УДК 681.3:519.872 **В.Л. Бурячок, В.А. Козачок, Л.В. Бурячок, П.М. Складанний**

ПЕНТЕСТІНГ ЯК ІНСТРУМЕНТ КОМПЛЕКСНОЇ ОЦІНКИ ЕФЕКТИВНОСТІ ЗАХИСТУ ІНФОРМАЦІЇ В РОЗПОДІЛЕНИХ КОРПОРАТИВНИХ МЕРЕЖАХ

В статті розглянуті основні принципи оцінки ефективності захисту інформації в розподілених корпоративних мережах. Обґрунтована необхідність створення систем комплексної оцінки захисту інформації в розподілених корпоративних мережах, в яких обробляється інформація з обмеженим доступом. Обґрунтовані основні положення проведення пентестінгу в інформаційно-телекомунікаційних системах.

Ключові слова:розподілена корпоративна мережа, комплексна система захисту інформації, пентестінг.

Постановка проблеми.

Захист державних секретів завжди був важливою складовою національної безпеки країни. З початком впровадження інформаційних систем (ІС) в різних, в першу чергу, силових відомствах виникла потреба щодо забезпечення розмежування доступу до ресурсів цих систем за аналогією з паперовими носіями. Вперше це завдання було вирішено у США, після появи у 1970 році моделі розмежування доступу ADEPT-50. Згодом, а саме у 1985 році, за результатами набутого практичного досвіду побудови систем захисту інформації (СЗІ) в державних структурах, Міністерство оборони США випустило перші критерії оцінки захищеності комп'ютерних систем – так звану «Помаранчеву книгу». Таким чином, саме держсектор став локомотивом подальшого стрімкого розвитку світового ринку інформаційної безпеки (ІБ). Напрацьовані ним технології успішно використовувалися в силових відомствах та згодом були поставлені на службу як в приватному бізнесі, так і для домашнього користувача. У процесі подальшої еволюції технологій і систем захисту інформації (СЗІ) виникла необхідність уніфікувати вимоги до їх створення та забезпечити деяку стандартизацію. Одним з найважливіших підсумків цієї роботи став міжнародний стандарт ISO/IEC 15408, так звані «Загальні критерії», що отримав визнання в багатьох країнах світу. Паралельно з критеріями захищеності, що оперують в якості мети оцінки сукупності програмно-апаратних засобів, розвивався напрямок стандартизації в частині менеджменту ІБ, результатом чого стало затвердження міжнародного стандарту ISO/IEC 27001 [1]. Впровадження системи управління інформаційною безпекою (СУІБ) відповідно до цього стандарту дозволяє правильно організувати процес захисту інформаційних ресурсів (ІР) та управління ризиками для цих ресурсів.

Україна на цьому шляху обрала власний вектор розвитку, розробивши серію нормативних документів (НД) системи технічного захисту інформації (ТЗІ) та фактично не приєднавшись до загальносвітового процесу стандартизації в частині менеджменту ІБ (рис.1) [2]. Так, й донині ключовим серед НД ТЗІ є документ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних систем від несанкціонованого доступу». Документ ґрунтується на «Канадських критеріях захищеності» 1993 року [3] та регламентує створення на об'єктах інформаційної діяльності (ОІД) комплексних систем захисту інформації (КСЗІ). При цьому власне визначення КСЗІ, як взаємозалежної сукупності організаційних та інженерно-технічних заходів, засобів і методів захисту інформації наводиться в Законі України «Про захист інформації в інформаційно-телекомунікаційних системах» [4]. Статус державного стандарту в частині менеджменту ІБ у нашій країні отримала при цьому тільки перша версія ISO/IEC 27001. Питання практичної застосовності цього документу залишається актуальним, але, тим не менш, слід зауважити, що зазначений стандарт у вигляді вимог СОУ Н НБУ 65.1 СУІБ 1.0: 2010 [5] нині є обов'язковим у банківській сфері.

Отже, на цей момент в Україні одночасно існують дві парадигми систем захисту: КСЗІ і СУІБ в банківській сфері. Етапи створення першої визначені в НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» [6]. Замовник своїми силами або із залученням підрядників розробляє технічне завдання на КСЗІ, погоджує його з Державною службою спеціального зв'язку та захисту інформації України (Держспецзв'язку), а потім, на підставі нього проектує та

впроваджує КСЗІ за допомогою сукупності організаційних заходів, програмно-апаратних та інженерних засобів і вводить в дослідну експлуатацію. Далі, на підставі отриманої заявки Держспецзв'язку замовник визначає компанію-ліцензіата, яка виступає організатором державної експертизи КСЗІ. Організатор експертизи, володіє штатом кваліфікованих експертів, розробляє програму і методику експертних випробувань, проводить їх і представляє результати своєї роботи у вигляді проекту експертного висновку на розгляд експертної ради з питань ТЗІ Держспецзв'язку. У разі позитивного рішення КСЗІ отримує атестат відповідності вимогам системи технічного захисту інформації. Така практика діє в нашій країні з початку 2000-х років і зазнала лише незначних змін. «Загальні Критерії» (стандарт ISO/IEC 15408) у нас на жаль взагалі не гармонізовані, а критерії захищеності 1999 року багато фахівців вважають застарілими, адже технології побудови інформаційно-телекомунікаційних систем (ІТС) за цей час пішли далеко вперед.

