DOI 10.15276/imms.v13.no1-2.75
УДК 004.42:004.056.57

Informatics and Mathematical Methods in Simulation
Vol.13 (2023), No. 1-2, pp. 75-86

# СИСТЕМИ АНАЛІЗУ КІБЕРБЕЗПЕКИ ПРОГРАМНО-ТЕХНІЧНОГО ЗАБЕЗПЕЧЕННЯ КОРПОРАТИВНИХ КОМП'ЮТЕРІВ ТА САЙТІВ

В.В. Задоров, Д.О. Фурман, О.А.Стопакевич, А.О.Стопакевич

Національний університет «Одеська політехніка»,
Проспект Шевченка, 1, Одеса, 65044, Україна; E-mail:
stopakevich@gmail.com

Корпоративні комп'ютери та сайти є основними мішенями для атак кіберзлочинців, оскільки вони містять цінну інформацію та забезпечують функціонування бізнес-процесів. Підприємства повинні бути готовими виявляти та запобігати потенційним загрозам, щоб уникнути фінансових втрат, втрати репутації та порушенням конфіденційності даних клієнтів. У цьому контексті системи аналізу кібербезпеки програмно-технічного забезпечення корпоративних комп'ютерів та сайтів виконують важливу роль. Вони дозволяють проводити повноцінний аудит інфраструктури, виявляти потенційні вразливості, оцінювати ризики та розробляти стратегії захисту. Ці системи надають комплексну інформацію про стан безпеки та допомагають приймати обґрунтовані рішення щодо поліпшення безпеки. В статті розглянуто дві програмні системи аналізу кібербезпеки. Перша програмна система забезпечує аналіз апаратного та програмного забезпечення комп'ютерів, виявляючи потенційні проблеми безпеки на рівні окремих пристроїв. Вона надає зручний графічний інтерфейс десктопної програми й дозволяє проводити докладний аналіз комп'ютерів, включаючи оцінку апаратного забезпечення та встановлених програм, і надає звіти про виявлені проблеми та рекомендації щодо поліпшення безпеки. Друга програма, реалізована як телеграм-бот, надає можливість віддалено аналізувати корпоративні сайти та сервери, спрощуючи процес контролю безпеки для спеціалістів з кібербезпеки та системних адміністраторів. Інтерфейс телеграм-бота дозволяє проводити віддалену діагностику довільного сервера без необхідності доступу до нього, встановлення та регулярного оновлення спеціального програмного забезпечення, що робить бот зручним для використання. Бот забезпечує аналіз різних складових сайту та серверу, на якому він розміщений, включаючи версію операційної системи сервера, сервіси сервера, CMS сайту, піддомени сайту, репутацію сервера та сайту та геолокацію сервера. Результати аналізу надаються у звіті, що допомагає виявити потенційні вразливості та надає рекомендації з покращення безпеки.

**Ключові слова:** корпоративна кібербезпека, сайт, сервер, аудит, програма, звіт, телеграм, бот, віддалена діагностика, проблеми безпеки, сервіс, вразливості.

**Вступ.** Актуальність розробки систем автоматизованого аналізу кібербезпеки набуває особливої ваги в сучасному цифровому світі, оскільки технології зламу постійно удосконалюються й стає все важчим слідкувати за змінами програмного та апаратного забезпечення корпоративних комп’ютерів та сайтів [1]. Зловмисники постійно шукають нові способи зламу інформаційних систем, використовуючи вразливості в програмному та апаратному забезпеченні. Новим викликом є розвиток штучного інтелекту, що відкриває нові можливості для створення систем зламу [2].

Стаття розглядає розв’язання двох задач аудиту кібербезпеки: задачі аудиту апаратного та програмного забезпечення корпоративних комп’ютерів та задачі аудиту корпоративних сайтів та серверів, на яких ці сайти розміщені.

Метою розв’язання першої задачі є виявлення потенційних проблеми безпеки на рівні окремих пристроїв. А саме, проблеми з апаратними компонентами, програмним забезпеченням, драйверами, патчами та іншими аспектами комп'ютерної інфраструктури, що дозволяє вчасно вжити заходів для виправлення помилок, забезпечуючи належну продуктивність та функціональність системи. Оскільки, багато компаній підлягають регуляторним вимогам щодо безпеки, захисту персональних даних, фінансової звітності та інших аспектів, то аудит комп'ютерів допомагає встановити відповідність цим вимогам та підтвердити, що комп'ютерна інфраструктура відповідає потрібним стандартам і регуляціям. Також аудит комп'ютерів може допомогти виявити зайве апаратне та програмне забезпечення, неефективне використання ресурсів, недієві процеси та інші фактори, які призводять до надмірних витрат. Аналізуючи результати аудиту, можна вжити не тільки заходи щодо кіберпезпеки, но і заходи по оптимізації забезпечень та зменшенню витрат.

