Вплив вразливостей на функціональні послуги безпеки КСЗІ

В.О. Поддубний[1], В.І. Заболотний[2], А.О. Бойко[3]

1. Кафедра Безпеки інформаційних технологій Харківський національний університет радіоелектроніки, Україна, м. Харків, пр. Науки, 14, E-mail: vadym.poddubniy@nure.ua

2. Кафедра Безпеки інформаційних технологій Харківський національний університет радіоелектроніки, Україна, м. Харків, пр. Науки, 14, E-mail: volodymyr.zabolotnyi@nure.ua

3. Приватне акціонерне товариство "Інститут інформаційних технологій", Україна м.Харків, вул. Бакуліна, 12, E-mail: boyko@iit.kharkov.ua

Коротка анотація –While creating IT system, it is not impossible to make mistakes, sometimes they can be almost useless, but some of them can be used to attack the software or the system. An exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware. Such behavior frequently includes things like gaining control of a computer system, allowing privilege escalation, or a denial-of-service (DoS or related DDoS) attack.

Nowadays there are several standards of information security management, such as ISO ISO/IEC 27000 series standards.

The purpose of this work is to offer a model of the relationship between vulnerabilities and security services implemented in information and telecommunication systems. Such a system would allow assessing the impact of each of the vulnerabilities on each of the security services implemented in information and telecommunication systems with a comprehensive information security system. Such a model is needed to assess the risks to existing systems and to mitigate the transition to international standards.

Ключові слова – CVSS, ISO/IEC 27000, вразливості, системи управління вразливостями, функціональні послуги безпеки

I Вступ

В сучасному світі неможливо обійтись без стандартизації, яка погоджує різні сфери діяльності, в тому числі і діяльність в галузі інформаційної безпеки. Україна обрала курс на введення міжнародних норм та правил на заміну національним стандартам. Наказ № 631 від 28.12.2010 «Про затвердження національних стандартів України та скасування чинності нормативних документів» [1] вводить до використання цілу низку міжнародних стандартів в різних галузях, в тому числі вперше введений стандарт ДСТУ ISO/IEC 27001:2010 «Інформаційні технології. Методи та засоби досягнення інформаційної безпеки. Системи керування інформаційною безпекою. Вимоги», в подальшому введені і інші стандарти цієї серії в наказах № 1494 від 30.12.2014 [2]; № 631 від 28.12.2010 [3]; № 193 від 18.12.2015 [4]; № 207 від 04.08.2017 [5].

Одним з процесів захисту інформації є процес оцінки ризиків при експлуатації, що передбачає оцінку ризиків від виявлених вразливостей. Зараз відсутні моделі та засоби оцінки впливу виявлених вразливостей на ІТС з КСЗІ. Тому необхідно створити власну модель оцінки вразливостей та її впливу на ІТС з КСЗІ. Така модель необхідна для оцінки ризиків для вже існуючих систем, та для пом'якшення переходу на міжнародні стандарти, оскільки процес переходу від національних до міжнародних стандартів та їх гармонізація займе деякий час.

II Вразливості

Під час розробки ПО виникають помилки, деякі помилки не несуть в собі небезпеки, а деякі становлять серйозну загрозу ІТЗ. Для усунення вразливостей виконується оновлення ПЗ. Однак оновлення може призвести до порушення працездатності ІТС. Так наприклад оновлення Windows 10 October 2018 містило помилки які призводили до видалення файлів користувачів , та та помилки роботи з архівами які могли призвести до втрати даних [6]. А оновлення KB4489894 для Windows 10 могло призводити до аварійного завершення роботи системи [7]. Тому необхідно пріоритезувати встановлення оновлень. Показником для встановлення пріорітета є співвідношення потенціальних ризиків від неусунення вразливостей та ризиків від встановлення оновлень.

Але для всіх систем управління ризиками необхідна база вразливостей, яка буде містити інформацію про вплив вразливості на ІТС. Для оцінки впливу вразливості зазвичай використовують систему оцінки вразливостей CVSS версії 2.0 або 3.0. За допомогою даної системи можна слідкувати за вразливостями, та приймати рішення що до мір реагування. CVSS намагається призначити показники критичності вразливості, що дозволяє респондентам визначати пріоритети дій та ресурсів відповідно до загрози. Оцінки розраховуються на основі формули, яка залежить від кількох показників. Оцінки коливаються від 0 до 10, де оцінка 10 означає найвищий ступінь критичності вразливості. Рівень небезпеки можна оцінити за шкалою **FortiGuard,** де оцінка за системою CVSS переводиться в рівні критичності.Оцінка від 0.1 до 3.9 значить низький рівень загрози, від 4 до 6.9 середній, від 7 до 8.9 високий, від 9 до 10 критичний. Так наприклад за період з 07.10.2019 по 13.10.2019 було виявлено 253 нові вразливості, 48,6% низької загрози, 26,1 середньої, 25,3 високої. При цьому 16,2% вразливостей не було виправлено на момент написання роботи [8].

