СИСТЕМЫ И ПРОЦЕССЫ УПРАВЛЕНИЯ

УДК 004.056.53

БЕЗПЕКА ІНТЕРНЕТ РЕСУРСІВ: АНАЛІЗ РОЗПОВСЮДЖЕНОСТІ ЗАГРОЗ ТА ТЕХНОЛОГІЇ ЗАХИСТУ

СЛОБОДЯНЮК О.В., ХАХАНОВА А.В., КОМОЛОВ Д.И.

Описуються основні підходи до класифікації відомих вразливостей веб-ресурсів. Аналізується активність найбільш розповсюджених типів загроз на основі звітів компаній, що займаються моніторингом інцидентів порушення безпеки веб-ресурсів. Розглядаються основні технології захисту від можливих реалізацій погроз.

Ключові слова: уразливість, загроза, OWASP, WASC, WAF.

Keywords*:* vulnerability, threat, OWASP, WASC, WAF.

Вступ

Питання захисту веб-ресурсів від несанкціонованих втручань ззовні є однією із найбільших проблем забезпечення їх сталого функціонування. Сучасний веб-ресурс являє собою досить складну програмну структуру, що включає у себе цілий ряд технологій із модульним підходом та можливістю постійної модифікації й вдосконалення. Як наслідок цього, більшість веб-сайтів та веб-сервісів характеризуються цілим рядом вразливостей, через які зловмисники мають реальні можливості проводити атаки на найрізноманітніші сайти із використанням досить широкого інструментарію. Дані вразливості викликані як ненавмисно допущеними помилками розробниками на стадії проектування, так і недосконалістю технологій, що були використані при створенні ресурсу. Окремо можна виділити зумисно допущені помилки, які генеруються недобросовісними розробниками, планують у подальшому використати їх для несанкціонованого втручання у роботу ресурсу. Як правило усі системи керування вмістом (CMS) та фреймворки, що використовуються при створенні веб-сайтів, мають великі спільноти шанувальників, завдяки яким вдається вчасно локалізувати та виправити помилки у підсистемах безпеки. Однак часто буває так, що служби підтримки ресурсів вчасно не проводять заходи щодо оновлення програмних модулів, не забезпечують належного контролю за даними, не виконують перевірки доступу та інше. Більшість вразливостей, що використовуються середньостатистичним зловмисником, не є архісклад-

дними і не вимагають високої кваліфікації для їх застосування.

1. Ризики безпеки веб-застосунків

При проведенні аналізу рівня захищеності веб-ресурсу найчастіше використовується поняття ризику та вразливості. Так, коли говорять про нездатність інформаційної системи протидіяти зовнішнім втручанням або протистояти реалізації певних загроз, то це мається на увазі поняття вразливості (англ. vulnerability) [5]. Під ризиком, згідно з документом «Основні поняття. НД ТЗІ 1.1-003-99: «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» розуміють функцію ймовірності реалізації певної загрози, виду і величини завданих збитків [5]. Також дуже часто організації, що займаються моніторингом та обліком інцидентів, пов'язаних з кібербезпекою, використовують поняття загрози (англ. threat).

Збором відомостей, моніторингом активності та класифікацією відомих чи нових вразливостей займається цілий ряд організацій та об'єднань, серед яких варто виділити відкритий проект забезпечення безпеки веб-застосунків (Open Web Application Security Project, OWASP), консорціум безпеки веб- застосунків (Web Application Security Consortium, WASC), науково-дослідницький центр корпорації MITRE (National Cybersecurity Center of Excellence's, NCCoE's)), центр комп'ютерної безпеки університету Карнегі Меллон (Computer Emergency Response Team Coordination Center, CERT/CC), центр ресурсів комп'ютерної безпеки уряду США (Computer Security Resource Center, CSRC) та інші. Звичайно кожна серйозна організація, що займається питаннями інформаційної безпеки веб-застосунків, має свої розроблені методики виявлення загроз та протидії ризикам їхніх впливів. Однак переважна більшість користуються класифікаторами OWASP, WASC TD та CWE/SANS.

