УДК 004.056.5

к.т.н. Шевченко А.С. (ВІТІ)
к.т.н. Самойлов І.В. (ВІТІ)
Толстих В.А. (ВІТІ)
Артюх С.Г. (ВІТІ)

МЕТОД ОЦІНЮВАННЯ РИЗИКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВНАСЛІДОК ОБМЕЖЕННЯ ПРОПУСКНОЇ СПРОМОЖНОСТІ МІЖМЕРЕЖНИМИ ЕКРАНАМИ НАСТУПНОГО ПОКОЛІННЯ ПРИ ВИКОРИСТАННІ ДОДАТКОВИХ АКТИВНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

У статті розглядається метод оцінювання ризиків який враховує додатковий ризик внаслідок порушення доступності інформації при передачі через обмеження пропускної спроможності міжмережними екранами нового покоління NGFW при застосуванні таких систем захисту інформації, як: системи виявлення та попередження вторгнень IDS/IPS, систем контролю додатків (Application Control), систем попередження втрати даних DLP, систем веб-контролю (Web Control), контролю електронної пошти (Email proxy), віртуальних приватних мереж VPN тощо.

Шевченко А.С., Самойлов. И.В., Толстих В.А., Артюх С.Г. Метод оценивания риска информационной безопасности вследствие ограничения пропускной способности межсетевыми экранами следующего поколения при использовании дополнительных систем защиты информации. *В статье рассматривается метод оценки рисков который учитывает дополнительный риск вследствие нарушения доступности информации при передаче из-за ограничения пропускной способности межсетевыми экранами нового поколения NGFW при применении дополнительных систем защиты информации.*

A. Shevchenko, I. Samojlov, V. Tolstikh, S. Artiukh Method of assessing the risk of information security due to the limitation of the throughput by next-generation firewalls with the use of additional information security systems. *The article presents method of risks estimation including additional risk of violation of information availability during it's transmission because of limited bandwidth allocation of new generation firewall (NGFW) by using additional security systems.*

Ключові слова: *рівень ризику, пропускна спроможність, міжмережні екрани нового покоління, доступність інформації.*

Вступ. З початку військового конфлікту в Україні значно загострився стан інформаційної безпеки. Значні обсяги інформації, що обертаються в кібернетичному просторі, зробили його сучасним полем бою. Противник реалізує концепції інформаційних та кібернетичних операцій, які направленні на особовий склад, системи управління ЗС України та загального користування. Кібернетичний простір ЗС спирається на інформаційно-телекомунікаційні системи (ІТС), які призначені для передачі команд бойового управління та здійснення повсякденної життєдіяльності.

Стрімкі темпи розвитку ІТС ЗС України в ході бойових дій збільшують їх масштаби, обсяги інформаційних ресурсів та інформації, яка обробляється, інтенсивність інформаційної взаємодії та кількість особового складу залученого до цього.

Все це призводить до значного збільшення кількості вразливостей та критичності захисту кіберпростору ЗС України. Для захисту кіберпростору ЗС України заходи захисту інформації реалізовуються на організаційному, технічному та правовому рівнях.

При організації захисту кіберпростору на технічному рівні використовуються такі технічні засоби як: міжмережні екрани (Firewall); системи криптографічного захисту інформації; віртуальні приватні мережі VPN; системи антивірусного захисту елементів ІТС; системи виявлення та запобігання вторгненням (IDS/IPS); системи попередження втрати даних (DLP); системи управління інформаційною безпекою та подіями (SIEM); системи аналізу захищеності (САЗ) та інші.

Усі технічні засоби захисту інформації поділяються на активні та пасивні. Активні здійснюють обробку інформації: фільтрація, обробка, кешування, криптографічні перетворення, інкапсуляція та інші. Пасивні – ґрунтуються, як правило, на прослуховуванні трафіка, аналізу та обробки даних. Використання активних засобів захисту інформації вносить певні обмеження елементів ІТС та ІТС в цілому: погіршення швидкості передачі, продуктивності тощо.

Найбільш поширеними активними технічними засобами захисту інформації є міжмережні екрани нового покоління (NGFW). Виконання функцій захисту NGFW призводить до зниження його пропускної спроможності, в результаті чого знижується швидкість передачі інформації, а відповідно і її доступність. Доступність є одним з сервісів безпеки, погіршення якого враховується при оцінці ризиків інформаційної безпеки.