III Функціональні послуги безпеки

В Україні на даний момент діє Нормативний документ НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від

несанкціонованого доступу». Цей документ є методологічною базою для визначення вимог з захисту інформації в комп'ютерних системах від несанкціонованого доступу; створення захищених комп'ютерних систем і засобів захисту від несанкціонованого доступу; оцінки захищеності інформації в комп'ютерних системах і їх придатності для обробки критичної інформації (інформації, що вимагає захисту).

В процесі оцінки спроможності комп'ютерної системи забезпечувати захист оброблюваної інформації від несанкціонованого доступу розглядаються вимоги двох видів:

1) вимоги до функцій захисту (послуг безпеки);

2) вимоги до гарантій.

В контексті документу комп'ютерна система розглядається як набір функціональних послуг. Кожна послуга являє собою набір функцій, що дозволяють протистояти певній множині загроз. Кожна послуга може включати декілька рівнів. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз. Рівні послуг мають ієрархію за повнотою захисту, проте не обов'язково являють собою точну підмножину один одного.

Функціональні послуги згруповані за властивостями інформації та ІТС. Кожна з властивостей (конфіденційність, цілісність, доступність, спостережність).

Послуги є взаємозв’язаною множиною, наприклад рівень послуги «Цілісність комплексу засобів захисту» НЦ-1 є необхідною умовою абсолютно для всіх рівнів всіх інших послуг [9].

IV Вплив вразливостей на функціональні послуги безпеки

Знайдена вразливість може вплинути на реалізацію однієї, або декількох послуг , або не мати впливу ІТС зовсім. Наприклад вразливість призводить до порушення конфіденційності, але у ІТС не висувається вимог до конфіденційності. Тому вразливість не є критичною. Або навпаки сама вразливість може бути не критичною, але вплив який вона спричиняє на низку взаємозв'язаних послуг є фатальним, така ситуація потребує негайного рішення. Враховуючи, властивості вразливостей необхідно знати як вплине наявність вразливості на кожну конкретну ІТС з КСЗІ, щоб підрахувати ризики пов’язані з наявною вразливістю в системи, та прийняти рішення що до усунення даної вразливості або продовження роботи ІТС незважаючи на неї. Тому необхідно розробити систему яка б відображала вплив властивостей вразливості на реалізовані функціональні послуги безпеки.

Висновок

На даний момент актуальною задачею є розробка моделі взаємозв’язку між вразливостями та послугами безпеки які реалізуються в ІТС. Така система дозволила б оцінити вплив кожної з вразливостей на кожну з послуг безпеки, які реалізуються в ІТС з КСЗІ. Така модель необхідна для оцінки ризиків для вже існуючих систем, та для пом’якшення переходу на міжнародні стандарти.

Література

[1] Наказ №631 від 28.12.2010 «Про затвердження національних стандартів України та скасування чинності нормативних документів»[Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/rada/show/v0631831-10

[2] Наказ №1494 від 30.12.2014 «Про прийняття європейських та міжнародних нормативних документів як національних стандартів України, змін до національних стандартів України, скасування національних стандартів України та міждержавних стандартів в Україні» [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/rada/show/v1494731-14

[3] Наказ № 631 від 28.12.2010 «Про затвердження національних стандартів України та скасування чинності нормативних документів» [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/rada/show/v0631831-10

[4] Наказ № 193 від 18.12.2015 «Про прийняття нормативних документів України, гармонізованих з міжнародними та європейськими нормативними документами, скасування національних стандартів України» [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua/rada/show/v0193774-15

[5] Наказ № 207 від 04.08.2017 «Про прийняття національних нормативних документів, гармонізованих з європейськими нормативними документами, поправки до національного нормативного документа, скасування національних нормативних документів» [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/rada/show/v0207774-17

[6] В Windows 10 October 2018 Update обнаружена очередная ошибка [Електронний ресурс]. – Режим доступу: https://www.securitylab.ru/news/496057.php

[7] Мартовское обновление для Windows 10 вызывает «синий экран смерти» [Електронний ресурс]. – Режим доступу: https://www.securitylab.ru/news/498417.php

[8] Vulnerability Database [Електронний ресурс] - Режим доступу: https://www.cybersecurity-help.cz/vdb/

[9] НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу»; Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. – 61с.(Нормативний документ)