УДК 004.681.3

к.т.н., доц. Гулак Г.М. (ДУІКТ)

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПРОГРАМНИХ ЗАСОБІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ ТА ОЦІНКА ЇЇ РІВНЯ

Створення засобів захисту інформації після початку широкого впровадження деякої інформаційної технології породжує загально відому проблему: засіб не інтегрується в технологію або його впровадження призводить до суттєвих втрат переваг вказаної технології.

Цю проблему достатньо легко продемонструвати на прикладі технологій безпровідного доступу мобільних абонентів до локальних обчислювальних мереж. Вочевидь, створення відносного дешевого апаратного засобу криптографічного захисту інформації (КЗІ), який б забезпечував необхідну швидкодію роботи та за габаритними характеристиками був достатньо малий для його вбудовування в об'єм ноутбука або нетбука, є досить складною та коштовною проблемою. При цьому окремо постає питання щодо вбудовування засобу у комп'ютер, що перебуває на гарантії виробника.

Шлях створення зовнішнього пристрою, що підключається за допомогою одного з стандартних інтерфейсів (наприклад, *USB2.0*), є простим, але можливість його впровадження обмежується швидкодією обміну за допомогою обраного порту. Це рішення також призводить до певного збільшення масо-габаритних показників обладнання, а також потребує впровадження додаткових організаційних заходів для захисту пристрою КЗІ від крадіжки або проведення атак за типом "midnight attack".

Застосування програмного засобу (ПЗ) КЗІ дозволяє уникнути перелічених проблем. При цьому ми розуміємо під програмним засобом КЗІ спеціальне програмне забезпечення, що працює на універсальній апаратній платформі під керуванням операційної системи, яка допущена для обробки інформації із визначеним грифом обмеження доступу.

До переваг програмного шифрування можливо також віднести універсальність, портативність, простоту використання та оновлення [1]. Програмне шифрування дозволяє повною мірою забезпечити ефективне використання окремих криптографічних функцій, що реалізовані у сучасних операційних системах [2].

В разі ефективної реалізації ПЗ вони здатні забезпечувати високу швидкодію криптографічних перетворень, яка залежно від обраної апаратної платформи може досягати десятка мбайт у секунду [3].

Суттєвим аргументом на користь ПЗ КЗІ є те, що вони не тільки коштують значно дешевше апаратних шифраторів, а й мають відносно невелику вартість порівняно з апаратно-програмними засобами, що слід враховувати у разі захисту інформації, з невисокім рівнем конфіденційності або цінності.

Для уникнення непорозумінь, будемо вважати, що має місце обробка конфіденційної інформації при цьому вимоги до захисту від ПЕМВН не висуваються. На комп'ютерній системі впроваджується комплексна система захисту інформації, що включає засоби та методи криптографічного та технічного захисту. Власник інформації, виходячи з її вартості (цінності), має намір оптимізувати ціну системи захисту.

Також вважаємо, що ключі до засобів КЗІ зберігаються лише на захищених носіях, а у пам'яті комп'ютера вони знищуються одразу після їх використання. Крім цього, відповідно до принципу В.Керкхофса, вважаємо алгоритм криптографічного перетворення інформації, що реалізований у ПЗ КЗІ, протоколи генерації, тестування та формування ключів загально відомими.

Виникає питання які саме методи доцільно впровадити для забезпечення безпеки шифрування та як оцінити рівень безпеки, що досягнутий.

Задача у тій чи іншій постановці, розглядалася в деяких роботах, зокрема можливо надати посилання на роботи у області безпеки та надійності програмних засобів [4-6], а також щодо безпеки реалізацій засобів КЗІ [2,7,8]. На відміну від [9] у даній роботі дослідження фокусується на особливостях функціонування засобів КЗІ та забезпечення стійкості криптографічних перетворень.

У даній роботі продовжено тему інженерного аналізу засобів захисту інформації, яку досліджено у роботі [10,11], зокрема уточнено взаємозв'язок понять «безпека» та «надійність», а також запропоновано оцінку рівня безпеки застосування засобів КЗІ.

