УДК 681.5.033.2

д.т.н., доц. **Бойченко О.В.** (ОДАТРЯ)
Лєнков О.С. (ВІКНУ)
Охрамович Л.В. (ВІКНУ)

МЕТОДИКА ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ РЕСУРСІВ АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ

У статті запропоновано методику оцінки захищеності інформаційних ресурсів автоматизованої системи управління на основі технології пошарового проектування програмного забезпечення. Основою методики є застосування пошарового модульного контролю захищеності шарів програмного забезпечення автоматизованої системи управління так, що кожен шар пов'язаний з певним етапом криптографічних перетворень. Розробленням методики створені умови для забезпечення постійного контролю за можливістю несанкціонованих впливів на програмне забезпечення інформаційної системи та підвищення показнику рівня стійкості інформаційної системи до несанкціонованих впливів та контролю за даними до 27%.

Ключові слова: автоматизована інформаційна система, інформаційні ресурси, пошарове проектування програмного забезпечення, несанкціоновані впливи, криптографічні перетворення.

Постановка проблеми. Проблема забезпечення інформаційної безпеки на усіх рівнях ієрархії автоматизованої системи управління (АСУ) може бути успішно вирішена тільки при наявності та функціонування комплексної системи захисту даних, яка охоплює увесь життєвий цикл інформаційної системи від розробки до її утилізації, а також усю технологічну ланку збору, обробки, зберігання та видачі інформації.

Аналіз останніх досліджень і публікацій. Дослідженням проблематики сучасних аспектів застосування різноманітних методик оцінки захищеності інформаційних ресурсів (ІР) АСУ щодо опису захищеності системи через деякі «бажані» стани даних систем, аналізі типових ситуацій загроз та діючих на них закономірностей свого часу займалися такі фахівці як Зегжда Д. П., Івашко О. М., Корченко О.Г., Борисов О. М., Алексєєв О.В., Меркур'єва Г.В., Громов Ю. Ю., Драчов В. О. та інші [1-4].

Постановка завдання. Необхідність проведення наукових досліджень щодо розробки нової методики оцінки захищеності ІР АСУ обумовлена доволі високою динамікою проявів загроз інформаційній системі та необхідністю упорядкованого реагування на них розробкою та застосуванням адекватних систем захисту даних АСУ.

Виклад основного матеріалу. Технологія прийняття рішення по застосуванню необхідної політики безпеки на основі існуючих та розроблюваних моделей безпеки з наступним застосуванням отриманої політики безпеки до інформаційної системи може бути подана наступним чином (рис. 1)

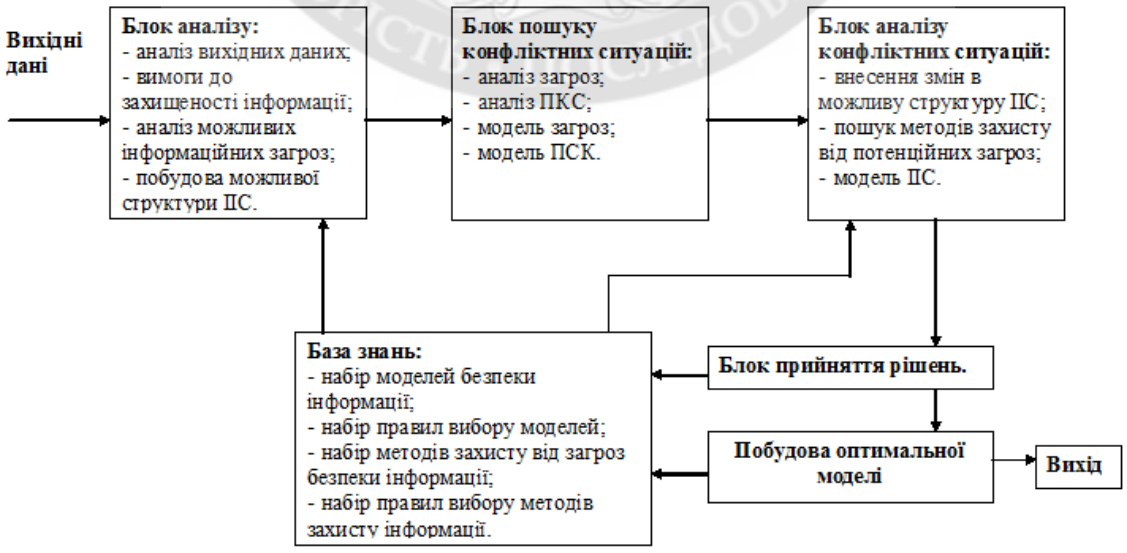

Рис. 1. Технологія прийняття рішення по застосуванню необхідної політики безпеки ІР АСУ

