об'єктів за рахунок прозорих середовищ. Існує декілька технологій рендерингу, часто поєднуваних разом [1].Для реалізації даного додатку було використано технологію Microsoft WPF (Windows

Presentation Fundation), так як вона орієнтована на створення додатків для Windows з нестандартним користувацьким інтерфейсом, при збереженні функціональності звичайних додатків Windows Forms. Дана технологія використовує принцип розмітки для створення інтерфейсу, що робить процес розробки набагато гнучкішим [2].В результаті було отримано продукт, в якому можна створити одну 3D – фігуру з певного списку. Даний проект в подальшому можна буде вдосконалити шляхом використання інших алгоритмів моделювання. Можна зробити висновок, що головною перевагою просторового моделювання є візуалізація, яка дозволяє виявити та усунути помилки і недоліки ще до завершення виконання графічної роботи чи проектування деталі [3].

Список використаних джерел

1. Сиденко Л. Компьютерная графика и геометрическое моделирование/ Л. Сиденко. – Санкт-Петербург: Питер, 2009. – 224 с.
2. Шилдт Г. Полное руководство C# 4.0 / Г. Шилдт. – М.: Айрис-пресс, 2011. – 1056 с.
3. Землянов Г.С. 3D-моделирование / Г.С. Землянов, В.В. Ермолаева // Молодой ученый. – 2015. – № 11.– С. 186-189.
Посилання
https://koloro.ua/ua/3d-modelirovanie-i-vizualizaciya.html

УДК 004.056:004.415.538

Михайловський С.М., здобувач 3 курсу спеціальність 125 «Кібербезпека»
Наукові керівники:
Загоруйко Л.В., к.т.н., доцент, доцент кафедри інформаційних технологій
Мартьянова Т.А. к.т.н., ст. викладач кафедри інформаційних технологій

ТЕСТУВАННЯ НА ПРОНИКНЕННЯ НА БАЗІ СТАНДАРТУ NIST SP 800-11

Донецький національний університет ім. Василя Стуса, м. Вінниця

Актуальність. Нині питання безпеки інформаційних систем об'єктів критичної інфраструктури набувають важливого значення. Водночас поточні завдання аудиту інформаційної безпеки (ІБ) об'єктів критичної інфраструктури,

як правило, обмежуються перевіркою їх на відповідність вимогам з ІБ з боку керівних документів. Однак за такого підходу до аудиту часто залишається незрозумілою захищеність цих об'єктів від реальних атак зловмисників. Для об'єктивної перевірки такої захищеності об'єкти піддають процедурі тестування, а саме - тестуванню на проникнення. Однак, стримуючим фактором у проведенні тестування на проникнення вітчизняних об'єктів критичної інфраструктури є відсутність єдиного вітчизняного стандарту проведення такого тестування.

У роботі проведено аналіз стандарту *NIST SP* 800-115, зокрема розглянуто: типи заходів оцінювання ІБ; етапи оцінювання ІБ; способи аналізу та тестування, які використовуються під час оцінювання ІБ; типи й послідовність проведення тестування на проникнення; вразливості, що перевіряються; рекомендований інструментарій проведення аналізу та тестування, що представлено в *NIST SP* 800-11. Зроблено висновки про сильні та слабкі сторони стандарту *NIST SP* 800-115..

Ключові слова: тестування на проникнення, комп'ютерна атака, NIST SP 800-115, тестування, тестування безпеки, соціальна інженерія, тестування програм, уразливість, сканування мережі.

Вступ

У переважній кількості випадків аудит ІБ ІС проводитися на основі порівняльного аналізу з нормативно-правовою документацією, що регламентує забезпечення ІБ, або на основі аналізу ризиків. Разом з тим, є необхідність формування ще одного типу практичного підходу до аудиту, а саме - аудиту на основі експериментальних досліджень системи або її прототипу. Даний тип аудиту, проводиться із застосуванням проти системи засобів або способів інформаційних впливів з метою практичної перевірки ефективності технічних або організаційних заходів захисту, а також виявлення нових вразливостей системи. У деяких роботах для такого підходу використовується термін "тестування на проникнення" (в англомовній літературі - "*penetration testing*"), а також інші терміни "активний аудит", "інструментальний аудит", "тестові інформаційно-технічні впливи", "тестові кібератаки" тощо, але при цьому суть подібного практичного підходу до аудиту не змінюється.