Вихідні дані для створення безпечних ПЗ КЗІ та оцінки досягнутого рівня безпеки мають бути сформульовані у моделі загроз безпеки функціонування ПЗ КЗІ, яка повинні включати наступні чинники, що впливають на рівень захисту інформації [2,7,13]:

1. Наявність у ПЗ КЗІ помилок, що не були виявлені під час його тестування та сертифікації.
2. Випадкове порушення порядку функціонування апаратної платформи та/або операційної системи комп'ютеру внаслідок збоїв або відмов його компонентів.
3. Випадковий шкідливий вплив на ПЗ КЗІ програм – вірусів, що можуть порушувати цілісність та працездатність компонентів ПЗ.
4. Помилкові ненавмисні дії користувачів ПЗ КЗІ, які не виконують приписи керівних документів.
5. Активні заходи порушників інформаційної безпеки, що спрямовані на отримання критичної інформації про стан та порядок функціонування ПЗ КЗІ.

Легко бачити, що поняття безпечних програмних засобів є складовою частиною надійних засобів [5]. Тобто убезпечення ПЗ КЗІ має включати перелік заходів, що спрямовані на підвищення його надійності [5,6]

Протидія перерахованим загрозам та дотримання визначеного рівня безпеки функціонування ПЗ КЗІ може забезпечуватися, зокрема, шляхом автентифікації суб'єктів та об'єктів інформаційного процесу, контролю повноважень [12], контролю за цілісністю ПЗ та періодичного моніторингу правильності (логічного контролю) виконання обчислювального процесу - криптографічних перетворень, ефективного знищення використаних ключових даних.

Ясне, що на відміну від апаратних засобів КЗІ реалізація логічного контролю криптографічних перетворень у програмних засобах шляхом дублювання окремих вузлів шифратору вже не на стільки ефективна, оскільки дублюючі елементи самі можуть бути блоковані або викривлені внаслідок реалізації відповідних самих загроз.

Особливого значення для забезпечення безпеки ПЗ КЗІ набуває проблема створення ефективного механізму контролю та блокування помилкових дій користувачів.

Можливі наслідки для безпеки функціонування ПЗ КЗІ внаслідок відмов, збоїв, помилок апаратних та програмних платформ або несанкціонованого втручання в їх роботу є предметом окремого дослідження. Загалом, можливо відмітити, що реалізація вказаних загроз може призводити до зниження стійкості шифрування, підвищення ймовірності ризику проведення успішних криптоаналітичних атак. Зокрема, у різних криптосистемах може відбуватися передача у відкритий канал зв'язку неякісно або зовсім не зашифрованої інформації, повторення сеансових ключів, скорочення загального періоду криптоперетворення та проява відносно коротких періодів, погіршення ймовірнісних характеристик шифруючої гами [7,13] тощо.

Для побудови системи контролю якості шифрування можливо використати певний набір статистичних критеріїв [8], які можуть суттєво зменшити ймовірність передачі в відкритий канал зв'язку неякісно зашифрованої інформації. Зокрема, бачиться ефективним побудова критерію поточного контролю стану шифратору на основі непараметричних критеріїв, які застосовуються у так званої задачі «виявлення місця збою» [14].

У останньому випадку вважаємо, що у послідовності незалежних випадкових величин $X=\{x_1,x_2,...,x_N\}$, що описують вихід шифратору, перші n величин мають вектор розподілу значень $(p_1,...,p_m)$, а наступні – $(q_1,...,q_m)$, при цьому $(p_1,...,p_m)\neq(q_1,...,q_m)$, де $p_i=P\{x_j=i\}$ для $j\in[1,n]$ та $q_i=P\{x_j=i\}$ для $j\in[n+1,N]$.

Для перевірки гіпотези щодо наявності «місця збою» можливо скористатися сімейством непараметричних статистик типу Колмогорова-Смірнова:

$$Y(n)=\left|\frac{1}{n}\cdot\sum_{j=1}^{n}x_j-\frac{1}{N-n}\cdot\sum_{j=n+1}^{N}x_j\right|$$

Гіпотеза H_0 щодо наявності «збою» приймається, якщо має місце нерівність:

$$Y(n)>C_{1-\alpha}$$

де $C_{1-\alpha}$ – границя критерію для заданого рівня значущості $1-\alpha$, α - ймовірність помилки першого роду.

Застосування відповідних тестів обмежується випадками, коли швидкість оброблення інформації відносно невелика, оскільки виконання тестів потребуватиме певного обчислювального ресурсу та неминуче призведе до уповільнення швидкодії засобу КЗІ.

