УДК 004.056
Безкоровайна Ю.М., старший викладач, Скалова В.А., старший викладач
Національний авіаційний університет

ОГЛЯД ЧИННИХ СТАНДАРТІВ ДЛЯ РОЗРОБКИ ЗАХИЩЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Безкоровайна Ю.М., Скалова В.А. Огляд чинних стандартів для розробки захищених інформаційних систем. У статті розглядається чинні стандарти для розробки захищених інформаційних систем на основі стандарту, який об'єднує чинні стандарти та заходи, які пропонуються реалізувати під час розробки захищених інформаційних систем.
Ключові слова: безпека, стандарти, розробка програмне забезпечення, інформаційні системи, захист.

Безкоровайная Ю.Н., Скалова В.А. Обзор действующих стандартов для разработки защищенных информационных систем. В статье рассматривается действующие стандарты для разработки защищенных информационных систем на основе стандарта, который объединяет действующие стандарты и меры, которые предлагаются реализовать при разработке защищенных информационных систем.
Ключевые слова: безопасность, стандарты, разработка программного обеспечения, информационные системы, защита.

Bezkorovaina Y.M., Skalova V.A. The review of existing standards for the development of secure information systems. The article examines the current standards for the development of secure information systems based on a standard that combines existing standards and measures that are proposed to implement in the development of secure information systems.
Keywords: security, standards, software development, information system, security.

Вступ.

На сьогоднішній день гострою проблемою стоїть питання про реалізацію та визначення захищених інформаційних систем (ІС). Однією з проблем забезпечення захисту інформації це розробка безпечного програмного забезпечення (ПЗ), які входять до його складу. Одним із важливих питань при розробці безпечного ПЗ - є питання вчасного впровадження та початок робіт з реалізації заходів з безпеки та результати цих заходів. Закордоном швидкими темпами розробляють та впроваджують стандарти та нормативні документи з розробки безпечного ПЗ. В статті буде розглянуто заходи та їх результат, які відповідають стандартам та нормативним документам, які чинні в Україні.

Аналіз останніх досліджень і публікацій. **Виділення невирішених раніше частин загальної проблеми**.

Невпинне розширення сфери застосування засобів комп'ютерної обробки інформації і комп'ютерних засобів телекомунікації залучають до сфери інформаційних технологій все більше коло людей, що підвищує ризики виникнення інформаційних загроз та їх реалізації. В 2016 закордоном був затверджений та введено в дію стандарт з розробки безпечного ПЗ, який об'єднує загальні вимоги при розробці безпечного ПЗ [4], на його основі було проаналізовані заходи та їх вплив на реалізацію безпечного ПЗ, апарат комплексів заходів [1, 2, 7]. Проте виникає проблема - цей стандарт не чинний на території України, хоча включає посилання на чинні стандарти та нормативні документи. В статті приводяться заходи та пов'язані з ними стандарти та нормативні документи.

Формулювання мети дослідження.

З огляду на зростання складності інформаційних систем актуальними стають проблеми загрози безпеки інформації, пов'язані з наявністю вразливості ПЗ, що використовуються в складі ІС. Для захисту від загроз, як правило, використовують комплекс заходів, які реалізовані в процесах експлуатації та супроводу ПЗ. Проте для забезпечення необхідного рівня захисту інформації потрібна реалізація заходів, які спрямовані на запобігання появи і усунення вразливостей ПЗ в процесах життєвого циклу (ЖЦ) ПЗ, пов'язаних з проектуванням, реалізацією і тестуванням [4].

Сучасний підхід до захисту інформації в ІС ґрунтується на ідеальних моделях процесу організації захищених систем та їх функціонування. Ідеальна модель передбачає комплексний підхід до створення безпечних ІС протягом всього життєвого циклу таких систем. У той же час відсутність загальної теорії захисту інформації призводить до того, що при створенні систем інформаційного захисту рішення щодо способів реалізації їх елементів приймаються на основі

евристичних моделей або експертних оцінок існуючих варіантів реалізацій систем захисту інформації [10].

Актуальними проблемами захисту інформації на сьогодні є: розробка елементів загальної теорії захисту інформації в захищених системах; створення та дослідження універсальних моделей безпечних ІС; створення та дослідження моделей загроз ІС; розробка методів і процедур об'єктивного аналізу ефективності прийнятих рішень при створенні систем інформаційної безпеки [10].

Виклад основної частини.

Безпечне ПЗ - це ПЗ, яке розроблене з використанням сукупності заходів, які направлені на попередження появи та усунення вразливості програми [4], тобто недоліків ПЗ, які використовується для реалізації вразливості безпеки інформації.

