УДК 681.518.3

Бойченко Олег Валерійович
Лєнков Сергій Васильович
Сєлюков Олександр Васильович
Шкуліпа Павло Альфредович

МЕТОДИКА ТЕСТОВИХ ВИПРОБУВАНЬ СТІЙКОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Постановка проблеми. Аналіз останніх досліджень і публікацій

Різноманіття і специфічність задач правоохоронних органів, що часто вирішуються в умовах невизначеності, неповної інформації, наявності випадкових чинників і ризику, вимагають розроблення й дослідження моделей і методів оцінювання стійкості, функціональної безпеки та живучості інформаційних систем спеціального призначення (ІССП), а також інформаційних технологій для створення гарантоздатних автоматизованих систем переробки інформації та управління критичного застосування [1-4].

Проведений аналіз практики застосування ІССП правоохоронної діяльності визначає низку недоліків, пов'язаних з невідповідністю поточного рівня показників живучості та безпечності функціонування ІССП, а також з невідповідністю характеристик відмово стійкості та відновлюваності програмного забезпечення ІССП. Наведене підтверджується результатами досліджень таких вчених, як В.М.Глушков, А.І. Сбітнєв, О.В. Барабаш та інших.

Формулювання мети статті. Виклад основного матеріалу

Одним із напрямів вирішення проблеми підвищення стійкості ІССП є удосконалення технології пошарового проектування (ТПП) стійкого програмного забезпечення (СПЗ) з використанням системного підходу, що дозволяє створити умови для розроблення специфікацій, які базуються на визнанні факту можливості виникнення перекручувань у роботі ПЗ і обчислювальних засобів (ОЗ).

Системний підхід до проектування СПЗ ІССП полягає в розробленні ПЗ контролю і виправлення помилок у роботі ОЗ, розробленні структури ПЗ, що використовує зворотний зв'язок між підпорядкованим і верхнім рівнем, а також розміщення засобів контролю виконання ПЗ відповідно до рівнів ієрархії в системі [5].

З метою визначення доцільності запровадження удосконаленої ТПП в практичну діяльність інформаційно-аналітичних підрозділів розроблено методику тестових випробувань стійкості ПЗ інформаційної системи (ІС) до несанкціонованих впливів (НСВ). Основою методики є проведення експерименту з порівняння реакції ІС за наявності та за відсутністю НСВ до та після впровадження ТПП СП.

Методика упроваджена таким конкретним чином: є 10 шарів захисту, кожен шар пов'язаний з певним етапом криптографічних перетворень. Є маркери відсутності несанкціонованих модифікацій в шарах ($S_1,\dots S_{10}$) і у всій структурі, що захищається (S). Якщо відповідний маркер дорівнює 1, то несанкціонована модифікація відсутня, якщо 0 – несанкціонована модифікація є. Якщо хоч би один маркер з ($S_1,\dots S_{10}$) рівний 0, то $S = 0$.

Самоконтроль тут організований таким чином: є два паралельні ідентичні потоки крипто перетворювань, що працюють в режимі реального часу і ще один потік (третій), який порівнює їх між собою в реальному режимі часу і фіксує значення $S_1,\dots S_{10}$ і S.

Передбачається, що програмно-апаратна архітектура така, що несанкціонований користувач, в принципі може дістати доступ до обчислювального процесу і модифікувати його, але лише до якогось одного в певний момент часу.

Якщо він проводитиме модифікацію одного з потоків крипто перетворювань, то між цими обчислювальними потоками з'явиться різниця, яка буде відбита в обчислювальному потоці порівняння і ця модифікація буде виявлена по ($S_1,\dots S_{10}$) та у підсумку S. Якщо ж раптом буде проводиться модифікація потоку порівняння, то потоки крипто перетворень будуть незаймані і весь процес шифрування-розшифровки пройде без порушення штатного режиму.

Недолік тут в тому, що сумарна обчислювальна ємкість підвищується приблизно в 3 рази (потрібно три потоки, замість одного), та натомість реалізується виявлення модифікації.

Для зручності проведення експерименту дослідження проводилися за двома основними напрямами (1 – фіксація реакції ІС на НСВ без запровадження ТПП СПЗ; 2 – фіксація реакції ІС на НСВ з запровадженням ТПП СПЗ) згідно вимог стандарту ГОСТ 28147-89 «Системи обробки інформації. Захист криптографічний. Алгоритм криптографічного перетворення» [6].

За кожним напрямом здійснено послідовність операцій тестових випробувань, яка включає три етапи: 1. Шифрування; 2. Розшифровування; 3. Перевірка правильності алгоритму шифрування та розшифрування.