Для побудови системи захисту ПЗ КЗІ уявляється доцільним застосування методів маскування [5] та контролю цілісності ПЗ у визначених точках виконання процесу.

Методи маскування (заплутування) мають на меті ускладнити можливості атакуючої стороні у плані дизасемблювання та аналізу структури коду, що виконується, та впровадженні певних деструктивних заходів.

Зокрема, можливі наступні рішення для захисту ПЗ.

Реалізація шифрування коду, що виконується, передбачає попереднє зашифрування ПЗ з наступним розшифруванням частин, що виконуються. Замість шифрування можуть використовуватися деякі безключові алгоритми, наприклад, стиснення даних, які забезпечують стиснення та розпакування коду програми залежно від її виконання.

У разі коректної реалізації метод шифрування практично унеможливлює аналіз зловмисником принципів побудови ПЗ и суттєво ускладнює задачу вибору точки деструктивного впливу. Зокрема, засіб КЗІ "КриптоПро CSP" версії 3.6 (виробництво ТОВ "КРИПТО ПРО, РФ) , який отримав сертифікат ФСБ Росії на відповідність вимогам щодо захисту конфіденційної інформації, реалізує захищене зберігання ключів користувача у ключовому контейнері з використанням шифрування, імітозахисту та автентифікації доступу [15].

Зауважимо, що використання криптографічних перетворень для захисту коду ПЗ КЗІ потребує значних витрат обчислювального ресурсу системи, що призводить до суттєвого уповільнення процесу оброблення даних. Тому методи шифрування та стиснення коду програми можуть бути рекомендовані для захисту даних відносно невеликого обсягу (ключи, критичні параметри тощо) переважно в умовах низко швидкісного синхронного або попереднього шифрування.

Обчислення складних математичних перетворень у процесі роботи ПЗ також забезпечує зміну його структури, але стійкість цих перетворень відносна – стійкість забезпечується лише до викриття формули обчислень, а швидкодія визначається власне математичною функцією, що описує ці перетворення.

Певною мірою процедуру зашифрування в режимі кодової книги нагадують алгоритми мутації, які використовують створені за визначеною схемою або випадковим чином таблиці відповідності операндів – синонімів. За допомогою цих таблиць здійснюються заміни в тілі програми при кожному її старті, а також реалізуються випадкові зміни структури програми. Цей метод більш швидкісний порівняно з попередніми, але стійкість його відносно можливих атак невисока.

Ще більш високу швидкодію можуть забезпечити алгоритми заплутування, впровадження яких передбачає застосування операцій нерегулярної (псевдовипадкової) передачі управління у різні адреси (частини) коду програми, розміщення частин коду по різних областях пам'яті, впровадження значної кількості псевдо параметрів та псевдо процедур - "пустушок", створення холостих циклів, викривлення деяких реальних параметрів ПЗ. Однак цей метод суттєво ускладнює роботу з розробки та подальшої модернізації ПЗ.

Перелічені методи можуть вбудовуватися безпосередньо у ПЗ КЗІ або створюватися у вигляді самостійних засобів. Останній спосіб реалізації бачиться менш ефективним, оскільки спрощується його блокування.

Захист коду звичайних програм може включати ще ряд методів та процедур, у т.ч. ускладнення процесів дизасемблювання та налагодження, впровадження нестандартних методів взаємодії з апаратною платформою, емуляцію процесорів та операційних систем. Але застосування цих методів для захисту ПЗ КЗІ не можливо вважати перспективним, оскільки для цілеспрямованого втручання у роботу засобу не потрібно повне відновлення відповідної програми.

З метою контролю цілісності програм і критичних даних доцільно використовувати криптографічно стійкі перетворення, а саме: обчислення імівставки (MAC кодів), геш-функції або цифрового підпису. При цьому слід враховувати, що швидкість обчислення/ перевірки цифрового підпису при інших рівних умовах найнижча.

Для визначення безпечного періоду контролю можливо запропонувати декілька підходів. По-перше, можливо скористатися визначенням та властивостями відстані єдності шифру L_0 [13]:

$$L_0 = \frac{\log_2 |K|}{\log_2 |I| - H} \tag{1}$$

де $|K|$ – потужність множини ключів шифру;

$|I|$ – потужність абетки символів відкритого тексту;

H – ентропія відкритого тексту.

