УДК 004.056
DOI: 10.31673/2409-7292.2021.014146

Васильченко Д.І., Лавровський І.М.

ОГЛЯД ТИПОВИХ УРАЗЛИВОСТЕЙ WEB-САЙТІВ ОРГАНІЗАЦІЙ У 2019-2020 РОЦІ

У даній роботі наведено відомості про основні веб-атаки на веб-сайт будь-якої організації. Проаналізовано статистику веб-атак за останні роки та уразливості, які дозволяють проведення цих веб-атак. Запропоновано рекомендації щодо захисту від основних веб-атак та захисту веб-сайту в цілому, яких необхідно дотримуватись задля уникнення фатальних наслідків у разі атаки зловмисника.

Ключові слова: веб-атака, веб-сайт, уразливості веб-сайту, пошук уразливостей, захист веб-сайту.

Вступ.

Разом зі збільшенням популярності Інтернету, зростає й інтернет-злочинність та з'являються кіберзлочинці. Згідно зі звітом SiteLock Website Security Insider [1], існує 113 мільйонів веб-сайтів, які мають уразливі місця в системі безпеки, та, в середньому, веб-сайт зазнає 50 спроб атаки на день. Майже з кожним днем їх кількість зростає. Кіберзлочинці створюють спеціалізовані інструменти, які шукають в Інтернеті загальні та розголошені уразливості. Після виявлення, знайдені уразливості використовуються для викрадення даних, розповсюдження шкідливого вмісту або введення зіпсованого та спам-вмісту на уразливий сайт.

Нині, компанії, які займаються інформаційною безпекою та захистом інформації, дедалі частіше розміщують на своїх офіційних сторінках інформацію щодо виявлення ними нових уразливостей у програмному забезпеченні веб-сайтів. Допомагають їм в цьому як працівники зі служби захисту інформації, так й, так звані, білі хакери, які повідомляють розробникам веб-сайту про знайдену уразливість, а не використовують її у своїх цілях.

Мета статті – аналіз сучасних веб-атак, які спрямовані на уразливості веб-сайтів.

Викладення основного матеріалу.

На сьогоднішній день, веб-атаки є найбільш поширеною та руйнівною загрозою безпеки, з якою стикається організація. Вони використовують різноманітні уразливості (дірки) в системі веб-сайту, намагаючись порушити його функціонування, отримати контроль над ним, або виконати з ним або його користувачами будь-які інші злочинні дії. Існує багато різновидів веб-атак, які використовують зловмисники. У даній статті розглянемо такі атаки, як: ін'єкції, міжсайтовий скриптинг, DoS та DDoS, шкідливе ПЗ, переповнення буферу, IP spoofing, Broken Authentication, мережева розвідка, брутфорс паролів, прогнозування сеансу, Man-In-the-Middle, Insecure deserialization, Cross-Site Request Forgery.

1) Ін'єкції

SQL ін'єкція. Цей тип атак складається з "ін'єкції" запиту SQL через вхідні дані від клієнта до програми, вставляючи шкідливий код у рядки, які згодом передаються екземпляру SQL Server для аналізу та виконання. Успішна програма SQL ін'єкцій може читати конфіденційні дані з БД, модифікувати дані БД, виконувати адміністративні операції з БД, відновлювати вміст даного файлу, який присутній у файловій системі СУБД, та в деяких випадках видавати команди операційній системі [3].

LDAP ін'єкція. LDAP ін'єкція являє собою техніку атаки, яка застосовується для використання веб-сайтів, які створюють оператори LDAP із введеного користувачем вводу. Веб-програми можуть використовувати введені користувачем дані задля створення власних операторів LDAP для динамічних запитів веб-сторінок. Коли веб-програмі не вдається належним чином виявити введені користувачем дані, зловмисник може змінити побудову оператора LDAP. Коли зловмисник зможе змінити оператор LDAP, процес буде виконуватися з тими самими дозволами, що й компонент, який виконав команду [4].

PHP ін'єкція. Даний тип ін’єкцій являє собою один з можливих варіантів взлому веб-сайту, який працює на мові PHP. Коли розробник використовує функцію PHP eval (), то зловмисник може змінювати та вводити код у додаток [5].

XPath ін'єкція. Дані, що зберігаються у XML, можна запитувати через XPath, який концептуально схожий на SQL. Це також мова запитів, яка використовується для пошуку конкретних елементів у документі XML. Тут немає дозволів на рівень доступу, та можна посилатися майже на будь-яку частину документа XML, на відміну від SQL, який дозволяє обмеження на БД, таблиці або стовпці.