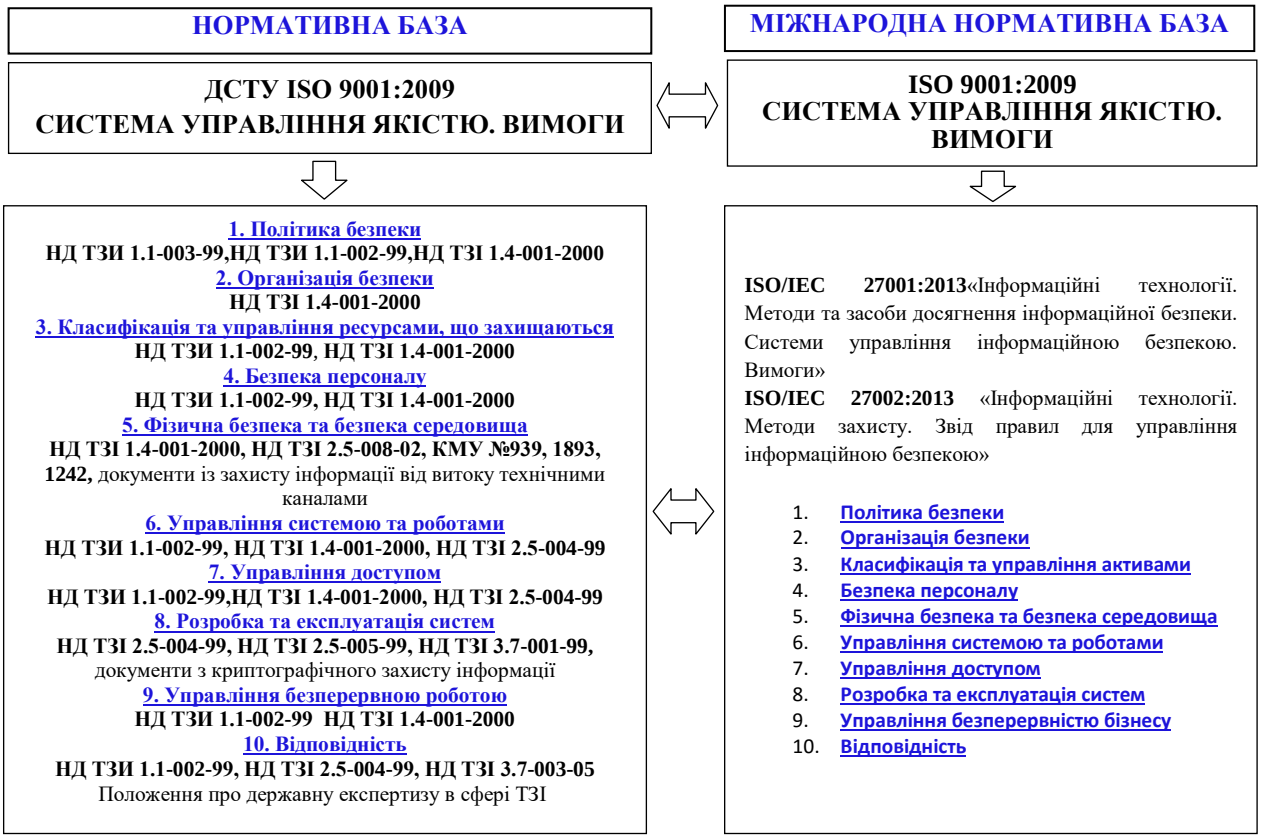

Рис.1. Порівняння національних та міжнародних документів у галузі ТЗІ

Разом з цим в існуючій системі створення КСЗІ можна знайти і ряд певних недоліків. Так, дійсно, для систем з різною архітектурою, різними вимогами щодо забезпечення безпеки, що ґрунтуються, в тому числі, і на різних категоріях доступу до інформації, існують стандартні функціональні профілі захищеності, тобто деякі фіксовані набори послуг безпеки. У той же час, розробник КСЗІ при формуванні технічного завдання (ТЗ) самостійно визначає об'єкти захисту, на які ці послуги поширюються. Експерти з Держспецзв'язку в процесі узгодження ТЗ перевіряють специфікації послуг, проте часто буває важко визначити адекватність висунутих вимог реально функціонуючій ІТС. Наступний етап контролю адекватності та повноти дій по створенню КСЗІ – експертиза. Втім, зазвичай організатор експертизи лише перевіряє якість реалізації заявлених послуг безпеки і комплектність документації на КСЗІ не вдаючись детально в технології обробки інформації. У кращих випадках експерти ще аналізують конфігурації програмно-апаратних засобів захисту, хоча для цього потрібні додаткові навички. Тим не менш, практично ніколи експертами якість впровадженої КСЗІ не перевіряється ***тестуванням на проникнення***. По-перше, цього не вимагає нормативна база, а по-друге, для проведення таких робіт потрібна серйозна практична підготовка. Так, кваліфікованих пентестерів у комерційному сегменті достатньо, проте серед

