1. Директива 2006/32/ЄС Європейського парламенту і ради від 05 квітня 2006 р. «Про ефективність кінцевого використання енергії та енергетичних послугах, а також про відміну Директиви Ради 93/76 / ЄЕС».
2. *Фіалко Н.М., Тимченко М.П., Халатов А.А., Черенковський Ю.В.* Інтелектуальні енергетичні системи теплозабезпечення будівель.//Вісник Національного університету "Львівська політехніка". Теорія і практика будівництва. – 2016. – № 844. – С.203-209. – Режим доступу: http://nbuv.gov.ua/UJRN/ .
3. *Коцарь О.В.* Применение АСКУЭ для контроля текущих параметров режимов электропотребления на промышленных предприятиях // Энергетика и электрификация. – 2004. – № 6. – С.24-29.
4. *Скляров В.Ф., Гуляев В.А.,* Диагностическое обеспечение энергетического производства. – К.: Техніка, 1985.
5. *Заде Л.* Понятие лингвистической переменной и его применение к принятию приближенных решений. – М.: Мир, 1976. – 166 с.
6. Patent US 7103452 G06F19/00, G06F15/00, G05B23/02 – Method and system for targeting and monitoring the energy performance of manufacturing facilities.

Поступила 12.03.2018р.

УДК 681.3.06

Б.Я. Корнієнко, Київ
Л.П. Галата, Київ

ДОСЛІДЖЕННЯ ІМІТАЦІЙНОГО ПОЛІГОНУ ЗАХИСТУ КРИТИЧНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ МЕТОДОМ IRISK

Abstract. In this article, the research of information system protection by analyzing the risks for identifying threats for information security is considered. A quantitative method iRisk for security estimation is used. The known vulnerabilities of used software and hardware are considered and the stability of the built simulation polygon for the protection of critical information resources to specific threats is calculated.

Keywords: simulation polygon, critical information resources, security, vulnerability, threat, control.

Актуальність

Для дослідження системи захисту інформації ІС періодично проводиться аналіз інформаційних ризиків, який дозволяє виявити загрози інформаційній безпеці і в свою чергу використовувати та впроваджувати відповідні міри по їх нейтралізації [1]. Спираючись на проведену розробку і дослідження імітаційного полігону захисту критичних інформаційних ресурсів на базі прикладного програмного забезпечення GNS3 [2], можна зробити висновок, що тестування і оцінку побудованої захищеної мережі варто розглядати в

контексті тестування технічних характеристик, впливу налаштувань на рівень захищеності АС в цілому, а також в контексті застосованих засобів захисту інформації. Опираючись на те, що кількісні методики при проведенні аналізу ризиків на програмно-технічному рівні захисту і якщо не враховувати організаційно-технічну складову, мають більшу ефективність, то слід обрати саме кількісну методику оцінки захищеності [3, 4].

Постановка задачі

Враховуючи те, що акцент робиться саме на програмно-апаратному та мережовому рівні захисту інформації, ставиться задача дослідження імітаційного полігону захисту критичних інформаційних ресурсів методом iRisk для ефективної оцінки рівня захищеності мережі.

Вирішення задачі

Метод iRisk характеризується формально однією з найпростіших оцінок кількісних ризиків інформаційної безпеки АС. В загальному вигляді розраховується за наступною формулою:

$$iRisk = (Vulnerability * Threat) - Controls \quad (1)$$

де Vulnerability - оцінка вразливості, Threat – оцінка загрози, Control – оцінка мір безпеки. Дана методика використовує в собі іншу методику Common Vulnerability Scoring System v3.0 (CVSS V3) для оцінки вразливостей.

Формально розрахунок відбувається за не складною формулою, проте через те, що методика в собі містить загальну систему оцінки вразливостей CVSS, яка на практиці підтримується лідерами ринку в сфері захисту інформації, що дає змогу користуватись постійно актуальними коефіцієнтами для розрахунку вразливостей, а також мати перелік всіх основних вразливостей, які пов'язані з всіма сучасними програмними продуктами, що можуть використовуватись в АС [5].