Аналіз останніх досліджень та публікацій. Згідно міжнародного стандарту ISO/IEC 27005 [1] оцінювання стану інформаційної безпеки здійснюється на основі оцінки ризиків. Огляд останніх публікацій [2 – 4] показав, що на сьогоднішній час оцінювання ризиків існує велика кількість методів, включаючи і найбільш широко розповсюджені: OCTAVE, CRAMM, Risk Watch, COBIT тощо. Вказані методи базуються на стандартизованих етапах оцінювання ризиків, які враховують лише імовірність загрози та рівень збитку від її успішної реалізації. Дані методи не враховують додатковий ризик, який виникає внаслідок впливу СЗІ на зниження пропускної спроможності NGFW.

Мета. У роботі ставиться за мету розробити метод оцінювання ризику інформаційної безпеки внаслідок обмеження пропускної спроможності міжмережними екранами наступного покоління при використанні додаткових активних систем захисту інформації.

Постановка завдання. Для досягнення мети у роботі необхідно розробити метод оцінюванні ризику, який би враховував додатковий ризик, що виникає при обмеженні пропускної спроможності NGFW при застосуванні додаткових СЗІ. В якості базового методу використовувати метод, який викладено в роботі [5].

Обмеження. В роботі обмежуємось розглядом систем захисту інформації міжмережних екранів наступного покоління та їх впливом на процес передачі інформації. Метод враховує вплив на пропускну спроможність одночасно лише однією системою захисту.

В роботі не розглядаються питання визначення важливості параметра (пропускної спроможності) NGFW, розміру та градацій збитку *Z*.

Викладення основного матеріалу дослідження.

У процесі розробки СЗІ і міжмережних екранів вчасності, необхідно враховувати всі можливі ризики, включаючи і ризики внаслідок обмеження пропускної спроможності, які вносять NGFW при застосуванні активних СЗІ.

На сьогоднішній час міжмережні екрани нового покоління NGFW включать наступні системи захисту інформації:

- системи виявлення та попередження вторгнень IDS/IPS;
- систем контролю додатків (Application Control);
- систем попередження втрати даних DLP;
- систем веб-контролю (Web Control);
- контролю електронної пошти (Email proxy);
- віртуальні приватні мережі VPN тощо.

Міжмережний екран вже давно став комплексних засобом захисту інформації для захисту критичного периметра інформаційної інфраструктури.

Усі вказані СЗІ міжмережного екрана вносять обмеження пропускної спроможності, і як правило, зазначаються виробником в технічних характеристиках міжмережного екрана. Але, проектування інформаційно-телекомунікаційної мережі питання досить складне і в ході цього важко визначити, як усі технічні засоби вплинуть на інформаційну безпеку, включаючи і самі СЗІ. Тому, для врахування додаткових ризиків інформаційної безпеки внаслідок обмеження пропускної спроможності міжмережних екранів актуальним є врахування цього в загальній методології ризик-менеджменту.

Суть заходів з управління ризиками полягає в оцінюванні їх величини, виборі ефективних підходів зниження величини ризиків та визначення залишкового ризику [3].

Для розробки методу визначення рівня ризику з урахуванням зниження пропускної спроможності NGFW пропонується пристосувати до предметної області метод, викладений у

статті [5]. Відповідно до цього, виведемо функцію ризику з урахуванням параметра зниження пропускної спроможності.

Базова функція оцінки ризиків, що приведена у роботі [5], на відміну від загальних функцій оцінки ризиків [2, 3, 5], враховує загальний показника зниження параметрів системи L:

$$R = L + \sum_{i=1}^{n} P_{\text{зб } i} \cdot Z_i \,, \tag{1}$$

де R – загальний ризик отримання збитку; $P_{\text{зб } i}$ – імовірність збитку внаслідок успішної реалізації i-ої кібернетичної загрози; Z_i – величина збитку від реалізації i-ої кібернетичної загрози; i – порядковий номер кібернетичної загрози, $i \in [1, n]$; n – загальна кількість кібернетичних загроз; L – загальний показник зниження параметрів системи, $L \in [0,1]$, $L = \sum_{j=1}^{n} l_j$; l_j – показник зниження j-го параметра; j – порядковий номер параметра, $j \in [1, m]$.

