NETWORK AND APPLICATION SECURITY

DOI 10.20535/2411-1031.2020.8.2.222603
УДК 004.056.53

АРТЕМ ЖИЛІН,
ДМИТРО ПАРФЕНЮК,
СЕРГІЙ МІТІН

ВИМОГИ ДО МІЖМЕРЕЖЕВИХ ЕКРАНІВ ВЕБ ЗАСТОСУНКІВ

Проаналізовано вітчизняні та іноземні нормативні документи, які стосуються захисту веб застосунків. Встановлено, що при розробленні комплексної системи захисту інформації повинні враховуватися вимоги до окремих її засобів захисту. Найефективнішим з елементів комплексу засобів захисту для автоматизованих систем класу 2 та 3, на яких функціонують веб сервери є міжмережевий екран веб застосунків, вимоги до якого у відкритих джерелах відсутні. Тому розроблення таких вимог є актуальною та нагальною проблемою, вирішення якої дозволить спростити розроблення комплексної системи захисту інформації. Виходячи з актуальності результатами роботи є сформовані вимоги до міжмережевих екранів веб застосунків. Одними з небагатьох відкритих джерел, які дозволяють реалізувати такий компонент комплексної системи захисту інформації як міжмережевий екран веб застосунків є перелік правил від корпорації MITRE та відкритого проекту забезпечення безпеки веб застосунків OWASP. Проте ці правила не реалізують розроблених вимог, тому додатково запропоновано та впроваджено правила фільтрації до міжмережевих екранів веб застосунків, які їм відповідають. Сформовано методику їхньої перевірки на відповідність встановленим вимогам. На основі таких утиліт як Metasploit FW, nikto, dirb, wafninja розроблено програмний застосунок, що реалізує зазначену методику. Він має безпосередній зв'язок з базою даних CVE, що дозволяє виявляти й перевіряти актуальні вразливості. Як компонент захисту використано OWASP ModSecurity, вихідний код якого знаходиться на офіційних репозиторіях й функціонує на базі веб сервера nginx. Можливості ModSecurity розширено розробленим динамічним конектором, що дозволяє використовувати міжмережевий екран веб застосунків як окремий засіб захисту інформації. В розробленому засобі захисту реалізовано визначені правила фільтрації. Цим задовольняються такі вимоги до комплексу засобів захисту в комплексній системі захисту інформації як безперервний захист комп'ютерних систем та модульна структура.

Ключові слова: веб застосунок, міжмережевий екран, вимога, комплексна система захисту інформації, комплекс засобів захисту, OWASP ModSecurity.

Постановка проблеми. Захисту від несанкціонованого доступу в усіх інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (ІТС) підлягає відкрита та конфіденційна інформація суб'єктів владних повноважень, військових формувань та будь-яких державних установ чи громадян, яка оприлюднюється в Інтернеті та інших інформаційних мережах і системах. Для забезпечення захисту цієї інформації в ІТС створюється комплексна система захисту інформації (КСЗІ). Процес створення КСЗІ полягає у здійсненні комплексу взаємоузгоджених заходів, спрямованих на розроблення і впровадження інформаційних технологій, які забезпечують оброблення інформації в ІТС згідно з вимогами, встановленими нормативно-правовими документами у сфері захисту інформації.

При створенні КСЗІ визначається загальна структура та склад, вимоги до можливих заходів, методів та засобів захисту інформації, допустимі обмеження щодо них. Також до технічного завдання включаються вимоги, які є загальними як для окремих складових ІТС,

так і для ІТС в цілому. При розробленні проектних рішень здійснюються організаційно-технічні заходи щодо забезпечення послідовності розроблення комплексів засобів захисту від несанкціонованого доступу (КЗЗ), архітектури, середовища функціонування відповідно до заданого рівня гарантій безпеки, згідно з нормативними документами.

Однак, на даний момент найкращим рішенням для захисту веб ресурсів є використання міжмережевого екрану веб застосунку (WAF), проте відповідних узагальнених вимог до нього не висунуто та загальнодоступної реалізації не представлено.

Аналіз останніх досліджень і публікацій. Більша частина наукових робіт за темою WAF присвячена його використанню щодо протидії відомим атакам на веб застосунки. Так, в [1] розглядається завдання використання WAF для протидії фішингу на об'єкти критичної інфраструктури. Проблему виправлення вразливостей WAF шляхом формалізації рішення задачі комбінаторної оптимізації, але лише щодо вразливостей типу SQL ін'єкцій, описано в [2]. Також ряд робіт, зокрема й [3], спрямовані на аналіз можливостей й підходів до застосування WAF щодо захисту веб застосунків. Тому доцільно проаналізувати існуючі вимоги до WAF, варіанти його реалізації та методики перевірки його відповідності існуючим та встановленим вимогам.

Метою роботи є формування вимог до реалізації міжмережевого екрану веб застосунків, а також розроблення методики й інструментарію перевірки відповідності WAF встановленим вимогам.

Виклад основного матеріалу. Міжмережевий екран веб застосунків – це програмний або програмно-апаратний комплекс, який виступає захисним елементом веб застосунку або комплексу веб застосунків.

Узагальнена структурна схема місця WAF в архітектурі мережі представлена на рис. 1, де Web-server – сервер, на якому запущено службу, Web application – веб застосунок, WAF – Web application firewall – міжмережевий екран веб застосунку, NSS – Network security systems – системи мережевої безпеки.