Vulnerability (вразливість). Спершу розрахуємо Vulnerability (вразливість), для чого використаємо стандарт CVSS v3 [6]. Під час обрахунку використовується велика кількість коефіцієнтів, тому для зручності скористаємось програмним забезпеченням Національного інституту стандартів і технологій і просто задавши правильно параметри отримаємо результат обчислень у вигляді шкали від 1 до 10, де 1 відповідатиме найнижчий рівень, тобто відсутність вразливості, а значенню 10 відповідатиме критична вразливість, яку необхідно негайно усунути. В стандарт входить три групи метрик, необхідних для розрахунку, базова, часова та контекстна.

Значення метрики прийнято публікувати у вигляді пари з вектора (конкретні значення окремих показників) і числового значення, розрахованого на основі всіх показників і за допомогою формули, визначеної в стандарті. На рис. 1 зображено всі необхідні параметри для прозрахунку контекстної метрики полігону полігону захисту критичних інформаційних ресурсів.

Оцінка загрози (Threat). Згідно з даним стандартом загроза пояснюється як негативна подія, котра може виникнути в результаті того, що буде використано переваги вразливості. Для того аби зробити рівняння

максимально простим і зрозумілим, методика iRisk концентрується на двох основних компонентах: вплив і ймовірність.

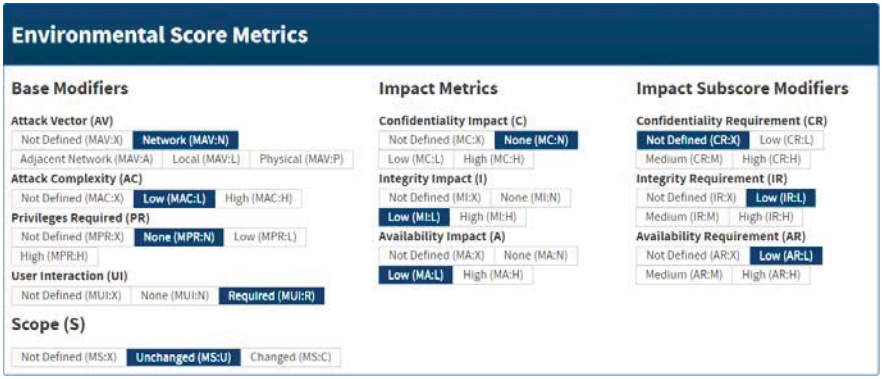

Рис. 1. Контекстна метрика полігону захисту критичних інформаційних ресурсів

Вплив (Impact) - це сума шкоди, яку цей інцидент принесе організації. В рамках рівняння iRisk SecureState в даний час використовуються наступні критерії для визначення впливу. За замовчуванням встановлено наступні значення, проте їх можна змінити відповідно до потреб оцінюваного об'єкту: фінансовий (25) – чи можуть загрози зруйнувати фінансові потоки організації; стратегічний (15) – чи можуть загрози призвести до довгострокових стратегіних втрат; операціний (25) – чи матимуть загрози вплив на безперебійність роботи; відповідність законодавству (25) – чи зможуть загрози вплинути на здатність дотримуватися стандартів; репутація (10) - чи може вплинути на відносини з клієнтами.

Іншим основним компонентом загрози є ймовірність. Для оцінювання ймовірності в iRisk береться до уваги два чинника, річна очікувана кількість реалізацій загроз і рівень знань та доступу необхідний зловмиснику (таблиця кореляції між рівнем знань/доступу та річною кількістю реалізації загроз (ARO) [6]).

Загроза розраховується за формулою 2, де Likelihood (кореляція з таблиці ARO [6]). Якщо загроза знаходиться в шкалі від 100 до 50 – рівень ризику високий, від 50 до 10 – середній від 1 до 10 – низький.

$$Threat = \text{Impact} * \text{Likelihood} \quad (2)$$

Control (оцінка мір безпеки). На підставі визначення організації ISACA в iRisk для забезпечення безпеки можуть застосовуватись профілактичні засоби, засоби направлені на виявлення, виправлення чи стримування.

Відповідно до стандарту заходи мають наступні рейтинги: профілактичний – 5, виявлення – 4, виправлення – 3, стримування –3.