2. Класифікація ризиків OWASP

OWASP являє собою проект забезпечення безпеки веб- застосунків. Спільнота OWASP є повністю відкритою й ставить собі за мету сприяння організаціям у розробці, придбанні та підтримці застосунків, безпеці яких можна довіряти. Структурно спільнота складається з корпорацій, освітніх організацій та приватних осіб зі всього світу. Для вирішення основних задач по збору й класифікації вразливостей веб-застосунків члени спільноти працюють над створенням наукових статей, навчальних посібників, документації, інструментів та технологій, які потім викладають у вільний доступ. Також OWASP пропонує безкоштовний доступ до інструментів та стандартів безпеки застосунків, детальних рекомендацій щодо тестування,

розробки та аналізу безпеки програм.

Один раз на три роки спільнота публікує зведений рейтинг ТОП-10 [7] найнебезпечніших ризиків (вразливостей), який відображає сучасні тенденції безпеки веб-застосунків. OWASP TOP-10 – це інформаційний документ, який широко використовується багатьма організаціями. Він актуальний в рамках програм винагород за виявлені вразливості (bug bounty programs), а також для класифікації вразливостей за рівнем небезпеки.

Остання версія документу була опублікована у 2017 році і містить такі типи найнебезпечніших ризиків веб-застосунків:

1) Вставка ін'єкцій (A1:2017 – Injection).
2) Некоректна аутентифікація та управління сеансами (A2:2017 – Broken Authentication).
3) Витік критичних даних (A3:2017 – Sensitive Data Exposure).
4) Вставка XML інструкцій (A4:2017 – XML External Entities (XXE).
5) Порушений контроль доступу (A5:2017 – Broken Access Control).
6) Неправильна конфігурація безпеки (A6:2017 – Security Misconfiguration).
7) Міжсайтове виконання сценаріїв (A7:2017 – Cross-Site Scripting (XSS).
8) Небезпечна десеріалізація (A8:2017 – Insecure Deserialization).
9) Використання компонентів з відомими вразливостями (A9:2017 – Using Components with Known Vulnerabilities).
10) Недостатнє журналювання та моніторинг (A10:2017 – Insufficient Logging&Monitoring) [7].

Якщо провести кількісний аналіз зафіксованих протягом 2017 року вразливостей у базі OWASP (рис. 1), то можна бачити, що кількість випадків міжсайтового виконання сценаріїв сумарно перевищує усі інші разом взяті типи вразливостей і доходить до 2 млн.

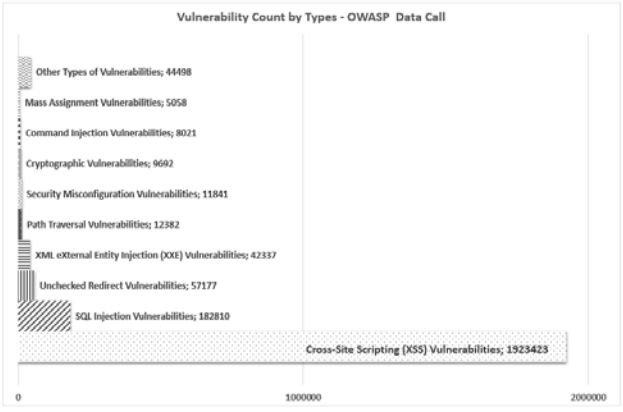

Рис. 1. Кількість зафіксованих у 2017 році вразливостей за їхніми типами згідно з даними OWASP