SSI ін’єкція. Дана ін’єкція являє собою експлойт на стороні сервера, який дозволяє зловмисникові надсилати код у додаток, який виконується пізніше локально веб-сервером. Цей тип атак може бути успішним лише тоді, коли веб-сервер дозволяє виконання SSI без належної перевірки [6].

2) Міжсайтовий скриптинг

XSS виникає, коли користувач вводить шкідливий сценарій на веб-сайт. Потім зловмисний сценарій запускатиметься у веб-браузері жертви, намагаючись викрасти інформацію про користувача, таку як: облікові дані, файли cookie та інші конфіденційні дані. Щоб уникнути цих атак, веб-розробник повинен переконатись, що введені користувачем дані перевіряються та кодуються, перш ніж виводити це як запит.

3) DoS та DDoS

Атака на відмову в обслуговуванні (DoS) являє собою атаку, яка має на меті перешкодити доступ до служби законним користувачам. Атака може бути націлена на будь-яких потенційних користувачів або, зокрема, на одного користувача. Наприклад, DoS атака може бути націлена на пристрій однієї людини, щоб перешкодити їй отримати доступ до Інтернету, або на веб-сайт, щоб заборонити доступ усім відвідувачам [7].

4) Шкідливе програмне забезпечення

Шкідливе ПЗ призначене для заподіяння шкоди. Щоб продовжувати таємно працювати, шкідливе ПЗ може бути спроектовано для паразитного існування в межах програми чи системи. Існує багато типів шкідливих програм, які намагаються порушити нормальну роботу комп’ютера, веб-сайту, веб-програми або мережі. До них можна віднести: Вірус, Троянський кінь, Шпигунське ПЗ, Рекламне ПЗ, Руткіт [8].

5) Переповнення буферу

Переповнення буфера відбувається, коли в буфер фіксованої довжини поміщається більше даних, ніж буфер може обробити. Додаткова інформація, яка повинна кудись піти, може перейти в сусідній простір пам’яті, пошкодивши або перезаписавши дані, що зберігаються в цьому просторі. Це переповнення зазвичай призводить до збою системи, але це також створює можливість для зловмисника запускати довільний код або маніпулювати помилками кодування для спонукання до зловмисних дій [9].

6) IP spoofing

Підробка IP дозволяє зловмиснику змінити вихідну IP-адресу заголовка пакета на підроблену IP-адресу. Зловмисник робить це, перехоплюючи IP-пакет та модифікуючи його, перш ніж відправити його за призначенням. Це означає, що IP-адреса виглядає так, ніби вона надіслана з надійного джерела - оригінальної IP-адреси, одночасно маскуючи її справжнє джерело [10].

7) Broken authentication

Такий тип атак, як «порушена аутентифікація» стосується не лише зловживання обліковими даними (наприклад, використання викрадених імен користувачів та паролів), як це можна інтерпретувати, але також стосується атак, що використовують управління сеансами (наприклад, викрадення сеансів, атаки фіксації), що дає право зловмисникам діяти від імені видаваного за себе користувача.

8) Мережева розвідка

Мережева розвідка – це великомасштабні дії по вивченню інформації про мережу з використанням доступної інформації та додатків. Коли хакери намагаються проникнути в

будь-яку мережу, то перед атакою вони повинні дізнатися максимум інформації про мережу. Розвідка може відбуватися у формі запитів DNS-сервера, сканування діапазону IP-адрес та сканування портів. Запити DNS-сервера можуть дати інформацію про те, хто має власний домен та які адреси були призначені цьому домену. Нарешті, хакери можуть вивчити характеристики додатків, що виконуються на хостах. Ця інформація буде корисна при спробі хакера порушити роботу системи.

9) Брутфорс паролів

Атака грубої сили являє собою криптографічний злом, який покладається на вгадування можливих комбінацій цільового пароля, поки не буде виявлений правильний пароль. Чим довший пароль, тим більше комбінацій потрібно перевірити. Атака грубої сили може зайняти багато часу, але якщо пароль слабкий, то це може зайняти секунди майже без зусиль. Брутфорс зазвичай використовуються для отримання особистої інформації, наприклад паролів, парольних фраз, імен користувачів та персональних ідентифікаційних номерів [11].