Наступним кроком є визначення Controls (ефективності), вона згідно

стандарту має п'ятибальну шкалу, оцінка 5 ставиться у тому випадку, якщо засоби захисту інформаціїї в мережі значно перевищують мету, 4 – перевищує мету, 3 – реалізація відповідає меті, 2 – реалізація не повністю задовольняє свою мету, 1 – трохи відповідає своїй меті.

Склавши показники за CVSS отримуємо наступні значення:

- optimized (801 – 1000) – засіб не може бути розроблений або реалізований краще;
- managed (601 – 800) – продовжує вдосконалюватись;
- defined (401 – 600) – засоби захисту чітко визначені та зменшують ризик до помірного;
- initial/Ad-Hoc (1 – 200) – забезпечує лише деяку цінність захисту.

Отже, три основні компоненти, які фігурують в методі iRisk збалансовують один одного. Найвищий можливий бал для загрози становть 100, який помножений на максимальну вразливість (10). Тобто потенційно 1000 балів, яка компенсується потенційно ідеально реалізованим захистом, в кінці лишатиме нульовий ризик. На практиці, це майже не досяжно і в будь-якому випадку лишається якась частина залишкового ризику. Тобто ризик варіюється в значеннях від 0 до 1000, в даному випадку чим менше значення отримуємо, тим захищенішою є АС.

Побудований імітаційний полігон кібербезпеки має не так багато вразливостей, через якісне обладнання, розмежування доступу, яке поділяє мережу на демілітаризовану зону, внутрішню та зовнішню мережу, а також налаштувань мережі, через які, обмежена можливість доступу до мережі ззовні, обмежена кількість половинчастих з'єднань, що призводить до зменшення ефективності DDoS атак, можливості сканування мережі та ін. [2]. Та все ж, залишаються вразливості на програмно-апаратному рівні. Далі ми розглянемо деякі з них, розрахунок захищеності полігону захисту критичних інформаційних ресурсів буде проведено методом iRisk.

Вразливість Cisco IOS Arbitrary Command Execution Vulnerability (CVE-2012-0384). Вразливість виникає через помилку у реалізації авторизації HTTP/ HTTPS AAA авторизації (user profile) AAA, що дозволяє автентифікованому користувачеві виконувати будь-які довільні команди програмного забезпечення Cisco IOS, налаштовані для рівня привілеїв користувача [7].

Для розрахунку Vulnerability обрахуємо базову метрику, для більшої коректності робимо поправку на захищеність полігону кібербезпеки і розраховуємо метрику середовища і часову, як і було описано вище.

Base Score Metrics {Attack Complexity = Low; Privileges Required = Low; User Interaction = None; Scope= Unchanged; Confidentiality Impact = High; Integrity Impact = High; Availability Impact = High}

Temporal Score Metrics Score Metrics {Exploitability = Functional exploit exist}

Environmental Score Metrics {Base Modifiers {Attack Vector = Local; Attack Complexity = Low; Privileges Required = Low; User Interaction = None} {Scope

= Unchanged} {Impact Metrics {Confidentiality Impact = Low; Integrity Impact = Low; Availability Impact = High}} {Impact Subscore Modifiers {Confidentiality Requirement = Low; Integrity Requirement = Low; Availability Requirement = Low}}}

Результуючим обчисленням базового рівня є оцінка разливості в 7.8 з 10, що і приведено на рис. 2.

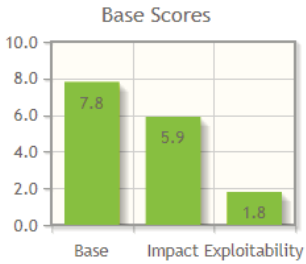

Рис. 2. Базова метрика вразливості CVE-2012-0384 для полігону кібербезпеки

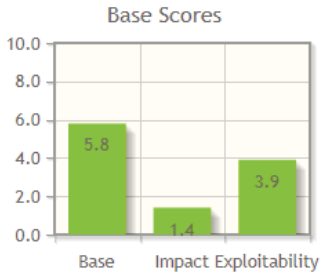

Рис. 3. Базова метрика вразливості CVE-2012-1342 для полігону кібербезпеки

Враховуючи те, що загроза повинна реалізовуватись з середини і перш за все орієнтована на те, що нею скористається звичайний користувач без адміністраторських прав, і очікувану кількість загроз оцінити як високу, то з таблиці ARO [6] оберемо кореляційне значення *Impact = 0.9*. Звісди, згідно формули 2 *Threat = 0.9 * 100 = 90.*

Судячи з наведеного вище, значення Controls оцінюємо в 650, що означатиме продовжує розвиватись.