експертів в частині КСЗІ вони практично відсутні. Те ж стосується і самих розробників КСЗІ: організацій, які одночасно володіють нормативно-правовою базою у сфері технічного захисту та кваліфікаціями в галузі захисту операційних систем, мереж передачі даних, систем віртуалізації і т.ін. в Україні мінімально недостатня кількість. Як правило вони є розробниками найбільших і найскладніших КСЗІ в розподілених ІТС. Серйозні обмеження на технічну складову в КСЗІ в органах державної влади також накладає недостатнє бюджетне фінансування закупівель відповідних програмно-апаратних засобів захисту. Тому часто захист державних ІР зводиться до так званої «паперової безпеки», коли КСЗІ начебто і побудована за всіма правилами, проте не в змозі ефективно протистояти сукупності сучасних загроз. Щось подібне ми спостерігали під час атаки на веб-сайти держорганів, пов'язаної з блокуванням порталу ex.ua в 2012 році. Тоді багато сайтів були або зламані, або піддалися масованим DDoS-атакам. Характерно, що при цьому не встояли і ті веб-ресурси, в яких були створені КСЗІ.

Для виникнення подібних ситуацій є ще одна вагома причина. Розробник може спроектувати і побудувати ідеальну КСЗІ, експерт – якісно перевірити її адекватність, однак за експлуатацію створеної системи надалі відповідає замовник. Не є секретом, що кваліфіковані технічні фахівці в органах державної влади присутні далеко не завжди – зарплати невисокі та й штатний розклад іноді не дозволяє взяти на роботу додаткових співробітників в Службу захисту інформації, хоча це й регламентовано вітчизняним законодавством. Очевидно, що затаких умов – умов некваліфікованої експлуатації, навіть найкраща система захисту з часом втрачає актуальність. Щоб цього не сталося, інспекція Держспецзв'язку періодично здійснює контроль за станом захищеності державних ІР, однак на жаль не проводить при цьому жодних інструментальних перевірок. Саме такий стан визначає й актуальність даної статті та регламентує необхідність комплексної оцінки ефективності захисту інформації в розподілених корпоративних мережах.

Аналіз останніх досліджень та публікацій. Загальні вимоги щодо необхідності створення КСЗІ в ІТС, а також системи оцінки ефективності захисту інформації визначені в [1, 2, 3, 4, 5]. Завданням щодо побудови комплексних систем оцінки захисту інформації для розподілених корпоративних мереж, які дозволили знайти відповідь хоча б на частину з означених у постановці проблеми питань не приділялось достатньої уваги й у повному обсязі вони нажаль ніким не вирішувалась. Зважаючи на таке **метою статті** є обґрунтування необхідності побудови комплексних систем оцінки захисту інформації (КСОЗІ) для розподілених корпоративних мереж.

Виклад основного матеріалу.

Головними групами інцидентів, які можуть призвести до припинення обслуговування клієнтів або розголошенню їх персональних даних згідно схеми, пропонованої Конвенцією Ради Європи 2001 року по боротьбі з кіберзлочинністю, є:

1) інциденти, спрямовані проти конфіденційності, цілісності й доступності комп'ютерних даних і систем;

2) шахрайство та підробки, пов'язані з використанням ПЕОМ;

3) інциденти, пов'язані з розміщенням у мережах протиправної інформації;

4) інциденти відносно авторських і суміжних прав.

Зловмисниками такі дії реалізуються згідно діаграми, поданої на рис. 2 [7].

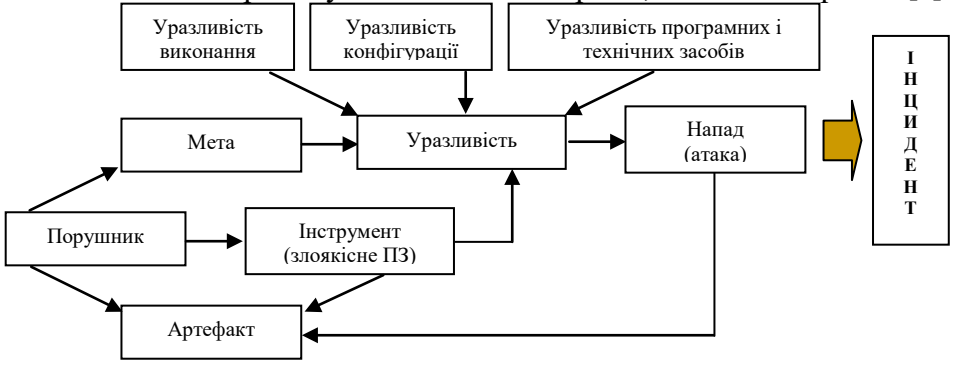

Рис. 2. Діаграма виникнення інцидентів

В умовах високої конкуренції вони неминуче можуть спричинити прямі збитки та репутаційні втрати, результати оцінки яких наведені на рис.3 та рис.4.

