УДК 004.056 **doi: 10.26906/SUNZ.2020.4.055**

В. О. Поддубний[1], О. В. Сєвєрінов[1], О. С. Пустомельник[2]

[1] Харківський національний університет радіоелектроніки, Харків, Україна
[2] Харківський національний університет Повітряних Сил імені І. Кожедуба, Харків, Україна

МЕНЕДЖМЕНТ ВРАЗЛИВОСТЕЙ ЯК СКЛАДОВА ЧАСТИНА ПОЛІТИКИ БЕЗПЕКИ ІТС

Анотація. Предметом дослідження в статті є менеджмент вразливостей у складі системи управління інформаційною безпекою. **Мета роботи** – розгляд сучасних стандартів, нормативних документів, що встановлюють та регулюють процеси управління вразливостями та ризиками, що пов'язані з вразливостями. В статі здійснюється розгляд процесу інтеграції менеджменту вразливостей в системі управління інформаційною безпекою та його форми. **Висновки**: в сучасних системах управління інформаційною безпекою належним чином не враховуються вразливості та ризики, пов'язані з вразливостями, сучасна нормативна база України майже не регулює та не встановлює вимог для систем захисту інформації в області вразливостей. В даний час процеси керування та оцінювання ризиків покладено на адміністраторів, тому для ефективного менеджменту вразливостей необхідна чітка система правил і методик. Розробка такої системи являється перспективною задачею, а при процесі модернізації стандартів, вимог України через деякий час стане необхідністю. При додаванні якісної системи оцінки вразливостей така система буде чіткою, нормованою та слугуватиме вказівником щодо дій в конкретній ситуації.

Ключові слова: Менеджмент вразливостей, СУІБ, CVSS, ISO/IEC 27005, ISO/IEC 27035, ISO/IEC 35001, NVD.

Вступ

Програмне забезпечення – це складова частина інформаційно-телекомунікаційної системи, проте під час розробки програмного забезпечення виникають помилки, деякі помилки не несуть в собі небезпеки, а деякі становлять серйозну загрозу інформаційно-телекомунікаційним системам (далі – ІТС). Для забезпечення безпеки та працездатності ІТС важливо вести контроль за виявленням, усуненням та супроводженням вразливостей в програмному забезпечені (далі – ПЗ).

Тому необхідно під час розробки та експлуатації системи здійснювати менеджмент вразливостей, який регламентує, яким чином виявляти вразливості, реагувати на тих та встановлює відповідальність за процеси менеджменту.

Однією із частин менеджменту вразливостей є оцінка ризиків, така оцінка необхідна для вибору рішень щодо реакції на певну вразливість [1]. Такими рішеннями може бути: оновлення програмного забезпечення, прийняття ризику, здійснення додаткових налаштувань, ручне усунення або виправлення, зменшення бізнес процесу тощо.

Проте слід зауважити, що хоча це досить важливий і необхідний процес, в Україні не існує вимог чи настанов, які зобов'язують чи допомагають організаціям в веденні такого менеджменту. Наслідки такого відношення можуть сприяти різноманітним кіберінцидентам, що несуть збитки бізнес процесам компаній. Так наприклад одні з найбільших кібератак в Україні (WannaCry і Petya) були здійснені через використання вразливостей протоколу SMB [2].

Тому управління вразливостями є необхідним процесом, що не виключить вразливості в ПЗ, проте пом'якшить або усуне наслідки від їх наявності, допоможе в встановленні відповідальності за процеси керування вразливостями та нормує дії в різних ситуаціях. Такий менеджмент також покращує розуміння впливу конкретної вразливості на окремі компоненти, або систему в цілому, це допомагає встановити коли необхідно приймати ризик (якщо влив мінімальний), а коли здійснювати виправлення, адже оновлення програмного забезпечення, або здійснення ручного виправлення може наражати систему на нові вразливості, а зупинка чи обмеження бізнес процесу несе за собою збитки для компанії.

Виклад основного матеріалу

Вразливості програмного забезпечення мають різний характер по своїй структурі, походженню, критичності, тощо. Тому постає питання правильного контролю за різними типами вразливостей. Для оцінки впливу вразливості зазвичай використовують систему оцінки вразливостей CVSS (Common Vulnerability Scoring System) 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 виразу, що 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 6.11.2020 по 12.11.2020 знайдено 401 нова вразливість (рис. 1), із них 7 критичних та 27 все ще не мають виправлень (рис. 2) [2].

