© Hryshchuk R., Okhrimchuk V. Formulation of the scientific tasks for the potentially dangerous patterns of cyber-attacks development // Ukrainian Scientific Journal of Information Security, 2015, vol. 21, issue 3, p. 276-282.

ПОСТАНОВКА НАУКОВОГО ЗАВДАННЯ З РОЗРОБЛЕННЯ ШАБЛОНІВ ПОТЕНЦІЙНО НЕБЕЗПЕЧНИХ КІБЕРАТАК

Руслан Грищук, Володимир Охрімчук

Житомирський військовий інститут імені С.П. Корольова, Україна

ГРИЩУК Руслан Валентинович, д.т.н.

Рік та місце народження: 1981 рік, с. Піщаниця, Овруцький р-н, Житомирська обл., Україна.
Освіта: Житомирський військовий інститут радіоелектроніки імені С. П. Корольова, 2003 рік.
Посада: начальник відділу інформаційної та кібернетичної безпеки наукового центру Житомирського військового інституту імені С. П. Корольова з 2015 року.
Наукові інтереси: інформаційна та кібернетична безпека держави.
Публікації: більше 165 наукових публікацій, серед яких монографія, підручники, навчальні посібники, наукові статті та патент на винахід.
E-mail: Dr.Hry@i.ua

ОХРІМЧУК Володимир Васильович

Рік та місце народження: 1984 рік, м. Житомир, Україна.
Освіта: Житомирський військовий інститут радіоелектроніки імені С. П. Корольова, 2006 рік.
Посада: науковий співробітник науково-дослідної лабораторії проблем забезпечення кібернетичної безпеки наукового центру Житомирського військового інституту імені С. П. Корольова з 2015 року.
Наукові інтереси: інформаційна та кібернетична безпека держави.
Публікації: більше 15 наукових публікацій, серед яких наукові статті матеріали та тези доповідей на конференціях.
E-mail: okhrimchuk84@ukr.net

Анотація. *Кібернетична безпека сьогодні є наріжним каменем безпеки комп'ютерних систем та мереж. Разом з питаннями забезпечення технічного захисту інформації на об'єктах інформаційної діяльності, безпеки інформаційних і комунікаційних систем, інформаційної безпеки держави – кібернетична безпека потребує постійного удосконалення механізмів її забезпечення. Удосконалення потребує також її методичне та практичне підґрунтя. З цією метою у статті розкрито базові технології побудови сучасних систем захисту інформації від кібератак та визначено перспективні напрямки підвищення ефективності функціонування перспективних систем захисту. Запропоновано новий підхід до розроблення шаблонів потенційно небезпечних кібератак, впровадження якого забезпечує усунення базового недоліку створення сигнатур шаблонів атак, а саме «ефекту запізнення» з вироблення потрібної сигнатури. Даний підхід дозволяє вендорам антивірусного програмного забезпечення оперативно розробляти шаблони потенційно небезпечних кібератак й ефективно виявляти нові кібератаки в комп'ютерних системах та мережах. Як результат відкрито новий дієвий механізм підвищення захищеності комп'ютерних систем та мереж різного цільового призначення від шкідливого програмного забезпечення.*

Ключові слова: *антивірусна система захисту інформації, кібератака, шаблон потенційно небезпечної кібератаки, комп'ютерна система та мережа, сигнатура, стандартний функціональний профіль захищеності.*

Постановка проблеми в загальному вигляді та її зв'язок із важливими практичними завданнями

Широке застосування комп'ютерних систем та мереж (КСМ) у різних сферах, наприклад, економічній, військовій, енергетичній, транспортній тощо, суттєво впливає на ефективність діяльності не тільки окремо взятої людини, але й суспільства та держави в цілому. Проте окрім усіх позитивних ефектів від впровадження КСМ у діяльність сучасного суспільства суттєво й не в кращий бік змінюється ситуація з їх безпекою [1, 2].