Рис.3. Оцінка втрат від внутрішніх інцидентів

Рис.4. Оцінка втрат від зовнішніх інцидентів

За оцінками McAfee, сукупні втрати від приведених на рис.3 та рис.4 дій можуть досягати до $ 1 трлн. на рік. Україна від таких дій отримує у середньому збиток в розмірі $ 200 тис. Згідно оприлюднених Лабораторією Касперського даних, за останні три роки ризик зараження через Інтернет в Україні суттєво збільшився. Цьому сприяє те, що технології реалізації атак з року в рік стають все доступнішими, а нові уразливості, в тому числі критичні, виявляються останнім часом здебільшого в самих популярних додатках, а також в IT-системах, обслуговуючих критичні об'єкти інфраструктури – газотранспортну систему, водопровідні мережі, електромережі й т. ін. Кількість вторгнень в ці сегменти державної економіки становить нині близько 560 тисяч на рік. Як результат за рівнем втрат у грошовому еквіваленті наша держава з 17 місця у 2012 році опустилась у 2014 на 6-ту позицію й нині входить до 10-ки країн з найбільшим ризиком зараження через Інтернет (рис.5).

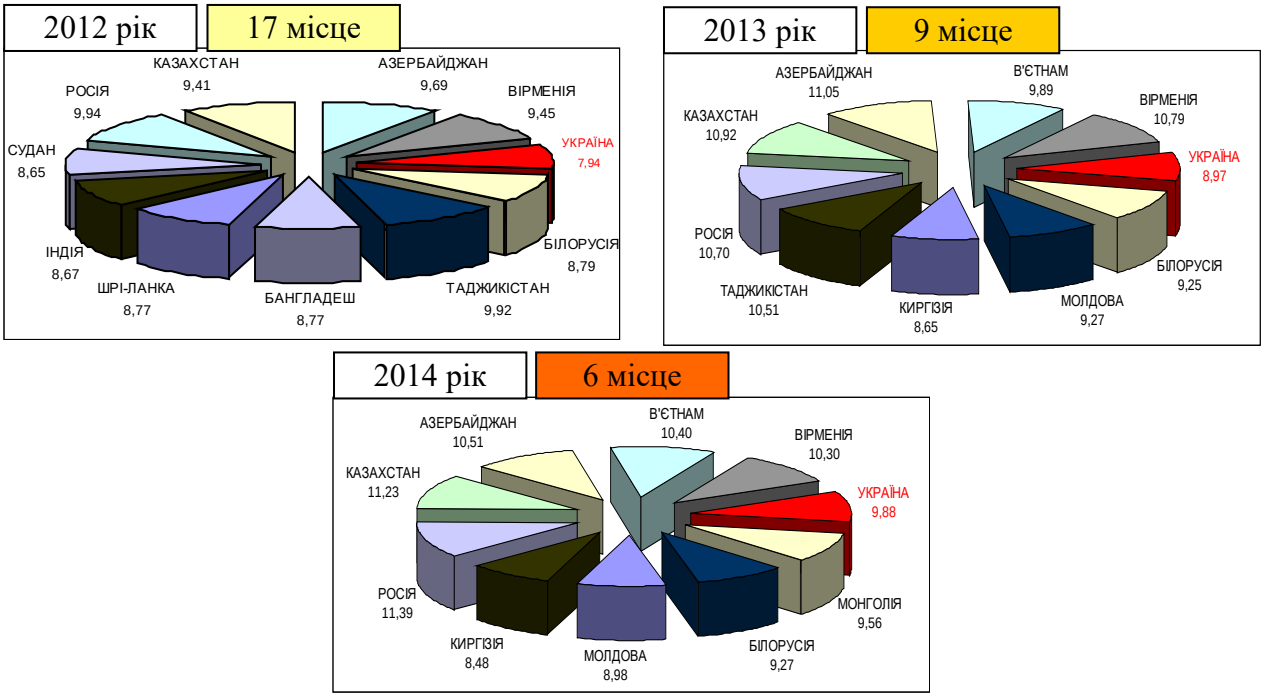

Рис. 5. Місце України у переліку країн з найбільшим ризиком зараження через Інтернет за даними Лабораторії Касперського

Згідно інформації CERT-UA «регіональна» статистика скомпрометованості IP-адрес українського сегменту Internet у 2014 році мала вигляд, наведений на рис.6.