Слід зауважити що в останні роки кількість знайдених вразливостей невпинно зростає (рис. 3), підставляючи під небезпеку все більше програмних засобів та систем в цілому [3-10]. Такий ріст зумовлений ускладненням структури програмних засобів, їх розробкою більшими колективами/компаніями або віддачою розробки на аутсорсінг.

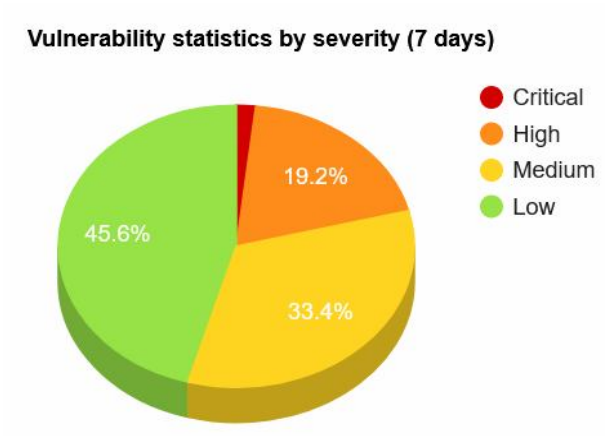

Рис. 1. Ранжування критичності знайдених вразливостей

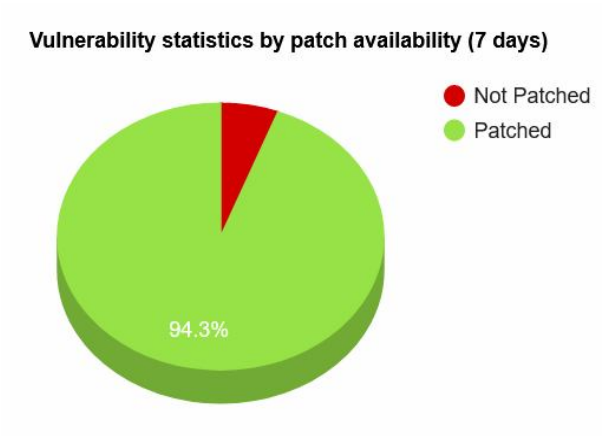

Рис. 2. Кількість невиправлених вразливостей

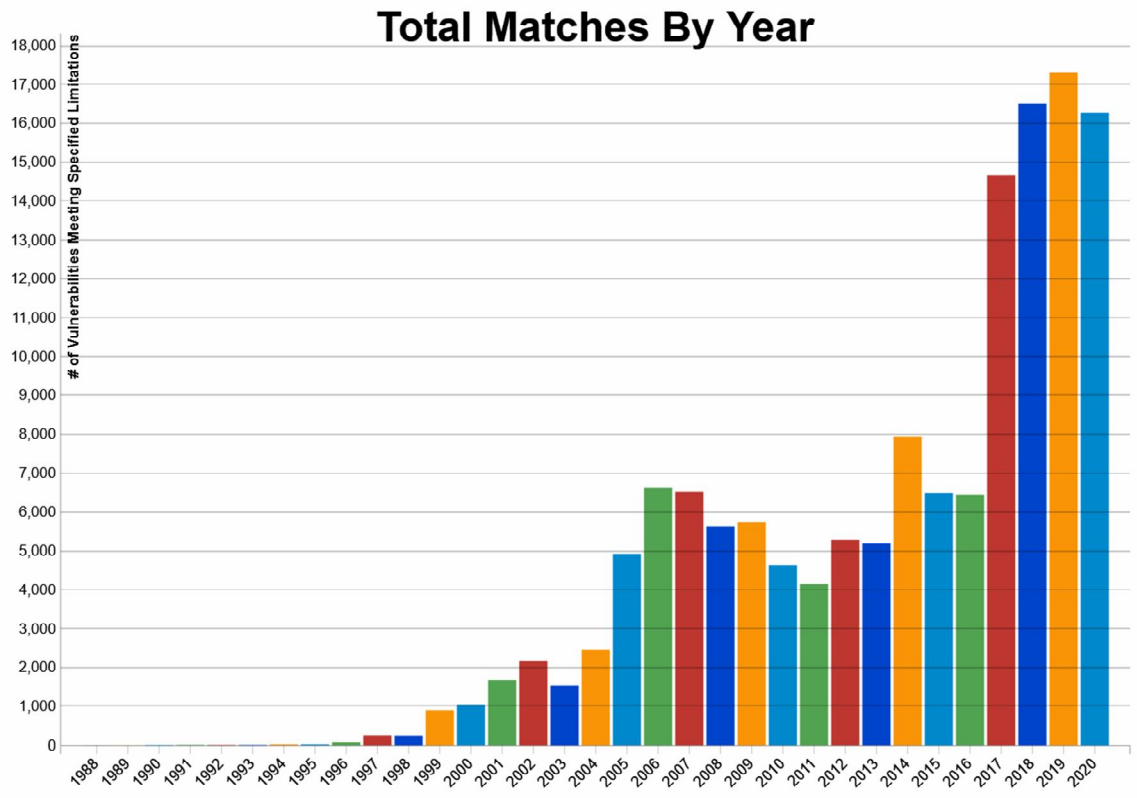

Рис. 3. Кількість виявлених вразливостей згідно National Vulnerability Database

Обробку даної інформації покладено на адміністраторів, які хоч і використовують сканери для виявлення цих вразливостей проте вимушені здійснювати оцінювання ситуації виходячи зі своїх знань та досвіду.

Такий підхід збільшує кількість помилок при прийнятті рішень щодо реагування із-за суб'єктивізації результатів та створює неоднозначність трактування результатів. Також це підвищує вимоги до персоналу, та час адаптації, адже новим адміністраторам необхідно знати добре структуру, склад особливості функціонування системи.

В даний час існують лише гармонізовані стандарти ISO/IEC [11-14], які надають вказівки щодо контролю вразливостей у СУІБ. Також існують додаткові методики такі як «Implementing a Vulnerability Management Process. SANS Institute Information Security Reading Room» [15] проте ні вони, ні гармонізовані стандарти не надають чітких інструкцій щодо оцінювання ризиків. Ці стандарти та методики мають загальний рекомендований характер щодо оцінювання ризиків, опису етапів менеджменту вразливостей, розподілу обов'язків у СУІБ, форми звітів, рекомендації щодо зв'язків з іншими організаціями тощо.

В даний час діє Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України № 269 від 14.05.2020 "Про встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації" [16] встановлює як вимогу наявність у кваліфікованого надава-

ча електронних довірчих послуг процедур з управління ризиками, персоналом, операційною безпекою, інцидентами. Цей наказ не встановлює чітких вимог, або форми процедур, проте процес гармонізації та внесення коректив в законодавчу базу показує рух України в даному напрямку. Розроблення, інтеграція, перехід та введення в дію нових вимог, стандартів, правил займе деякий час, проте вже зараз можна сказати, що даний процес вже запущений. Тому менеджмент вразливостей через деякий час стане не додатковим інструментом, а важливою необхідністю.