10) Прогнозування сеансу

Прогнозування сеансу або ідентифікаційних даних (також відоме як викрадення сеансу) – це метод викрадення чи видання себе за авторизованого користувача веб-сайту. За допомогою передбачення сеансу/облікових даних зловмисник визначає або вгадує унікальне значення, яке ідентифікує певний сеанс або користувача. Також відомі як викрадення сеансу, такі види атак дають зловмисникам можливість надсилати запити веб-сайтів із порушеними привілеями користувача.

11) Man-in-the-Middle

Атака "людина посередині" є типом атаки підслуховування, коли зловмисники переривають існуючу розмову або передачу даних. Вставивши себе в "середину" передачі, зловмисники прикидаються законними учасниками. Це дозволяє зловмиснику перехоплювати інформацію та дані будь-якої зі сторін, одночасно надсилаючи шкідливі посилання або іншу інформацію обом законним учасникам. Під час нападу середній учасник маніпулює розмовою, невідомою жодному з двох законних учасників, діючи для отримання конфіденційної інформації та іншим чином заподіюючи шкоду.

12) Insecure deserialization

Серіалізація являє собою процес перетворення складних структур даних, таких як об'єкти та їх поля, у "більш рівний" формат, який можна надсилати та приймати у вигляді послідовного потоку байтів. У той час, десеріалізація є процесом відновлення цього байтового потоку до повністю функціональної копії вихідного об’єкта в точному стані, як він був серіалізований. Тоді логіка веб-сайту може взаємодіяти з цим десеріалізованим об’єктом, як й з будь-яким іншим об’єктом. Небезпечна десеріалізація – це коли веб-сайт десеріалізує керовані користувачем дані. Це потенційно дозволяє зловмиснику маніпулювати серіалізованими об'єктами для передачі шкідливих даних у код програми [12].

13) Cross-Site Request Forgery

Атака на підробку міжсайтових запитів (CSRF) має на меті виконати операцію на веб-сайті від імені користувача без його явної згоди. Загалом, атака не викрадає безпосередньо особу користувача, але використовує користувача, щоб здійснити дію без його волі. Наприклад, вона може змусити користувача змінити свою електронну адресу або пароль у своєму профілі, або навіть здійснити переказ грошей [13].

Тенденції поширення веб-атак у 2019-2020 р.р.

Згідно статистики за 2019 рік можна сказати, що рівень захищеності веб-сайтів продовжує поступово зростати, але все ще залишається досить низьким. Несанкціонований доступ можливий на 39% веб-сайтів. Крім того, в 2019 році повний контроль над системою був отриманий в 16% веб-додатків, а в 8% систем повний контроль над сервером веб-додатку дозволяв проводити атаки на локальну мережу організації. В середньому, на одну систему припадають 22 уразливості, чотири з яких мають високий рівень ризику [14].

Дані щодо захищеності веб-сайтів організацій у різних сферах наведено на рис. 1.