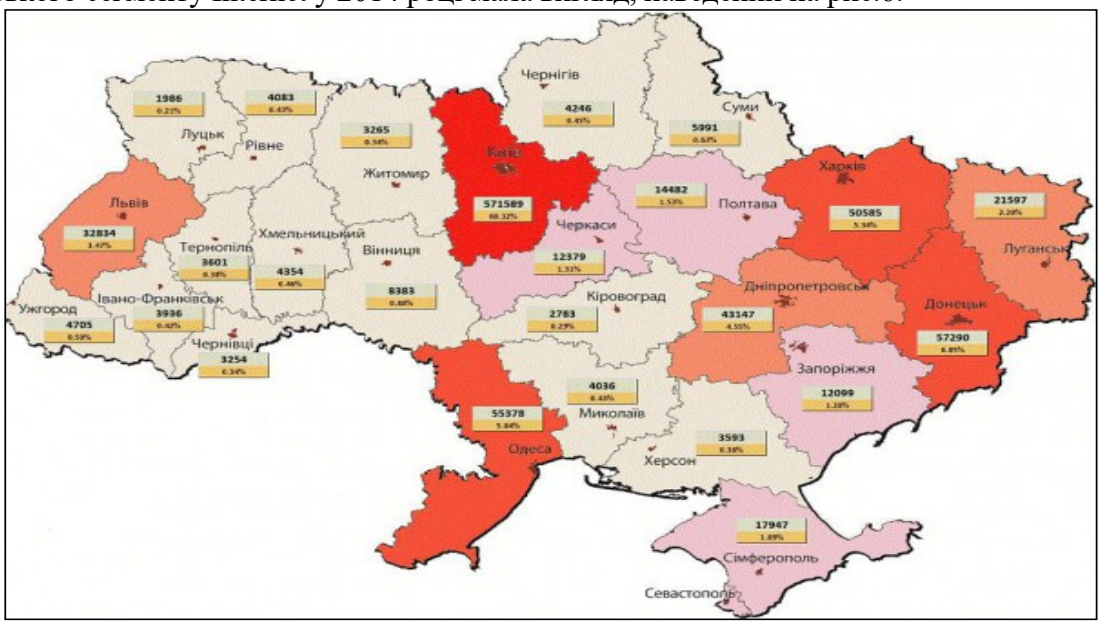

Рис. 6. «Регіональна» статистика скомпрометованості IP адрес українського сегменту Інтернет у 2014 році за даними CERT-UA

Не зважаючи на те, що IT-системи об’єктів інформаційної діяльності (ОІД) будуються з урахуванням вимог щодо забезпечення найменшої уразливості до атак та унеможливлення витоку даних – перевірити їх стійкість можна тільки на практиці. Для цього застосовують, як правило, технологію проведення тестів на проникнення (пентестінгу) або інакше етичного хакінгу, яка передбачає виявлення вразливостей на ОІД та проведення контрольованих атак, спрямованих, наприклад, як на окремі інформаційні системи – CMS, CRM, ERP та інтернет клієнт-банк, так і на всю інфраструктуру ОІД в цілому – зовнішній периметр мережі (периметр IP-адрес і Web-сайтів), бездротові мережі, внутрішню або корпоративну мережу тощо. При цьому експлуатують такі чинники, як:

-відсутність у керівництва компанії об'єктивної інформації про стан ІБ;

-нерозуміння того, якою може бути величина збитку при здійсненні хакерської атаки;

-недосконаліть системи ІБ або ж відсутність комплексу заходів щодо її забезпечення.

Фактично пентестінг це ні що інше, як імітація процесу проникнення в інформаційне середовище в контрольованих рамках, або інакше – моделювання процесу банального злому з явними результатами. Його проведення дозволить: дізнатися можливості здійснення загроз безпеці інформації; оцінити наслідки спрямованої хакерської атаки; визначити уразливості в захисті інформаційної системи; оцінити ефективність засобів захисту інформації; оцінити ефективність менеджменту інформаційної безпеки; оцінити ймовірний рівень кваліфікації порушника для успішної реалізації атаки; отримати аргументи для обґрунтування подальшого вкладення ресурсів в ІБ; виробити список контрзаходів, що дозволяють знизити можливість реалізації атак. Як результат, це допоможе отримати об'єктивну інформацію проступінь захисту ресурсів компанії та отримати, з урахуванням мотивації третьої сторони – фінансової, політичної чи моральної, реальну базу для забезпечення багаторівневої системи захисту.