Особливо гостро сьогодні постають питання забезпечення технічного захисту інформації на об'єктах інформаційної діяльності, безпеки інформаційних і комунікаційних систем, інформаційної безпеки [3]. Кібернетична безпека взагалі знаходиться на піку напруженості ситуації. Так, за останні п'ять років суттєво збільшилась не тільки кількість, а й технологічна складність кібератак (КбА) на КСМ [4–6]. При цьому

актуалізується питання забезпечення кібернетичної безпеки для об'єктів з критичною кібернетичною інфраструктурою [7, 8]. Не в останню чергу це пов'язано з тим, що відомі на даний час технології, покладені в основу функціонування антивірусних систем захисту інформації (СЗІ), ґрунтуються на таких підходах до створення сигнатур шаблонів атак, які створюють передумови для виникнення «ефекту запізнення» з вироблення потрібної сигнатури. Для усунення даного недоліку на сьогодні можна виділити кілька перспективних напрямків підвищення ефективності функціонування СЗІ. Одним з них є підхід, що ґрунтується на урівноваженні можливостей вендорів антивірусного програмного забезпечення (АПЗ) й розробників шкідливого програмного забезпечення (ШПЗ), що досягається за рахунок створення шаблонів потенційно небезпечних КбА для визначених КСМ.

Таким чином, як показано вище, проблема забезпечення безпеки КСМ і надалі залишається актуальною. Її розв'язання потребує вирішення ряду частинних наукових завдань, одним з яких є розроблення нових та модифікація відомих методів побудови шаблонів КбА.

Аналіз останніх досліджень і публікацій [1–8] показав, що, незважаючи на значну кількість КСМ, проблема їх безпеки й надалі залишається актуальною, з нею також пов'язані питання технологічного [9], організаційного [10], дефініційного [11] характеру тощо.

У технологічному плані сьогодні відбувається комплексування відомих підходів до побудови сигнатур шаблонів атак. Кожен з провідних вендорів АПЗ, зокрема, Kaspersky Lab, Panda Security, Intel Security-McAfee, ESET, Dr.Web Dr.Web тощо, тримає в комерційній таємниці підходи до побудови шаблонів атак. Відомі доступні наукові публікації [12], які в кожному окремому випадку потребують адаптації.

Організаційна складова проблеми безпеки КСМ обумовлена протиріччями між усталеними в світовій практиці підходами до організації процесу забезпечення захищеності та їх повільною ратифікацією в національному масштабі не тільки в межах України, а й усіх країн пострадянського простору.

Дефініційна проблема безпеки є відлунням організаційної. Навіть провідні вчені в галузі безпеки КСМ на сьогодні не мають єдиного бачення на вирішення питання забезпечення технічного захисту інформації на об'єктах інформаційної діяльності, безпеки інформаційних і комунікаційних систем, інформаційної та кібернетичної безпеки як окремої складової безпеки КСМ, так і безпеки системи в цілому.

Як показав критичний аналіз відомих публікацій за темою дослідження означена вище проблема, незважаючи на її багатогранність, і досі залишається актуальною та потребує свого розв'язання.

Метою статті є встановлення сутності та змісту завдання з розроблення шаблонів потенційно небезпечних КбА, його формалізоване подання, що забезпечить відкриття нового дієвого механізму підвищення захищеності КСМ різного цільового призначення від ШПЗ.

Викладення основного матеріалу дослідження

Оцінимо ситуацію з питань забезпечення кібербезпеки КСМ, обравши за вихідні дані звітні матеріали провідних вендорів АПЗ [5, 13–15]. Так, наприклад, за даними Panda Security об'єми створення та розповсюдження нових зразків ШПЗ в 2015 році зростали за геометричною прогресією та щоденно становили в середньому до нових зразків [16]. Дані від глобальної мережі сенсорів безпеки Check Point показують, що близько третини державних установ і приватних компаній, які вони обслуговують, вже, починаючи з 2013 року, завантажували хоча б один файл, заражений невідомим зразком ШПЗ [17]. Також особливо актуальним залишається питання забезпечення кібербезпеки об'єктів з критичною кібернетичною інфраструктурою, на які покладаються функції із забезпечення національної безпеки й оборони будь-якої розвиненої держави світу.