Метою розв’язання другої задачі є виявлення потенційних проблем безпеки корпоративних сайтів. А саме: відсутність актуальних версій програмного забезпечення серверу та сайту, надмірна кількість відкритої інформації про програмне забезпечення серверу, відкритий доступ до служб, які призначені для застосування в локальних мережах, наявність працюючих служб з застарілими протоколами чи таких, які не відповідають цільовому призначенню корпоративних серверів, застосування небезпечних та застарілих CMS, перевантаженість сервера сайтами, відсутність сертифікату чи ненадійний центр сертифікації, низька репутація сервера та сайту, геолокація сервера в недружніх до України країнах й країнах, в яких не дотримуються законодавчих норм щодо доступу до приватної інформації. Наслідки зламу корпоративних сайтів можуть бути дуже неприємними, зокрема: зупинка роботи сайту; крадіжка та розповсюдження персональних даних користувачів, фінансових даних, логінів та паролів; втрата цінної інформації, яка складає корпоративну таємницю. Якщо злам стає відомим, то це, звичайно, має негативний вплив на ділову діяльність та репутацію компанії. Втрата довіри користувачів може вплинути на лояльність клієнтів, зниження трафіку та втрату бізнесу. Крім того, багато країн та регуляторних органів встановлюють обов'язкові вимоги щодо захисту даних, конфіденційності та приватності даних користувачів на веб-сайтах. Невиконання цих вимог може призвести до штрафів, правових санкцій та інших негативних наслідків для підприємства. Регулярний аудит сайтів дозволяє також оцінити причини низької швидкості доступу до сайтів, виявити моральну застарілість застосованого програмістами та системними адміністраторами програмного забезпечення та технологій програмування.

**Система аналізу кібербезпеки програмно-технічного забезпечення корпоративних комп'ютерів**. Вимогою до системи є наявність зручного графічного інтерфейсу, швидкість роботи та адекватний перелік параметрів для порівняння. Програмні інтерфейси ОС Windows не відрізняються високою швидкістю отримання параметрів, що пов’язано з архітектурними особливостями операційної системи (ОС) [3, 4]. Інформація про кожний компонент в певний момент часу не доступна для ОС й має отримуватись через інтерфейси відповідних драйверів, доступ до який знаходиться через відповідні ключі реєстру. Ця інформація також не записується в певній централізованій базі при запуску операційної системи, коли ініціалізуються

драйвери. Тому звичайно програми для отримання системної інформації або відображують тільки базову інформацію або структурують відображення по категоріям та підкатегоріям, щоб користувач міг отримати тільки конкретну інформацію, коли це потрібно. Отримання всієї інформації, яку можливо отримати про комп'ютер за допомогою інтерфейсів ОС, звичайно займає на порівняно сучасному ПК біля 10 хвилин. Тому програма для аудиту має вибирати тільки ті параметри, які відносяться до значимих, не змінюються кожного запуску ОС. Перелік досліджуваних параметрів має бути невеликий й однозначно зрозумілий користувачеві програми.

Для ще більшого спрощення роботи з програмою найбільш типові перевірки кібербезпеки системою мають виконуватись за запитом. Для цього треба реалізувати окрему функцію – автоматичне проведення аудиту. В результаті аналізу отримана інформація (як поточна конфігурація, так і її зміни) аналізується з точки зору кібербезпеки. Аналіз зазначає які результати перевірки відповідають вимогам кібербезпеки ПК, які їх порушують, а які вимагають додаткового ручного аналізу.

Розроблена система, яка відповідає зазначеним вимогам, реалізована як програма мовою Python [5, 6], з орієнтацією на застосування в ОС Windows. Проводиться отримання таких значимих параметрів як:

– апаратне забезпечення комп'ютера (BIOS, процесору, пам'яті, дисків тощо);

– основні параметри операційної системи (номера збірки, дати встановлення, папки встановлення тощо);

– перелік встановленого програмного забезпечення (видалення, додавання, зміна версії);

– перелік програмного забезпечення, яке запускається разом з ОС та при вході в акаунт;

– перелік встановлених оновлень операційної системи (ОС) Windows;

– наявність та активності брандмауера Windows, антивірусів Windows Defender та інших основних виробників, актуальності задіяної бази даних антивірусів.

Система відповідає наступним ключовим технологічним вимогам:

– можливість збереження поточного переліку параметрів комп'ютера, як еталонну конфігурацію в портабельному та зручному для обробки форматі JSON;

– можливість порівняння поточної конфігурації та будь-якої зі збережених конфігурацій в якості еталонної;

– час отримання необхідного переліку параметрів не перевищує 1 хв.;

– проведення автоматичного аудиту з генерацією звіту оновлень операційної системи, наявності та активності брандмауера Windows, антивірусів Windows Defender та інших основних виробників, актуальності задіяної бази даних антивірусів.

При розробці системи використані наступні інструменти програмної інженерії:

– мова програмування Python 3.10 в дистрибутиві Anaconda;

– бібліотека для реалізації графічного інтерфейсу PyTK;

– інтерфейси ОС для доступу до WMI [7], реєстру [8] тощо;

– утиліта autoruns [9], результати якої використовуються для гарантованого знаходження всіх програм в автозапуску ОС (що, при бажанні гарантованого результату, не є простою справою);

– технології інтернаціоналізації програми.

Під час роботи з системою аудитор може зберігати поточну конфігурацію як еталонну й порівнювати в наступний раз зміни в комп'ютері відносно неї. Для збереження конфігурації в системі застосований зручний портабельний формат JSON.

Приклад перевірки конфігурації комп'ютера після оновлення його технічного забезпечення приведений на рис.1.