Проведення пентестінгу є трудомістким завданням, вимоги до компетенції фахівців дуже високі. Пентестер повинен володіти навичками використання величезного числа технік, розуміти всі нюанси технічної та організаційної складової ІБ, застосовувати творчий підхід, володіти навичками соціальної інженерії та дотримуватись певних стандартів накшталт: Penetration Testing Execution Standard (PTES), OSSTMM 3.0. - The Open Source Security Testing Methodology Manual, Open Web Application Security Project (OWASP) Testing Project, Penetration

Testing Model (BSI), ISACA IS auditing procedure «Security assessment-penetration testing and vulnerability analysis», Payment Card Industry Data Security Standard (PCI DSS), v.3.0, ASV Security Scanning Procedures, PCI SSC і Information Supplement: Requirement 11.3 Penetration Testing, PCI SSC.Найприкметнішим серед наведених стандартів є стандарт OWASP заснований навосьми базахданих від семи компаній, що включає чотири консалтингові фірми і трьох вендорів SaaS. Загальна база стандарту містить понад 500 тисяч вразливостей.

Розглянемо особливості проведення пентестінгу на прикладі імітації атаки на внутрішніх користувачів системи шляхом застосування реверсивних "троянів". Ця прогресивна технологія злому, в якій використовуються уразливості клієнтського ПЗ робочих станцій і методи соціальної інженерії, дозволяє проникати в захищені корпоративні мережі та контролювати їх зсередини. По суті, вона дискредитувала концепцію захисту від атак шляхом забезпечення безпеки тільки зовнішнього периметра мережі, змусивши захищати кожне робоче місце за допомогою комплексу заходів верхнього рівня відповідно до ISO 17799.

Зазвичай в тестах на проникнення використовуються допрацьовані методики Національного інституту стандартів і технології США (NIST) Draft Guideline on Network Security Testing і Open-Source Security Testing Methodology (OSSTM). Для цього вибираються об'єкти дослідження, задається модель порушника (включаючи його можливості) і обмовляється режим роботи на основі рівня початкових знань виконавця про тестовані системи (Black Box або White Box) та рівня інформованості замовника про випробування (режим Black Hat або White Hat). При виборі рівня Black Box виконавцю необхідні лише діапазон зовнішніх IP-адрес і, можливо, адреси e-mail внутрішніх користувачів системи. У режимі White Box доступна для пентестера інформація значно ширше. У режимі Black Hat про проведення робіт знають тільки керівники служби ІБ. При цьому завдання групи тестувальників – повністю імітувати дії зловмисника, діючи максимально непомітно і не залишаючи слідів. У такому випадку вдається перевірити рівень оперативної готовності до атак мережевих адміністраторів і адміністраторів ІБ. У режимі White Hat будь-яких заходів приховування атакуючих дій не застосовується, а виконавці тестів працюють у постійному контакті з ІБ-службою замовника. Їх основне завдання зводиться до виявлення можливих вразливостей і оцінці ризику проникнення в систему.

Аудит інформаційних систем починається зі сканування стандартними інструментами (рис.7), які мають різну чутливість до різного роду загроз. Цей етап дозволяє визначити потенційні проломи (незалатані уразливості ПЗ, відкриті порти й т.ін.), але не дає уявлення про те, чи можна скористатися ними на практиці, а також експлуатувалися вони чи ні раніше.

Pwn Pad

Пристрій оснащений потужним чотирьох ядерним процесором (Qualcomm Snapdragon S4 Pro, 1,5 Ггц), 7-дюймовим екраном з дозволом 1900 x 1200 і потужною батареєю, що забезпечує до дев'яти годин активної роботи (3950 мА/ч), 2 Гб ОЗУ и 32 Гб внутрішньої пам’яті. У комплекті йдуть три адаптери: дві потужні зовнішні антени для пентеста 802.11b/g/n бездротових мереж і Bluetooth, а також перехідник USB - Ethernet, що дозволяє перевіряти на міцність провідні мережі.
Його головною складовою є програмна компонента: Metasploit, SET, Kismet, Aircrack-NG, SSLstrip, Ettercap-NG, Bluelog, Wifite, Reaver, MDK3, FreeRADIUS-WPE, Evil AP, Strings Watch, Full-Packet Capture, Bluetooth Scan і SSL Strip.

CreepyDOL

Спеціальне ПЗ й пристрій на базі Raspberry Pi за допомогою яких можна створити мережу, що буде перехоплювати Wi-Fi-трафік і збирати конфіденційну інформацію про користувачів. Як результат, пристрій дозволяє позиціонувати власника пристрою. Вся інформація обробляється на центральному сервері, там же можна в реальному часі відслідковувати пересування власника телефону і його перехоплені дані.

DEMYO POWER STRIP

Призначений для перевірки на міцність Ethernet-, Wi-Fi- і Bluetooth-Мереж. Побудований на базі популярного одноплатного комп'ютера Raspberry Pi і оснащений ARM-процесором 700 Мгц, який можна розігнати до 1 Ггц. Також на борті є 512 Мб оперативної пам'яті, SD-Карта на 32 Гб, ну й, зрозуміло, Ethernet-, Bluetooth-, Wi-Fi-Адаптери. У якості ОС використовується Debian Linux з набором попередньо встановлених security-тулз: Nmap, OpenVPN, w3af, aircrack-ng, btscanner, ophcrack, John the Ripper і інші.