В Україні згідно з [5] за 11 місяців 2015 року зафіксовано 194 випадки КбА на державні та комерційні інформаційні ресурси. Крім того, спеціалістами компанії ESET у березні 2015 року в національному сегменті кіберпростору виявлено модифіковані зразки ШПЗ BlackEnergy (кіберзагроза Win32/Rootkit.BlackEnergy, Backdoor.Win64.Blakken) на деяких стратегічних об'єктах державного управління, зокрема в Уряді, військовому відомстві, інформаційному агентстві тощо [18].

Спираючись на результати власних досліджень, наприклад [19], та оприлюднених в інших джерелах [20], розкриємо статистику реалізації КбА на державні інформаційні ресурси об'єктів з критичною кібернетичною інфраструктурою (рис. 1)

Аналіз рис. 1 показує, що, незважаючи на незначне зменшення кількості КбА на державні інформаційні ресурси в 2015 році порівняно з попередніми трьома роками, їх кількість залишається достатньо великою, а, враховуючи технологічну складність, наслідки при порушенні безпеки КСМ у перспективі можуть мати катастрофічний характер для національної безпеки й оборони. Отже, організація протидії новим КбА, особливо тим з них, які мають високу технологічну складність, обумовлює нарощення можливостей вендорів АПЗ шляхом удосконалення діючих технологій розроблення сигнатур шаблонів атак, динамічного переходу на хмарні обчислення з використанням можливостей інтелектуального аналізу даних.

На ринку інформаційних технологій СЗІ від КБА представлені досить широким спектром програмних та програмно-апаратних засобів, зведені дані щодо яких подано в табл 1

Спираючись на принципи роботи найрозповсюдженіших зразків СЗІ від КбА, таких як АПЗ [21],

міжмережні екрани [22] та засоби аналізу захищеності [23], у тому числі й найсучасніших з них[24], розкриємо сутність базових технологій, покладених в основу розроблення шаблонів КбА (рис. 2).

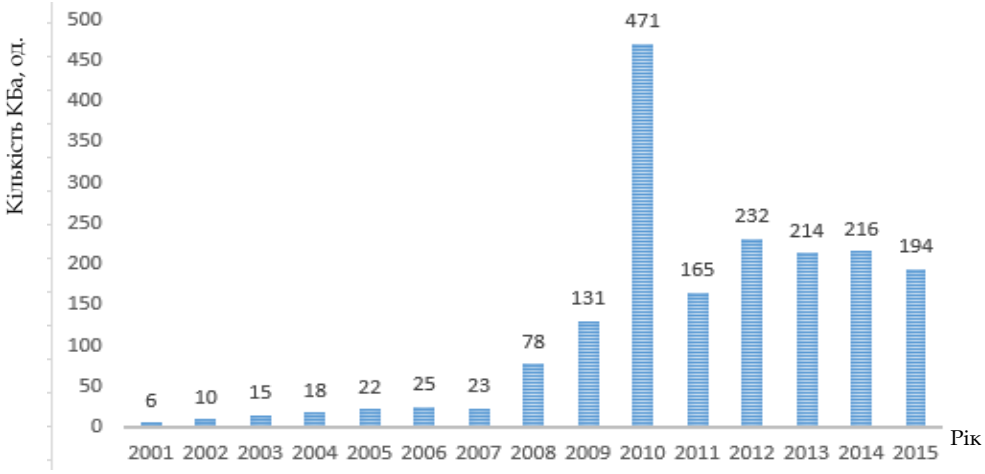

Рис. 1. Статистика КбА на державні інформаційні ресурси в Україні (період спостереження – 2001–2015 роки)