Відповідно до прийнятого рішення щодо застосування політики безпеки доцільно запропонувати методику оцінки стану захищеності даних АСУ на основі тестування компонентів системи інформаційної безпеки.

Як відомо, показниками якості функціонування сучасних АСУ є доволі великих перелік факторів, найважливішими з яких є вірогідність надання необхідної інформації в заданий термін, вірогідність відсутності прихованих випадкових помилок в представленій за запитом користувача інформації, вірогідність збереження актуальності інформації на момент її використання, вірогідність запобігання несанкціонованому доступу та збереження конфіденційності інформації.

Аналіз практики застосування АСУ спеціального призначення, що часто функціонують в умовах невизначеності, наявності доволі суттєвого функціонального впливу сторонніх факторів (об'єктивної та суб'єктивної природи), а також швидкої зміни обстановки та скорочення термінів часу для прийняття управлінського рішення, потребують запровадження заходів, що направлені на підвищення оптимальності функціонування автоматизованих комп'ютерних систем.

Зокрема, моделювання процесів представлення інформації в умовах ненадійності програмно-технічних засобів може бути подана наступним алгоритмом у складі основних трьох етапів:

1. Вихідні припущення (аналіз практики застосування інформаційно-телекомунікаційних систем спеціального призначення перебором відомих станів функціонування інформаційної системи у реальному часі);

2. Прогнозні варіанти функціонування інформаційної системи по наданню даних в умовах ненадійності програмно-технічних засобів (у першому випадку відбувається надійне надання інформації, а в другому та третьому випадках відбувається непредставлення інформації по запиту);

3. Розрахунок надійності функціонування інформаційної системи (визначення вірогідності надійного надання інформації $P_{над}$ при виконанні функціонального завдання в умовах ненадійності програмно-технічних засобів)

$$P_{над} = \frac{n^2 (n^{-1} + w^{-1})}{(\nu + n)},$$

де n^{-1} - середній час напрацювання програмно-технічних засобів на відмову; w^{-1} - середній час відновлення програмно-технічних засобів; ν^{-1} - середній час виконання відповідного функціонального завдання [5].

Зазначені методики є доволі ефективними для оцінки надійності захисту інформаційних ресурсів сучасних АСУ спеціального призначення. Однак їх застосування є обмеженим відносно часових обмежень та забезпечення постійного контролю за можливістю несанкціонованого впливу на ІР АСУ.

У такому випадку доцільним є застосування методики оцінки захищеності ІР АСУ спеціального призначення на основі технології пошарового проектування стійкого програмного забезпечення АСУ [6] відповідно вимог стандарту ГОСТ 28147-89 «Системи обробки інформації. Захист криптографічний. Алгоритм криптографічного перетворення» [7].

В основі методики є здійснення послідовності операцій тестових випробувань шифрування, розшифровування та перевірки правильності алгоритму шифрування та розшифрування з ІР обсягом 640 біт (10 блоків по 64 біта).

Методика оцінки передбачає пошаровий модульний контроль захищеності шарів програмного забезпечення (ПЗ) АСУ так, що кожен шар пов'язаний з певним етапом криптографічних перетворень. У складі методики застосовано два типи маркерів контролю несанкціонованого впливу на ПЗ АСУ (S) (якщо відповідний маркер дорівнює 1, то

несанкціонована модифікація відсутня, а якщо 0 – несанкціонована модифікація так, якщо хоч би один маркер з ($S_1,\dots S_{10}$) рівний 0, то $S = 0$).

Отримані наукові результати. Перевагою методики є можливість постійного самоконтролю стану захищеності ПЗ АСУ через застосування двох паралельних ідентичних потоків крипто перетворювань, що працюють в режимі реального часу та третього потоку, який порівнює їх між собою в реальному режимі часу і фіксує значення $S_1,\dots S_{10}$ і S.

