УДК 004.056

Киричок Р.В., аспірант; **Складанний П.М.**, аспірант;
Бурячок В.Л., д.т.н; **Гулак Г.М.**, к.т.н.; **Козачок В.А.**, к.т.н.

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КОНТРОЛЮ ЗАХИЩЕНОСТІ КОРПОРАТИВНИХ МЕРЕЖ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ

Kyrychok R.V., Skladannyi P.M., Buryachok V.L., Hulak H.M., Kozachok V.A. The problems of controlling the security of corporate networks and solutions.

This paper discusses the use of penetration testing as a tool for comprehensive assessment of the effectiveness of information protection in information-telecommunication systems and networks. Provides information regarding the main threats to information security and vulnerabilities of IT systems (vulnerability of network services and applications). Are considered the technology implementation of a penetration testing (pentest), the typical scheme, and also presents an algorithm for pentest. The necessity of pentest in the IT systems (networks) of authorities and critical infrastructures (social funds and various state registries), for an objective assessment of the level of safety of these structures in today's information and cyber war being waged against our country.

Keywords: IT system, network, pentest, hacking, vulnerability, attack.

Киричок Р.В., Складанний П.М., Бурячок В.Л., Гулак Г.М., Козачок В.А. Проблеми забезпечення контролю захищеності корпоративних мереж та шляхи їх вирішення.

В даній статті наведено інформацію щодо основних загроз безпеці інформації та вразливих місць ІТ-систем. Розглянуто технологію реалізації тестування на проникнення (пентест), типову схему, а також представлено алгоритм проведення пентесту. Обґрунтована необхідність проведення пентесту в ІТ-системах (мережах) органів влади та критичних інфраструктур (соціальних фондів та різних державних реєстрів), задля об'єктивної оцінки рівня безпеки цих структур в умовах сучасної інформаційної та кібервійни, яка ведеться проти нашої країни.

Ключові слова: ІТ-система, мережі, пентест, проникнення, уразливість, атака.

Киричок Р.В., Складанный П.М., Бурячок В.Л., Гулак Г.Н., Козачок В.А. Проблемы обеспечения контроля защищенности корпоративных сетей и пути их решения.

В данной статье приведена информация относительно основных угроз безопасности информации, а также уязвимостей ИТ-систем. Рассмотрено технологию реализации тестирования на проникновение (пентест), типовую схему, а также представлен алгоритм проведения пентесту. Обоснована необходимость проведения пентесту в ИТ-системах (сетях) органов власти и критических инфраструктур (социальных фондов и различных государственных реестров), для объективной оценки уровня безопасности этих структур в условиях современной информационной и кибервойны, которая ведется против нашей страны.

Ключевые слова: ИТ-система, сети, пентест, взлом, уязвимость, атака.

Вступ

«Хто володіє інформацією, той володіє світом», – цій цитаті Н. Ротшильда більше двохсот років, однак саме сьогодні її популярність виросла в рази. Зважаючи, що історія розвитку інформаційного суспільства тісно переплетена з інформаційними операціями саме заходи з маніпуляції інформацією, дезінформації конкуруючих сторін та/або введення їх одна одну в оману стали останнім часом невід'ємною частиною внутрішньої й зовнішньої політики переважної більшості держав земної кулі.

Головну роль у цих процесах останнім часом відіграє Internet – п'ята влада світу. Саме тому все частіше вислів Н. Ротшильда звучить у новому трактуванні: «Хто володіє ІНТЕРНЕТОМ, той володіє світом». Й це зрозуміло, бо саме вибухове зростання обсягів інформації, до якої завдяки новітнім Інтернет-технологіям отримали доступ пересічні громадяни та винайдення потужних комп'ютерів, електронною артерією яких стали сучасні інформаційно-телекомунікаційні (ІТ) системи і мережі – сприяло як глобальній інтелектуалізації та розвитку промисловості, так й суттєво розширило можливості міжнародного бізнесу.

Разом з тим, як відомо, впровадження сучасних Інтернет-технологій у всі сфери діяльності світового суспільства призвело й до значної залежності передусім критично-

важливих галузей та секторів світової економіки (табл.1) від загроз антропогенного і техногенного характеру, а також природних катаклізмів.

Таблиця 1

Перелік критично-важливих секторів та галузей світової економіки

Галузь	**Сектори**
Енергетика	- електрика; - нафта і природній гас
Водопостачання	- дамби; - очисні та розподільні системи тощо
Транспорт та транспортні перевезення	- судноплавство та - авіація; - залізничний та автомобільний транспорт; - логістика тощо
Харчова промисловість	- торгівля продуктами харчування; - сільське господарство тощо
Засоби масової інформації та культурні активи	- радіо і преса; - культурна спадщина тощо
Фінанси та страхування	- банки; - фондові біржі; - страхові компанії; - фінансові послуги тощо
Охорона здоров'я	- охорона здоров'я; - аптечна справа тощо
Освіта	- дошкільні та шкільні заклади; - професійно-технічні заклади; - вищі навчальні заклади тощо
Інформаційно-комунікаційні технології	- телекомунікації (включаючи супутники); - інформаційно-телекомунікаційні системи; - програмне та апаратне забезпечення тощо
Державне управління та адміністрування	- уряд; - парламент; - правові інститути тощо

Останнім часом кількість державних і комерційних структур, які потерпають від таких дій значно збільшилась. Цьому сприяє «продуктивна робота» дійових осіб інформаційного та кіберпросторів (рис.1), які, будучи підкріпленими новими можливостями щодо злому

Рис. 1. Дійові особи інформаційного та кіберпросторів

веб-сайтів, серверів додатків та баз даних, здатні заподіяти не тільки прямі фінансові збитки критично-важливим об'єктам інфраструктури країн світу (енергетичним і транспортним магістральним мережам, нафто- та газопроводам, каналам швидкісного і урядового зв'язку, високотехнологічним підприємствам та підприємствам оборонно-промислового комплексу, центральним органам влади, закладам освіти та охорони здоров'я, фінансовому сектору тощо), а й паралізувати їх роботу та привести як до репутаційних втрат, так і до конкурентних переваг (рис. 2).