Таблиця 1

Найрозповсюдженіші зразки систем захисту інформації від КбА

Система захисту інформації від кібератак		
Антивірус	Міжмережний екран	Засіб аналізу захищеності
Avira Antivirus Pro	NetDefend UTM	NMap
BitDefender Internet Security	ZoneAlarm Free Firewall	CIS Windows 2000 Level 1 Scoring Tool
Kaspersky Internet Security	Windows 10 Firewall Control	
Norton Security	AVS Firewall	«Ревизор сети»
F-Secure Internet Security	Outpost Firewall Free	ASET для ОС Solaris або MBSA (Microsoft Security Baseline Analyzer
Trend Micro Internet Security	Private Firewall	
McAfee Internet Security	TinyWall	
AhnLab V3 Internet Security	Comodo Firewall	Nessus
AVG Internet Security	Fortinet Fortigate	Acunetix Web Vulnerability Scanner
Avast Free Antivirus	Cisco ASA Firewall	
BullGuard Internet Security	pfSense Firewall	Symantec NetRecon
eScan Internet Security Suite	Cyberoam: UTM Firewall	XSpider
Panda Free Antivirus	FireEye Firewall	«Сканер-ВС»
ESET NOD32 Smart Security	WatchGuard XTM Firewall	Qualys Web Application Scanning
Comodo Internet Security	Sophos XG Firewall	Secure Web Application Tactics
G Data InternetSecurity	Checkpoint Firewall	Rapid7 AppSpider
K7 TotalSecurity	vSRX Integrated Virtual Firewall	PT Application Inspector
Symantec (Norton Security)	Cisco SourceFire Firewall	N-Stalker Web Application Security Scanner
360 Total Security	та ін.	Kali Linux 2.0
Dr.Web Cureit		та ін.
Microsoft Security Essentials		
COMODO Internet Security 2015		
NANO Антивірус		
Zillya		

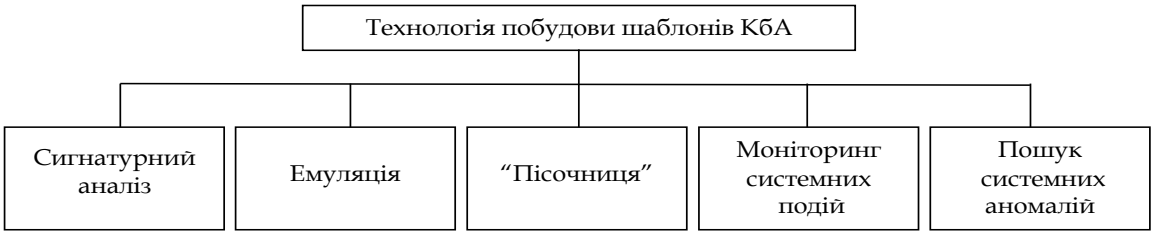

Рис. 2. Базові технології побудови шаблонів КбА в сучасних системах захисту інформації

З метою визначення переваг і недоліків базових технологій (див. рис. 2) проаналізуємо принципи побудови шаблонів КбА на їх основі. З [25] відомо, що основним принципом виявлення

ШПЗ СЗІ є порівняння за визначеним правилом мережевого трафіка в комп'ютерній мережі або файлового коду в комп'ютерній системі із сигнатурою шаблону атаки, який зберігається в базі даних. При цьому якість захисту суттєво залежить від наявності відповідної сигнатури, а в разі її відсутності – від оперативності її розроблення, тестування та запису до бази даних і подальшого використання за призначенням.

У другому випадку за технологією емуляції системою захисту здійснюється побайтове порівняння трафіка (файлу) з відомою сигнатурою та часткове його виконання як програми дій. Наступна з відомих технологій – це «пісочниця» (див. рис. 2) сутність якої полягає в запуску програми дій у ядрі операційної системи за певними, заздалегідь визначеними правилами. Технології моніторингу системних подій та пошуку системних аномалій зводяться до одночасного моніторингу усіх подій, що відбуваються в системі, та порівнянні поведінки «неінфікованої» та «інфікованої» КСМ відповідно. Базовим недоліком даних технологій є потреба залучення потужних обчислювальних ресурсів, що не завжди раціонально в державних установах та організаціях.

Незважаючи на велике різноманіття СЗІ від КбА (див. табл. 1), більшість з них і надалі ґрунтуються на сигнатурних принципах побудови та виявлення КбА. Як наслідок, наявність «ефекту запізнення», що виникає через часові затримки, зумовлені потребами пошуку та вироблення потрібної сигнатури, суттєво знижує захищеність КСМ від нових КбА, особливо тих з них, які мають високу технологічну складність. Таким чином, на сьогодні склалася парадоксальна ситуація: засоби захисту на крок відстають від засобів нападу.