Водночас, у провідних зарубіжних країнах розроблено та введено в дію численні стандарти та методики тестування на проникнення, зокрема, такі як *OSSTMM, ISSAF, OWASP, PTES, NIST SP* 800-115, *BSI, PETA, PTF* . Доцільно взявши за основу ці зарубіжні стандарти і методики, провести їх аналіз, і на його основі сформувати науково-обґрунтований вітчизняний проект стандарту на проникнення, який би вбирав у себе найкращі зарубіжні практики в галузі тестування.

Для формування конкретних, більш повних, переліків вразливостей, що перевіряються в процесі тестування, у стандарті *NIST SP* 800-115 рекомендується використовувати такі *web*-ресурси:

1) Common Configuration Enumeration (CCE): https://nvd.nist.gov/config/cce/index; 2) Common Vulnerabilities and Exposures (CVE): http://cve.mitre.org;

3) Common Weakness Enumeration (CWE): http:// cwe.mitre.org;

4) Список паролів за замовчуванням: http://www.phenoelit-us. org/dpl/dpl.html;

5) National Vulnerability Database (NVD): http://nvd. nist.gov;

6) Open Source Vulnerability Database (Open Source Vulnerability Database): http://www. osvdb.org;

7) Open Web Application Security Project (OWASP) Vulnerabilities: http://www.owasp.org/index.php/ Category:Vulnerability;

8) Security Focus Vulnerabilities: http://www. securityfocus.com/vulnerabilities;

9) SecurityTracker: http://www.securitytracker.com;

10) The Hacker's Choice (THC): http://freeworld.thc.org;

11) United States Computer Emergency Readiness Team (US-CERT) Vulnerability Notes Database: http:// www.kb.cert.org/vuls;

12) Wireless Vulnerabilities and Exploits (WVE): http://www.wirelessve.org.

Стандарт NIST SP 800-115 для проведення тестування на проникнення рекомендує використання таких програмних комплексів:

1) BackTrack: https://www.backtrack-linux.org;

2) Knoppix Security Tools Distribution (STD): https://s-t-d.org/download.html;

3) F.I.R.E.: https://www.dmzs.com/tools;

4) INSERT Rescue Security Toolkit: http://www.inside-security.de/insert_en.html;

5) PHLAK: http://sourceforge.net/projects/phlakproject;

6) Top 100 інструментів мережевої безпеки: http://sectools.org.

Аналіз стандарту *NIST SP* 800-115 показав, що за своєю шириною та глибиною охоплення питань проведення тестування його доцільно використовувати під час розроблення вітчизняного стандарту тестування на проникнення.

Перевагами стандарту *NIST SP* 800-115 є те, що стандарт охоплює у сферу оцінювання ІБ не тільки питання проведення тестування, а й питання документації організації, політик гарантування безпеки, а також питання використання способів соціальної інженерії та їхній вплив на підсумковий рівень безпеки організації. Саме ці переваги доцільно запозичити з *NIST SP* 800-115 під час розроблення вітчизняного проекту стандарту тестування на проникнення.

Слабкими сторонами стандарту *NIST SP* 800-115 є такі. По-перше, *NIST SP* 800-115 не містить вичерпного переліку вразливостей, рекомендованих до перевірки. Класифікація вразливостей інформаційних систем". По-друге, у *NIST SP* 800 115 не наведено конкретних реалізацій і сценаріїв комп'ютерних атак, призначених для перевірки конкретних вразливостей. У цій частині *NIST SP* 800-115 істотно програє таким методикам як *PTES* і *OWASP*, що містять конкретний

перелік широко поширених вразливостей і рекомендації щодо способів їх перевірки.

Приклад програмних засобів зі складу комплексу *BackTrack*, які можуть використовуватися для тестування