Рис. 2. Види зломів та причини витоку даних

Тобто, як бачимо, чим більше ІТ-технології розвиваються й інтегруються у наше повсякденне життя, тим більш важливою стає інформаційна безпека (ІБ). Підтвердженням цьому можуть слугувати:

- статистичні дані, оприлюднені корпорацією WASC (Web Application Security Consortium), згідно яких уразливими до хакерських атак є понад 96,85% веб-сайтів;
- твердження фахівців з міжнародної організації CERT (Computer Emergency Response Team), які вважають, що кількість інцидентів в інфосфері та кількість виявлених уразливостей кожного року суттєво збільшується (рис. 3).

Рис. 3. Статистика та типи уразливостей

При цьому і в прикладному та системному програмному забезпеченні (ПЗ), і в серверних додатках домінують, як видно, уразливості на кшталт відмови в обслуговуванні, компрометації системи та підвищення привілей. Для унеможливлення впливу таких і ним подібних уразливостей на інфраструктуру країн світу та захисту їх від низки різноманітних загроз нині витрачаються великі кошти.

Але, доволі часто буває так, що при цьому, придбавши коштовне антивірусне ПЗ та коштовні апаратні брандмауери, – переважна більшість замовників не отримує майже нічого, окрім теоретичних доказів того, що вкладені кошти роблять їх мережі від хакерських атак більш захищеними. Щоб вберегтися від зайвих втрат значна кількість державних і комерційних структур нині застосовують доволі популярну в усьому світі послугу в галузі інформаційної безпеки, *яка отримала назву* «тестування на проникнення» (тести на подолання системи захисту, penetration testing, pentest) *й означає* санкціоновану спробу обійти існуючий комплекс засобів захисту власних ІТ-систем і мереж з метою виявити в них слабкі місця (за рахунок ідентифікації максимально можливої кількості уразливостей за обмежений час при заданих умовах й поточному стані) та впевнитись в їх ефективності.

Викладення основного матеріалу

Тестування на проникнення є складовою частиною етичного хакінгу (рис. 4) – процесу пошуку та виявлення уразливостей ІБ, а також проведення контрольованих атак, спрямованих, наприклад, як на окремі ІТ-системи – CMS, CRM, ERP та інтернет клієнт-банк, так і на інфраструктуру об'єкта інформаційної діяльності (ОІД) в цілому.

«Знай ворога й знай себе, і ти пройдеш сотню битв без поразки» (Сунь Цзи) – *ключова ідея етичного хакінгу.*

Рис. 4. Етичний хакінг

Проведення пентестінгу є трудомістким завданням. В ході *pentest* роль зловмисника відіграє фахівець, який повинен здійснити атаку на веб-сервер, сервер застосувань або баз даних, персонал або корпоративну мережу, визначити рівень захищеності, виявити уразливості, ідентифікувати найбільш вірогідні шляхи злому і визначити наскільки добре працюють засоби виявлення і захисту ІС від атак на підприємстві. Для цього пентестер повинен володіти навичками використання величезної кількості технік, розуміти всі нюанси технічної та організаційної складової ІБ, володіти навичками соціальної інженерії та дотримуватись певних стандартів, на кшталт:

- Penetration Testing Model (BSI);
- Payment Card Industry Data Security Standard (PCI DSS);
- Information System Security Assessment Framework (ISSAF);
- Penetration Testing Execution Standard (PTES) http://www.pentest-standard.org/;
- Open Source Security Testing Methodology Manual (*OSSTMM, http://www.isecom.org/research/osstmm.html*);
- Open Web Application Security Project Testing Guide (*OWASP, https://www.owasp.org/index.php/OWASP_Testing_Project*);
- NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment (*NIST SP 800-115, http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf*)

тощо.

Окрім технік, рекомендованих даними стандартами (*найефективнішим серед них доречі є стандарт OWASP, заснований на восьми базах даних від семи компаній, що включає чотири консалтингові фірми і трьох вендорів SaaS та містить понад 500 тисяч уразливостей*) в ході тестування пентестером можуть бути змодельовані й перевірені й інші вектори атак, спрямовані на користувачів корпоративних систем (соціальна інженерія), зовнішній периметр мережі (периметр IP-адрес і Web-сайтів), безпровідні мережі IEEE 802.11(Wi-Fi), 802.15(Bluetooth) і 802.16(Wi-Max), а також переносимі комп'ютери та мобільні пристрої (табл. 2).

Таблиця 2

Вектор атаки	Опис
Фізичний	Атаки з використанням безпосереднього фізичного доступу в середину периметра корпоративної мережі (якщо такий є), що захищається
Мережевий	Дистанційні атаки на мережеві ресурси і протоколи
Електронна пошта	Атаки з використанням електронної пошти (в тому числі з елементами соціальної інженерії)
Додатки	Атаки з використанням специфічних додатків використовуваних Замовником (наприклад, web портал)
Бездротові мережі	Атаки спрямовані на бездротові протоколи передачі даних 802.11 (Wi-Fi), 802.15 (Bluetooth), 802.16 (Wi-Max)
Клієнтські додатки	Атаки на клієнтські програми
Мобільні пристрої	Атаки на мобільні пристрої (мобільні і переносні комп'ютери, смартфони і т.д.)
Соціальна інженерія	Атаки на користувачів з використанням методів соціальної інженерії