Причинами даної ситуації є перш за все те, що розроблення шаблонів КбА у вигляді складних сигнатур є переважно рутинною процедурою, визначну роль у реалізації якої відіграє антивірусний аналітик або «дятел» за термінологією Kaspersky Lab [26]. Інший підхід з розроблення шалонів КбА – це їх автоматична генерація роботами [27, 28]. Але зростаючий поліморфізм та метаморфізм ШПЗ нівелюють ефективність автоматично згенерованих шаблонів.

Таким чином, у результаті проведеного дослідження встановлено, що на сьогодні існує об'єктивне протиріччя між постійним збільшенням кількості й одночасним зростанням технологічної складності КбА на КСМ, з одного боку, та відставанням темпів створення шаблонів потенційно небезпечних КбА, що обумовлено інертністю застосовуваних для їх створення технологій, з іншого (рис. 3).

Рис. 3. Сутність наукового завдання з розроблення шаблону потенційно небезпечних КбА

Наявність протиріччя (див. рис. 3) зумовлює виникнення актуальної наукової проблеми, яка полягає в підвищенні захищеності КСМ від ШПЗ, у рамках якої конкретне наукове завдання з розроблення методу побудови шаблонів потенційно небезпечних КбА потребує нового розв'язання.

Першим кроком на шляху вирішення поставленого наукового завдання є реалізація процедури визначення множини найбільш актуальних загроз кібербезпеці об'єкта з критичною кібернетичною інфраструктурою. На сьогодні для повного визначення множини найбільш актуальних загроз слід враховувати достатньо велику кількість різноманітних параметрів [29]. З цією метою розширенню підлягає множина ознакового простору опису КбА не тільки на відомі їх класи, а й розширення її для опису нових невідомих класів. Дане завдання може бути вирішене шляхом комплексування можливостей ознакової класифікації КбА [25] та стандартних функціональних профілів захищеності комп'ютерних систем згідно з нормативним документом системи технічного захисту інформації НД ТЗІ 2.5 - 005 - 99. Так, нехай у формалізованому вигляді для деякої множини відомих класів КбА Y у КМС розроблено стандартний функціональний профіль захищеності (СФПЗ) A, який призначений для їх перекриття. Тобто

$$A = \{a_i\}, \quad (1)$$

де a_i – i-а мінімально необхідна послуга безпеки, $i = \overline{1,n}$.

Стандартний функціональний профіль захищеності (1) у загальному вигляді є множиною мінімально необхідних рівнів послуг a_i, які повинні бути реалізовані СЗІ від КбА КСМ для гарантованого виконання висунутих вимог до забезпечення захищеності інформації. Нехай правило формування СФПЗ (1) матиме такий вигляд:

$$\begin{cases} \{A', F\} \to a^*; \\ F \to \max E, \end{cases} \quad (2)$$

де A' – СФПЗ для досліджуваної КСМ, визначений згідно з [30]; F – правило вибору визначених послуг безпеки для досліджуваної КСМ; a^* – визначений згідно з правилами вибору F набір мінімально необхідних a_i послуг безпеки; E – рівень захищеності КСМ від КбА.

Другим кроком на шляху розв'язання поставленого наукового завдання (див. рис. 3) є опис відомих на сьогодні класів КбА у вигляді деякої множини Y, тобто

$$Y = \{y_l^m\}, \quad (3)$$

де y_l^m – шаблон, що описує відомий клас КбА (l – тип відомої КбА, $l = \{DoS, U2R, R2L, Proba\}$ [30], m – спосіб реалізації відомої КбА l – типу).

Наприклад, клас КбА типу *DoS* згідно з [31] та (3) може бути описаний як $y_{DoS}^{htpflood}$, де значення індексу l показує, що дана атака спрямована на відмову в обслуговуванні системи, яку атакують, на основі способу m у вигляді *httpflood*.