Дана статистика кардинально відрізняється від позицій у ТОП – 10, оскільки при складанні рейтингу OWASP використовує методологію, що основана на методиці оцінки ризиків. Для кожної позиції рейтингу оцінюється типовий ризик, який кожне слабке місце може викликати у типовому веб-застосунку, розглядаючи фактори, що впливають на ймовірність та на наслідки для кожного слабкого місця. Потім складається рейтинг Топ-10 відповідно до слабких місць, що, як правило, стають причиною найбільш значущих ризиків для застосунку. Методика оцінки ризиків OWASP визначає численні фактори для розрахунку ризиків визначеної уразливості. Однак Топ 10 призначений для розгляду загальних випадків, а не конкретних вразливостей у реальному застосунку. Саме тому OWASP ніколи не прагне досягти точності, аналогічної тій, яку можуть досягти власники систем при розрахунку ризиків для своїх застосунків. Зазначена методика включає в себе три фактори, що впливають на ймовірність для кожного слабкого місця (поширеність, можливість виявлення та легкість вторгнення), та один фактор, що впливає на наслідки (технічні наслідки). Поширеність слабкого місця – це фактор, який, як правило, не потрібно розраховувати. Дані щодо поширеності отримують від різних організацій і потім обраховують з цих даних середнє значення для визначення ймовірності їх включення у Топ-10 за поширеністю. Потім ці дані поєднують з іншими двома факторами ймовірності (можливість виявлення та легкість вторгнення) з метою розрахунку рейтингу ймовірності кожного слабкого місця. Після цього отримані результати множать на розраховані технічні наслідки для кожної позиції і, як результат, отримують загальний рейтинг ризиків по кожній позиції Топ-10 [7].

3. Класифікація загроз WASD

The WASC Threat Classification – це результати спільної роботи членів консорціуму безпеки вебзастосунків, які спрямовані на опис та упорядкування відомих загроз безпеки веб-сайтів. Даний проект був створений для розробки та популяризації стандартної термінології опису зазначених проблем. Це дає можливість розробникам застосунків, спеціалістам в області безпеки, виробникам програмних продуктів та аудиторам використовувати спільну термінологічну базу для взаємодії. Цілями учасників консорціуму є: визначення всіх відомих класів атак на вебзастосунки; узгодження назв для кожного з класів; розробка структурованого підходу до класифікації атак; створення документації, що містить загальний опис кожного з класів.

Згідно з класифікатором атаки на веб-застосунки поділяються на:

1. Аутентифікація (Authentication) – атаки, які спрямовані на використовувані веб-застосунком методи перевірки ідентифікатора користувача, служби або програми. Аутентифікація використ-

товує як мінімум один з трьох механізмів (факторів): «щось, що ми маємо», «щось, що ми знаємо» або «щось, що ми є». Атаки даного класу спрямовані на обхід або експлуатацію вразливостей в механізмах реалізації аутентифікації веб-серверів.

2. Авторизація (Authorization) – атаки, що направлені на методи, які використовуються веб-сервером для визначення того, чи має користувач, служба або застосунок необхідні для виконання операції зміни дозволів. Багато веб-сайтів дозволяють тільки певним користувачам отримувати доступ до деякого вмісту або функцій програми. Доступ іншим користувачам повинен бути обмежений. Використовуючи різні техніки, зловмисник може підвищити свої привілеї і отримати доступ до захищених ресурсів.

3. Атаки на клієнтів (Client-side Attacks) – атаки на користувачів веб-сервера. Під час відвідування сайту між користувачем і сервером встановлюються довірчі відносини як в технологічному, так і в психологічному аспекті. Користувач очікує, що сайт буде надавати йому легітимний вміст. Крім того, користувач не очікує атак з боку сайту. Експлуатуючи цю довіру, зловмисник може використовувати різні методи для проведення атак на клієнтів сервера.

4. Виконання коду (Command Execution) – клас атак, які спрямовані на виконання коду на веб-сервері. Всі сервери використовують дані, що були надіслані користувачем при обробці запитів. Часто ці дані використовуються при складанні команд, що застосовуються для генерації динамічного вмісту. Якщо при розробці не враховуються вимоги безпеки, зловмисник отримує можливість модифікувати виконувані команди.