Однією із форм такого менеджменту є введення його в політику безпеки. Така політика повинна відповідати на ряд питань, а саме: яким чином виявляти вразливості, яким чином оцінювати ризики, як реагувати на вразливості, які дії повинне виконати адміністратор безпеки та аудиту, системний адміністратор, правління, де знаходиться межа прийняття ризику. Для того щоб дати відповіді на ці питання необхідно правильно оцінювати кожну конкретну вразливість, що виникає при експлуатації ІТС.

Тому під час розробки такої політики не обійтися від системи оцінки вразливостей, яка буде здійснювати оцінку впливу як на всю ІТС та на окремі компоненти. Така система повинна сформувати якісні оцінки впливу а при додаванні критичності компонентів системи отримаємо сформовану оцінку ризику конкретної вразливості. Вже описана CVSS, якраз надає якісний бал та вектор впливу, який можна використовувати при реалізації системи менеджменту вразливостей. Цей вектор надає інформацію про вплив на конфіденційність, цілісність, доступність, вектор атаки, наявність виправлень, наявність програмної реалізації експлойту, тощо. Політика безпеки в даному випадку, встановлюватиме лише дії які необхідно виконати при конкретному значенні ризику.

Для такої системи необхідно правильно оцінювати компоненти та взаємозв’язки компонентів, так як вплив вразливостей може виходити за границі одного об’єкту чи процесу, або вплив вразливості на різні компоненти сколюватиметься й призводитиме до більш значних наслідків.

Схематично така модель матиме вигляд як показано на рис. 4.

В такій системі на вхід подається опис критичності ресурсів в числовому представленні (такі показники формуються заздалегідь під час створення політики безпеки ІТС), та конкретні оцінки вразливостей зі сканерів вразливостей. Ці данні накладаються на опис системи для визначення впливу вразливості на конкретні компоненти, взаємозв'язки між компонентами та загалом на систему. Після цього отримана якісна оцінка впливу слугує вказівником щодо оцінки ризику та вибору конкретних дій. Різні показники матимуть різну методику, щодо виправлень, або прийняття вразливості, якщо вона не є критичною або не впливає на роботу системи.