Розробка ПЗ поділяється на процеси ЖЦ ПЗ, в якому виділяють основні, допоміжні та організаційні процеси ЖЦ ПЗ за стандартом ДСТУ ISO 12207 [5]. До основних відноситься: аналіз вимог до ПЗ, проектування архітектури ПЗ, конструювання ПЗ та тестування ПЗ; до допоміжних та організаційних: інсталяція та впровадження, менеджмент документації та конфігурації ПЗ, інфраструктури середовища розробки та людських ресурсів [5].

За стандартом [4] розробка безпечного ПЗ поділяється на дев'ять заходів на основі процесів ЖЦ ПЗ. На рисунку 1 зображено взаємозв'язок між процесами ЖЦ ПЗ та заходи, які необхідно документувати за стандартами.

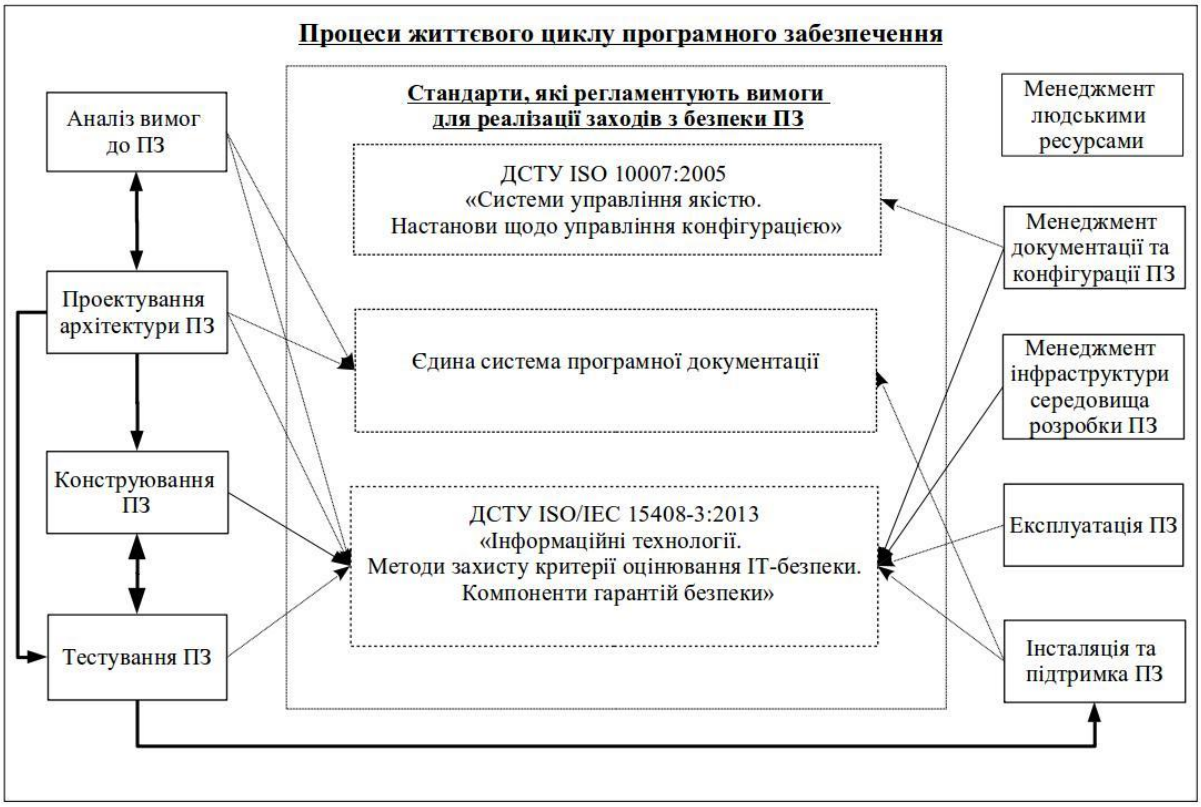

Рис. 1. Взаємозв'язок між процесами ЖЦ ПЗ та стандартами

Аналіз вимог до ПЗ. При аналізі вимог до ПЗ розробник повинен визначити вимоги до безпеки, які висуваються до ПЗ. Для реалізації необхідно створити документи за стандартами ГОСТ 19.201-78 «ЄСПД. Технічне завдання» [3, с. 43-44; 8] та відповідно з вимогами сімейства ASE «Оцінка завдання з безпеки» за стандартом ДСТУ ISO/IEC 15408 [6].