5. Розголошення інформації (Information Disclosure) – атаки, що спрямовані на отримання додаткової інформації про веб-застосунок. Використовуючи ці вразливості, зловмисник може визначити використовувані дистрибутиви, номери версій клієнта й сервера, а також встановлені оновлення. В інших випадках в інформації, що витікає, можуть міститися відомості про розташування тимчасових файлів або резервних копій. У багатьох випадках ці дані не потрібні для роботи користувача. Більшість серверів надають доступ до надмірного обсягу даних, однак необхідно мінімізувати обсяг службової інформації. Чим більші знання про програму буде мати у своєму розпорядженні зловмисник, тим легше йому буде скомпрометувати систему.

6. Логічні атаки (Logical Attacks) – спрямовані на експлуатацію функцій застосунка або логіки його функціонування. Логіка застосунка – це очікуваний процес функціонування програми при виконанні певних дій. Як приклади можна навести відновлення паролів, реєстрацію облікових записів, аукціонні торги, транзакції в системах електронної комерції. Застосунок може вимагати від користувача коректного виконання декількох послідовних дій для певного завдання. Зловмисник може обійти або використовувати ці механізми в своїх цілях [9].

На відміну від OWASP консорціум не веде статистику активності та кількості проведених на веб-ресурси атак. Однак таким займаються організації-члени консорціуму. Однією з них є компанія Positive Technologies. Аналіз звіту за 2016 рік [6] показує, що кожен третій виявлений недолік відноситься до високого класу небезпеки (рис. 2).

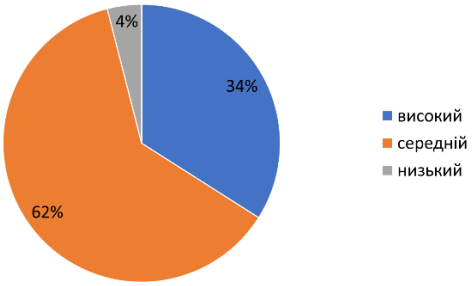

Рис. 2. Доля вразливостей різного ступеня ризику

Хоча більшість виявлених вразливостей характеризуються середнім рівнем ризику (62%), а 4% віднесені до низького рівня ризику, але абсолютно усі застосунки, які були досліджені, містили щонайменше одну вразливість середнього рівня небезпеки. Розподіл знайдених спеціалістами компанії вразливостей різного класу небезпеки веб-застосунках протягом 2011-2015 років показано на рис. 3.

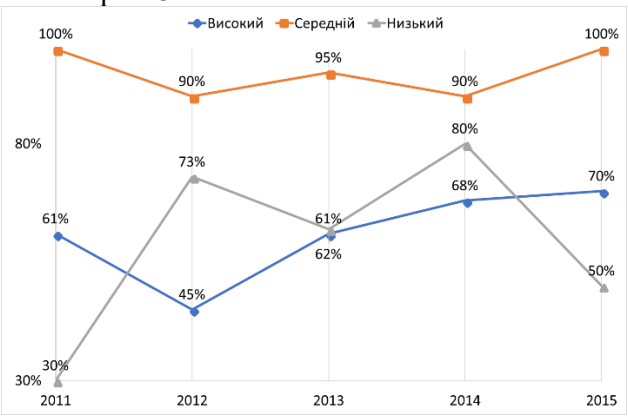

Рис. 3. Доля сайтів із вразливостями різного ступеня ризику

Незважаючи на те, що дані досліджень не є достатньо репрезентативними через відносно невелику кількість проаналізованих веб-ресурсів, але вони гарно показують загальну тенденцію зростання класу небезпеки вразливостей, що ідентифікуються спеціалістами із кібербезпеки. Це викликано як різким зростанням складності технологій, що використовуються під час розробки сучасних веб-застосунків (зростає ймовірність

виникнення помилки, використання засобів розробки із непідтвердженим рівнем безпеки тощо), так і створенням більш ефективних інструментів несанкціонованого втручання у роботу програмних систем.