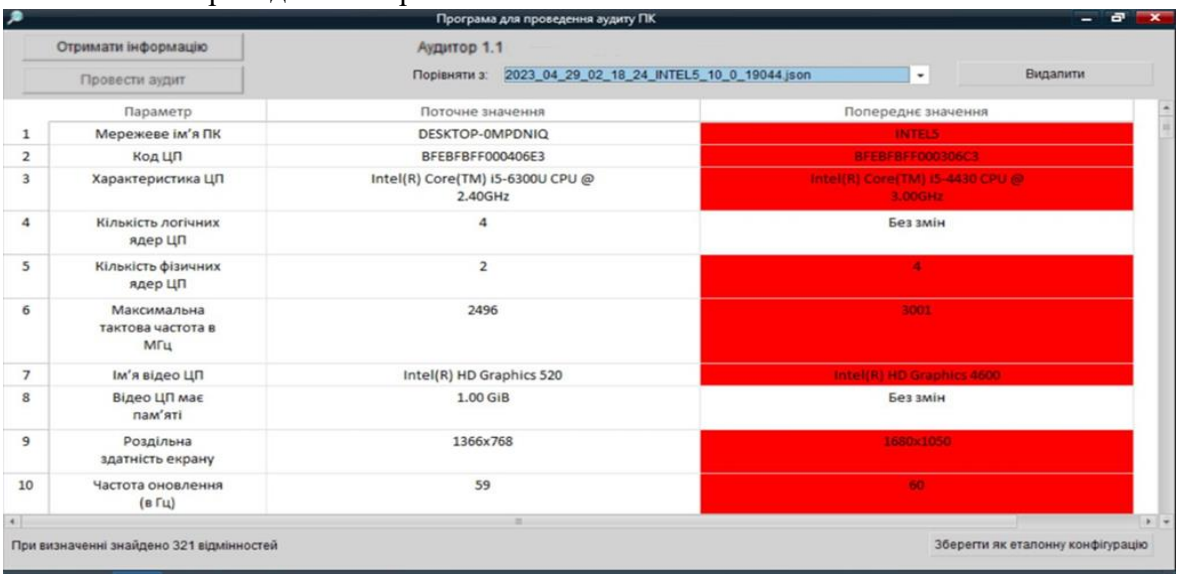


**Рис.1.** Приклад перевірки конфігурації комп'ютера після оновлення його технічного забезпечення

Приклад перевірки конфігурації комп'ютера після оновлення його програмного забезпечення приведений на рис. 2.

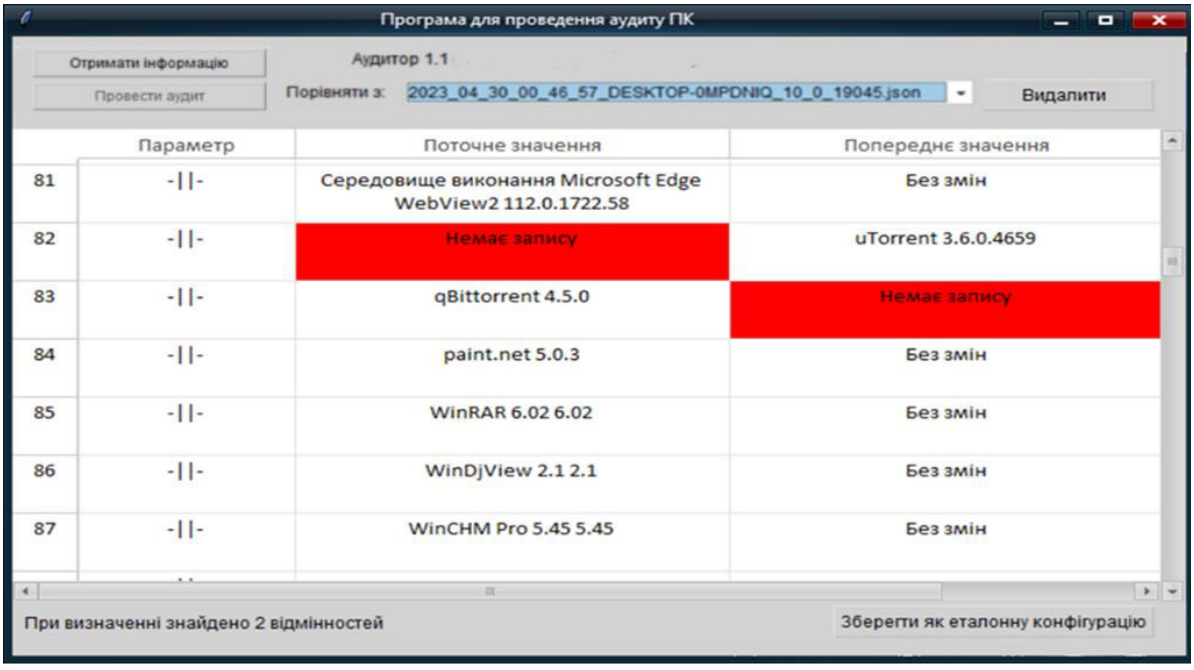


**Рис.2.** Приклад перевірки конфігурації комп'ютера після оновлення його програмного забезпечення

Для спрощення роботи користувачів, система може автоматично згенерувати звіт аудиту. Приклад звіту приведено на рис. 3.