Тобто значення для вразивості Cisco IOS Arbitrary Command Execution Vulnerability (CVE-2012-0384) *iRisk = (7.8 * 90) – 650 =50.*

Вразливість Cisco Access Control Bypass Vulnerability (CVE-2012-1342). Вразливість маршрутизаторів Cisco, яка дозволяє віддаленим атакам обходити Access Control List (ACL) та відправляти мережний трафік, який повинен бути відхилений. Реалізація вразливості призводить до порушення цілісності АС [8].

За аналогічною схемою як і для вразливості CVE-2012-0384 розрахуємо значення iRisk.

Base Score Metrics {Attack Vector = Network; Attack Complexity = Low; Privileges Required = None; User Interaction = None; Scope= Changed; Confidentiality Impact = None; Integrity Impact = Low; Availability Impact = Impact None}

Що при розрахунку в CVSS v3.0 калькуляторі дає значення *Vulnerability = 5.8* (рис. 3).

Розрахунок значення *Threat* (загрози) = *1.4*0.72*100 = 108,* звідси значення iRisk= (5.8 * 108) – 610 =16.4, що означатиме, що вразливість буде

приблизно рівна нулю, тобто можна зробити висновок, що даною вразливістю зловмисник може скористатись з малою ймовірнюстю.

Вразливість EternalBlue (CVE-2017-0144). Дана вразливість використовує вразливість в реалізації протоколу Server Message Block v1 (SMB). Зловмисник, сформувавши і передавши на віддалений вузол особливим чином підготовлений пакет, здатний отримати віддалений доступ до системи і запустити на ній довільний код [9].

Проведемо розрахунок значення iRisk для вразливості CVE-2017-0144 EternalBlue.

Базова метрика для вразливості EternalBlue буде мати наступні параметри. Результат відображено на рис. 4.

Base Score Metrics {Attack Vector = Network; Attack Complexity = High; Privileges Required = None; User Interaction = None; Scope= Unhanged; Confidentiality Impact = High; Integrity Impact = High; Availability Impact = High}

Так як атака проводиться ззовні і ймовірність її є дуже великою, зловмисник повинен бути експертом зі злому, згідно методології iRisk в данному випадку значення загрози *Threat = Impact*Likelihood*, значення *Impact= 100*, а кореляційне значення *Likelihood = 0.7*.

Звідси можна розрахувати значення iRisk для CVE-2017-0144, без патча безпеки від 14 березня 2017. *iRisk = (8.1*70) – 0 = 567*

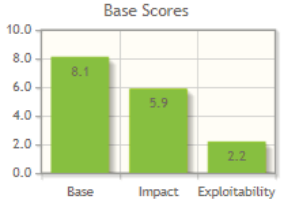

Рис. 4. Базова метрика вразливості CVE-2017-0144 EternalBlue

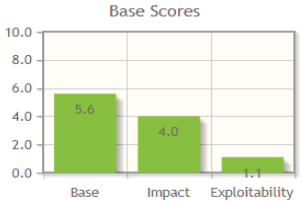

Рис. 5. Базова метрика вразливості CVE-2017-5754 Meltdown

Вразливість Meltdown (CVE-2017-5754). Вразливість експлуатує побічний ефект out-of-order execution виконання поза чергою в сучасних процесорах. Атака не залежить від операційної системи і не експлуатує программні вразливості. Meltdown по суті ламає всю систему безпеки засновану на ізоляції адресного простору в тому числі віртуального. Meltdown дозволяє читати частину пам'яті інших процесів і віртуальних машин. Патч KAISER виключає дану вразливість, проте зменшує швидкодію процесора [10].

Розрахуємо значення iRisk для полігону кібербезпеки, рахуючи, що не встановлений патч KAISER.