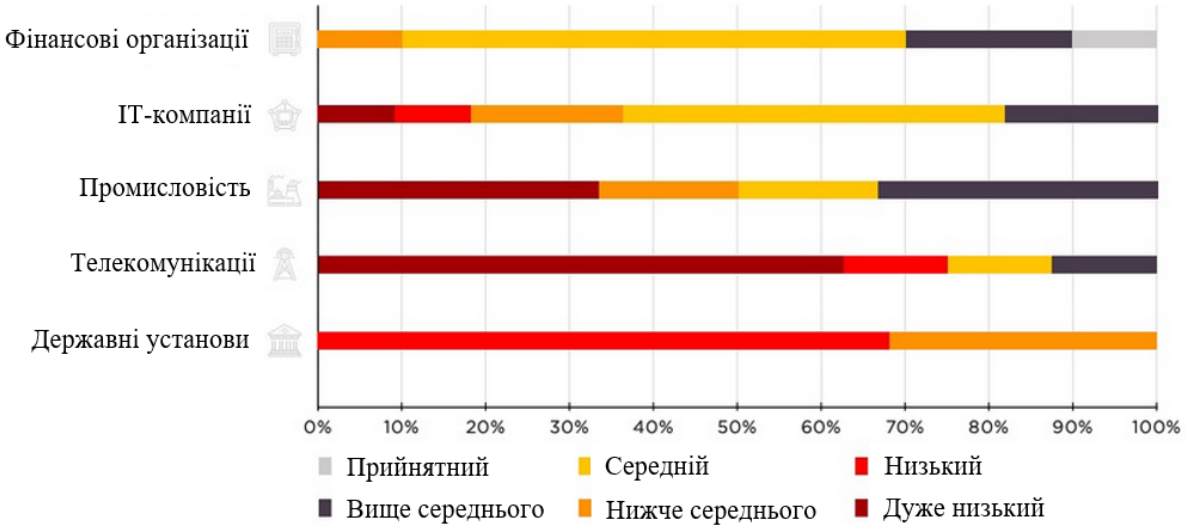

Рис. 1. Рівень веб-захищеності організацій

Згідно цієї статистики можна сказати, що найбільш захищеними є фінансові організації, у той час, коли організації у сфері телекомунікацій, переважно, мають дуже низьку захищеність. Найпоширеніші уразливості за списком OWASP Top 10 наведено на рис. 2.

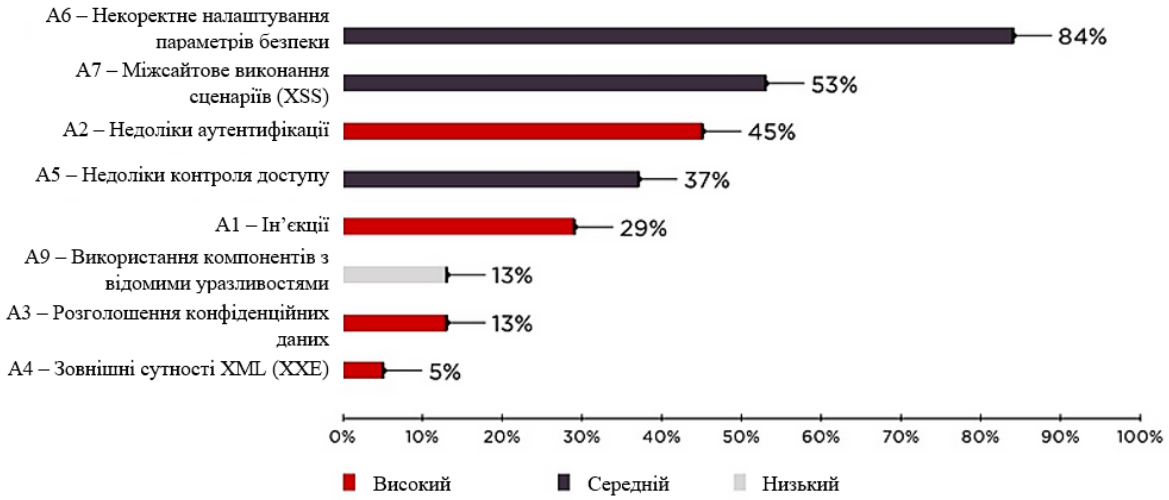

Рис. 2. Найпоширеніші уразливості веб-сайтів

Як бачимо, найбільше всього було виявлено некоректне налаштування параметрів безпеки веб-сайту та міжсайтовий скриптинг, які є середнього рівня ризику. Міжсайтовий скриптинг дозволить зловмиснику отримати так званий «ідентифікатор сесії юзера» та, за допомогою його, виконувати власні зловмисницькі дії від імені даного користувача. Також, на жаль, були виявлені недоліки аутентифікації та ін'єкції з високим ступенем ризику у достатньо чималій кількості.

Топ-5 найпоширеніших загроз показано на рис. 3.

Витік важливої інформації є другою найбільш актуальною загрозою безпеки веб-сайтів. Так, майже в половині витоків (у 47%) під загрозу потрапили персональні дані, а в 31% – облікові дані користувачів. Як показує аналіз кіберінцидентів за 2019 рік, саме крадіжка інформації є пріоритетною метою зловмисників [16].

У період з 2016 по 2019 рік кількість уразливостей високої та середньої тяжкості неухильно зменшувалась щороку. У 2020 році кількість дещо зросла, скоріш за все, в результаті ділових рішень, пов'язаних із впливом COVID-19 на організацію роботи по

всьому світу. Високий рівень уразливостей вказує на те, що зловмисник може повністю порушити конфіденційність, цілісність або доступність системи без необхідності спеціалізованого доступу, взаємодії користувача чи обставин, які не піддаються контролю зловмиснику. Середній рівень вказує на те, що зловмисник може частково порушити конфіденційність, цілісність або доступність системи. Йому може знадобитися спеціалізований доступ, взаємодія користувача або обставини, які не піддаються контролю зловмиснику. Такі уразливості можуть використовуватися разом з іншими вразливими місцями для ескалації атаки.