Правила реагування на конкретну оцінку повинні бути сформовані заздалегідь, погоджені з керівництвом та адміністраторами.

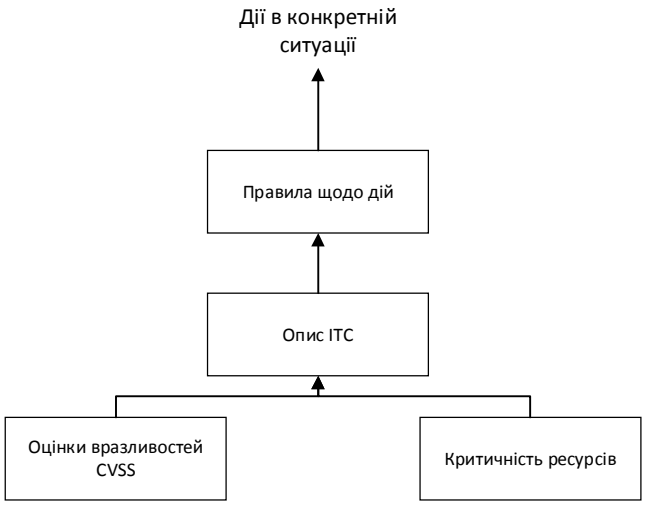

Рис 4. Приклад моделі керування вразливостями в СУІБ

З набору правил вибирається оптимальний варіант щодо дії виходячи з якісної оцінки впливу. Після цього адміністратор здійснює необхідні дії щодо усунення або прийняття ризику пов’язаним з наявністю вразливості.

В даній системі етап оцінки ризику повністю знятий з адміністратора, це означає можливість автоматизації процесів контролю вразливостями , усунення суб'єктивизації небезпеки, однозначність результатів.

Проте незважаючи на переваги такої системи менеджменту вона має один суттєвий недолік, а саме: в даний час не існує правил чи методик які б слугували правилами щодо опису ІТС. Тобто на даний момент сучасний опис ІТС не підходить для реалізації вказаної системи керування вразливостями, такий опис не показує належним чином взаємозв'язки компонентів, процесів, ресурсів, та не може бути використаний для реалізації системи керування вразливостями в СУІБ.

Створювана на базі такого опису система менеджменту не лишиться його недоліків, й матиме вигляд загальних вказівок та рекомендацій, які не матимуть чіткості й будуть схожі на вже існуючі стандарти та методики.

Тому однією з перспективних та необхідних задач на ряду з системою керування вразливостями в СУІБ є модель опису ІТС, яка б дозволила належним чином відтворити процеси та об'єкти в ІТС, їх взаємозв'язки, була б гнучкою в використанні та простою в освоєні.

Однією із таких моделей є формалізований опис ІТС. На відміну від неформалізованого опису системи формалізований має чітку структуру та форму опису, відображає взаємозв’язки процесів, є гнучким та універсальним. В такій системі вплив вразливості легко відслідкувати від точки контакту до всіх об’єктів інформаційної системи. Формалізація дає змогу виявити загальну структуру системи, сформулювати на цій основі загальні закони і правила, за якими відбувається визначення впливу вразливостей на ІТС.

Також формалізація необхідна для рівнів гарантій (Г-3, Г-4, Г-5 стиль опису ІТС повинен бути частково-формалізований, для Г-6 та Г-3 формалізований).

Висновок

Отже менеджмент вразливостей є досить важливою частиною функціонування ІТС, і з кожним роком його важливість збільшується. Як варіант пропонується суміщення політики безпеки з менеджментом вразливостей. Для інтеграції менеджменту з політикою безпеки необхідна наявність гнучкої системи оцінки впливу вразливостей на ІТС, яка б надавала якісну оцінку впливу для оцінки ризику та визначення дій що-до реагування.

Розробка такої системи являється перспективною задачею, а при процесі модернізації стандартів, вимог України через деякий час стане необхідністю. При додаванні якісної системи оцінки вразливостей така система буде чіткою, нормованою та слугуватиме вказівником щодо дій в конкретній ситуації.

Однією із важливих частин частин такої системи являється опис ІТС, тому необхідно сформувати правила опису які б були універсальними та показували взаємозв'язки між компонентами і процесами системи.

Як варіантом такий опис повинен бути формалізованим, для покращення наглядності взаємозв’язків процесів, гнучкості, та автоматизації процесів.