Кожний шаблон y_l^m є набором з s вхідних інформативних параметрів мережного з'єднання, які підлягають контролю, $s = \overline{1,41}$ [31]. В умовах обмеженого часу на розроблення шаблону потенційно небезпечної КбА $y_l^{m\prime} \notin Y$ використання визначеної кількості з s параметрів не є раціональним підходом. Вважається за доцільне в такому разі оптимізувати кількість параметрів з s до s', де $s' \le s$. Дане припущення є справедливим, оскільки у [32] доведено, що кожен з відомих, а відповідно, і невідомих класів КбА може бути описаний своєю множиною з s' параметрів, які його однозначно визначають.

Таким чином, наукове завдання з розроблення шаблонів потенційно небезпечних КбА Y' з урахуванням (1)–(3) у формалізованому вигляді визначається як:

розробленню підлягають шаблони потенційно небезпечних КбА

$$Y' \notin Y,$$

для яких виконуються умови :

$$y_l^{m\prime} \notin y_l^m \text{ при } s' \le s,$$

та

$$E^{opt} = \min_{A' \in A} \max_{Y' \notin Y} E,$$

при обмеженні $t_{Y'} \le t_Y$, де Y' – шаблони потенційно небезпечних КбА; E^{opt} – оптимальне значення рівня захищеності E, величини якої намагається досягнути розробник ШПЗ унаслідок реалізації КбА; $t_{Y'}$ – час, що витрачається на розроблення потенційно небезпечних шаблонів КбА; t_Y – усереднене значення часу, затраченого на розроблення сигнатури для конкретного шаблону y_l^m.

Необхідними та достатніми умовами, що забезпечують розроблення ефективних шаблонів потенційно небезпечних КбА, які у подальшому підлягають збереженню у базах даних систем захисту інформації для виявлення КбА є умови вигляду

$$\begin{cases} P_{Y'}^{пропн} \to \min; \\ P_{Y'}^{хибн} \le P_Y^{хибн}, \end{cases} \quad (4)$$

де $P_{Y'}^{пропн}$ – ймовірність пропуску системою захисту КбА за розробленим потенційно небезпечним шаблоном Y';

$P_{Y'}^{хибн}$ – ймовірність хибних спрацювань системи захисту при заданій деякій їх кількісній величині не гірше $P_Y^{хибн}$ для множини відомих класів КбА Y.

Висновки та перспективи подальших досліджень

Уперше запропоновано новий підхід до розроблення шаблонів потенційно небезпечних КбА, який на відміну від відомих усуває базовий недолік відомих підходів – «ефект запізнення» при створенні сигнатури. Перспективним напрямом подальших досліджень є теоретичне обгрунтування та практична апробація визначених у статті кроків, що забезпечують вирішення поставленого наукового завдання.

Література

[1] Geers K. Cyber War in Perspective : Russian Aggression against Ukraine / K. Geers. — Tallinn : CCDCOE, 2015. — 176 с.

[2] Грищук Р.В. Атаки на інформацію в інформаційно-комунікаційних системах / Р.В. Грищук // Сучасна спеціальна техніка — 2011. — №1 (24). — С.61-66.

[3] Олифер В.Г. Безопасность компьютерных сетей / В.Г. Олифер, Н.А. Олифер. — М. : Горячая линия — Телеком, 2015. — 644 с.

[4] Звіт CERT-UA за 2010-2013 роки [Електронний ресурс]. — 2014. — Режим доступу до ресурсу : http://cert.gov.ua/?p=316

[5] Киберщит Украины: кто стоит на страже кибергранниц страны [Електронний ресурс]. — 2015.

— Режим доступу до ресурсу: http://zillya.ua/ru/kibershchit-ukrainy-kto-stoit-na-strazhe-kibergranits-strany.

[6] Ларина Л. Кибервойны XXI века. О чем умолчал Эдвард Сноуден / Л. Ларина, В. Овчинский. — М. : Книжный мир, 2014. – 352 с.

[7] Lewis T. Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation / Ted G. Lewis., 2014. – 400 с. – (Wiley).