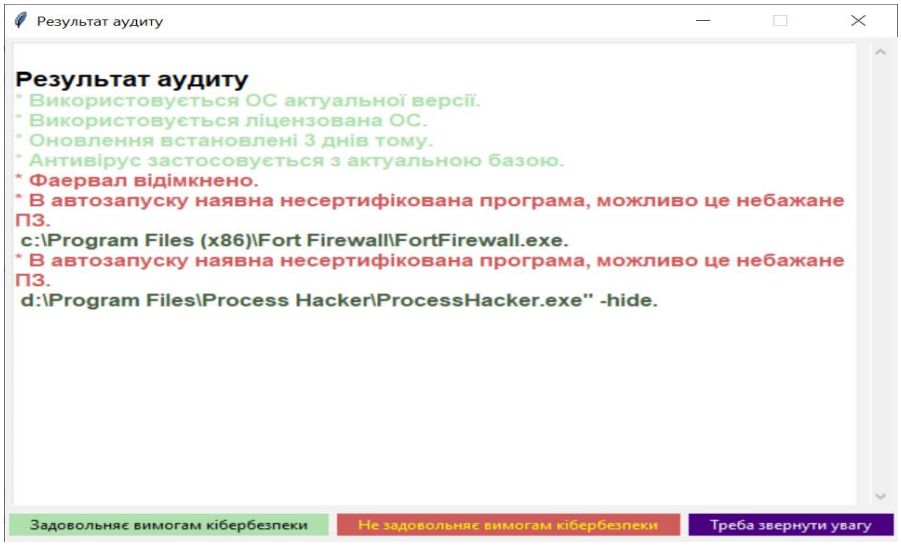


**Рис.3.** Приклад автоматично згенерованого звіту

При проведенні аудиту при умові, що проблем не знайдено, аудитор має зберегти поточну конфігурацію в файл як еталонну, назва якого за замовченням містить мережеве ім'я комп'ютера та дату. В наступний раз аудитор вже звіряє конфігурацію з тою, що збережена. Якщо зміни позитивні, то нова конфігурація зберігається як еталонна.

**Система аналізу кібербезпеки програмного забезпечення корпоративних сайтів**. Вимогою до системи є забезпечити зручний для користувача швидкий аудит сайту й серверу, на якому він розміщений, з метою визначення ступеню захисту й основних можливих проблем. При цьому спеціаліст оцінює сайт та серверне програмне забезпечення (ПЗ) ззовні, тобто аналізує яка інформація може бути доступна зацікавленому хакеру. Визначення стану безпеки ззовні має певні недоліки – отримана інформація може бути не повна чи навіть недостовірна, якщо адміністратор спеціально над цим працював. Однак, істотна перевага такого визначення – незалежність від адміністратора сервера й програмістів сайтів, які можуть й не знати про факт такої перевірки. Оцінку вірності прийняти рішень системним адміністратором сервера та програмістами сайту проводить програма, таким чином виникає можливість погляду на ситуацію збоку.

Критеріями вразливості сайтів при зовнішній діагностиці є наступні [10]:

– Використання застарілої операційної системи на сервері сайту. Як правило, програмне забезпечення (в тому числі для реалізації інтернет-сервісів) для застарілих ОС, особливо в світі UNIX-подібних ОС, не оновлюється, це призводить до того що знайдені вразливості в старших версіях не виправляються й цим можуть скористатись хакери.

– Використання застарілих служб на сервері сайту. Причина така ж сама – служба, версія якої не підтримується може стати джерелом зламу

– Використання на сервері сайту служб, що реалізують застарілі протоколи. Кожна служба, яка доступна користувачу в інтернеті є джерелом потенційної небезпеки. Використовувати служби, які реалізують неактуальний функціонал в загальному випадку непотрібно й краще знаходити сучасні альтернативи

– Надмірна кількість сайтів на сервері. Кожен сайт може мати вразливе ПЗ, через яке можливо потенційно отримати доступ до всього серверу. Чим більше сайтів, ти такий ризик більший. Якщо на корпоративному сайті зберігається важлива інформація, то треба уникати його розміщення на хостингу с сотнями сайтів на одному сервері.

– Надмірна кількість субдоменів. Субдомени виділяються для служб (наприклад, ftp чи smtp) та сайтів. Іноді адміністратори зловживають субдоменами, розміщуючи в інтернет непотрібний контент

– Використання CMS. Використання типового й відомого програмного забезпечення є джерелом небезпеки. Звичайно, різні CMS мають різний ступінь захисту та якість виконання, вимоги до адміністрування тощо. Сайти з CMS звичайно зламуються в першу чергу.

– Репутація сайту. Інтернет служби та пошукові системи мають власні інструменти для визначення факту зламу сайтів, також є спеціальні сервіси, в яких розміщують жалоби користувачів на аномальну активність серверів.

– Географічна локація сайту**.** Хоча вона не є прямим показником кібербезпеки, однак розміщення сайтів в деяких країнах є небезпечним оскільки законодавство там не дуже діє, тому доступ до інформації можуть отримати фізично чи шляхом встановлення спеціальних аналізаторів трафіку за місцем встановлення серверу.

Для проведення зовнішньої діагностики розроблено багато програмних утиліт, тому при розробленні системи не доцільно займатись розробкою нових інструментів, а бажано застосовувати максимальну кількість відпрацьованих рішень. Призначення системи буде в тому, щоб проаналізувати отримані оцінки й представити їх в зрозумілій формі аудитору.