Тестування на проникнення може проводитись як у складі ***аудиту ІБ*** на відповідність зазначеним вище стандартам, ***аналізу уразливостей*** або ***атестації інформаційної (автоматизованої) системи***, так і у вигляді самостійної роботи:

Тест на проникнення != аудит інформаційної безпеки

Тест на проникнення != аналіз уразливостей

Тест на проникнення != атестація

Власне аудит ІБ починається з аналізу ризиків і загроз. Він призначений для виявлення найбільш небезпечних загроз з точки зору системи захисту. Елементи *pentest* при проведенні **аудиту** на відповідність стандарту ISO 17799 можуть використовуватися для оцінки ефективності реалізації таких захисних механізмів, як «захист від злоякісного коду», «мережева безпека» тощо. В ході тестування аудитор відіграє роль зловмисника, мотивованого на порушення безпеки ІТ-систем (мереж) замовника (державної або комерційної структури). Його завдання полягає в тому, щоб знайти відповіді на такі питання: «як простіше потрапити в середину системи, порушити її працездатність або що-небудь отримати», «якою, як результат, виявиться мнімальна ціна взлому». Інтенсивним перевіркам при цьому піддаються передусім програмні і технічні засоби захисту ІТ-систем і мереж, що спрямовані на визначення потенційних проломів в системі захисту – незалатаних уразливостей ПЗ, відкритих портів тощо [1 - 3].

При **аналізі уразливостей** елементи *pentest* можуть використовуватися для оцінки використовуваного в ІТ-системах (мережах) програмного і апаратного забезпечення на предмет спроби їх експлуатації для проникнення в систему. В ході **атестації об'єктів** інформатизації елементи *pentest* можуть використовуватися для демонстрації на практиці того, що невідповідність вимогам стандартів або іншим нормативно-правовим документам з безпеки інформації може привести до успішної компрометації системи. В ході **самостійної роботи** елементи *pentest* можуть використовуватися для обґрунтування необхідності проведення робіт з підвищення захищеності або отримання незалежної оцінки рівня безпеки ІТ-системи.

За місцем розташування аудитора відносно до мережевого периметру корпоративної системи, *pentest* може бути внутрішнім, зовнішнім або комплексним (рис. 5) [3].

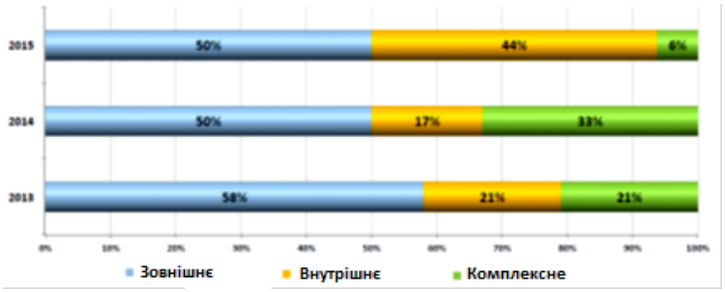


Рис. 5. Види pentest

Зовнішнє тестування на проникнення педбачає тестування зовнішнього периметру мережі, тестування web-сайтів та спец додатків тощо. Внутрішнє – орієнтоване головним чином на внутрішні ресурси (рис. 6).

За обсягом інформації, яка надається аудитору про тестовану систему тест на проникнення може проводитись за методами чорного (Black Box) або білого (White Box) ящиків (табл. 3).

Таблиця 3

Black Box	Виконавець імітує групу хакерів, які мають лише назву компанії й практично нульові відомості про систему, що є метою дослідження. Для реалізації поставленого завдання йому необхідні лише діапазон зовнішніх IP-адрес і, можливо, адреси e-mail внутрішніх користувачів системи.
White box	Виконавець має доступ до систем і повну інформацію про них. Така модель тестування використовується як частина організаційно-технічного аудиту організації IT і передбачає аналіз процесів і процедур.

Зовнішнє тестування на проникнення

Тип тестування	Опис
Тестування зовнішнього периметру мережі	Аналіз включає тільки зовнішні IP-адреси компанії, доступні з Інтернет
Тестування WEB сайтів	Аналіз включає в себя тільки WEB-сайти і сервіси компанії, доступні необмеженому кола зовнішніх користувачів
Тестування спеціалізованих додатків	Аналіз включає різні додатки, доступні зовнішнім користувачам, що взаємодіють з серверами компанії
Тестування співробітників на стійкість до методів соціальної інженерії	Спроба отримання доступу до систем компанії з використанням методів соціальної інженерії. Оцінка рівня обізнаності співробітників у питаннях ІБ
Тестування безпроводових мереж	Аналіз можливостей зловмисника, який знаходиться в зоні радіспостережності безпроводових мереж компанії, але не має до них санкціонованого підключення
Імітація «втраченого» корпоративного пристрою	Аналіз можливостей потенційного зловмисника, який заволодів корпоративним мобільним пристроєм

Внутрішнє тестування на проникнення

Тип тестування	Опис
Тестування внутрішнього периметру	Оцінка можливостей зловмисника, який має санкціонований обмежений доступ до корпоративної мережі, аналогічний рівню доступа рядового співробітника або гостя, який має доступ тільки в гостьовий сегмент, або ж має доступ тільки до мережевої розетки
Тестування окремого компонента/системи	WEB-додатки, ERP, СУБД

Рис. 6. Зовнішній і внутрішній pentest

За рівнем інформованості замовника про випробування *pentest* може проводитись:

– з повідомленням адміністраторів тестованого об'єкта (White Hat);

– без повідомлення адміністраторів і фахівців з безпеки тестованого об'єкта (Black Hat).

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 оцінки ризику проникнення в систему.