З визначення відстані єдності шифру слідує наступне. Якщо логічний контроль стану функціонування ПЗ КЗІ, який реалізує синхронне шифрування, здійснюється частіше ніж кожні L_0 тактів шифрування, у випадку настання збою у роботі шифратору перехоплений атакуючою стороною відрізок вихідної послідовності не забезпечуватиме однозначне розшифрування.

Наприклад, у разі використання криптоалгоритму ГОСТ 28147-89 без урахування довготермінового ключа або криптоалгоритму AES с довжиною ключа 256 біт для шифрування повідомлень у коді КОИ-8 (256 символов) для ентропії $H=1$ розрахунок за формулою (1) дає значення $L_0 \approx 37$ символів або 296 біт. Тобто у цьому випадку контроль має здійснюватися один раз на 296 зашифрованих біт.

Якщо в алгоритмі ГОСТ врахувати секретний довготерміновий ключ, то потужність множини ключів дорівнює:

$$|K| = 2^{256} \cdot (16!)^8$$

Останній вираз можливо обчислити за допомогою формули Стірлінга для асимптотичної оцінки факторіалів:

$$n! = \sqrt{2\pi n} \cdot n^n \cdot e^{-n}(1 + o(1))$$

Що дає $|K| \approx 2^{618}$, тому в умах зроблених припущень отримуємо $L_0 \approx 88$ символів або 704 біт. Таким чином, період контролю у цьому випадку може бути збільшений майже у 2.4 рази.

Другій підхід передбачає використання того факту, що для визначення істинного ключу атакуючої стороні необхідно скористатися статистичним критерієм відкритого тексту [13]. При цьому, будь який статистичний тест матиме певні похибки: 1-го роду α – ймовірність

помилково відхилити істинний текст, а також 2-го роду β - ймовірність помилково обрати випадковий текст у якості істинного. При цьому, стала робота тесту забезпечується лише на достатній довжині тексту [8]. Якщо довжина тексту буде недостатньою, критерій буде занадто часто відхиляти вірні варіанти ключу або помилкові варіанти обирати за істинні.

Якщо логічний контроль стану здійснюється із відносно короткім періодом, зловмисник не зможе відрізнити у загальному потоці символів відрізок відкритого тексту від рівномірно розподілених послідовностей символів.

Таким чином, комплексне застосування на усіх етапах життєвого циклу загальних методів підвищення надійності та спеціальних методів захисту ПЗ КЗІ повинно забезпечити необхідний рівень безпеки їх функціонування.

Для оцінки рівня безпеки ПЗ КЗІ введемо множину попарно несумісних подій $\{A_1,...,A_N\}$, що відповідають достатні умовам для проведення можливих атак $\{\Re_1,\ldots,\Re_N\}$ на криптографічну систему. Якщо у випадку виникнення події A_i $i\in[1,N]$ утворюються достатні умови для проведення декількох атак будемо пов'язувати з цією подією лише ту атаку, що матиме найгірші наслідки для безпеки інформації, яка захищається за допомогою цього засобу.

Позначимо через A_0 подію, яка відповідає режиму штатної експлуатації ПЗ КЗІ (безпечний режим роботи):

$$A_0 = \Omega \setminus \bigcup_{i=1}^{N} A_i$$

де Ω - простір елементарних подій. При цьому ймовірність виникнення події A_i, $i\in[1,N]$ дорівнює $p_i\neq 0$.

Вектор ймовірностей $P=(p_0,p_1,...,p_N)$ у загальному випадку залежить від багатьох факторів, зокрема, від обраних проектних рішень, якості та повноти тестування та сертифікації ПЗ КЗІ, надійності апаратної платформи, адекватності побудованої комплексної системи захисту інформації можливим загрозам тощо.

Далі, оскільки інформація може здобуватися не тільки криптоаналітичними методами, а й, наприклад, за рахунок перехоплення побічних електромагнітних випромінювань від обчислювальної техніки, агентурними методами, методами оптичної розвідки тощо, логічно оцінювати «привабливість» методів дешифрування для порушника інформаційної безпеки відносним показником c_i/C, де $C\neq 0$ – найменша вартість здобування певного обсягу інформації не криптоаналітичними методами, c_i – вартість створення спеціалізованих обчислювальних засобів та спеціального програмного забезпечення для розв'язання задачі дешифрування зі складністю краще метода тотального перебору ключів $w_i << \frac{|K|+1}{2}$ (відповідає атаці $\Re_i$) за визначений час, а також підтримки їх функціонування протягом необхідного часу.