Для визначення операційної системи доцільно застосовувати результати програми nmap [11-13], яка використовує механізм fingerprinting. База даних програми nmap складається з ідентифікаторів різних ОС та відповідних до них маркерів. Обсяг БД складається більше ніж з 7000 тисяч записів. Слід зазначити, що процедура визначення принципово має ймовірнісний характер, тобто, наприклад Linux 6.2 [14, 15] може бути з ймовірністю 90%, а Linux 6.0-6.4 з ймовірністю 89% і т.п. Крім того, адміністратори серверів можуть застосовувати методи фальсифікації показів [16, 17]. В роботі [18] наведено літературний огляд методів підвищення ймовірності визначення. Для підвищення точності оцінювання треба перевірити достовірність оцінки, орієнтуючись на співпадіння з іншими визначеними параметрами (службами ОС, веб-сервером, застосованими серверними мовами програмування тощо). Уточнення версії також досягається за рахунок застосування методів аналізу трафіку HTTPS [19] і DNS.

Для визначення та оцінки сервісів операційної системи також доцільно орієнтуватись в першу чергу на алгоритми програми nmap, які застосовують декілька механізмів визначення переліку працюючих сервісів та програмного забезпечення, що їх реалізує.

Оцінка застосованих сервісів ОС за призначенням доцільно проводити виходячи з наступної класифікації [3, 13, 14, 15]:

1. Сервіси, нормальні для інтернет-сервера, які є актуальні й рекомендовані: ftps, ftps, ftps-data, ftps-data, smtp, http, https, imap, imap4-ssl, imaps, xmpp, xmpp-client, http-proxy, http-alt,https-alt, submission

2. Сервіси, нормальні для інтернет-сервера, протоколи яких застарілі й такі сервіси краще замінити на більш безпечні аналоги (наприклад, telnet на ssh, irc на

мессенджери та ін.): ftp-data, ftp, telnet, rtelnet, tam, nntp, tftp, via-ftp, gopher, irc, talk, conference, rtsp, rsync, telnets, ircs, pop3, pop3s, time, scp, scp-config

3. Сервіси для віддаленого управління сервером, які мають контролюватись брандмаурером чи не бути віддалено бути доступні взагалі: ssh, vnc, vnc-1, vnc-2, vnc-3, vnc-http,, vnc-http-1, vnc-http-2, vnc-http-3,teamviewer, ms-wbt-server, msrpc

4. Стандартні мережеві сервіси операційних систем, сервіси баз даних, X-сервер та ін., все що має не бути доступно через мережу інтернет й має в більшості випадків використовуватись лише в межах локальної мережі: sqlserv, sqlnet, netbios-ns, netbios-dgm, netbios-ssn, snmp, ipx, microsoft-ds, printer, http-rpc-epmap, login, dhcpv6-client, dhcps, nfs, mysql, mysql-proxy, postgresql, ms-olap2, ms-olap1, rsqlserver, rsqlserver, dns, x11, X11, X11:1,X11:2,X11:3,X11:4, X11:5, X11:6, X11:7, X11:8, X11:9

5. Сервіси майнінгу, які не мають бути присутніми на сервері: bitcoin, litecoin.

6. Спеціальні сервіси для розробників, наявність яких на корпоративному інтернет сервері скоріше не бажані: git, cvspserver, cvsup. Для цих сервісів краще виділити окремий сервер, якщо це дозволяє фінансування.

З точки зору безпеки краще, якщо не можливо визначити програмне забезпечення, яке реалізує сервіс чи хоча б версію програми. Для оцінки достовірності оцінки програмного забезпечення необхідно додатково для критичних служб застосовувати додаткові алгоритми. Наприклад, для веб-сервера слід перевірити додатково версії протоколу HTTP, що підтримуються (наприклад, HTTP/2 підтримують далеко на всі веб-сервери). Заголовки веб-серверів в деяких випадках містять інформацію про операційну систему, наприклад в дистрибутиві Ubuntu за замовчуванням в заголовці HTTP сервера міститься повна версія дистрибутиву. Перехресна перевірка дозволяє уточнити точність визначення ОС.

Визначення та оцінка CMS сайту [20, 21] може спрощено проводитись за допомогою аналізу HTML коду. Однак більш точні дані надає сервіс whatcms. Цей сервіс дозволяє визначити CMS з високою долею ймовірністю. Однак все ж таки дані треба перевірити на відповідність з простим алгоритмом оцінки за HTML кодом.

Визначення та оцінка переліку піддоменів може проводитись як за аналізом SAN запису SSL сертифікату [10], так і брутфорс методом за допомогою перебору за словником програмою subbrute [22]. Другий метод є більш надійний, оскільки сертифікат часто видають не на окремі піддомени, а на всі разом. Велика кількість піддоменів звичайно є небезпечною, часто в піддоменах розміщують певні тестові версії сайтів, за якими потім не слідкують.

Визначення переліку інших сайтів, розміщених на сервері та оцінка їх кількості може проводитись за допомогою механізму зворотного запису DNS. Найбільш зручний сервіс визначення надає служба Reverse2IP. Кожний сайт, розміщений на сервері, є джерелом небезпеки. Тому краще для корпоративного сайту, який містить важливі персональні дані не розміщуватись на дешевих хостингах з сотнями інших сайтів.