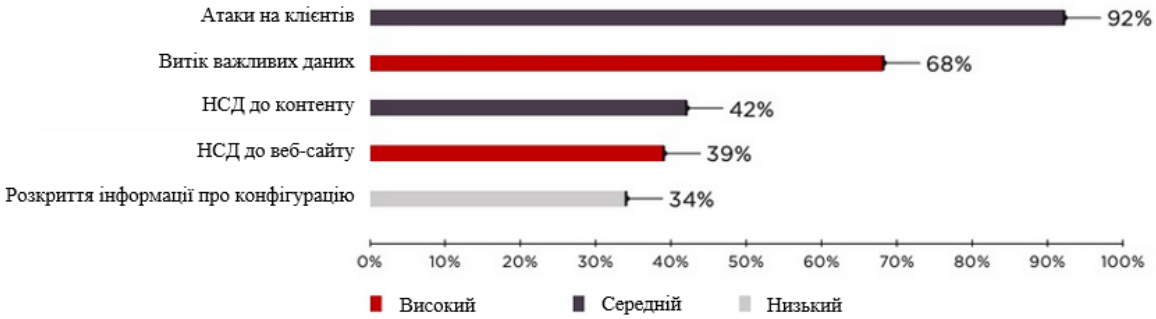

Рис. 3. Найпоширеніші загрози для організації

Загальна тенденція: зростає значимість хакінгу в атаках на організації. За результатами 2020 року частка цього методу складає 24% (на 10% пунктів більше, ніж в 2019 році). На «Темній мережі» відзначено зростання ринків з продажу доступів в компанії та підвищений інтерес до теми злому сайтів. Це можна пов'язати з масовим переходом організацій в онлайн-формат роботи.

Ключовим фактором, який вплинув на безпеку веб-сайтів у 2020 році, був початок пандемії COVID-19. Ця подія вплинула на безпеку так, що підприємствам довелося перенаправляти свої IT-ресурси. Пандемія змусила їх змінити організацію праці. Команди безпеки не мали ресурсів для вирішення багатьох питань безпеки, включаючи ті, що були виявлені в 2019 році або раніше. Результатом цього є загальна відсутність покращення рівня безпеки веб-сайтів. Пандемія COVID-19 також сприяла появі нових зловмисників, тому загалом 2020 рік можна вважати поганим роком для безпеки веб-сайтів.

Найбільше всього зловмисників цікавили комерційні таємниці, персональні та облікові дані. Всі ці три типи даних займають близько 71% від всієї інформації, яку крадуть зловмисники під час атаки на веб-сайт організації. У серпні 2020 року APT-угрупування Charming Kitten в ході однієї зі своїх кампаній, спрямованої на вчених з університетів Хайфи й Тель-Авіва, зламала сайт Deutsche Welle для розміщення на ньому шкідливого посилання. При переході по цьому посиланню жертві пропонувалося пройти процедуру авторизації, а введені облікові дані відправлялися зловмисникам. У вересні 2020 року хакери зламали понад 2800 інтернет-магазинів на платформі Magento та впровадили там шкідливий скрипт, який збирав особисту інформацію та дані платіжних карт клієнтів. У серпні та вересні 2020 року була помічена серія атак, спрямованих на сайти ЮНЕСКО, урядових організацій, Національного інституту охорони здоров'я та великих освітніх установ. На цих ресурсах хакери розмістили фішингову рекламу інструментів для злому акаунтів у відомих соціальних мережах та читерства в онлайн-іграх. Вони переслідували дві мети: крадіжку даних платіжних карт та поширення шкідливого ПЗ [15].

Нещодавно, OWASP розмістив попередній варіант OWASP Top 10 на 2021 рік [17], заснований на статистиці за останні 4 роки. Як бачимо, все також Injection та Broken Authentication залишаються лідерами на своїх позиціях й займають перше та друге місце. Також можна помітити, що XSS, який у 2017 році перебував на 7 місці, перемістився аж на третє місце у список OWASP 2021, закривши ТОП 3 найкритичніших уразливостей сайтів на наступні 3-4 роки, так як ця статистика оновлюється в такому проміжку. Якщо взяти

кількісну статистику, по якій і було перебудовано критичність топового списку, то Injection було виявлено 34061 разів, за ними слідує Broken Authentication – 13735 разів та закриває трійку XSS, яку виявили аж 433 353 рази.