4. Методи та підходи до захисту веб-застосунків

Вислів «Попереджений – значить озброєний!» повністю працює в галузі безпеки веб-застосунків та веб-ресурсів в цілому. Тому найпершим засобом захисту від ризиків є періодичне проведення аудиту безпеки та своєчасне оновлення програмних модулів.

Існує декілька методологій проведення аудиту застосунку. Вони є найбільш ефективними у окремі періоди життєвого циклу програмного забезпечення. Кожен з них представляє певні цикли часу, зусилля, витрати щодо знаходження цих уразливостей.

1) Метод «білої скриньки» або аудит коду. Особа, що проводить аудит, глибоко розуміє застосунок та вручну переглядає початковий код, записуючи вразливості безпеки. Аудитору надається доступна вичерпна інформація про структуру застосунку, особливості побудови всіх його елементів та забезпечується коректність взаємодії його частин.

2) Метод «чорної скриньки». Даний вид аудиту передбачає те, що інформація про досліджуваний об'єкт повністю відсутня. Функції об'єкта можна визначити лише за реакцією його на зовнішні фактори. До початку аудиту за цим методом аудитор має визначити внутрішню архітектуру. Саме тестування проводиться за допомогою імітаційного моделювання відомих типів атак на веб-ресурси.

3) Інструментарій. Аудит проводиться із застосуванням автоматизованих інструментів, які перевіряють наявність недоліків та дефектів безпеки, часто з більшою позитивною швидкістю, ніж залучення людини. До такого інструментарію відносяться сканери, брандмауери, антивіруси, фільтри тощо [1].

Для організації захисту інформаційної інфраструктури використовується велика кількість типів захисних рішень – Firewall, IPS/IDS (система запобігання вторгнень/система виявлення вторгнень), NGFW (Next Generation Firewall), WAF (Web-Application Firewall). Однак сьогодні понад 80% атак експлуатують уразливості саме веб-застосунків, а не мережевої архітектури. Тому класичні системи захисту мереж виявляються малоефективними проти сучасних кіберзагроз. До того ж сьогодні існує величезна кількість веб-застосунків (кожен з яких потенційно може містити в собі певні вразливості), тобто загальна кількість вразливостей набагато більша, ніж кількість сигнатур в базах сучасних систем запобігання вторгнень. За оцінками багатьох експертів з кібербезпеки, саме проникнення через веб-застосунки останнім часом стають основним вектором атак на корпоративні мережі, причому традиційні системи безпеки, такі як брандмауер та антивірусна система, не здатні ефективно запобігати подібним атакам. Для надійного захисту необхідний кардинально інший підхід: з глибоким аналізом змісту пакетів і хорошим знанням структури веб-застосунків, включаючи URL-параметри, форми введення даних і ін. Таким умовам задовольняє Web Firewall Application – брандмауер для застосунків, які здійснюють передачу даних через HTTP і HTTPS [3].

Принцип дії WAF нагадує прозорий проксі-сервер або міст. Підтримується, як правило, також реплікація трафіка. Для виявлення атак WAF застосовує як сигнатурний, так і поведінковий підходи. Другий метод також дуже важливий, оскільки для атак на веб-застосунок кіберзлочинці можуть застосовувати уразливості нульового дня (0day vulnerability), що зводить до нуля ефективність сигнатурного аналізу. Основним компонентом WAF є модуль машинного навчання, який призначений для створення еталонної моделі комунікації з об'єктом захисту. При цьому передбачається, що при проведенні першого раунду перевірки вразливості веб-застосунку не експлуатуються. Таким чином, формується список дозволених ідентифікаторів доступу і будується модель нормального функціонування застосунку. На відміну від класичних брандмауерів, які генерують великі обсяги помилкових спрацьовувань на різні підозрілі події, WAF здатний аналізувати тисячі подій і будувати ланцюг розвитку атаки – від першого етапу до останнього.