Типова схема «Penetration Testing» приведена на рис. 7.

Рис. 7. Схема Penetration Testing

У загальному випадку порядок проведення робіт наступний (рис. 8).

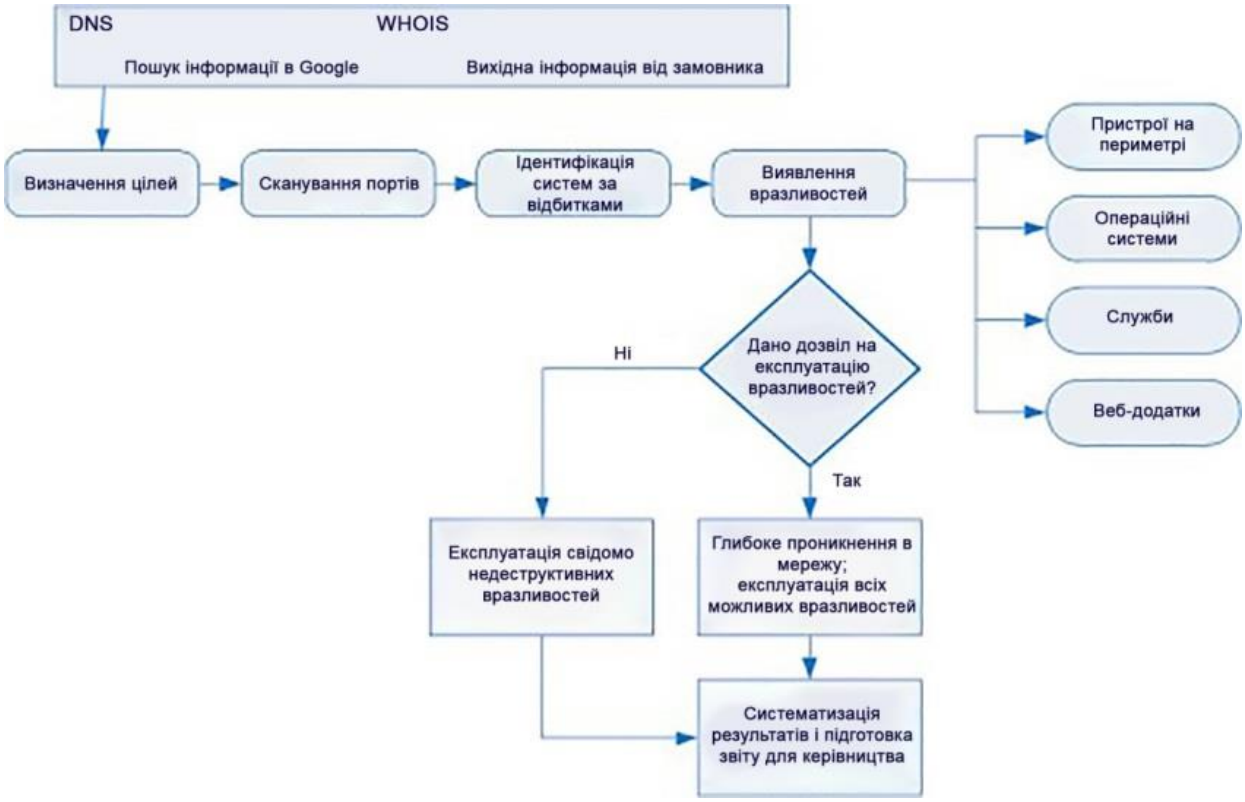


Рис. 8. Алгоритм проведення пентестінгу

1) Отримання попередньої інформації про мережу замовника та планування проведення тесту на проникнення. Для цього можуть бути використані як пасивні (Google Hacking; Google Cache; WHOIS інформація; Shodan; Wayback Machine (http://www.archive.org); офіційний сайт компанії; публикації про компанію та її співробітниках у ЗМІ; сайти пошуку роботи; прес-релізи інтеграторів; сторінки співробітників у соціальних мережах; блоги та форуми; пошук у фізичному мусорі компанії – Dumpster Diving тощо), так і активні (Ping Sweep, Fingerprint, сканування портів, аналіз повертаємих банерів мережевих служб, NetBios Enumeration, SNMP Enumeration, LDAP Enumeration, NTP Enumeration, SMTP Enumeration, DNS Enumeration, соціальна інженерія тощо) методи. Як результат – формування карти мережі, визначення типів пристроїв, ОС, додатків по реакції на зовнішній вплив.

2) Пошук та ідентифікація уразливостей мережевих служб і додатків. Може проводитися як вручну, так і з використанням різних сканерів від компаній MaxPatrol, Nessus, OpenVAC та інших.

Перевіряється наявність і можливість використання вразливих місць, а саме:
- SQL Injection (використання операторів SQL);
- Source code injection (виконання довільного коду);
- OS Commanding (виконання команд ОС);
- Client-side Attacks (атак на клієнтів);
- Cross-Site Scripting, XSS (міжсайтового виконання сценаріїв);
- Content Spoofing (підміни вмісту);
- Buffer Overflow (переповнення буфера);
- механізмів авторизації та аутентифікації і інше.

За даними компанії Positive Technologies в ході проведення *pentest* для внутрішніх тестів найчастіше використовуються уразливості, що наведені на рис. 9, а для зовнішніх – такі, що наведені на рис. 10.