Для реалізації операцій шифрування та розшифровки відповідно до ГОСТ 28147-89 (1-я ітерація, для всіх 32-х ітерацій буде дуже велика модель, вони всі ідентичні по структурі) написано програму з використанням MATHCAD 15 (лістинг представлено в xmcd-форматі).

Інформація, що піддається шифруванню, – 640 біт (10 блоків по 64 біта).

На першому етапі (шифрування) для всіх чотирьох напрямів тестових досліджень (1 – на ІС НСВ не здійснюється, ТПП СПЗ не запроваджена; 2 – на ІС здійснюється НСВ, ТПП СПЗ не запроваджена; 3 – на ІС НСВ не здійснюється, запроваджена ТПП СПЗ; 4 – на ІС здійснюється НСВ, запроваджена ТПП СПЗ) послідовність передбачає виконання 14 операцій згідно вимог ГОСТ 28147-89, при чому для моделювання НСВ у 10 пункті проводиться зрушення 32-бітних під блоків вліво на 12 розділів.

Зазначимо, що за відсутності НСВ, як у випадку запровадження технології, так і її відсутності алгоритми шифрування та розшифровування співпадають. Наявність НСВ призводить до неспівпадання алгоритмів шифрування та розшифровування, але фіксація зазначеної обставини можлива лише за наявності факту запровадження до ІС ТПП СПЗ. Тому зазначимо лише послідовність дій етапів крипто перетворень в умовах здійснення НСВ на систему, до якої запроваджено ТПП СПЗ, оскільки усі етапи крипто перетворень аналогічні по суті.

На першому етапі (шифрування) послідовність дій наступна:

1. Завантаження тексту з файлу (блоки по 64 біта). Маркер S_1. забезпечує контроль можливого НС впливу таким чином, що $S_1 = 1$

$$S1 := \begin{cases} 1 & \text{if } \sum_{i1=0}^{63} \sum_{j1=0}^{rows(T)-1} \left| Tmatch_{j1,i1} - T_{j1,i1} \right| = 0 \\ 0 & \text{otherwise} \end{cases}$$

2. Розбивка блоків на 32-бітні L- і R-підблоки. Маркер S_2 забезпечує контроль можливого НС впливу таким чином, що $S_2 = 1$

$$S2 := \begin{cases} 1 & \text{if } \left(\sum_{g1=0}^{31} \sum_{j1=0}^{rows(T)-1} \left| L11_{j1,g1} - L1_{j1,g1} \right| \right) + \left(\sum_{g1=0}^{31} \sum_{j1=0}^{rows(T)-1} \left| R11_{j1,g1} - R1_{j1,g1} \right| \right) = 0 \\ 0 & \text{otherwise} \end{cases}$$

3. Визначення номеру підключа. Маркер S_3 забезпечує контроль можливого НС впливу таким чином, що $S_3 = 1$

$$S3 := \begin{cases} 1 & \text{if } |KEY11 - KEY1| = 0 \\ 0 & \text{otherwise} \end{cases}$$

4. Задавання 32-бітного ключа (частина 256-бітного ключа)

5. Сумування (по mod 2^{32}) R-підблоку з 32 бітним підключем. Маркер S_4 забезпечує контроль можливого НС впливу таким чином, що $S_4 = 1$

$$S4 := \begin{cases} 1 & \text{if } \left(\sum_{g1=0}^{31} \sum_{j1=0}^{rows(T)-1} \left| Rpr111bin_{j1,g1+1} - Rpr11bin_{j1,g1+1} \right| \right) = 0 \\ 0 & \text{otherwise} \end{cases}$$

6. Розбивка результату сумування на 4-бітні S-блоки. Маркер S_5 забезпечує контроль можливого НС впливу таким чином, що $S_5 = 1$

$$S5 := \begin{cases} 1 & \text{if } \left(\sum_{p1=0}^{7} \sum_{j1=0}^{rows(T)-1} \left| RP1_{j1,p1} - RP_{j1,p1} \right| \right) = 0 \\ 0 & \text{otherwise} \end{cases}$$

7. Задавання таблиці замін для S-блоків

8. S-блоки після перестановки за допомогою таблиці замін

9. Конкатенація S-блоків в 32-бітні під блоки. Маркер S_6 забезпечує контроль можливого НС впливу таким чином, що $S_6 = 1$

$$S6 := \begin{cases} 1 & \text{if } \left(\sum_{g1=0}^{31} \sum_{j1=0}^{rows(T)-1} \left| RS111bin_{j1,g1} - RS11bin_{j1,g1} \right| \right) = 0 \\ 0 & \text{otherwise} \end{cases}$$