В результаті вдалої реалізації заходів формується перелік вимог до безпеки, що пред'являється до ПЗ та враховується при проектуванні архітектури ПЗ.

*Проектування архітектури ПЗ***.** При проектуванні архітектури ПЗ реалізовується моделювання загрози безпеки інформації та уточнюється проекту архітектури ПЗ з урахуванням

результатів моделювання. Це сприяє створенню та документуванню проекту архітектури ПЗ з урахуванням вимог з безпеки, для його подальшого використання в процесах ЖЦ ПЗ, пов'язаних з реалізацією та тестуванням ПЗ; формування вихідних даних для виконання динамічного аналізу коду програми, тестування на проникнення в рамках процесу кваліфікаційного тестування ПЗ.

Проект архітектури ПЗ розробляється з урахуванням необхідності виконання вимог з безпеки; формують перелік виявлених потенційних загроз безпеки інформації, які використовуються при проведені динамічного аналізу коду програми та тестування на проникнення на етапі тестування. Розробник ПЗ повинен виконувати моделювання загроз безпеки інформації, які можуть виникнути в наслідок використання ПЗ.

Для організації робіт необхідно документально оформити проект архітектури ПЗ за стандартами ГОСТ 19.402-78 «Опис програми» [3, с. 51-52; 8] та ГОСТ 19.404-79 «Пояснювальна записка. Вимоги до вмісту та оформлення» [3, с. 56-57; 8] та відповідно стандарту ДСТУ ISO/IEC 15408 [6] вимог сімейства:

- AOV.FSP «Функціональна специфікація»;
- AOV.TOS «Проект ОО»;
- AOV.ARC «Архітектура безпеки».

Конструювання ПЗ. При конструюванні ПЗ необхідно реалізувати наступне: використовувати при розробці ПЗ ліцензійні інструментальні засоби, створити вихідний код на основі уточненого проекту архітектури ПЗ з дотриманням порядку оформлення вихідного коду, який містить перелік правил та рекомендацій; провести статичний аналіз та експертизу вихідного коду, виявити та усунути недоліки (вразливих конструкцій) в вихідному коді, в іншому випадку документувати обґрунтування факту в кожному випадку відмови від використання у вигляді коментарів в вихідному коді; задокументувати вихідні дані для виконання динамічного аналізу коду та тестування на проникнення в рамках процесу тестування ПЗ; забезпечувати проведення статичного аналізу та експертизу вихідного коду з ціллю виявлення недоліків програми в вихідному коді, який необхідно проводити по відношенню до компонентів, які запозичені у сторонніх розробників ПЗ, якщо для цих компонентів доступний вихідний код програми.

За результатами статичного аналізу та експертизи вихідного коду програми можна проводити доопрацювання програми.

Для організації робіт документацію розробника ПЗ необхідно розроблювати у відповідності стандарту ДСТУ ISO/IEC 15408 [6] вимог сімейства:

- ALC.TAT «Інструментальні засобі і методи»;
- ALC_CMC «Можливості управління конфігурацією»;
- ALC.CMS «Область управління конфігурацією».

Тестування ПЗ. При тестуванні ПЗ розробник ПЗ необхідно реалізовувати наступні заходи: функціональне тестування програми; тестування на проникнення; динамічний аналіз коду; фаззінг тестування.

Документація розробника ПЗ повинна містити: план тестування; опис виконуваних тестів та інструментальних засобів, які використовують для тестування; фактичні результати тестування; звіти, які містять списки виявлених невідповідностей вимогам безпеки та вразливості; опис дій, які направлені на їх усунення, обґрунтовування неможливості або відсутність необхідності в усуненні невідповідності вимогам та вразливості, виявлені при моделюванні дій потенційних порушників; проекту архітектури ПЗ, в тому числі інформації про запозичені у сторонніх розробників ПЗ компоненти; результати моделювання загроз безпеки інформації; результати тестування на проникнення; результатів динамічного аналізу вихідного коду.

За результатами тестування можна проводити доопрацювання, яке направлено на усунення виявлених невідповідностей вимогам безпеки та/або вразливості.

Документацію розробника ПЗ необхідно розробляти у відповідності стандарту ДСТУ ISO/IEC 15408 [6] вимог сімейства:

- ATE_COV «Покриття»;
- ATE_OPT «Глибина»;
- ATE_FUN «Функціональне тестування»;
- AVA_VAN «Аналіз вразливостей».

