, що має і профілактичний характер, який впливає як на технічний аспект, так і на організацію вірного змісту пристроїв (включаючи і робочі станції), так і на дисциплінарний елемент психології людей, що обслуговують систему і безпосередньо вводять інформацію вручну. Це до деякої міри повільно діючий, але дуже ефективний захід активного захисту. Крім того, необхідний і подібний автоматичний облік допущених помилок у прогнозах, виявлених після здійснення передбачуваних подій.

Усі ці активні програмні міри варто застосовувати одночасно, вони повинні бути зв'язані між собою і доповнювати одна одну.

ЛІТЕРАТУРА

1. Bhashar K. Computer Security: Threats and Countermeasures. – Oxford: NCC Blackwell. – 786 p.

2. Конноли Т., Бегг К., Страчан А. Бази даних. Проектування, реалізація і супровід. Теорія і практика. – М.: Вільямс, 2000. – 1112 с.

Надійшла до редколегії 13.03.2001