Однак не все так райдужно, як би хотілося, і з WAF. Так, в силу своїх функціональних обмежень, він не здатний захистити веб-застосунок від усіх можливих вразливостей. WAF не видаляє вразливість, а лише (частково) закриває вектор атаки.

Висновки

Аналізуючи ситуацію навколо питань безпеки веб-ресурсів, можна зробити висновок, що даний напрямок є наразі найбільшою «гарячою точкою» в інформаційній безпеці загалом. Зростання у геометричній прогресії кількості типів нових вразливостей та офіційно зафіксованих успішних атак на веб-ресурси може свідчити про те, що даний напрямок ще доволі довго залишатиметься найбільш популярним у кіберзлочинців та спеціалістів із комп'ютерної безпеки.

На превеликий жаль, доводиться констатувати той факт, що до цих пір не запропоновано більш ефективної технології захисту, ніж регулярне проведення аудиту вразливостей. При цьому найбільшу якість може гарантувати лише ручна перевірка за складеними чек-листами і залученням відповідних спеціалістів. Наприклад, на популярних Bug Bounty платформах (hackerOne, BugCrowd, Synack, Zerocopter, Cobalt, Intigrity, HackenProof та інші).

Література: 1. *Безпека* додатків [Електронний ресурс]. 2018. Режим доступу до ресурсу: https://bit.ly/2LL77JC. **2.** *Годовой* отчет Cisco по информационной безопасности [Електронний ресурс]. 2017. Режим доступу до ресурсу: https://www.cisco.com/c/ru_ru/products/security/security-reports.html. **3.** *Захист* веб-додатків: чому це важливо? [Електронний ресурс]. 2016. Режим доступу до ресурсу: https://itbiz.ua/ua/zashhita-veb-prilozheniy-pochemu-yeto-vazhn. **4.** *Основні* поняття. НД ТЗІ 1.1-003-99: Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. [Електронний ресурс] // Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. 1999. Режим доступу: http://iszzi.kpi.ua/images/Info_bezpeka/ND_TZI/4_НД_ТЗІ_1.1-003-99.pdf. **5.** *Поповский В.В.* Защита информации в телекоммуникационных системах: учебник / В.В. Поповский, А.В. Персиков. Х.: ООО "Компания СМИТ", 2006. Т. 2. 292 с. **6.** *Уязвимости* веб - приложений [Електронний ресурс] // Positive Technologies. 2016. https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Web-Vulnerability-2016-rus.pdf. **7.** *OWASP* Top 10 – 2017. The Ten Most Critical Web Application Security Risks. [Електронний ресурс]. 2017. https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf. **8.** *Prakhar P.* Mastering Modern Web Penetration Testing / Prasad Prakhar. – BIRMINGHAM - MUMBAI: Packt Publishing, 2016. 298 с. **9.** The WASC Threat Classification v2.0 [Електронний ресурс] // WEB APPLICATION SECURITY CONSORTIUM – Режим доступу до ресурсу: http://projects.webappsec.org/f/WASC-TC-v2_0.pdf. **9.** *Yaworski P.* Web Hacking 101. How to Make Money Hacking Ethically [Електронний ресурс] / Peter Yaworski // Lean Publishing. 2017. Режим доступу до ресурсу: http://leanpub.com/web-hacking-101.