Розрахуємо базову метрику для вразливості Meltdown (CVE-2017-5754), результат якої відображено на рис. 5.

Base Score Metrics {Attack Vector = Local; Attack Complexity = High; Privileges Required = Low; User Interaction = None; Scope= Changed; Confidentiality Impact = High; Integrity Impact = None; Availability Impact = Impact None}

Враховуючи, що зловмисник може діяти як зовні так і з середини і атака може проводитись часто, а зловмисник може мати просто продвинутий рівень навичок, і код атаки викладено в великих кількостях статей, то це дасть кореляційне значення *Impact = 0.9*, а значення *Threat* (загрози) буде рівним *100*0.9 = 90*

Результуюче значення iRisk для Meltdown (CVE-2017-5754) буде рівним *iRisk=5.6*90*-0 = 504, так як без патча KAISER данна вразивість ніяк не виявлялась і була закладена в архітектуру більшості сучасних процесорів.

Вразливість SPECTRE (CVE-2017-5753, CVE-2017-5715). Даній вразливості присвоєно одразу два ідентифікатори CVE-2017-5753, CVE-2017-5715. По своїй суті дії вона схожа на Meltdown, проте з деякими відмінностями, зокрема тим, що в ході спекулятивного виконання коду процесор може виконати інструкції, які він не став би виконувати за умови строго послідовного (неспекулятивного) обчислення, і, хоча в подальшому результат їх виконання відкидається, його відбиток залишається в процесорному кеші і може бути використаний. Інший варіант реалізації Specter полягає в «перебаченні розгалужень» - в процесорі є аналогічний блок передбачення переходів, суть роботи якого полягає в передбаченні адреси за якою буде здійснений перехід чергової інструкції непрямого переходу (Meltdown, але тут вони грають іншу роль) [11].

Розрахуємо значення iRisk для вразливості Spectre. Базова метрика в обох варіацях реалізації вразливостей однакова, результати розрахунку представлені на рис. 6.

Base Score Metrics {Attack Vector = Local; Attack Complexity = High; Privileges Required = Low; User Interaction = None; Scope= Changed; Confidentiality Impact = High; Integrity Impact = None; Availability Impact = Impact None}

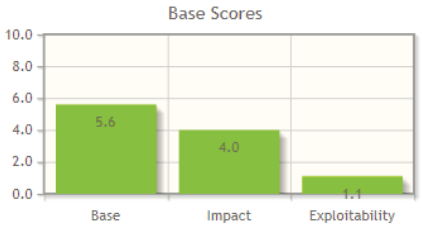

Рис. 6. Базова метрика вразливості Spectre CVE-2017-5753 і CVE-2017-5715

В обох випадках з Spectre ми маємо справу з тим, що процесор вчиться швидше виконати один процес на прикладі виконання іншого процесу, тим самим фактично дозволяючи другому процесу контролювати хід виконання

першого. Універсальних патчів для виправлення Specter пока немає, і захистом від CVE-2017-5715 пропонується постійно очищувати кеш і прибирати код з ядра.

Розрахуємо значення iRisk для CVE-2017-5715, враховуючи складність точної реалізації і вплив лише на конфіденційність інформації, тому значення *Impact = 50*, (включаючи фінансовий, репутаційний та стратегічний вплив), враховуючи те, що вразливістю будуть намагатися скористатися в основному зовні і зловмисник повинен мати продвинуті технічні навички, то кореляційне значення *Likelihood = 0.*64. Дані параметри характерні як для CVE-2017-5753 так і CVE-2017-5715.

Проте параметри *Controls* в данному випадку треба оцінювати по різному, зокрема враховуючи що для вразливості CVE-2017-5715 випущені патчі які частково вирішують дану проблему лише в деяких випадках, то значення *Controls* можна вважати *Initial/Ad-Hoc=100* забезпечує лише деяку цінність захисту, що стосується CVE-2017-5753, то *Controls* можна вважати ріним 0, так як наразі дана проблема не вирішена.

Звідси для CVE-2017-5715 *iRisk* = (5.6*50*0.64) – 100 = 79.2.