Аналіз мережі	Autonomous System Scanner, Ettercap, Firewalk, Netdiscover,Netenum, Netmask, Nmap, P0f, Tctrace, Umit
"Сніффери" і програми захоплення трафіку	Dsniff, Ettercap, Kismet, Mailsnarf, Msgsnarf, Ntop,Phoss, SinFP, SMB Sniffer, Wireshark
Ідентифікація портів і мережевих сервісів	Amap, AutoScan, Netdiscover, Nmap, P0f, Umit, UnicornScan
Сканування вразливостей	Firewalk, GFI LANguard, Hydra, Metasploit,Nmap, Paros Proxy, Snort, SuperScan
Сканування бездротових мереж	Airsnarf, Airsnort, BdAddr, Bluesnarfer, Btscanner,FakeAP, GFI LANguard, Kismet, WifiTAP
Перевірка цілісності файлів	Autopsy, Foremost, RootkitHunter, Sleuthkit
Злом паролів	Hydra, John the Ripper, RainbowCrack, Rcrack, SIPcrack,SIPdump, TFTP-Brute, THC PPTP, VNCrack, WebCrack
Тестування віддаленого доступу	IKEProbe, IKE-Scan, PSK-Crack, VNC_bypauth
Тестування на проникнення	Driftnet, Dsniff, Ettercap, Kismet, Metasploit,Nmap, Ntop, SinFP, SMB Sniffer, Wireshark
Тестування безпеки додатків	CIRT Fuzzer, Fuzzer 1.2, NetSed, Paros Proxy, Peach

Приклад програмних засобів зі складу комплексу *Knoppix STD Toolkit*, які можуть використовуватися для тестування

Аналіз мережі	Cryptcat, Ettercap, Firewalk, Netcat, Nmap, P0f
"Сніффери" і програми захоплення трафіку	Dsniff, Ettercap, Ethereal, Filesnarf, Kismet, Mailsnarf,Msgsnarf, Ngrep, Ntop, TCPdump, Webspy
Ідентифікація портів і мережевих сервісів	Amap, Netcat, Nmap, P0f
Сканування вразливостей	Exodus, Firewalk, Nmap, Snort
Сканування бездротових мереж	Airsnarf, Airsnort, GPSdrive, Kismet, MACchanger
Перевірка цілісності файлів	Autopsy, Biew, Bsed, Coreography, Foremost, Hashdig, Rifiuti, Sleuthkit
Злом паролів	Allwords2, chntpw, Cisilia, Djohn, Hydra, John the Ripper, Rcrack

Тестування віддаленого доступу	Apache Server, IKE-Scan, Net-SNMP, SSHD, TFTPD, VNC Server
Тестування на проникнення	Driftnet, Dsniff, Ethereal, Ettercap, Kismet, Nessus,Netcat, Ngrep, Nmap, Ntop, TCPdump
Тестування безпеки додатків	NetSed

Список використаних джерел

1. Макаренко С. І. Аудит інформаційної безпеки: основні етапи, концептуальні засади, класифікація заходів // Системи управління, зв'язку та безпеки. 2018. № 1. С. 1-29.

2. Марков А. С., Цирлов В. Л., Барабанов А. В. Методи оцінки невідповідності засобів захисту інформації / за ред. А.С. Маркова. - М.: Радіо і зв'язок, 2012. - 192 с.

3. Бойко А. А., Дьякова А. В. Спосіб розроблення тестових віддалених інформаційно-технічних впливів на просторово розподілені системи інформаційно-технічних засобів // Інформаційно-керуючі системи. 2014. № 3 (70). С. 84-92.

4. Бойко А. А. Бойова ефективність кібератак: аналітичне моделювання сучасного бою // Системи управління, зв'язку та безпеки. 2020. № 4. С. 101-133.

5. Бойко А. А. Бойова ефективність кібератак: практичні аспекти // Системи управління, зв'язку та безпеки. 2020. № 4. С. 134-162.

6. NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment (NIST SP 800-115). - Computer Security Resource Center, 2008. - 80 p.- URL: http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

УДК 004.023, 004.852

Нескородєва Т.В.1, завідувач кафедри інформаційних технологій
Федоров Є.Є. 1, професор кафедри інформаційних технологій
Нечипоренко О.В.2, доцент кафедри робототехніки та спеціалізованих комп'ютерних систем

МЕТОДОЛОГІЯ СТВОРЕННЯ ІНТЕЛЕКТУАЛЬНИХ АГЕНТІВ

[1]Донецький національний університет ім. Василя Стуса, м. Вінниця
[2]Черкаський державний технологічний університет, м. Черкаси

Четверта промислова революція або Industry 4.0 призвела до швидких змін у технологіях, виробничих та соціальних і процесах у 21 столітті через зростаючий взаємозв'язок та інтелектуальну автоматизацію [1]. Частиною цієї фази промислових змін є побудова комп'ютерних систем шляхом об'єднання штучного інтелекту з робототехнікою, що стирають межі між фізичним, цифровим та біологічним світами. Одним із підходів до побудови таких комп'ютерних систем є використання мультиагентних систем. В даний час