Величина збитку Z_i від реалізації кібератак визначається відповідно до відомих методів оцінювання збитків [3]. Загальний показник зниження параметрів L внаслідок застосування СЗІ є відносним значення величини параметра без впровадження засобів захисту та після впровадження, та враховує декілька параметрів систем: час та швидкість передачі, дальність зв'язку та інші. Загальний показник зниження параметрів L розраховується за виразом, що приводиться в статті [6]:

$$L = \sum_{j=1}^{n} l_j = \sum_{j=1}^{n} (1 - \alpha_j) \cdot W_j \,, \tag{2}$$

де l_j – показник зниження j-го параметру, $l_j = (1 - \alpha_j) W_j$, α_j – відносне значення зміни j-го параметру системи, $\alpha_j \in [0, 1)$; W_j – коефіцієнт важливості параметра СЗІ; j – порядковий номер параметра, $j \in [1, m]$; m – загальна кількість параметрів СЗІ.

Відповідно до виду СЗІ загальний показник зниження параметра L може є сумою показників l_j в залежності від типу параметра, які взяті з різними коефіцієнтами важливості параметра W_j, що і враховано в формулі (2).

Відносне значення зміни параметра системи внаслідок впровадження СЗІ розраховується як відношення:

$$\alpha_j = \frac{Q_{\text{фп}}}{Q_0} \,, \tag{3}$$

де $Q_{\text{фп}}$ – значення фактичного параметра, після впровадження СЗІ, Q_0 – величина параметра без використання СЗІ.

Зазвичай, зниження параметра СЗІ проявляється як зниження продуктивності системи в процесі обробки і передачі інформації. З точки зору інформаційної безпеки, зниження параметрів системи еквівалентне порушенню доступності інформації, а показник зниження параметра системи відповідає величині збитку Z_i від реалізації атаки.

Видозмінимо вирази (1) – (3) до часного випадку – врахування лише обмеження пропускної спроможності.

Предметом статті є розгляд зміни пропускної спроможності міжмережних екранів внаслідок застосування додаткових активних СЗІ. Тому, кількість параметрів системи зменшується до одного – пропускної спроможності. Крім того, для спрощення математичного виразу обмежимось реалізацією лише однієї кібернетичної атаки.

Відповідно до виразу (3) показник зниження пропускної спроможності матиме вигляд [5]:

$$\alpha_{\text{пз}} = C_{\text{фп}} / C_0 \,, \tag{4}$$

де C_0 – пропускна спроможність без впливу СЗІ, $C_{фп}$ – пропускна спроможність з врахуванням обмеження СЗІ.

З урахуванням початкових даних, після підстановки формул (2) та (4) у формулу (1) отримаємо кінцеве значення для проведення моделювання:

$$R = P_{зб} \cdot Z + (1 - \frac{C_{фп}}{C_0})W . \quad (5)$$

Множина параметрів пропускної спроможності міжмережних екранів складається з параметрів пропускної спроможності при використанні кожної з СЗІ:

$$C_{фп} = \{C_{АТР}, C_{UTM}, C_{IPS}, C_{VPN}, C_{AV}\},$$

де $C_{АТР}$ – пропускна спроможність при використанні системи захисту від загроз АТР (Advanced Threat Protection); C_{UTM} – пропускна спроможність при використанні систем уніфікованого управління загрозами UTM (Unified Threat Management), C_{IPS} – пропускна спроможність при використанні систем породження вторгнень IPS, C_{VPN} – пропускна спроможність при використанні віртуальних приватних мереж VPN, C_{AV} – пропускна спроможність при використанні антивірусу.

Розглянемо конкретні технічні характеристики сучасних міжмережних екранів наступного покоління ланки середній/малий бізнес передових виробників NGFW за результатами тестування NSS Lab та Gartner (табл. 1) [7, 8].

Таблиця 1

Порівняльна характеристика залежності пропускної спроможності NGFW для малих та середніх організацій в залежності від систем захисту інформації

Пропускна спроможність NGFW, мбіт/с	Позначення параметра	Зразки міжмережних екранів наступного покоління					
		Palo Alto PA-500	Check Point 1120	Fortinet FortiGate FG-30E	WatchGuard Firebox T10	Forcepoint NGFW 100	Cisco ASA 5506-X
Пропускна спроможність NGFW (для TCP)	C_0	250	350	200	400	150	300
Пропускна спроможність при використанні АТР	$C_{АТР}$	100	–	150	–	–	–
Пропускна спроможність при використанні UTM	C_{UTM}	–	–	–	90	–	–
Пропускна спроможність при використанні IPS	C_{IPS}	–	50	150	160	400 (відносно UDP)	125
Пропускна спроможність при використанні VPN (IPSec, AES-128)	C_{VPN}	50	140	75	100	500 (відносно UDP)	100
Пропускна спроможність при використанні антивірусу	C_{AV}	–	50	–	120	–	–

В таблиці 1 представлена порівняльна характеристика зміни пропускної спроможності міжмережного екрана в залежності від функціонування активних СЗІ фаерволу зразків технічних засобів різних виробників [9 – 14].