Рис. 9. Уразливості, характерні для проведення внутрішніх тестів

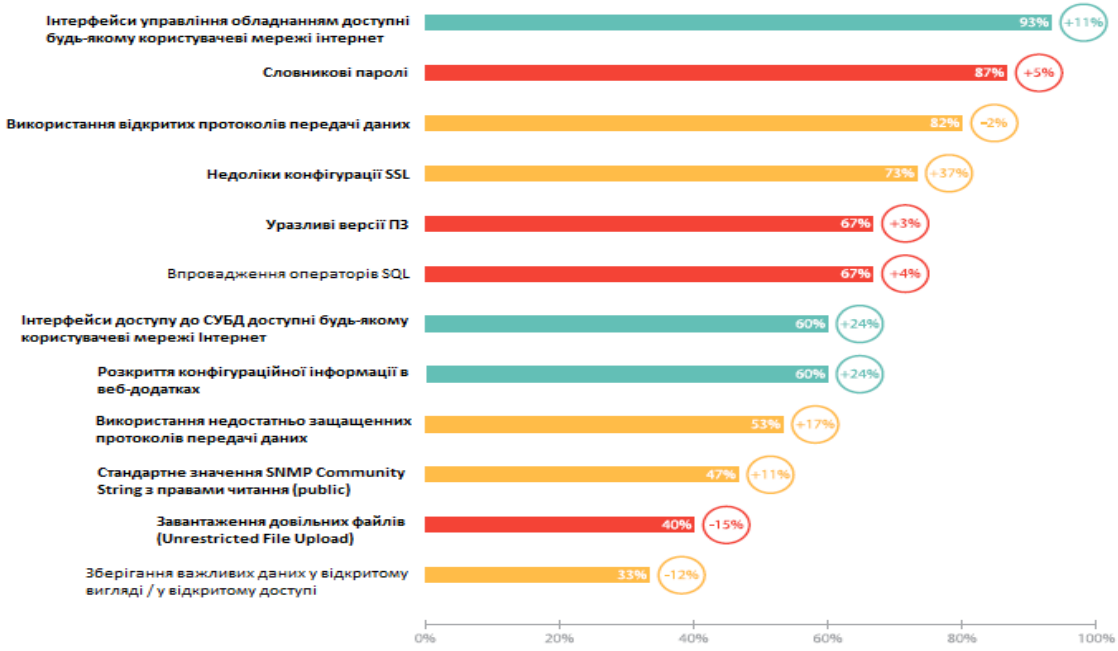
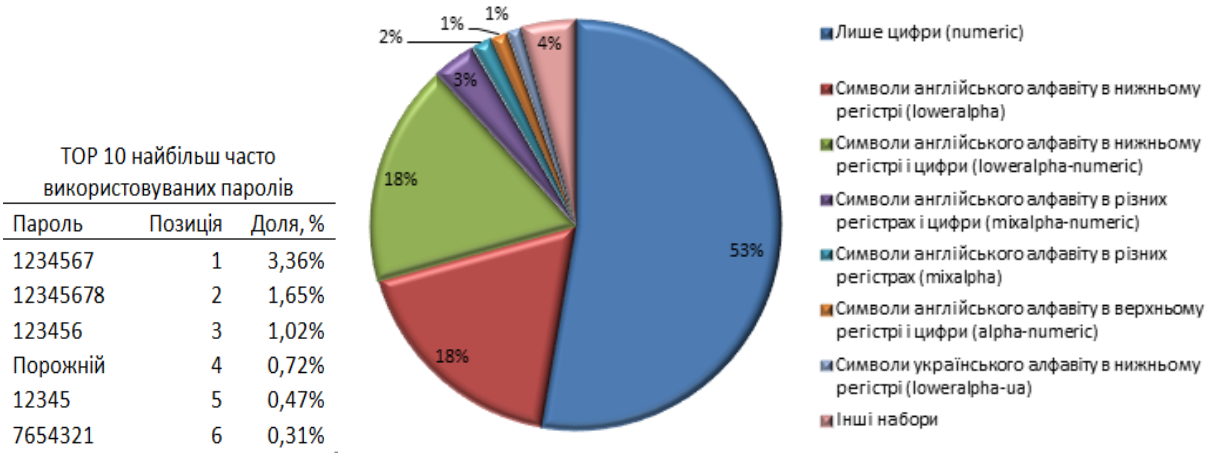


Рис. 10. Уразливості, характерні для проведення зовнішніх тестів

3) Експлуатація уразливостей. Отримавши перелік можливих уразливостей аудитор проводить їх експлуатацію. Методи та інструментарій вибираються при цьому індивідуально для кожного типу уразливості. Особлива увагу приділяється: підбору паролів до різних мережевих сервісів; проведенню атак типу «людина посередині» для перехоплення паролів користувачів (рис. 11) тощо [2].



TOP 10 найбільш часто використовуваних паролів

Пароль	Позиція	Доля, %
1234567	1	3,36%
12345678	2	1,65%
123456	3	1,02%
Порожній	4	0,72%
12345	5	0,47%
7654321	6	0,31%

Рис. 11. TOP-10 найбільш часто використовуваних користувачами паролів

Атаки типу «Man-in-the-Middle» (рис. 12) полягають у перехопленні зловмисником каналу зв'язку між двома системами, отриманні доступу до ресурсів мережі та активному втручанні в протокол передавання інформації з метою її крадіжки, знищення, фальсифікації або модифікації.

З цією метою аудиторами використовується як інструментарій власної розробки, так і загальнодоступні утиліти такі, як: <u>експлойти</u>: https://www.exploit-db.com; http://www.rapid7.com/db/; http://ru.0day.today; http://www.ussrback.com тощо, а також <u>фреймворки</u>: Metasploit; Cobalt Strike; Core Impact; Immunity CANVAS. Після отримання доступу до будь-якої системи аудитор намагається максимально розширити свої привілеї й отримати доступ до інших систем, а також скомпрометувати максимальну кількість облікових записів користувачів.