Рис. 7. Приклади пристроїв, використовуваних для проведення пентестінгу

Далі проводиться аналіз інформації, наявної у відкритому доступі (адреси користувачів, іноді більш чутлива інформація, викладена персоналом), моделюються найбільш ймовірні сценарії проведення вторгнень (в тому числі і DDoS атаки, які вкрай рідко реалізуються на практиці). Найбільш трудомісткою частиною тестування на проникнення є атаки з використанням методів соціальної інженерії, коли зловмисник атакує не саму інформаційну систему, а людину, яка має до неї доступ. Для успіху таких вторгнень спеціальні технічні засоби не обов'язкові – експлуатуються передусім людськи слабкості. Далі виконуються симуляції спрямованих атак. Вони дозволяють виявити в системі «дірки», що з'явилися в результаті некоректного налаштування та технічних помилок, а також операційних недоліків у процесах і засобах контролю.

Як бачимо, пентестінг охоплює безліч векторів: зовнішні (з інтернету, з використанням віддаленого доступу) і внутрішні (через бездротове корпоративне з'єднання, з використанням повноважень і знань гостя, рядового співробітника або співробітника IT департаменту). Він може бути обмежений окремими об'єктами (найчастіше це поштові сервери, веб-сервера та програми, бездротові мережі) або охоплювати тільки нові елементи інфраструктури. Його головними етапами є: аналіз відкритих джерел, інструментальне сканування, аналіз/оцінка виявлених уразливостей і вироблення рекомендацій, підготовка звіту та аудит ІБ. При цьому режим тестування вибирається на основі рівня початкових знань виконавця про тестовану систему (Black Box або White Box) і рівня інформованості замовника про випробування (режим Black Hat або White Hat), рис.8. У випадку, коли необхідно визначити наскільки ефективно IT підрозділ реагує на вторгнення, проводиться прихований аудит – в цьому випадку зовнішньому агенту надається тільки діапазон IP-адрес (щоб у процесі тестування не постраждали інші компанії).

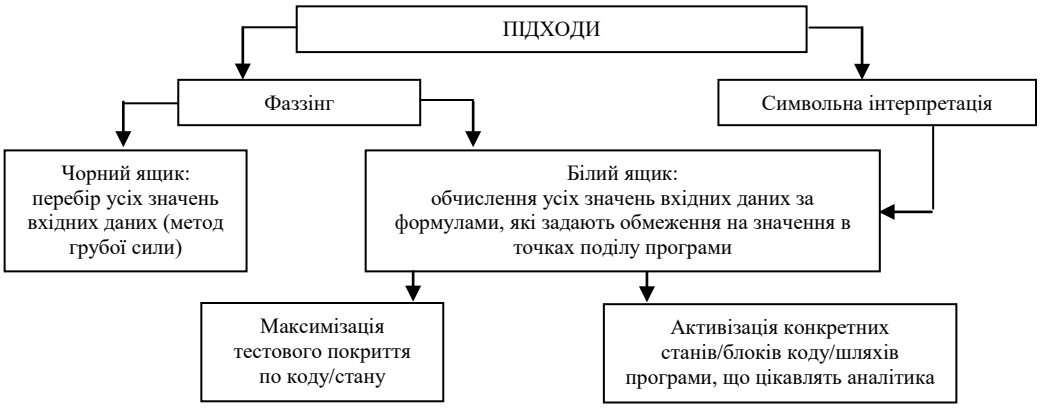

Рис.8. Сучасні підходи щодо проведення пентестінгу

За статистикою української компанії «Інком», зібраної в ході реалізації проектів, при тестуванні на проникнення в 50% випадків вдалося отримати доступ до веб-сайту, в 40% – доступ до пошти, у 35% – до бізнес-програм, в 29% – до системи банківського обслуговування, 10% – до IP телефонії. Повний контроль над інфраструктурою був захоплений в 25% проектів, і тільки в 5% – взагалі не вдалося подолати периметр. У п'ятірку найбільш популярних експлойтів входять: міжмережеве виконання сценаріїв (50%), наявність інтерфейсів віддаленого управління (47%), доступна інформація про додатки (45%), впровадження SQL коду (63%). Найпопулярнішою вразливістю стали останнім часом прості паролі адміністраторів. Вони були виявлені в 80% проектів, часом навіть у тих випадках, коли в організації були впроваджені політики щодо складності паролів пересічних користувачів. Саме підбір паролів дав можливість експертам проникнути в систему в 70% проведених проектів, уразливості веб-додатків і некоректно налаштоване обладнання несуть значно менші ризики і стали ключем до злому відповідно в 46% і 38% випадків. Відсутність оновлень сприяло успішному проведенню тестових атак в 25% компаній, а недоліки архітектури – в 9%.