Очікується, що в 2021 році будуть вдосконалюватися методи соціальної інженерії, експлуатуючі теми, пов'язані з установкою в світі, зокрема COVID-19: до прикладу, однією з популярних схем можуть стати веб-сайти, на яких зловмисники будуть пропонувати замовити препарати для лікування коронавірусу, записатися на платну вакцинацію, отримати інформацію о проходженні вакцинації та інше. Також можливо очікувати, що фішинг стане більш індивідуальним, зловмисники будуть виходити на жертву через месенджери та соціальні мережі. Для подолання корпоративних засобів захисту, взлом все частіше буде проводитися через домашні комп'ютери працівників.

Висновки

Досліджено найбільш поширені атаки на веб-сайти, а також можливі уразливості, які дозволяють проведення даних веб-атак. Проаналізовано тенденції поширення веб-атак, які організації більше потерпали від атак, статистику найбільш поширених уразливостей, які призводять до проведення цих веб-атак. Визначено можливі сценарії поширення веб-атак у поточному році та необхідність їх своєчасного виявлення.

Перелік посилань

1. Кібербезпека та звіт про веб-сайти SiteLock [Електронний ресурс] – Режим доступу до ресурсу: https://www.sitelock.com/resources/cybersecurity-report.
2. Захист веб-сайтів [Електронний ресурс] – Режим доступу до ресурсу: http://citforum.ck.ua/security/web/hierarchy/.
3. Атака введення SQL [Електронний ресурс] – Режим доступу до ресурсу: https://www.neuralegion.com/blog/sql-injection-attack/.
4. Ін’єкція LDAP [Електронний ресурс] – Режим доступу до ресурсу: https://www.synopsys.com/glossary/what-is-ldap-injection.html.
5. Ін'єкції коду PHP [Електронний ресурс] – Режим доступу до ресурсу: https://beaglesecurity.com/blog/vulnerability/php-code-injection.html.
6. Термінологія безпеки додатків [Електронний ресурс] – Режим доступу до ресурсу: https://www.whitehatsec.com/glossary/.
7. DoS та DDoS атаки [Електронний ресурс] – Режим доступу до ресурсу: https://www.futurelearn.com/info/courses/teaching-cybersecurity/0/steps/57188.
8. Різновиди мережевих атак [Електронний ресурс] – Режим доступу до ресурсу: https://www.cnews.ru/reviews/free/security/part7/net_attack.shtml.
9. Атака переповнення буфера [Електронний ресурс] – Режим доступу до ресурсу: https://www.imperva.com/learn/application-security/buffer-overflow/.
10. IP-підробка: що це таке і як це працює? [Електронний ресурс] – Режим доступу до ресурсу: https://us.norton.com/internetsecurity-malware-ip-spoofing-what-is-it-and-how-does-it-work.html.
11. Що таке атака грубої сили? [Електронний ресурс] – Режим доступу до ресурсу: https://phoenixnap.com/blog/brute-force-attack.
12. Небезпечна десеріалізація [Електронний ресурс] – Режим доступу до ресурсу: https://portswigger.net/web-security/deserialization.
13. Запобігання атакам фальсифікації запитів [Електронний ресурс] – Режим доступу до ресурсу: https://auth0.com/blog/cross-site-request-forgery-csrf/.
14. Уразливості та загрози веб-додатків у 2019 році [Електронний ресурс] – Режим доступу до ресурсу: https://www.ptsecurity.com/ru-ru/research/analytics/web-vulnerabilities-2020/.
15. Підсумки минулого року та прогнози на 2021 рік: від руйнівних наслідків віддаленої роботи - до моделювання бізнес-ризиків на кіберполігонах [Електронний ресурс] – Режим доступу до ресурсу: https://www.ptsecurity.com/ru-ru/about/news/itogi-ushedshego-goda-i-prognozy-na-2021-god/.
16. Звіт Acunetix про веб-вразливості [Електронний ресурс] – Режим доступу до ресурсу: https://www.acunetix.com/wp-content/uploads/2021/04/Invicti-AppSec-Indicator-Spring-2021-Edition-Acunetix-Web-Vulnerability-Report.pdf.
17. OWASP Top-10 2021. Пропозиція на основі статистики [Електронний ресурс] – Режим доступу до ресурсу: https://lab.wallarm.com/owasp-top-10-2021-proposal-based-on-a-statistical-data/.

Надійшла: 16.02.2021 Рецензент: д.т.н., професор Гайдур Г.І.