Транслітерований список літератури

1. Bezpeka dodatkiv [Elektronnij resurs]. – 2018. – Rezhim dostupu do resursu: https://bit.ly/2LL77JC.
2. Godovoj otchet Cisco po informacionnoj bezopasnosti [Elektronnij resurs]. – 2017. – Rezhim dostupu do resursu: https://www.cisco.com/c/ru_ru/products/security/security-reports.html.
3. Zahist veb-dodatkiv: chomu ce vazhlivo? [Elektronnij resurs]. – 2016. – Rezhim dostupu do resursu: https://itbiz.ua/ua/zashhita-veb-prilozheniy-pochemu-yeto-vazhn.
4. Osnovni ponjattja. ND TZI 1.1-003-99: Terminologija v galuzi zahistu informacij v komp'juternih sistemah vid ne-sankcionovanogo dostupu. [Elektronnij resurs] // Kiïv: Depa-rtament special'nih telekomunikacijnih sistem ta zahistu informacij Sluzhbi bezpeki Ukraïni. – 1999. – Rezhim dostu-pu do resursu: http://iszzi.kpi.ua/images/Info_bezpeka/ND_TZI/4_ND_TZI_1.1-003-99.pdf.
5. Popovskij V.V. Zashhita informacii v telekommunikacionnyh sistemah: uchebnik / V.V. Popovskij, A.V. Persikov. – H.: OOO "Kompanija SMIT", 2006. T. 2. – 292 s.
6. Ujazvimosti veb prilozhenij [Elektronnij resurs] // Positive Technologies. – 2016. – Rezhim dostupu do resursu: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Web-Vulnerability-2016-rus.pdf.
7. OWASP Top 10 – 2017. The Ten Most Critical Web Appli-cation Security Risks. [Elektronnij resurs]. – 2017. – Rezhim dostupu do resursu: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf.
8. Prakhar P. Mastering Modern Web Penetration Testing / Prasad Prakhar. – BIRMINGHAM - MUMBAI: Packt Publishing, 2016. – 298 s.
9. The WASC Threat Classification v2.0 [Elektronnij resurs] // WEB APPLICATION SECURITY CONSORTIUM – Rezhim dostupu do resursu: http://projects.webappsec.org/f/WASC-TC-v2_0.pdf.
10. Yaworski P. Web Hacking 101. How to Make Money Hacking Ethically [Elektronnij resurs] / Peter Yaworski // Lean Publishing. – 2017. – Rezhim dostupu do resursu: http://leanpub.com/web-hacking-101.

Надійшла до редколегії 06.06.2018

Рецензент: д-р техн. наук, проф. Бараннік В.В.

Слободянюк Олександр Васильович, канд. техн. наук, доцент кафедри інформатики Кам'янець-Подільського національного університету імені Івана Огієнка, Кам'янець-Подільський, e-mail: slobodyanyuk.olexandr@kpnu.edu.ua.

Хаханова Анна Володимирівна, канд, техн. наук, доцент, докторант кафедри АПОТ ХНУРЕ. Наукові інтереси: обробка інформації. Адреса: Україна, 61166, Харків, пр. Науки, 14. E-mail: Ann.hahanova@gmail.com.

Комолов Дмитро Іванович, канд. техн. наук, старший викладач кафедри ІМІ ХНУРЕ. Наукові інтереси: обробка інформації. Адреса: Україна, 61166, Харків, пр. Науки, 14, e-mail: elsdefan@gmail.com.

Slobodyanyuk Oleksandr, PhD, Associate Professor at Kamianets-Podilskyi National Ivan Ohiienko University, e-mail: slobodyanyuk.olexandr@kpnu.edu.ua

Hahanova Anna, Candidate of Technical Science, docent, post doc, Design Automation Department, Kharkov National University of Radioelectronics. Scientific interests: processing of information. Address: Ukraine, 61166, Kharkiv, Nauki Ave, 14, e-mail: Ann.Hahanova@gmail.com.

Komolov Dmitry Ivanovich, PhD, Senior Lecturer of the Department of INI, Kharkiv National University of Radioelectronics. Scientific interests: processing of information. Address: 61166, Kharkiv, avenue. Sciences 14, e-mail: elsdefan@gmail.com