СПИСОК ЛІТЕРАТУРИ

1. Замула А.А., Северинов А.В., Корниенко М.А. Анализ моделей оценки рисков информационной безопасности для построения системы защиты информации //Наука і техніка Повітряних Сил Збройних Сил України. – 2014. – №. 2. – С. 133-138.
2. Cybersecurity Help s.r.o. [Електроний ресурс]:[Веб-сайт]-Режим доступу: https://www.cybersecurity-help.cz/.
3. National Vulnerability Database [Електроний ресурс]:[Веб-сайт]-Режим доступу: https://nvd.nist.gov/vuln/search/statistics?form_type=Advanced&results_type=statistics&search_type=all.
4. Кучук Н.Г., Гавриленко С.Ю., Лукова-Чуйко Н.В., Собчук В.В. Перерозподіл інформаційних потоків у гіперконвергентній системі / С.Ю. Гавриленко. *Сучасні інформаційні системи*. 2019. Т. 3, № 2. С. 116-121. DOI: https://doi.org/10.20998/2522-9052.2019.2.20
5. Nechausov A., Mamusuĉ I., Kuchuk N. Synthesis of the air pollution level control system on the basis of hyperconvergent infrastructures. *Сучасні інформаційні системи*. 2017. Т. 1, № 2. С. 21-26. DOI: https://doi.org/10.20998/2522-9052.2017.2.04
6. Mozhaiev M., Kuchuk N., Usatenko M. (2019) The method of jitter determining in the telecommunication network of a computer system on a special software platform. *Innovative technologies and scientific solutions for industries*, 2019. Vol. 4 (10), pp. 134-140. doi: https://doi.org/10.30837/2522-9818.2019.10.134
7. Зиков І. С., Кучук Н. Г., Шматков С. І. Синтез архітектури комп'ютерної системи управління транзакціями e-learning. *Сучасні інформаційні системи*. 2018. Т. 2, № 3. С. 60–66. DOI: https://doi.org/10.20998/2522-9052.2018.3.10
8. Гахов Р.П. Моделирование трафика беспроводной сети передачи данных / Р. П. Гахов, Н. Г. Кучук// Научные ведомости БелГУ. – 2014. – № 1 (172). – Вып. 29(1). – С. 175-181.
9. Коваленко А. А., Кучук Г. А. Методи синтезу інформаційної та технічної структур системи управління об’єктом критичного застосування. *Сучасні інформаційні системи*. 2018. Т. 2, № 1. С. 22–27. DOI: https://doi.org/10.20998/2522-9052.2018.1.04
10. Кучук, Г.А. Розрахунок навантаження мультисервісної мережі [Текст] / Г.А. Кучук, Я.Ю. Стасєва, О.О. Болюбаш // Системи озброєння і військова техніка. – 2006. – № 4 (8). – С. 130 – 134.
11. Сєвєрінов О. В., Черниш В. І., Молчанова М. Є. Управління інформаційною безпекою згідно міжнародних стандартів //Системи управління, навігації та зв'язку.–Вип. – 2011. – Т. 4. – С. 250-253.
12. ISO/IEC 27035:2016. Information technology — Security techniques — Information security incident management, 2016.
13. ISO/IEC 27005 Information technology — Security techniques — Information security risk management, 2018.
14. ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements, 2013.
15. Tom Palmaers, Dennis Distler, Implementing a Vulnerability Management Process //SANS Institute Information Security Reading Room, 2013. - 24 c.
16. Про встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації: затв. Адміністрацією Державної служби спеціального зв’язку та захисту інформації України від 14.05.2020 №269.

Received (Надійшла) 29.09.2020
Accepted for publication (Прийнята до друку) 28.10.2020

Vulnerability management as an integral part of its security policy

V. Poddubnyi, O. Sievierinov, O. Pustomelnik

Abstract. The subject of research in the article is the management of vulnerabilities in the information security management system. **The purpose** of the work is to consider modern standards that establish and regulate the management of vulnerabilities and risks associated with vulnerabilities. The article considers the process of integration of vulnerability management into information security management system and its form. **Conclusions:** modern information security management system does not properly take into account vulnerabilities and risks associated with vulnerabilities, the current regulatory framework of Ukraine almost does not regulate and does not set requirements for information security systems in the field of vulnerabilities. Currently, the processes of risk management and assessment are entrusted to administrators, so effective management of vulnerabilities requires a clear system of rules and methodologies. The development of such a system is a promising task, and in the process of modernization of standards, requirements of Ukraine after some time will become a necessity. When adding a quality vulnerability assessment system, such a system will be clear, standardized and will serve as a guide to action in a particular situation.

Keywords: Vulnerability Management, ISMS, CVSS, ISO / IEC 27005, ISO/IEC? 27035 ISO/EC 35001, NVD.