Після проведення всіх необхідних робіт по проникненню повинен бути наданий звіт, який надалі презентується керівництву компанії і фахівцям ІТ та ІБ. Деякі стандарти пред'являють цілком певні вимоги до звіту, чим можна керуватися при його складанні. Практика ведення бізнесу в Україні показує, що найбільш оптимальною структурою звіту є його розбиття на 3 рівні: для вищого керівництва, для менеджерів ІБ і для технічних фахівців. Звіт повинен містити: методику проведення тесту; висновки для керівництва, що містять загальну оцінку рівня захищеності; опис виявлених недоліків системи управління ІБ (СУІБ); опис ходу тестування з інформацією по всіх виявлених вразливостей і результатами їх експлуатації; рекомендації щодо усунення виявлених вразливостей. Після проведення тесту можливі залишкові сліди тесту, так звані артефакти, які необхідно усунути. Наприклад, якщо був отриманий доступ до якої-небудь системі, то необхідно провести зміну паролів для всіх її користувачів, у разі використання вірусів їх також слід видалити, і т. ін.Логічним продовженням тесту на проникнення можуть бути роботи з проектування та впровадження системи управління рівнем захищеності, моніторингу захищеності периметра корпоративної мережі, розробки програми підвищення обізнаності в області ІБ та впровадження СУІБ.

Висновки

1. В умовах сучасної інформаційної та кібервійни, яка ведеться проти нашої країни, забезпечення безпеки ІС на ОІД й, передусім, ІС органів влади має стати державним завданням. Особливу увагу необхідно приділити захисту критичних інфраструктур, а також централізованих БД, зокрема, соціальних фондів та різних державних реєстрів. Незважаючи на всі поточні складнощі, завдання захисту державних ІР не повинні фінансуватися за залишковим принципом.

2. Існуюча нормативна база, яка крім іншого не містить вимог до розробки політики безпеки та оцінки ризиків, повинна бути істотно допрацьована. Один шлях – гармонізація зі стандартами ISO/IEC 27001 та ISO/IEC 15408, що дасть можливість і великим комерційним структурам легально брати участь у державній або приватній сертифікації своїх систем захисту інформації (рис.9) [2].

Інший шлях – вироблення власних, якісно нових стандартів безпеки для органів державної влади та критичних інфраструктур. При цьому доцільно розглянути варіант розробки деяких полегшених вимог, які можна було б використовувати в сегменті малого та середнього бізнесу для забезпечення захисту, наприклад, персональних даних. Окремим шляхом, який знаходиться поза межами розгляду даної статті, варто визнати можливість легального використання міжнародних стандартів криптографічного захисту інформації.

3. Процес державної експертизи у сфері ТЗІ необхідно доповнити тестуванням захищеності систем на проникнення. Це дозволить сформувати інститут експертів, що володіють широким спектром кваліфікацій, і залучити кращих фахівців галузі для підвищення інформаційної безпеки країни.

Рис.9. Гармонізація НД ТЗІ з ISO 15408

4. Для підвищення ефективності роботи комплексної системи захисту інформації в Україні доцільно переглянути реєстр інформаційно-телекомунікаційних систем, виділити з них найбільш важливі і сконцентрувати зусилля саме там. Зміна нормативно-правової бази у сфері захисту інформації – це виклик часу, однак лише в такому випадку на питання «бути чи не бути КСЗІ», нехай і в трансформованому вигляді, можна буде дати позитивну відповідь.

Література

1. ISO/IEC 27001:2013. *Information technology — Security techniques — Information security management systems —Requirements.* [Електрон. ресурс]: – Режим доступу: http://www.itgivernance.co.uk/standards.arx.

2. Гавриленко О.В. Відповідність національної нормативної бази у сфері технічного захисту інформації міжнародним стандартам: зіставлення документів, шляхи гармонізації. Матеріали XVII Міжнародної науково-практичної конференції «Безпека інформації у інформаційно-телекомунікаційних системах», м.Київ, 2015.

3. НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу". [Електрон. ресурс]: – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40386&cat_id=38835.

4. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 5 липня 1994 року № 80/94-ВР, Відомості Верховної Ради України (ВВР), 1994, № 31. – с.286

5. СОУ Н НБУ 65.1 СУІБ 1.0:2010. Настанова. Методи захисту в банківській діяльності. Система управління інформаційною безпекою. [Електрон. ресурс]: – Режим доступу: http://www.uk.xlibx.com/4yuridicheskie/1354389-1-sou-nbu-651-suib-10-2010-standart-organizacii-ukraini-nastanova-metodi-zahistu-bankivskiy-diyalnosti-siste.php.

6. НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі". [Електрон. ресурс]: – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article ?art_id=46074&cat_id=38835.

7. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – 288 с.

Надійшла 18.08.2015 р. Рецензент: д.т.н., проф. Богданович В.Ю.