Визначення геолокації серверу може бути проведена за допомогою безкоштовного сервісу ip2geotools. В деяких країнах не бажано розміщення сайтів підприємств України й перевірка за переліком ненадійних країн є бажаною.

Визначення репутації серверу може бути проведена за допомогою сервісу abusedb. Цей сервіс автоматично проводить оцінку шкідливості та небезпеки сайту за 100 бальною шкалою. Отримання інформації з подібних сервісів дозволяє оцінити чи

був факт зламу серверу чи використання його для незаконної чи недозволеною в мережі діяльності за період в 2-3 останні роки.

З використанням зазначеного вище переліку потенційних вразливостей сайтів та запропонованих методів їх визначення була розроблена система, яка реалізована як Python програма з інтерфейсом чат-боту мессенджера Telegram [23, 24]. Бот проводить віддалену діагностику, не залежить від адміністраторів сайту та не вимагає дозволу для доступу до сервера. Для використання боту обов'язкова реєстрація користувачів та робиться детальний звіт всіх дії користувачів. Дані отримуються за допомогою зовнішніх інструментів та різна інформація про конкретний сайт оновлюється з різними інтервалами з метою захисту від DDoS атак.

Для розробки бота використана версія системи програмування Python 3.10 з дистрибутива Anaconda. Використано Aiogram – сучасний та повністю асинхронний фреймворк для API Telegram Bot, написаний на Python за допомогою інтерфейсу asyncio. Для збереження інформації о користувачах використана локальна СКБД SqLite.

Інтерфейс головного вікна програми приведений на рис.4.

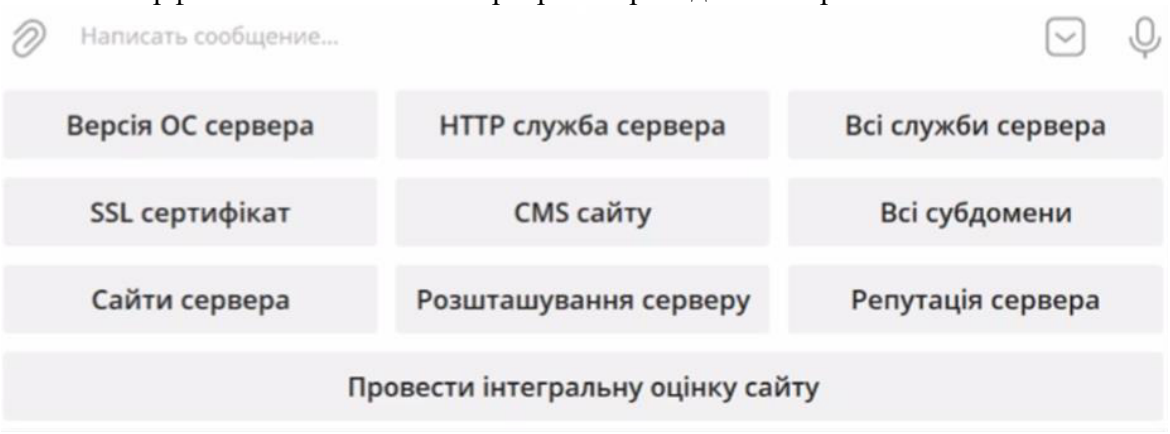


**Рис.4.** Меню інтерфейсу чат-боту

Деякі фрагменти з результатів аналізу системи приведені нижче.

1. **Аналіз версії ОС сервера де розміщено сайт ukr.net**

Операційна система сервера
Ймовірність присутності ОС:
Linux 5.0 - 5.4 - 87 процентів
Якщо ця версія вірна: Використовується актуальна версія ядра Linux. Це безпечно.

2. **Аналіз служб сервера де розміщено сайт ukr.net**

Всі сервіси сервера
Знайдені служби:
TCP 80: http Cloudflare http proxy – Це безпечна для інтернет-сервера служба.
TCP 443: https cloudflare – Це безпечна для інтернет-сервера служба.
TCP 8080: http Cloudflare http proxy – Це безпечна для інтернет-сервера служба.
TCP 8443: https-alt cloudflare – Це безпечна для інтернет-сервера служба.
Використовуються дані програми nmap

3. **Аналіз SSL сертифікату сайту ukr.net**

Криптографічний захист сайту
Сертифікат працюючий. На сайт можна зайти за допомогою HTTPS
Результати детальної перевірки сертифікату

Сертифікат дійсний в період : 2023-02-07 00:00:00-2024-02-07 23:59:59
Спільне ім'я сертифікату: ukr.net
SAN: *.ukr.net, ukr.net
Сертифікат видано: Cloudflare Inc ECC CA-3
Це безпечно

**4. Аналіз CMS сайту ukr.net**

CMS сайту
Результати перевірки за допомогою аналізу HTML коду – CMS не знайдена
Інформація від сервісу whatcms: – CMS не знайдена
Це безпечно

**5. Аналіз всіх субдоменів сайту ukr.net**

Піддомени сайту
За SSL сертифікатами – *.ukr.net, ukr.net
Спеціальний агресивний метод за словником зі 100 слів (програма subbrute):
ukr.net, www.ukr.net, mail.ukr.net, ftp.ukr.net, localhost.ukr.net, webmail.ukr.net, smtp.ukr.net, pop.ukr.net, ns1.ukr.net, …. , sms.ukr.net, office.ukr.net, exchange.ukr.net. ipv.ukr.net
Кількість піддоменів завелика, можливо деякі з них непотрібні для зовнішніх користувачів.
Не зовсім безпечно