Побудуємо графік функції для відображення процесу зміни рівня ризику при обмеженні пропускної спроможності внаслідок застосування активних СЗІ на приклади характеристик міжмережного екрана WatchGuard Firebox T10 на основі виразу (5) [12].

Початкові данні. Для побудови графіків функції (5) приймемо наступні початкові значення: нехай рівень збитку буде дорівнювати Z =10 відповідно до градації збитків згідно NIST 800-30 rev.1 [15], $Z \in [1, 10]$, кількість кібернетичних загроз i =1; кількість параметрів NGFW j =1 (розглядаємо лише пропускну спроможність); коефіцієнт важливості параметра W_1 =1 (при $W_j \in [1, 5]$). Значення імовірності збитку $P_{зб}$ представлені в табл. 2, та залежать від інтенсивності кібератаки. Дані результати отримані зі статті [16], де проводилось імітаційне

моделювання для загального випадку реалізації двоетапної атаки, що дозволяє використовувати результати для побудови графіків функції (5).

Таблиця 2

Початкові дані імовірності збитку внаслідок реалізації кібернетичних атак

	Інтенсивність кібернетичної атаки, λ (кількість атак/ λ^{opt} [16])				
Імовірність збитку, $P_{зб}$	0,2	0,4	0,6	0,8	1,0
	0,4105	0,4142	0,4177	0,4203	0,4249

Аналіз графіків функції, для різних значень пропускної спроможності міжмережного екрана WatchGuard Firebox T10 показує характер зміни рівня ризику від зміни його пропускної спроможності (рис. 1).

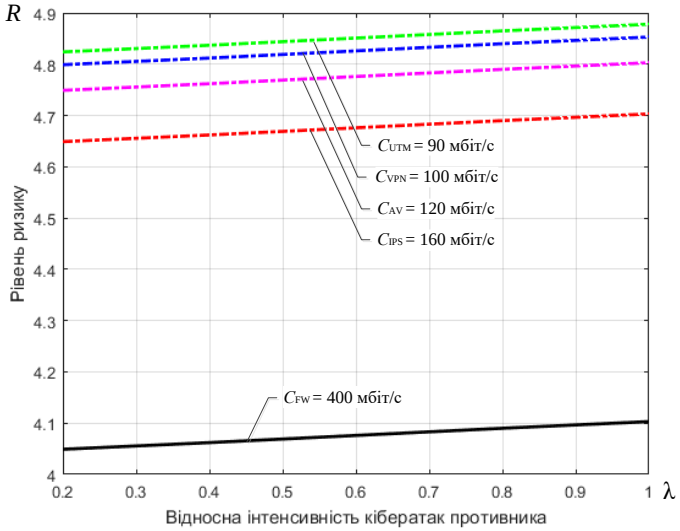

Рис. 1 Графіки залежності рівня ризику від відносної інтенсивності кібератак з урахуванням зміни пропускної спроможності міжмережного екрана WatchGuard Firebox T10

Так, на рис. 1 видно, що зі зменшенням пропускної спроможності збільшується рівень ризику. Даний додатковий ризик викликаний загрозою порушення доступності інформації. Крім того наглядно можна бачити, що врахування показник зниження перепускної здатності $L = (1 – C_{рп}/C_0)W$ в загальній формулі оцінки ризиків дозволяє враховувати додатковий ризик, який для даного міжмережного екрана склав від 0,6 до 0,88 одиниць.

Висновки.

В роботі знайшов подальший розвиток метод оцінювання додаткового ризику інформаційної безпеки внаслідок обмеження пропускної спроможності міжмережними екранами наступного покоління при використанні додаткових активних систем захисту інформації.