Особливістю методики є запровадження припущення щодо принципової можливості доступу несанкціонованого користувача до виділеного обчислювального процесу та його модифікації в певний момент часу. Таким чином, при проведенні модифікації одного з потоків крипто перетворювань, між цими обчислювальними потоками з'явиться різниця, яка буде відбита в обчислювальному потоці порівняння, що забезпечить виявлення модифікації по ($S_1,\dots S_{10}$) та у підсумку S.

Висновки. В результаті проведення досліджень встановлено, що запровадження методики оцінки стану захищеності ІР АСУ на основі технології пошарового проектування стійкого програмного забезпечення відповідно вимог стандарту ГОСТ 28147-89 «Системи обробки інформації. Захист криптографічний. Алгоритм криптографічного перетворення» дозволяє забезпечувати постійний контроль за можливістю несанкціонованих впливів на ПЗ інформаційної системи.

Проведені дослідження визначають підвищення показнику стану захищеності ІР АСУ (рівня стійкості інформаційної системи до несанкціонованих впливів та контролю за даними до 27%).

Отримані наукові результати можуть знайти подальше застосування під час наукових досліджень в напрямку розроблення методичних основ оцінки стану захищеності прикладного програмного забезпечення інформаційних систем спеціального призначення.

ЛІТЕРАТУРА:

1. Зегжда Д.П. Основы безопасности информационных систем: монография / Д.П. Зегжда, А.М. Ивашко. – М.: Горячая линия – Телеком, 2000. – 263 с.

2. Корченко А.Г. Построение защиты информации на нечетких множествах. Теория и практика решения: монография / Корченко А.Г. - М.: МК-пресс, 2006. – 256 с.

3. Борисов А.Н. Обработка нечеткой информации в системах принятия решений: монография / А.Н. Борисов, А.В. Алексеев, Г.В. Меркурьева. – М.: Радио и связь, 1989. – 103 с.

4. Громов Ю.Ю. Задача выбора политики безопасности при функционировании информационной системы в условиях неопределенности / Ю.Ю. Громов, В.О. Драчов, Т.Г. Самхарадзе // Инженерная физика. – М.: Научтехлитиздат, 2009. - №1. – С. 32-36.

5. Бойченко О.В. Оцінка якості та оптимізація функціонування інформаційних систем / О.В. Бойченко // Захист інформації. – К.: НАУ, 2011. – № 2 (51). – С.105-107.

6. 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.

7. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования: ГОСТ 28147-89. – [Действителен от 1990-07-01]. – М.: ИПК Издательство стандартов, 1996. – 28 с.

Рецензент: д.т.н., проф. Толубко В.Б., Державний університет телекомунікацій

д.т.н., доц. Бойченко О.В., Ленков А.С., Охрамович Л.В.

МЕТОДИКА ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ

В статье предложена методика оценки защищенности информационных ресурсов автоматизированной системы управления на основе технологии послойного проектирования программного обеспечения.

Основой методики является применение послойного модульного контроля защищенности слоев программного обеспечения автоматизированной системы управления так, что каждый слой связан с определенным этапом криптографических превращений.

Разработкой методики созданные условия для обеспечения постоянного контроля за возможностью несанкционированных влияний на программное обеспечение информационной системы и повышение показателю уровня стойкости информационной системы к несанкционированным влияниям и контролю за данными до 27%.

Ключевые слова: автоматизирована информационная система, информационные ресурсы, послойное проектирование программного обеспечения, несанкционированные влияния, криптографические превращения.

O. Boitchenko, A. Lenkov, L. Ohramovich

METHODS OF PROTECTION OF INFORMATION RESOURCES AUTOMATED CONTROL SYSTEM

In the article the method of estimation protected of informative resources automatic control system of management is offered on the basis of technology of the layer planning of software.

Basis of method is application of layer module control of protected of layers automatic control system of management software so, that every layer is related to the certain stage of cryptographic transformations.

By development of method the created terms for providing of permanent control after possibility of unauthorized influences on informative system software and increase to the index of level firmness of the informative system to unauthorized influences and control after information to 27%.

Keywords: automatic control system of management, informative resources, layer planning of software, unauthorized influences, cryptographic transformations, is automated.