10. Циклічне зрушення 32-бітних під блоків вліво на 12 розділів. (здійснюється моделювання НСВ на криптографічний алгоритм). При моделюванні НСВ здійснено підхід, який полягає в виборі найближчого до вимог стандарту 28147-89 показника циклічного зрушення

$$S7 := \begin{cases} 1 & \text{if } \left(\sum_{g1=0}^{31} \sum_{j1=0}^{rows(T)-1} \left| Rsdvig1_{j1,g1} - Rsdvig_{j1,g1} \right| \right) = 0 \\ 0 & \text{otherwise} \end{cases}$$

Маркер S_7, що забезпечує контроль можливого НС впливу на цьому шарі, дозволяє встановити наявність модифікації даних неспівпаданням показників таким чином, що $S_7 = 0$

11. Сумування по mod2 отриманих 32-бітних під блоків з L-підблоками

$$S8 := \begin{cases} 1 & \text{if } \left(\sum_{g1=0}^{31} \sum_{j1=0}^{rows(T)-1} \left| Rmod21_{j1,g1} - Rmod2_{j1,g1} \right| \right) = 0 \\ 0 & \text{otherwise} \end{cases}$$

Несанкціонована модифікація була відстежена при самоконтролі і маркер $S_8 = 0$ (за рахунок удосконаленої ТПП СПЗ ІССП).

12. Формування L-підблоку на виході (R-підблоком на виході є під блоки, отримані в п. 4.11). Маркер $S_9 = 1$

$$S9 := \begin{cases} 1 & \text{if } \left(\sum_{g1=0}^{31} \sum_{j1=0}^{rows(T)-1} \left| Lout11_{j1,g1} - Lout1_{j1,g1} \right| \right) = 0 \\ 0 & \text{otherwise} \end{cases}$$

13. Формування шифротексту (поблоково блоками по 64 біта) шляхом конкатенації L- і R-підблоків на виході. Маркер $S_{10} = 1$

$$S10 := \begin{cases} 1 & \text{if } \left(\sum_{i1=0}^{31} \sum_{j1=0}^{rows(T)-1} \left| C11_{j1,i1} - C1_{j1,i1} \right| \right) = 0 \\ 0 & \text{otherwise} \end{cases}$$

14. Запис шифротексту в файл

$$S := S1 \cdot S2 \cdot S3 \cdot S4 \cdot S5 \cdot S6 \cdot S7 \cdot S8 \cdot S9 \cdot S10$$

На другому етапі проводиться розшифрування операцій в зворотній послідовності дій.

На третьому етапі проводиться перевірка правильності алгоритму шифрування-розшифрування

$$ZERO := \left| \frac{\sum_{m=0}^{64(rows(C1))-1} X_m - 64(rows(C1))}{64(rows(C1))} \right| \cdot 100$$

та встановлюється процент неспівпадань бітів у відкритому тексті (між вихідним та після алгоритму шифрування-розшифрування)

$$ZERO = 0$$

За відсутністю в моделі несанкціонованих дій з модифікації ПЗ, це відстежується і виявляється в тому, що S_1 S_{10} і S дорівнюють 1 ($S = 1$).

За умови здійснення несанкціоновані дії з модифікації програмних блоків та реалізованого додаткового захисту за удосконаленою ТПП СПЗ проводиться фіксація модифікації перетворень.

Зокрема, оскільки за рахунок розробленої технології ППСПЗ ІСПР на шарі 7 маркером S_7 зафіксовано несанкціонований вплив на систему, це відбилося на наступних шарах контроль НС впливу, в результаті $S = 0$

У такому випадку, при проведенні перевірки правильності алгоритму шифрування-розшифровування на третьому етапі крипто перетворень встановлюється процент неспівпадань бітів у відкритому тексті (між вихідним та після алгоритму шифрування-розшифровування)

$$ZERO = 26.875$$

Таким чином, оскільки були проведені несанкціоновані дії з модифікації програмних блоків при шифруванні (конкретно в прикладі: у 10-му пункті криптографічних перетворень замість циклічного зрушення вліво на 11 розрядів з приводу несанкціонованої модифікації виробляється циклічне зрушення на 12 розрядів), несанкціонована модифікація була відстежена при самоконтролі і маркер $S_7 = 0$.