**6. Аналіз наявності інших сайтів на сервері де розташовано сайт ukr.net**

Знайдено сайтів:21:
a678ff.com, acromegalie.nl, … , ukr.net, ukr.net.ua, ukrnet.net.ua, vismasolutions.com, www.aussiebeeflamb.com, vn.cdn.cloudflare.net, www.leatest.site, xodi.bet, yslbeauty.sa
Чим більше сайтів на сервері, тим ймовірніше його злам через програмне забезпечення. Кількість сайтів представляє небезпеку. Це небезпечно. Рекомендується змінити сервер.

**7. Аналіз розташування сервера, де розташовано сайт ukr.net**

Географічна локація сервера
Місто – Toronto, Регіон: Ontario, Країна: CA, Широта: 43.6534817, Довгота: -79.3839347
IP2Geotools
Це не дуже безпечно для сайту, який призначений для обслуговування переважно України

Фрагмент інтегральної оцінки сайту op.edu.ua приведено на рис. 5.

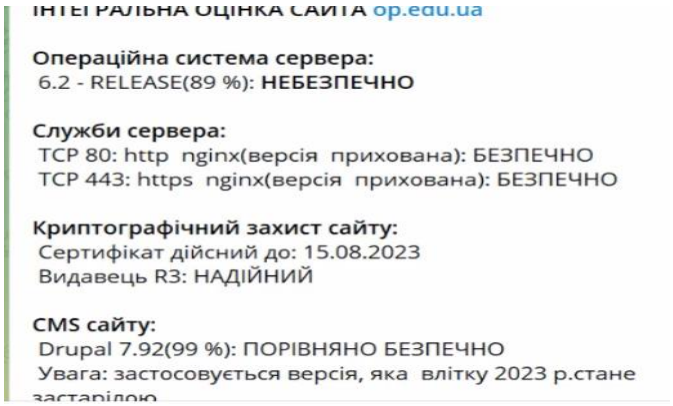


**Рис.5.** Фрагмент інтегральної оцінки сайту op.edu.ua

Таким чином, Демонстрація роботи програми при діагностиці різних сайтів показує успішність вибраних інструментів та алгоритмів оцінки складових безпеки корпоративних сайтів.

**Висновки.** Розглянуті дві задачі аудиту кібербезпеки: аналіз апаратного та програмного забезпечення комп'ютерів і аналіз корпоративних сайтів та серверів.

Метою першої задачі було виявлення потенційних проблем безпеки на рівні окремих комп'ютерних пристроїв, що дозволяє вжити заходів для виправлення помилок і забезпечити безпеку і надійність комп'ютерної інфраструктури. Виконуючи аудит комп'ютерів, можна встановити відповідність регуляторним вимогам, забезпечити захист персональних даних, фінансової звітності та інших аспектів, а також знизити витрати шляхом оптимізації ресурсів та процесів.

Перша задача розв’язана шляхом розробки програми для аудиту корпоративних комп’ютерів, основними відмінностями якої є швидкість роботи та автоматичний аналіз зміни конфігурації та її змін з точки зору спеціаліста з кібербезпеки.

Друга задача полягала у виявленні потенційних проблем безпеки корпоративних сайтів та серверів. Аудит сайтів дозволяє виявити такі проблеми, як застаріле програмне забезпечення серверів, недотримання законодавчих вимог, відкритий доступ до служб, використання небезпечних та застарілих CMS і багато інших. Злам корпоративних сайтів може мати серйозні наслідки, включаючи втрату конфіденційної інформації, зупинку роботи сайту та негативний вплив на репутацію компанії. Аналізуючи результати аудиту, можна прийняти необхідні заходи для забезпечення безпеки сайту та виконання вимог щодо захисту даних користувачів.

Друга задача розв’язана шляхом розробки програми для аудиту корпоративних сайтів, основними відмінностями якої є визначення наявності потенційних вразливостей шляхом віддаленої діагностики. Програма реалізована як чат-бот. Особливістю програми є використання алгоритмів оцінки достовірності отриманих з різних джерел даних та наявність зручної для спеціаліста з кібербезпеки інтегральної оцінки безпеки сайту, яка не вимагає наявності доступу до сервера, на якому він розміщений.

Розробка систем автоматизованого аналізу кібербезпеки має велике значення в сучасному цифровому світі, де зловмисники постійно шукають нові способи зламу інформаційних систем. Застосування таких систем дозволяє вчасно виявляти потенційні загрози та вразливості, вживати відповідні заходи для їх усунення і забезпечувати безпеку та надійність комп'ютерних систем і корпоративних сайтів. Запровадження аудиту кібербезпеки є необхідним кроком для захисту важливих даних, забезпечення дотримання регуляторних вимог і зміцнення довіри до організацій в сфері кібербезпеки.