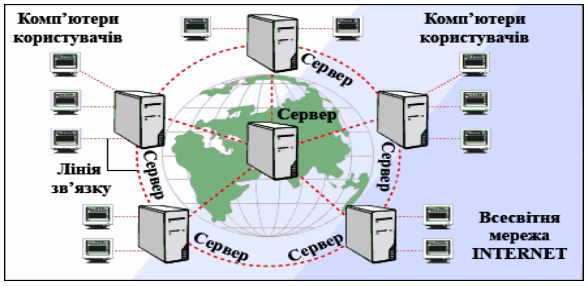


Рис. 12. Схема атаки типу Man-in-the-Middle

За погодженням із замовником при цьому може проводитися перевірка:

- базових робіт з контроля захищеності бездротових мереж;
- зовнішнього периметру і відкритих ресурсів на DOS (DDOS) атаки, а також оцінки ступеня стійкості мережевих елементів і можливого збитку при їх проведенні;
- стійкості мережі, шляхом моделювання атак на протоколи канального рівня STP, VTP, CDP, ARP;
- стійкості маршрутизації, шляхом моделювання фальсифікації маршрутів і проведення DOS (DDOS) атак проти використовуваних протоколів маршрутизації;

- мережевого трафіку, з метою отримання важливої інформації (паролі користувачів, конфіденційні документи та ін.);

- можливості отримання зловмисником НСД до конфіденційної інформації або інформації обмеженого доступу замовника. Проводиться перевіркою прав доступу до різних IP замовника з привілеями, отриманими на різних етапах тестування.

4) Отримана в ході аналізу уразливостей і спроб їх експлуатації інформація документується та аналізується з метою вироблення рекомендацій у формі звіту, що спрямований на поліпшення захищеності IT систем (мереж). Практика ведення бізнесу в Україні показує, що найбільш оптимальною структурою звіту є його розбиття на три рівні: для вищого керівництва, для менеджерів ІБ і для технічних фахівців [1].

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 вразливостях і результатами їх експлуатації;
- рекомендації щодо усунення виявлених вразливостей.

Приклади звітів за результатами тестів на проникнення та рекомендації щодо їх написання наведено на таких сайтах:

- https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf (від Offensive Security, ENG);
- http://www.slideshare.net/devteev/pt-penetration-testing-report-sample (від Positive Technologies, RUS). Результат сканування в режимі "Pentest" з використанням програмного засобу контролю захищеності й відповідності стандартам MAXPATROL подано на рис. 13, а варіант звіту по PCI DSS на рис.14;
- https://www.sans.org/reading-room/whitepapers/bestprac/writing-penetration-testing-report-33343 (від Writing a Penetration Testing Report - SANS Institute);
- http://resources.infosecinstitute.com/writing-penetration-testing-reports/ (від The Art of Writing Penetration Test Reports).

Після проведення тесту можливі залишкові сліди тесту, так звані артефакти, які необхідно усунути. Наприклад, якщо був отриманий доступ до якої-небудь системи, то необхідно провести зміну паролів для всіх її користувачів. У разі використання вірусів їх також необхідно 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.

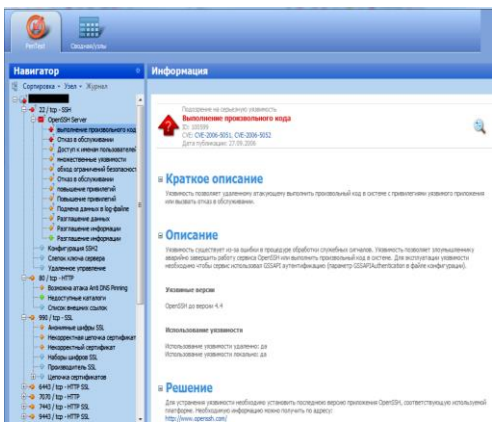


Рис. 13. Приклад сканування

Рис. 14. Звіт по PCI DSS

Критеріями завершення тесту на проникнення є отримання:

– доступу до внутрішньої мережі з боку мережі Інтернет;

– доступу до певного сегменту мережі (наприклад, сегмент АСУТП);

– привілеїв в основних інфраструктурних та інформаційних системах / сервісах (Active Directory, мережеве обладнання, СУБД, ERP і т.п.);

– доступу до певних інформаційних ресурсів;

– доступу до певної інформації (наприклад, електронна пошта директора);

– всього, до чого вдасться дотягнутися за певний час;

– першого серйозного збою, викликаного діями аудитора.

Станом на травень – червень 2016 року середня ціна початкового *pentest* коливається в районі 50$, що позитивно позначається для кінцевого замовника. Якщо ж компанія звертається за проведенням інформаційного аудиту з пентестом всього інформаційного середовища, сума може досягати сотень тисяч, а для початкового корпоративного сайту – тисяч доларів (табл. 4).

Таблиця 4

Вартість злому різних сайтів і сервісів

Послуга	Термін виконання	Вартість послуги
Аналіз відкритої інформації про організацію	от 1 до 3-х тижнів	990 грн.
Вивчення базової інформації про мережеву інфраструктуру	7 діб	1250 грн.
Аналіз соціальних мереж	3 доби	640 грн.
Аналіз вакансій, резюме на HR-сайтах	1-2 доби	200 грн.
Аналіз форумів	10 діб	1780 грн.
Сканування портів	1-2 доби	180 грн.
Визначення додатків і веб додатків	до 5 діб	1145 грн.
Визначення операційних систем	9 діб	1350 грн.
Ідентифікація мережевих маршрутизаторів і міжмережевих екранів	2-3 доби	1490 грн.
Пошук вразливостей (автоматизовані сканування і ручний аналіз)	5-10 діб	1650 грн.
Аналіз отриманої інформації і розробка сценаріїв злому	2-3 доби	1775 грн.
Проведення атак на компоненти IT інфраструктури	1 місяць	9965 грн.
Визначення взаємодії додатків і підтвердження вразливостей	5-10 діб	1890 грн.
Оформлення та презентація звіту	1-3 доби	600 грн.