Даний метод дозволяє враховувати додатковий ризик внаслідок порушення доступності інформації при внесенні обмеження пропускної здатності міжмережними екранами які впровадженні в ІТС ЗС України. Графіки функції, представлені на рис. 1, наглядно демонструють зміну рівня ризику в залежності від зміни пропускної спроможності – обмеження які вносить NGFW. Ризиком, викликаним обмеженнями параметрів СЗІ, зазвичай нехтують, що не є вирішенням проблеми. Як показали результати розрахунків для реального міжмережного екрана, даний додатковий ризик має достатньо вагомі значення.

Тому, для зниження даних ризиків необхідно враховувати обмежуючі властивості СЗІ на етапі проектування ІТС. Представлений метод, може застосовуватись під час проектування ІТС з впровадження NGFW, та дозволить досягти рівноваги між такими показниками системи, як продуктивність та захищеність.

Напрямками подальшого дослідження є проведення натурних експериментів та оцінювання значень пропускної спроможності при застосування систем захисту інформації міжмережних екранів нового покоління.

ЛІТЕРАТУРА

1. ISO/IEC 27005: 2008 Information technology – Security techniques – Information security risk management.

2. Астахов А. М. Искусство управления информационными рисками. – М.: ДМК Пресс, 2010. – 312 с.

3. Петренко С. А. Анализ рисков в области защиты информации / С. А. Петренко. – СПб.: Афина, 2009. – 153 с.

4. Certified Information Security Manager (CISM) [Електроний ресурс] // офіційний сайт ISACA, Information Systems Audit and Control Association. – Режим доступу: http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Pages/default.aspx.

5. Шевченко А. С. Метод оцінювання ризиків з урахуванням впливу механізмів захисту інформації на параметри безпроводових інформаційно-телекомунікаційних систем під час інформаційних операцій / А. С. Шевченко, О. В. Кокотов // Науково-практичний журнал „Безпека інформації”. – 2014. – № 1. – С. 7 – 11.

6. Скоробагатько Е.А. Методика количественной оценки защищенности телекоммуникационных систем / Е.А. Скоробагатько // Захист інформації. – 2011. – № 3. – С. 9 – 13.

7. Security Value Map. Next Generation Firewall (NGFW) [Електроний ресурс] // офіційний сайт NSS Labs. – Режим доступу: https://research.nsslabs.com/ reports?Cat0=44#cat0=25.

8. Gartner 2017 Magic Quadrant for Enterprise Network Firewalls [Електроний ресурс] // офіційний сайт Forcepoint. – Режим доступу: https://www.forcepoint.com/resources/industry-analyst-reports/gartner-2017-magic-quadrant-enterprise-network-firewalls.

9. Datasheet PA-500 [Електроний ресурс] // офіційний сайт Palo Alto Networks – Режим доступу: https://www.paloaltonetworks.com/products/secure-the-network/next-generation-firewall/ pa-500.

10. Datasheet: Check Point 1100 Appliances [Електроний ресурс] // офіційний сайт – Check Point Software Technologies. – Режим доступу: https://www.checkpoint.com/ru/ downloads/product-related/datasheets/1100-appliance-datasheet.pdf

11. FortiGate/FortiWiFi–30E [Електроний ресурс] // офіційний сайт Fortinet. – Режим доступу: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/ FortiGate_FortiWiFi_ 30E.pdf.

12. WatchGuard Firebox T10/T10-W [Електроний ресурс] // офіційний сайт WatchGuard. – Режим доступу: https://www.watchguard.com/wgrd-products/appliances-compare/216/ 3592/3593.

13. Datasheet: Forcepoint NGFW 100 Series [Електроний ресурс] // офіційний сайт Forcepoint. – Режим доступу: https://www.forcepoint.com/sites/default/files/resources/files/ datasheet_forcepoint_ngfw_100_series_en.pdf.

14. ASA 5506-X with FirePOWER Services [Електроний ресурс] // офіційний сайт Cisco. – Режим доступу: https://apps.cisco.com/ccw/cpc/guest/content/ucsProductDetails/prod_ ASA5506-K9.

15. NIST Special Publication 800-30: Revision 1. – Information security. – 2012. – p. 95.

16. Шевченко А. С. Диференційно-ігрові моделі поведінки безпроводових інформаційно-телекомунікаційних систем при реалізації двоетапних атак під час інформаційного конфлікту / А. С. Шевченко // Збірник наукових праць ВІТІ НТУУ „КПІ”. – 2012. – № 2. – С. 96 – 106.