Окрім цього це також відбилося і в маркері $S_8 = 0$, який не пов'язаний безпосередньо з модифікованим програмним блоком, а пов'язаний з іншим програмним блоком (у якому модифікація не вироблялася), але є непрямий зв'язок в обчислювальній структурі потоку, яка і привела до $S_8 = 0$ (у цьому якраз виявилася циклова структура захисту за розробленою методологією). У результаті маркер $S = 0$ – несанкціонована дія присутня.

Сторона, що виробляє шифрування тепер знає про те, що було вироблене несанкціоноване втручання в процес криптографічних перетворень і його несанкціонована модифікація.

Можна модифікувати різні блоки (так аби зберігалася загальна працездатність обчислювальних потоків), виявлення здійснюється завдяки впровадженню ТПП СПЗ ІССП.

Висновки

В результаті проведення досліджень встановлено, що запровадження удосконаленої ТПП СПЗ дозволяє створити умови для якісного поліпшення рівня стійкості ІССП до НСВ забезпеченням постійного контролю за станом роботи системи, а також за дотриманням вимог актуальності, доступності, достовірності, масштабності та повноти даних. Це дає змогу підвищити ефективність рівня стійкості ІССП до НСВ та контролю за даними до 27%.

Отримані наукові результати можуть знайти подальше застосування під час наукових досліджень в напрямку розроблення перспективних зразків стійкої інформаційної системи для управління правоохоронною діяльністю.

Література

1. Бойченко О.В. Окремі питання функціонування системи забезпечення інформаційної безпеки / О.В. Бойченко, К.С. Герасименко // Кримський юридичний вісник. – Сімферополь, 2010. – Вип. 1(8). – Ч. 1. – С. 46-54. **2. Бойченко О.В.** Перспективи використання засобів технічного захисту інформації у правоохоронних органах України / О.В. Бойченко // Спеціальна техніка у правоохоронній діяльності: міжнар. наук.-практ. конф., 20-21 квіт. 2004 р.: тези допов. (Част. 1). – К.: Національна академія внутрішніх справ України, 2005. – С.121-127. **3. Бойченко О.В.** Організаційно-правові та програмно-технічні проблеми захисту інформації в автоматизованих системах ОВС України / О.В. Бойченко, К.С. Герасименко // Проблеми правознавства та правоохоронної діяльності. – Донецьк: Донецький юридичний інститут Луганського державного університету внутрішніх справ ім. Є.О. Дідоренка, 2010. – №2. – С. 68-73. **4. Бойченко О.В.** Інформаційна безпека телекомунікаційних систем спеціального призначення / О.В. Бойченко // Новітні мережні технології в Україні: 14-а міжнар. наук.-практ. конф., 23-25 верес. 2011 р. : тези допов., АР Крим, с. Партеніт – К.: УНДІЗ, 2011. – № 1. – С. 119-124. **5. Бойченко О.В.** Структурне проектування програмного забезпечення складних інформаційних систем реального часу / О.В. Бойченко С.В. Лєнков, П.А. Шкуліпа // Сучасна спеціальна техніка. – К.: ДНДІ МВС України, 2012. – № 4(31). – С. 92-97. **6. Системы** обработки информации. Защита криптографическая. Алгоритм криптографического преобразования: ГОСТ 28147-89. – [Действителен от 1990-07-01]. – М.: ИПК Издательство стандартов, 1996. – 28 с.

В статье предложено методику тестовых испытаний стойкости информационной системы специального назначения на основе технологии послойного проектирования программного обеспечения.

Основой методики является применение последовательности операций тестовых испытаний, включающей три этапа криптографических превращений. В результате разработки созданы условия для обеспечения постоянного контроля за состоянием функционирования информационной системы.

Разработкой методики созданы условия для получения количественных показателей эффективности внедрения технологии послойного проектирования программного обеспечения с целью улучшения уровня стойкости информационной системы специального назначения к несанкционированным влияниям.

Ключевые слова: устойчивая информационная система, послойное проектирование программного обеспечения, несанкционированные влияния, тестовые испытания.

The article offers the method of test tests of firmness the informative system of the special setting is offered on the basis of technology the layer planning of software.

Basis of method is application of sequence operations of test tests, including three stages of cryptographic transformations. As a result of development terms are created for providing of permanent control after the state of functioning the informative system.

Development of method is create terms for the receipt of quantitative indexes of efficiency introduction technology of the layer planning of software with the purpose of improvement of level firmness the informative system of the special setting to unauthorized influences.

Key words: steady informative system, layer planning of software, unauthorized influences, test tests.