Ситуації: $c_i=\infty$, $i\in[1,N]$ або $c_i<\infty$ та $c_i/C >> 1$, $i\in[1,N]$ є тривіальними, при цьому здобування інформації криптоаналітичними методами неможливо або економічно недоцільно. Перша ситуація має місце, наприклад, у випадку шифру Вернама з випадковою рівномірно розподіленою гаммою шифру.

Будемо вважати, що існує хоча б одно значення i для якого $c_i<\infty$ та $c_i/C = O(1)$ або $c_i/C \le 1$.

Добуток $p_i^{-1} \cdot w_i \cdot \frac{c_i}{C}$ будемо називати зваженою складністю атаки $\Re i$. Нескладно бачити, що задача протидії «розробник криптосистеми - порушник інформаційної безпеки» полягає у тому, що сторона, яка захищається вживає заходів щодо збільшення зважених складностей атак за рахунок реалізації захисних заходів та підвищення надійності системи, порушник у свою чергу що обирає атаку з мінімальною зваженою складністю:

$$\min_i \max_P (p_i^{-1} \cdot w_i \cdot \frac{c_i}{C}) \qquad (2)$$

Саме величину, що визначена формулою (2) пропонується використовувати у якості мірі безпеки ПЗ КЗІ.

Запропонована формула достатньо легко може бути проілюстрована на прикладі криптоалгоритма DES с ключем 56 біт. Нехай, складність найкращий комбінованої атаки на алгоритм, яка побудована на методі диференційного аналізу становить $2^{40} \approx 10^{12.}$. Вважаємо, що $c_i / C \cong 1$. Також вважаємо, що проведення атаки необхідно отримати $2^{30} \approx 10^9$ пар відкритий – шифрований текст (блоків довжиною 2^6 біт). Якщо засіб забезпечує шифрування зі швидкістю 10^5 кбіт/сек для отримання визначеної кількості матеріалу (застосовується метод “midnight attack”) порушнику необхідно мати доступ до шифратору на $6.4 \cdot 10^5$ сек. Виходячи з мінімізації ймовірності не перекриття повідомлень [13] розрахуємо припустимий час дії мережного ключу, нехай він діє 14 діб=$14 \cdot 86400 \approx 1.21 \cdot 10^6$ сек. Таким чином для отримання порушником вихідного матеріалу необхідно, щоб шифрувальник з ймовірністю що найменш 0.5 був відсутнім на робочому місті. Якщо це виконано, зважена складність атаки становитиме $5 \cdot 10^{11}$.

Таким чином запропонована міра безпеки ПЗ КЗІ може бути застосована на для оцінки ефективності обраних організаційних, проектних та технічних заходів, що обираються на етапах життєвого циклу засобу КЗІ.

Список літератури

1. Б.Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. –М.: ТРИУМФ, 2002, –816с.

2. Щербаков А., Домашев А. Прикладная криптография. Использование и синтез криптографических интерфейсов., –М.: «Русская редакция», 2003, –416 с.

3. А.Винокуров, Э. Применко Сравнение стандарта шифрования РФ и нового стандарта шифрования США, http://www.enlight.ru/crypto/articles/vinokurov/__gosaes.htm

4. М.Ховард, Д.Лебланк. Защищенный код. –М.: «Русская редакция», 2003, –671с.

5. Казарин О.В. Теория и практика защиты программ, –М.: МГУЛ, 2004, –450с

6. A.Spillner, T.Linz, H.Schaefer. Software Testing Foundations. –Heidelberg: Dpunk.verlag, 2006, –266с.

7. Семьянов П.В. Почему криптосистемы ненадежны? Тезисы доклада на конференции «Методы и технические средства обеспечения безопасности информации», СПбГТУ, 1996

8. Гулак Г., Ковальчук Л. Різні підходи до визначення випадкових послідовностей //НТЗ «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні», вип. 3, –К.: 2001, –с.127-133.