[8] Ten C.-W. Cybersecurity for critical-infrastructures : Attack and defense modeling / C.-W. Ten, G. Manimaran, C.-C. Liu // IEEETrans. Syst., Man Cybern. A , 2010. — vol. 40. —№. 4. — pp. 853 -865.

[9] Ленков С.В. Методы и средства защиты информации: монография [в 2-х т.] Т. 2. Информационная безопасность / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко. — К. : Арий, 2008. — 344 с.

[10] Юдін О.К. Інформаційна безпека. Нормативно-правове забезпечення / О. К. Юдін. — К. : НАУ, 2011. — 640 с.

[11] Безкоровайный М.М. Кибербезопасность – подходы к определению понятия / М.М. Безкоровайный, А.Л. Татузов // Вопросы кибербезопасности. — 2014. — №1 (2). — С. 22–27.

[12] Грищук Р.В. Диференціально-ігрова модель шаблону атаки на Web-сервер / Р.В. Грищук // Збірник наукових праць ВІКНУ ім. Т. Шевченка. — 2010. — №21. — С. 104–112.

[13] Касперський Є. Про Kaspersky Lab [Електронний ресурс] / Є. Касперський // http://www.kaspersky.ua/about#. – 2015

[14] Our Top Products [Електронний ресурс] // McAfee Internet Security. —2015. — Режим доступу до ресурсу: https://www.mcafee.com/consumer/en-us/store/m0/catalog.html?PIFld=-1&rfhs=1&culture=EN-US.

[15] Обеспечение безопасности во всем мире — наша постоянная миссия [Електронний ресурс] // Symantec (Norton Security). — 2015. — Режим доступу до ресурсу : http://www.symantec.com/ru/ru/

[16] Прогноз 2016: атаки на Android и масштабные инфекции — одни из основных угроз безопасности [Електронний ресурс] // Хабрахабр. – 2015. — Режим доступу до ресурсу: http://habrahabr.ru/company/panda/blog/273689/

[17] Check Point: 84% компаний загружают вредоносное ПО каждые 10 минут [Електронний ресурс] // Check Point Software Technologies. — 2015. — Режим доступу до ресурсу : http://servernews.ru/ 820500.

[18] Кибершпион атакует спецслужбы Украины [Електронний ресурс] // ESET. — 2015. — Режим доступу до ресурсу: http://eset.ua/ru/news/view/390/operation-potao.

[19] Бурячок В.Л. Політика інформаційної безпеки / В.Л. Бурячок, Р.В. Грищук, В.О. Хорошко ; під заг. ред. проф. В.О. Хорошка. — К. : ПВП «Задруга», 2014. — 222 с.

[20] Метод побудови класифікатора кібератак на державні інформаційні ресурси : автореф. дис. на здобуття наук. ступеня канд. техн. наук : спец. 21.05.01 «інформаційна безпека держави». —К., 2015. — 160 с.

[21] Лучшие антивирусы для Windows 10. Тестирование от AV-Test [Електронний ресурс] // SoftPortal.com. — 2015. — Режим доступу до ресурсу: http://www.softportal.com/article-536.html

[22] Лучшие бесплатные файрволы, брандмауэры и межсетевые экраны для Windows [Електронний ресурс] // Ida-Freewares.ru. — 2015. — Режим доступу до ресурсу: http://ida-freewares.ru/ best-free-firewall-protection.html.

[23] Хонин А. Сканеры защищенности веб-приложений (WASS) - обзор рынка в России и в мире [Електронний ресурс] / А. Хонин // Аналитический центр Anti-Malware.ru. — 2015. — Режим доступу до ресурсу: https://www.anti-malware.ru/reviews/web_application_security_scanners_market_russia_worldwide.

[24] Kali Linux 2.0 Released [Електронний ресурс] // Kali Linux. — 2015. — Режим доступу до ресурсу: https://www.kali.org/news/kali-linux-20-released/.

[25] Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения : монография /Корченко А. Г. — К. : «МК-Пресс», 2006. — 320 с.

[26] Савина А. Офисный словарь: «Лаборатория Касперского» [Електронний ресурс] / А. Савина // Kaspersky Lab. — 2014. — Режим доступу до ресурсу: http://www.lookatme.ru/mag/live/dictionary/201385-kaspersky.