**Список літератури**

1. Boskamp E. 30 crucial cybersecurity statistics [2023]: data, trends and more. Zippia. URL: https://www.zippia.com/advice/cybersecurity-statistics/
2. Meah J. AI in Cybersecurity: The Future of Hacking is Here. Technopedia. https://www.techopedia.com/ai-in-cybersecurity-the-future-of-hacking-is-here/2/34520
3. Panek C. Windows Server Administration Fundamentals. Hoboken, NJ: Willey & Sons, 2020

4. Yosifovich P., Ionesku A., Russinovich M. E., Solomon D. A. Windows internals. Part1: System architecture, processes, threads, memory management, and more. Microsoft Press, 2017.
5. Васильєв О. Програмування мовою Python. Київ: Навчальна книга – Богдан, 2019.
6. Руденко В., Жугастров О. Основи алгоритмізації та програмування мовою Python. Київ: Ранок, 2019.
7. Lissoir A. Leveraging WMI Scripting: Using Windows Management Instrumentation to Solve Windows Management Problems. Digital Press, 2003.
8. Palne L. The Defender's Guide to the Windows Registry. URL: https://posts.specterops.io/the-defenders-guide-to-the-windows-registry-febe241abc7
9. Systntelnals autoruns. URL : https://download.sysinternals.com/files/Autoruns.zip
10. Dalziel H. How to Attack and Defend Your Website. N.Y.: Elsevier, 2015
11. Chauhan A.S. Practical Network Scanning: Capture network vulnerabilities using standard tools such as Nmap and Nessus. Packt Publishing, 2018
12. Brown N. Nmap 7: From Beginner to Pro. Packt Publishing, 2021
13. Calderon P. Nmap Network Exploration and Security Auditing Cookbook. Packt Publishing, 2021
14. Calcatinge A., Balog J. Mastering Linux Administration: A Comprehensive Guide to Installing, Configuring, and Maintaining Linux Systems in the Modern Data Center. Packt Publishers, 2021
15. Рамський Ю., Олексюк В., Балик А. Адміністрування комп'ютерних мереж та систем. Тернопіль: Богдан, 2010.
16. Kalia S., Singh M. Masking approach to secure systems from operating system fingerprinting. *TENCON*. 2005. Vol.1. No.6. P.21-24.
17. Greenwald L.G., Thomas T.J. Understanding and preventing network device fingerprinting. *Bell Lab Tech J*. 2007. Vol. 3. P. 149–166.
18. Kumar A., Soni I., Kumar, M. Operating System Fingerprinting Using Machine Learning. Algorithms for Intelligent Systems. Singapore: Springer, 2022. P. 157-161. URL: http://doi.org/10.1007/978-981-16-7136-4_13
19. Lastovicka M., Spacek S., Velan P., Celeda P. Using TLS Fingerprints for OS Identification in Encrypted Traffic. IEEE/IFIP Network Operations and Management Symposium. 2020. P.1–6. URL: https://doi.org/10.1109/NOMS47738.2020.9110319
20. Barker D. Web Content Management: Systems, Features, and Best Practices. Sebastopol, CA: O'Reilly, 2016
21. Jain N. WordPress Website Security Guide. Oxford: IP, 2019
22. Prakhar P. Mastering modern Web penetration testing. Birmingham, U.K.: Packt Publishing, 2016.
23. Modrzyk N. Building Telegram Bots: Develop Bots in 12 Programming Languages Using the Telegram Bot API. Tokyo: Apress, 2019
24. Демиденко А. Telegram Bot. Руководство по созданию бота в мессенджере Telegram. SelfPub, 2023

В.В. Задоров, Д.О. Фурман, О.А.Стопакевич, А.О.Стопакевич

# CYBER SECURITY ANALYSIS SYSTEMS OF SOFTWARE AND TECHNICAL SUPPORT OF ENTERPRISE COMPUTERS AND SITES

V.V.Zadorov, D.O.Furman, O.A.Stopakevych, A.O.Stopakevych

National Odesa Polytechnic University, Shevchenko str., 1, Odesa, 65044, Ukraine
stopakevich@gmail.com

Enterprise computers and websites are prime targets for cybercriminals because they contain sensitive information and provide business processes. Businesses must be prepared to spot and prevent potential threats to avoid financial losses, reputational damage, and violations of customer data privacy. In this context, cybersecurity analysis systems for software and hardware of enterprise computers and websites play an important role. They allow to conduct a full-fledged infrastructure audit, discover potential vulnerabilities, assess risks, and develop protection strategies. These systems provide comprehensive information about the security status and help to make reasonable decisions on how to improve security. The article discusses two software systems for cybersecurity analysis. The first software system analyzes computer hardware and software, identifying potential security issues at the level of individual devices. It provides a user-friendly graphical interface of a desktop program and allows to perform a detailed analysis of computers, including an assessment of hardware and installed programs, and provides reports on the detected problems and recommendations for improving security. The second program, implemented as a Telegram bot, allows remote analysis of corporate websites and servers, simplifying the security control process for cybersecurity specialists and system administrators. The Telegram bot interface allows remote diagnostics of an arbitrary server without the need to access it, install and regularly update special software, which makes the bot comfortable to use. The bot analyzes various components of the website and the server on which it is hosted, including the server operating system version, server services, website CMS, website subdomains, server and website reputation, and server geolocation. The analysis results are presented in a report that helps identify potential vulnerabilities and provides recommendations for improving security.

**Keywords**: corporate cyber security, site, server, audit, software, telegram boat, remote diagnostics, security problem, service, vulnerability.