Для CVE-2017-5753 *iRisk* = (5.6*50*0.64) – 0 = 179.2

Висновки

Для дослідження було обрано методологію iRisk, перш за все тому, що дана методика є безкоштовною, достатньо інформативною, включає в собі іншу методику CVSS v3 для оцінки вразливостей, яка активно підтримується Національним інститут стандартів і технологій. Протестовано АС відносно наступних вразливостей: Cisco IOS Arbitrary Command Execution Vulnerability (CVE-2012-0384), Cisco Access Control Bypass Vulnerability (CVE-2012-1342), EternalBlue (CVE-2017-0144), Meltdown (CVE-2017-5754), Spectre (CVE-2017-5753) (CVE-2017-5715), зроблено висновки щодо стійкості побудованої мережі до конкретних загроз методом iRisk, де значення ранжуються від 0 до 1000, а нулю відповідає АС, в якій можна знехтувати даною вразливістю, тоді як при максимально великому значенні, якщо воно перевищує 100 необхідно вирішувати данну вразливість. Чим вище значення iRisk тим критичнішою є вразливість і має більший пріоритет для захисту АС.

1. *B.Y. Korniyenko, L.P. Galata* Design and research of mathematical model for information security system in computer network // Науковий журнал «Наукоємні технології». – 2017, № 2 (34), С. 114 - 118.

2. *L. Galata, B. Korniyenko, A. Yudin*. Research of the simulation polygon for the protection of critical information resources // Информационные технологии и безопасность. Материалы XVII Международной научно-практической конференции ИТБ-2017. – К.: ООО "Инжиниринг", 2017. – С. 35-51. ISBN 978-966-2344-59-2

3. *Корниенко Б.Я.* Информационная безопасность и технологии компьютерных сетей : монография // ISBN 978-3-330-02028-3, LAMBERT Academic Publishing, Saarbrucken, Deutschland. − 2016. – 102 с.

4. *Korniyenko B.* Modeling of security and risk assessment in information and communication system /B. Korniyenko, L. Galata, O. Kozuberda/ Sciences of Europe. –

2016. – V. 2. – No 2 (2). – P. 61 -63.
5. *Chris Clymer, Ken Stasiak, Matt Neely, Stephen Marchewitz.* IRisk Equatuion [Електронний ресурс] – Режим доступу: https://securestate.en/iRisk-Equation-Whitepaper.pdf
6. Common Vulnerability Scoring System v3.0: User Guide [Електронний ресурс] – Режим доступу: https://www.first.org/cvss/user-guide
7. Cisco IOS Software Command Authorization Bypass [Електронний ресурс] – Режим доступу: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328pai
8. Cisco Web Security Appliance Administrative Interfaces Access Control Bypass Vulnerability [Електронний ресурс] – Режим доступу: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170719-wsa5
9. Эксплойт EternalBlue [Електронний ресурс] – Режим доступу: https://habrahabr.ru/company/panda/blog/329044
10. Meltdown [Електронний ресурс] – Режим доступу: https://meltdownattack.com/meltdown.pdf
11. Spectre Attacks: Exploiting Speculative Execution [Електронний ресурс] – Режим доступу: https://spectreattack.com/spectre.pdf

Поступила 19.02.2018р.

УДК 519.711

Д.В. Савельєв, Київ

МОДЕЛЬ ЗАГРОЗ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ У СФЕРІ ЯДЕРНОЇ ЕНЕРГЕТИКИ

Abstract. The article describes the process of constructing a model of cybersecurity threats, contains a list of possible cybersecurity threats of critical information infrastructure objects in the nuclear power industry, describe the possible consequences of implementing each type of threats.

Вступ

Міжнародні організації, такі як Міжнародне агентство з атомної енергії (МАГАТЕ), Міжнародна електротехнічна комісія (МЕК), а також національні органи регулювання ядерної та радіаційної безпеки різних країн працюють над питанням вивчення та регулювання інформаційної безпеки АЕС, що викликано трьома основними факторами – масовою тенденцією переходу від аналогових до цифрових інформаційних та керуючих систем АЕС, вразливістю таких систем до кіберзагроз та підвищенням кількості випадків зловмисних дій щодо інформаційних систем з серйозними наслідками [1].

Забезпечення інформаційної безпеки є важливим завданням, адже