[27] Лаборатория Касперского: экскурсия и взгляд изнутри [Електронний ресурс] // Редакция THG. — 2009. — Режим доступу до ресурсу : http://www.thg.ru/business/kaspersky_tour/onepage.html

[28] 8000000-й вирус добавлен в вирусные базы Zillya! [Електронний ресурс] // Zillya!. — 2013. — Режим доступу до ресурсу : http://zillya.ua/ru/8000000-i-virus-dobavlen-v-virusnye-bazy-zillya

[29] Грищук Р.В. Науково-технічне обґрунтування вибору підходу до формування множини інформативних параметрів для систем захисту інформації / Р.В. Грищук, В.Л. Бурячок, В.М. Мамарєв // Специальные телекоммуникационные системы и защита информации. — 2014. — № 2 (26). — С. 82-86.

[30] НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу».

[31] UCI Knowledge Discovery in Databases Archive : [Електронний ресурс]. — Режим доступу до ресурсу : http://kdd.ics.uci.edu

[32] Грищук Р.В. Метод скорочення розмірності потоку вхідних даних для мережних систем виявлення атак / Р.В. Грищук, В.М. Мамарєв // Сучасний захист інформації. — 2012. — Спецвипуск. — С. 16–19.

УДК 004.056.53 (045)

Грищук Р.В., Охримчук В.В. Постановка научной задачи по разработке шаблонов потенциально опасных кибератак

Аннотация. *Кибернетическая безопасность сегодня является краеугольным камнем безопасности компьютерных систем и сетей. Вместе с вопросами обеспечения технической защиты информации на объектах информационной деятельности, безопасности информационных и коммуникационных систем, информационной безопасности государства – кибернетическая безопасность требует постоянного совершенствования механизмов ее обеспечения. В модернизации и улучшении также нуждаются ее методические и практические основы. С этой целью в статье раскрыто базовые технологии построения современных систем защиты информации от кибератак и определены перспективные направления повышения эффективности функционирования перспективных систем защиты. Предложен новый подход к разработке шаблонов потенциально опасных кибератак. Внедрение разработанного подхода обеспечивает устранение базового недостатка, характерного классическому подходу к созданию сигнатур шаблонов атак, а именно «эффекта задержки» по выработке нужной сигнатуры. Новый подход позволяет вендорам антивирусного программного обеспечения оперативно разрабатывать шаблоны потенциально опасных кибератак и эффективно выявлять новые кибератаки в компьютерных системах и сетях. В результате проведенного исследования открыт новый механизм повышения защищенности компьютерных систем и сетей различного целевого назначения от вредоносного программного обеспечения.*

Ключевые слова: *антивирусная система защиты информации, кибератака, шаблон потенциально опасной кибератаки, компьютерная система и сеть, сигнатура, стандартный функциональный профиль защищенности.*

Hryshchuk R., Okhrimchuk V. Formulation of the scientific tasks for the potentially dangerous patterns of cyber-attacks development

Abstract*. The basic technology for building modern information security systems from cyber-attacks is exposed and perspective directions of advanced protection systems efficiency increase are defined. A new approach for the development of potentially dangerous patterns of cyber-attacks is proposed. Its implementation ensures elimination of basic deficiency in well-known approaches in creation a pattern signature of attacks, such as «lag effect» in developing of the necessary signatures. Implementation of the developed approach also allows vendors of antivirus software to design effectively templates of potentially dangerous cyber-attacks and effectively detect new cyber-attacks in computer systems and networks. Thus, at present based on the task essence and content setting on patterns development of potentially dangerous cyber-attacks, which formalized presentation is disclosed in the article, a new effective mechanism for improving the security of computer systems and networks of different special destination against deleterious software is disclosed.*

Key words*: antivirus information security system, cyber-attacks, potentially dangerous patterns of cyber-attacks, computer system and network, signature, functional security profile.*

Отримано *1 жовтня 2015 року*, затверджено редколегією *5 листопада 2015 року*