Інсталяція та підтримка ПЗ. При інсталяції та підтримки ПЗ необхідно реалізувати наступні заходи: забезпечити захист ПЗ від загроз безпеки інформації, пов'язаних з порушенням цілісності, в процесі його передачі користувачу; поставка користувачеві експлуатаційну документацію. В склад ПЗ, яке постачається, повинні бути включені експлуатаційні документи в об'ємі, достатньому для правильного налаштування та безпечного використання програми.

Документація розробника ПЗ повинна містити опис виконаних технічних та організаційних заходів, які використовуються для визначення модифікацій ПЗ або будь-якого розходження між оригіналом та версією, отриманою користувачем — розроблюється експлуатаційні документи відповідно вимогам ГОСТ 19.101-78. «ЄСПД. Види програм та програмних документів» [3, с. 18-20; 8] та відповідно стандарту ДСТУ ISO/IEC 15408 [6] вимог сімейства:

- ALC_DEL «Постачання»;
- ACD.OPE «Керівництво користувача з експлуатації»;
- AGO.PRE «Підготовчі процедури».

Експлуатація ПЗ. В процесі експлуатації ПЗ розробник повинен реалізовувати наступні заходи: реалізація та використання процедури відстеження та виправлення виявлених помилок ПЗ та вразливостей програми; систематичний пошук вразливості програми. При реалізації даних заходів необхідно визначити причини помилок ПЗ та вразливості програми та прийняти заходи з попередження подібних помилок ПЗ та вразливостей програми в майбутньому. Процедура виправлення помилок ПЗ та вразливостей програми повинна забезпечити прийом та обробку повідомлень від користувачів про помилки ПЗ та вразливостей програми та запроси на їх усунення. За результатами обробки повідомлень від користувачів про помилки ПЗ та вразливостей програми можна проводити доопрацювання програми.

Документація ПЗ повинна містити опис альтернативних способів тимчасових рішень проблеми, пов'язаних з екстреною ситуацією; опис методів доведення до користувачів інформацію про вразливість програми та рекомендації по їх усуненню; опис методів прийому та обробки повідомлень від користувача; опис процедури відстеження та виправлення виявлених помилок ПЗ та його вразливості; перелік екстрених ситуаціях, при яких можливий випуск оновлень ПЗ в обхід стандартної процедури випуску нових версій ПЗ; список виявлених помилок ПЗ та вразливість програми та опис дій, які направлені на їх усунення, або обґрунтування неможливості або відсутності необхідності в їх усунені — розробляти відповідно до стандарту ДСТУ ISO/IEC 15408 [6] вимог сімейства:

- ALC.FLR «Усунення недоліків»;
- ALC.TAT «Інструментальні засобі і методи»;
- ALC.CMC «Можливості управління конфігурацією»;
- ALC.CMS «Область управління конфігурацією».

Менеджмент документації та конфігурації ПЗ. В процесі менеджменту документації та конфігурації ПЗ розробник повинен реалізовувати наступні заходи: реалізація та використання процедури унікального маркування кожної версії ПЗ; використання системи управління конфігурацією ПЗ.

Для організації робіт та підтвердження відповідності вимогам необхідно реалізувати: опис методів, які використовуються для унікального маркування кожної версії ПЗ та ідентифікації елементів конфігурації; перелік елементів конфігурації, які пов'язані з реалізацією функцій безпеки ПЗ та повинні контролюватися системою керування конфігурацією ПЗ; порядок використання системи керування конфігурацією ПЗ з ціллю визначення всіх елементів конфігурації, на які впливає модифікація елемента конфігурації відповідно стандарту ДСТУ ISO 10007:2005 «Системи управління якістю. Настанови щодо управління конфігурацією» [9], розробляти відповідно стандарту ДСТУ ISO/IEC 15408 [6] вимог сімейства:

- ALC.CMC «Можливості управління конфігурацією»;
- ALC.CMS «Область управління конфігурацією».

Менеджмент інфраструктури середовища розробки ПЗ. В процесі менеджменту інфраструктури середовища розробки ПЗ розробник повинен реалізувати наступні заходи: захист від несанкціонованого доступу до елементів конфігурації; резервне копіювання елементів конфігурації; реєстрація подій, які пов'язані з фактами змін елементів конфігурації.

Документація розробника ПЗ повинна містити: відомості про періодичність та перелік елементів конфігурації, які підлягає резервному копіюванні; опис застосованих технічних та організаційних заходів, які забезпечують захист від несанкціонованого доступу до елементів конфігурації, резервне копіювання та відновлення визначених елементів конфігурації, реєстрацію всіх подій, які пов'язані з фактами змінення елементів конфігурації, в журналі реєстрації подій; перелік елементів конфігурації, які повинні бути захищені від загроз безпеки інформації, які пов'язані з порушенням конфіденційності, цілісності та доступності - необхідно розробити у відповідності стандарту ДСТУ ISO/IEC 15408 [6] вимог сімейства:

- ALC_DVS «Безпека розробки»;
- ALC.CMC «Можливості управління конфігурацією».