9. Ленков С.В., Гришин С.П., Ленков А.С., Слюняев А.С. Оценка надежности программных систем защиты информации// Вісник Східноукраїнського національного університету, №6(136), 2009, Ч.1, –с.218-221

10. Гулак Г.М. Оцінка ризиків у ходи проведення інженерного аналізу безпеки стеганографічних систем //Сборник научных трудов НАУ «Защита информации», Спецвыпуск, –К.: 2008, –с.259-264.

11. Гулак Г.М. Характеристика небезпечних відмов засобів, що реалізують стеганографічні методи перетворення інформації // Науково-технічний журнал «Захист інформації», №1(42), –К.: 2008, –с.56-59.

12. Перегудов Д.А., Берназ Н.М., Гришин С.П., Ленков Е.С. Программные средства защиты информации// Вісник Східноукраїнського національного університету, №6(136), 2009, Ч.1, –с.214-218

13. Бабаш А.В., Шанкин Г.П. Криптография. –М.: «Солон-Р», 2002, –512с.

14. Brodsky B.E., Darkhovsky B.S. Nonparametric Methods in Change-Point Problems. –Kluwer Academic Publishers, The Netherlands, 1993, –209с.

15. Заключение ФСБ России на СКЗИ "КриптоПро CSP" версии 3.6, 08.05.2009, http://www.cryptopro.ru/cryptopro/news/default.asp?n=223

У статті розглядаються питання проведення інженерного аналізу програмних засобів криптографічного захисту інформації, визначені фактори, що впливають на рівень безпеки їхнього функціонування, надані пропозиції щодо оцінки рівня безпеки програмних шифраторів.
Ключові слова: криптографія, рівень безпеки, програмні шифратори.

В статье рассмариваются вопросы проведения инженерного анализа программных средств киптографической защиты информации, определены факторы, влияющие на уровень безопасности их функционирования, наданы предложения по оценке программных шифраторов.
Ключевые слова: криптография, уровень безопасности, программные шифраторы.

The article is devoted to the questions of reverse engineering of a cryptographic data protection software. The factors that influence on their level of safety have been defined. The propositions to the evaluation of programmed cipherers have been made.
Key words: cryptography, level of safety, programmed cipherers.

Надійшла 27.01.2010

УДК 004.057.5
к.т.н., доц. Казакова Н.Ф. (МГУ, м.Одеса)

ОРГАНІЗАЦІЯ ПРОЦЕСУ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ЗАХИЩЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Постановка проблеми в загальному вигляді та її зв'язок з науковими і практичними завданнями. Програмне забезпечення – це та рушійна сила, яка сьогодні забезпечує функціонування торгівлі, промисловості, системи державного управління і зв'язує воєдино різні шари суспільства. Програмне забезпечення (в тому числі – для захищених інформаційних систем) допомагає створювати інформацію, надавати до неї доступ та візуалізувати її, причому все це великою множиною немислимих способів і в неймовірних формах. Саме приголомшливий прогрес в області програмного забезпечення допоміг справитися з розвитком світової економіки. На сьогоднішній день програмне забезпечення є невід'ємною частиною сучасного суспільства.

Звичайно ж, професійних розробників програмного забезпечення радує те, що світова економіка стає все більш залежною від програмного забезпечення. Завдяки розвитку техніки стало можливим створення програмних систем, які постійно ростуть, ускладнюються, розповсюджуються і стають все більш важливими. Крім того, росте ще й суспільний попит на ці системи.

Аналіз наукової і технічної літератури (наприклад [1...7]) показує, що збільшення складності, важливості і все більш широке розповсюдження програмних систем обмежують людські здібності до розуміння принципів розробки продуктів у сфері програмного забезпечення для захищених інформаційних систем. Спроба поліпшення існуючих систем в цілях їх адаптації до новітніх технологій приводить до виникнення ряду технічних та організаційних проблем. Ситуацію ускладнює ще й те, що комерційна галузь вимагає все більш ефективних та якісних продуктів, що розробляються і поширюються надзвичайно швидко. Крім того, на сьогодні розробники не в змозі повністю задовольнити існуючий попит.

Отже, на сьогоднішній день створення та технічна підтримка програмного забезпечення є надзвичайно важким та організаційно недосконалим процесом. Крім того, для створення якісного програмного забезпечення саме для захищених інформаційних систем важко синтезувати уніфікований процес, який можна повторити і результати дії якого можна