В Державному університеті телекомунікацій (ДУТ) навчання за програмою «Тестування на проникнення та етичного хакінгу» здійснюється в межах міжнародного проекту «Магістерська програма нового покоління експертів в інформаційній безпеці» згідно угоди 2013-5084/001-001 про співробіт ництво між Україною та Євросоюзом за підтримки Європейської комісії: агентства з освіти, культури та аудіовізуальних засобів (EACEA, Tempus IV). Метою проекту є створення нової магістерської програми в галузі інформаційної безпеки для студентів Європейського союзу, як відповіді на актуальні проблеми пов'язані з кіберзагрозами, яка ґрунтується на успішному досвіді втілення подвійних дипломів серед студентів ЄС, Європейській кредитно-трансферної системи та взаємному визнанні вчених ступенів. Від ДУТ проект реалізується кафедрою Інформаційної та кібернетичної безпеки [4].

Навчання техніці проведення тестів на проникнення здійснюється як за спеціалізованими програмами, так й шляхом проведення командних змагань (CTF). За *першим сценарієм* найбільш відпрацьованими є курси підготовки фахівців з «Етичного хакінгу» від компаній EC-Council, Offensive Security та SANS, що дозволяють проводити тестування таких фахівців за напрямом безпеки мереж (табл. 5).

Таблиця 5

Перелік спеціалізованих програм для підготовки фахівця з *pentest*

Спеціалізована програма	**Сертифікаційний іспит**
Програмне забезпечення від компанії **EC-Council**	
Certified Ethical Hacker (CEH)	CEH, тест
Certified Security Analyst (ECSA)	ECSA, тест
Програмне забезпечення від компанії **Offensive Security**	
Penetration Testing with Kali Linux (PWK)	Offensive Security Certified Professional (OSCP)
Offensive Security Wireless Attacks (WiFu)	Offensive Security Wireless Professional (OSWP)
Cracking the Perimetr (CTP)	Offensive Security Certified Expert (OSCE)
Advanced Windows Exploitation (AWE)	Offensive Security Exploitation Expert (OSEE)
Advanced Web Attacks & Exploitation (AWAE)	Offensive Security Web Expert (OSWE)
Metasploit Unleashed (MSFU)	---
SEC504: Hacker Tools, Techniques, Exploits and Incident Handling	GIAC Certified Incident Handler (GCIH)
SEC542: Web App Penetration Testing and Ethical Hacking	GIAC Web Application Penetration Tester (GWAPT)
SEC560: Network Penetration Testing and Ethical Hacking	GIAC Penetration Tester (GPEN)
SEC567: Social Engineering for Penetration Testers	---
SEC573: Python for Penetration Testers	---
SEC580: Metasploit Kung Fu for Enterprise Pen Testing	---
SEC617: Wireless Ethical Hacking, Penetration Testing, and Defenses	GIAC Assessing and Auditing Wireless Networks (GAWN)
Програмне забезпечення від компанії **SANS**	
SEC642: Advanced Web App Penetration Testing and Ethical Hacking	---
SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
SEC760: Advanced Exploit Development for Penetration Testers	GIAC Penetration Tester (GPEN)
SEC561: Immersive Hands-On Hacking Techniques	---
SEC575: Mobile Device Security and Ethical Hacking	GIAC Mobile Device Security Analyst (GMOB)

Метою другого є оцінка вміння учасни-ків атакувати й захищати IT-системи (мережі). Навчання й здавання іспитів – online, окрім AWE и AWAE. Всі іспити – це практичні завдання. По завершенню складають звіт (англійською мовою).

Певна частина курсів є безкоштовною.

В процесі навчання застосовується низка спеціалізованих інструментів (табл. 6), які мають різну чутливість до різного роду загроз.

Таблиця 6

Стандартні інструменти, використовувані для для проведення *pentest*

Pwn Pad 	Пристрій призначений для проведення прихованого pentest. Пристрій оснащений потужним чотирьох ядерним процесором (Qualcomm Snapdragon S4 Pro, 1,5 Ггц), 7-дюймовим екраном з дозволом 1900 х 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 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. Причому від стеження не врятує навіть використання VPN, так як, наприклад, на iOS пристроях підключитися до VPN можна тільки після підключення до Wi-Fi.
Demyo power strip 	Пристрій призначений для перевірки на міцність Ethernet-, Wi-Fi- і Bluetooth-мереж. Побу-дований на базі популярного одноплатного комп'ютера Raspberry Pi і оснащений ARM-процесором 700 МГц, який можна розігнати до 1 ГГц. Також на борту є 512 Мб оперативної пам'яті, SD-карта на 32 Гб, 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. Відсутні інструменти можна доставити самостійно.

Збірку посилань за тематикою тестування на проникнення можна знайти у джерелі «The Open Penetration Testing Bookmarks Collection». Mind-карту з підбором великої кількості online-місць (EnigmaGroup, hACME Game, Hax.Tor, Exploit Exercises и т.д.), а також спеціалізованих образів, віртуальных машин з уразливостями (Damn Vulnerable Linux, Metasploitable, pWnOS тощо) для навчання – на сайті http://www.amanhardikar.com/mindmaps/Practice.png.

Висновки

1) За статистикою української компанії «Інком», зібраної в процесі реалізації проектів із створення/оновлення корпоративних мереж, в ході *pentest* тестувальникам вдається, як правлило, отримати доступ до:

- веб-сайтів – у 50% випадків;
- бізнес-програм – у 35% випадків;
- IP телефонії – у 35% випадків;
- електронної пошти – у 40% випадків;
- систем дистанційного банківського обслуговування – у 29%.