Менеджмент людськими ресурсами. В процесі менеджменту людськими ресурсами розробник ПЗ повинен реалізовувати наступні заходи: періодичність навчання співробітників; періодичний аналіз програми навчання співробітників.

Для підтвердження відповідності вимогам документація розробника ПЗ повинна містити: правила та програми навчання; відомості про періодичність навчання; відомості про проходження співробітників навчання.

Висновки.

В процесі огляду стандартів було виявлено актуальність стандартів, які чині на території України [3, 5, 6, 8, 9], відсутність нормативних посилань на таких етапах процесу ЖЦ ПЗ, як менеджмент людськими ресурсами та особливість при розробці захищених ІС.

Напрям подальшого дослідження є виявлення суміжних стандартів та їх опрацювання для подальшого дослідження проблеми захисту ІС у зв'язку з скасуванням міждержавного стандарту ГОСТ 19 серії (починаючи з 2018 року) [8] та стандартів з менеджменту людськими ресурсами, які не враховані в оглянутому стандарті [4].

1. 28 магических мер безопасностого програмного обеспечения [Електронный ресурс] : Материалы VI Всероссийской конференции «Безопасные информацыионные технологии« Вопросы кибербезопасности / Барабанов А.В., Марков А.С., Цирлов В.Л. - 2015 - Выпуск №5(13) - С. 2-10. - Режим доступу: http://cyberrus.com/wp-content/uploads/2015/12/02-10-513-15_1.-Баранов.pdf
2. Борисов С. СОИБ. Анализ. Разработка безопасного ПО [Електронний ресурс]. / С. Борисов - 08.08.2016 р. - Режим доступу до статті: http://www.securitylab.ru/blog/personal/sborisov/308857.php
3. Единая система программной документации: сборник / Национальные стандарты. – Изд. официальное. – М. : Стандартинформ изд., 2005. – 128с.
4. Защита информации. Разработка безопасного программного обеспечения. Общие требования : ГОСТ Р 56936-2016. - [Действует от 2016-06-01]. - М.: Стандартинформ, 2016. - 24 с. - (Национальный стандарт Российской Федерации).
5. Інженерія систем і програмного забезпечення. Процеси життєвого циклу програмного забезпечення (ISO/IEC 12207:2008, IDT) : ДСТУ ISO/IEC 12207:2014. - [Чинний від 2016-01-01]. - К. : Держспоживстандарт України, 2016. - 106 с. - (Національний стандарт України).
6. Методи і засоби забезпечення безпеки. Критерії оцінки безпеки інформаційних технологій. Частина 3. Вимоги довіри до безпеки (ISO/IEC 15408-3:2008) : ДСТУ ISO/IEC 15408-3:2013. - [Чинний від 2013-12-05]. - К. : Держспоживстандарт України, 2013. - 142 с. - (Національний стандарт України).
7. Методический аппарат анализа и синтеза комплекса мер разработки безопасного программного обеспечения [Електронний ресурс] / А.В. Барабанов, А.С. Марков, В.Л. Цирлов : Международный научно-практический журнал «Программные продукты и системы» : Главный редактор С.В.Емельянов - 2015. -№4 (112). - С. 166-174. - Режим доступу к журн. http://www.swsys.ru/index.php?page=article&id=4086&lang=
8. Про скасування міждержавних стандартів в Україні, що розроблені до 1992 року : наказ ДП «УкрНДНЦ» №184 від 14.12.2015 р. [Електронний ресурс] - Режим доступу: http://ukrndnc.org.ua/files/2015/12_14/N184_2015-12-14.rtf
9. Системи управління якістю. Настанови щодо керування конфігурацією (ISO 10007:2003, IDT) : ДСТУ ISO 10007:2005. - [Чинний від 2007-08-01]. - К. : Науково-дослідний інститут метрології вимірювальних і управляючих систем (ДП «НДІ «Система»), 2007. - 12 с. - (Державний Стандарт України).
10. Технології програмування і захист інформаційних систем [Електронний ресурс] / О.Є. Коваленко, В.М. Антоненко // Інститут проблем математичних машин і систем НАН України (Академія ДПС України). - 2003. - Режим доступу: http://nc.asta.edu.ua/Kyrsi%202003/tezi/images_tezi/197.htm