Повний контроль над інфраструктурою може бути захоплений в 25% проектів і тільки у 5% – взагалі не вдається подолати периметр.

2) У п'ятірку найбільш популярних експлойтів нині входять:

– міжмережеве виконання сценаріїв (50%);
– наявність інтерфейсів віддаленого управління (47%);
– доступна інформація про додатки (45%);
– впровадження SQL коду (63%).

3) *Найпопулярнішою уразливістю останнім часом стали прості паролі адміністраторів*. Вони мають місце у 80% проектів, інколи навіть у тих випадках, коли в організації були впроваджені політики щодо забезпечення складності паролів пересічних користувачів. *Уразливості веб-додатків* та *некоректно налаштоване обладнання* несуть за собою значно менші ризики, й тому нині вони є ключем до злому відповідно в 46% і 38% випадків.*Відсутність оновлень* сприяє успішному проведенню тестових атак у 25% компаній, а *недоліки архітектури* – в 9%.

4) Враховуючи таке, саме проведення *pentest* 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, щоб знизити можливість реалізації атак.

5) Не зважаючи на доволі часту критику *pentest*, технологія реалізації якого не може гарантувати замовнику те, що:

– тестувальник виявив усі «дірки» в системі його безпеки; а також знайдені тестувальником «дірки» не будуть колись використані для того, щоб викрасти його інформацію;

– діяльність тестувальника може бути проконтрольована, - в умовах сучасної інформаційної та кібервійни, яка ведеться проти нашої країни, завдання забезпечення безпеки інформаційних систем на ОІД й, передусім, ІТ-систем (мереж) органів влади та критичних інфраструктур (соціальних фондів та різних державних реєстрів), а також об'єктивної оцінки рівня безпеки цих структур без проведення *pentest* практично неможливо.

Література

1. Бурячок В.Л. Політика інформаційної безпеки: підручник. / В.Л. Бурячок, Р.В. Грищук, В.О. Хорошко / За заг. ред. докт. техн. наук, проф. В.О. Хорошка. – К.: ПВП «Задруга», 2014. – 222 с.

2. Бурячок В.Л. Політика інформаційної безпеки: навчальний посібник. / В.Л. Бурячок, Р.В. Грищук, В.О. Хорошко / За заг. ред. докт. техн. наук, проф. В.О. Хорошка. – К.: ПВП «Задруга», 2014. – 134 с.

3. Бурячок В.Л. Пентестінг як інструмент комплексної оцінки ефективності захисту інформації в розподілених корпоративних мережах. / В.Л. Бурячок, В.А. Козачок, Л.В. Бурячок, П.М. Складанний / Сучасний захист інформації. - 2015. - №3. С. 4 -12.

4. Бурячок В.Л. Рекомендації щодо побудови та запровадження профілю навчання «кібернетична безпека» в Україні / В.Л. Бурячок, В. М. Богуш // Безпека інформації. - 2014. Т. 20. - С. 126 – 131.

Автори статті

Киричок Роман Васильович - аспірант кафедри Інформаційної та кібернетичної безпеки, Державний університет телекомунікацій, Київ, Україна, Тел.: +38 067 153 82 27. E-mail: ikb_dut@i.ua

Складанний Павло Миколайович - аспірант кафедри Інформаційної та кібернетичної безпеки, Державний університет телекомунікацій, Київ, Україна, Тел.: +38 093 047 45 17. E-mail: ikb_dut@i.ua

Бурячок Володимир Леонідович - д.т.н., професор, завідувач кафедри Інформаційної та кібернетичної безпеки, Державний університет телекомунікацій, Київ, Україна. Тел.: +38 093 869 08 29. E-mail: ikb_dut@i.ua

Гулак Геннадій Миколайович - к.т.н., доцент, професор кафедри Інформаційної та кібернетичної безпеки, Державний університет телекомунікацій, Київ, Україна. Тел.: +38(067)244-94-49. E-mail: gena.gulak@gmail.com

Козачок Валерій Анатолійович - к.т.н., доцент, доцент кафедри Інформаційної та кібернетичної безпеки, Державний університет телекомунікацій, Київ, Україна. Тел.: +380 93 869 08 29. E-mail: ikb_dut@i.ua

Authors of the article

Kyrychok Roman Vasyl'ovych - post-graduate student, assistant of Department of Information and cyber security, State university of telecommunications, Kyiv, Ukraine. Tel.: +380 67 153 82 27. E-mail: ikb_dut@i.ua

Skladannyy Pavlo Mykolayovych - post-graduate student, assistant of Department of Information and cyber security, State university of telecommunications, Kyiv, Ukraine. Tel.: +380 93 047 45 17. E-mail: ikb_dut@i.ua

Buryachok Volodymyr Leonidovych - sciences Doctor (technic), professor, head of Department of Information and cyber security, State university of telecommunications, Kyiv, Ukraine. Tel.: +38 093 869 08 29. E-mail: ikb_dut@i.ua

Hulak Hennadiy Mykolayovych - candidate of Science (technic), associate professor, professor of Department of Information and cyber security, State university of telecommunications, Kyiv, Ukraine. Tel.: +38 067 244-94-49. E-mail: gena.gulak@gmail.com

Kozachok Valeriy Anatoliyovych - candidate of Science (technic), associate professor, associate Professor of Department of Information and cyber security, State university of telecommunications, Kyiv, Ukraine. Tel.: +380 93 047 45 17. E-mail: ikb_dut@i.ua

Дата надходження в редакцію: 01.07.2016 р. Рецензент: д.т.н., с.н.с. В.О. Наконечний