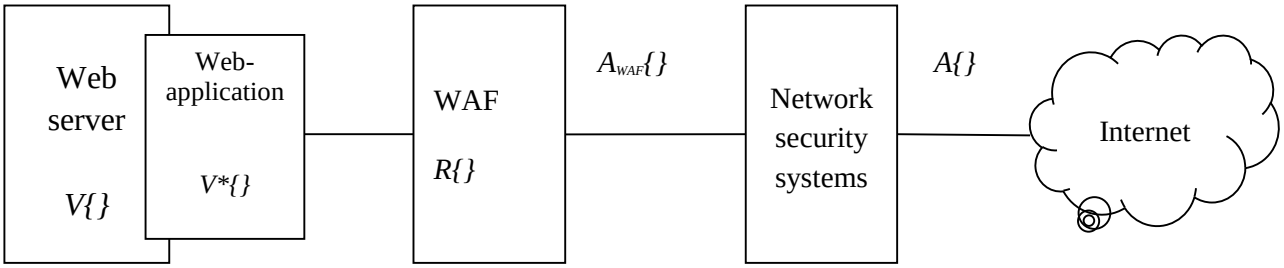

Рисунок 1 – Узагальнена структурна схема місця WAF у мережі

Нехай:

$V = \{v_n\}$ – множина вразливостей веб-серверу, $n = \overline{1,N}$.

$V^* \subset V$ – множина вразливостей веб застосунку, яка є підмножиною множини вразливостей веб-серверу;

$A = \{a_k\}, k = \overline{1,K}$ – множина можливих атак;

$A_{WAF} \subset A$ – множина атак спрямованих на веб застосунок, які повинен нейтралізувати міжмережевий екран.

Тоді, декартовим добутком множин можливих атак і вразливостей буде множина, елементами якої будуть впорядковані пари атака-вразливість

$$A \times V = \{(a_k, v_n)\}, k = \overline{1,K}; n = \overline{1,N}.$$

Виходячи з цього, можна визначити відображення (функцію):

$$F : A \times V \to \{0,1\},$$

яка для заданої пари $(a_k, v_n) \in A \times V$, для будь-яких $k = \overline{1,K};\ n = \overline{1,N}$, ставить у відповідність значення 0 (неможливість використання атакою a_k вразливості v_n), або 1 (атака a_k використовує вразливість v_n), тобто

$$F(a_k, v_n) = \begin{cases} 0, a_k \text{ не використовує } v_n, \\ 1, a_k \text{ використовує } v_n \end{cases}.$$

Зауваження. Певна атака a_k може використовувати декілька вразливостей.

За відсутності WAF з'являється умова реалізації атак з множини A_{WAF} через вразливості V^*. Тобто, можна розглянути звуження функції F з області визначення $A \times V$ на $A_{WAF} \times V^*$. Тоді

$$F^* : A_{WAF} \times V^* \to \{0,1\}.$$

Беручи за основу попередні викладення уточнимо

$$\forall a_k \in A_{WAF}, v_n \in V^* : F^*(a_k, v_n) = \begin{cases} 0, a_k \text{ не використовує } v_n, \\ 1, a_k \text{ використовує } v_n \end{cases},$$

при чому $\forall a_k \in A_{WAF}\ \exists v_n \in V^* : F^*(a_k, v_n) = 1$

Якщо $|A| = K;\ |V| = N$, то функція F має $2^{K \cdot N}$ різних аргументів, а всі значення можна представити як бітовий рядок довжини $2^{K \cdot N}$.

Нехай $R = \{r_i; i = \overline{1,I}\}$ – множина вимог до міжмережевого екрану веб застосунків щодо протидії можливим успішним атакам з множини A_{WAF} на веб застосунки.

При цьому будь-яка вимога може бути реалізована певною кількістю механізмів захисту. Отже, позначимо $P = \{p_l; l = \overline{1,L}\}$ множину механізмів захисту. Нехай $B(P)$ – булеан множини P, тобто множина всіх підмножин множини P. Тоді має бути встановлена відповідність:

$$(\forall r_i \in R)(\exists P_i \in B(P)) \quad (1)$$

тобто r_i визначає механізми захисту, що можуть бути реалізовані.

Якщо розглянути $P_i \in B(P)$ – підмножину механізмів захисту, що реалізують певну вимогу, то вони визначають підмножину вразливостей, яка буде нейтралізована за допомогою цих механізмів $v_i \in B(V) (або\ V^*)$.

Тобто $P_i \in B(P) \to v_i \in V$ визначає відповідність між P_i та v_i. При чому для будь-якої вимоги r_i існує підмножина механізмів захисту P_i, які їх реалізують. Тому ця підмножина визначає множину вразливостей V_i й відповідним її елементам можливі успішні атаки $F^*(a_k, v_n) = 1$, що будуть нейтралізовані

$$(\forall r_i \in R)(\exists P_i \in B(P)) : (P_i \to v_i \text{ так,що} (\forall v_n \in V_i)(\exists a_k \in A_{WAF}) : F^*(a_k, v_n) = 1)$$

при чому всі A_i будуть закриті.

Умови успішності та неуспішності проведення атаки:

$$(\forall (a_k, v_n) : F(a_k, v_n) = 1)(\forall p_i \in P) :$$

$$S(v_n, p_i) = \begin{cases} 1, \text{ якщо механізм } p_i \text{ не закриває вразливість}, \\ 0, \text{ якщо механізм } p_i \text{ закриває вразливість}. \end{cases}.$$

Отже, для будь-якої пари атака-вразливість (a_k, v_n) за умови її можливості $F^*(a_k, v_n) = 1$ й для будь-якого механізму захисту $\forall p_i \in P$ можливий варіант, що вибраний механізм захисту нейтралізує або ні наявну вразливість.

Вразливість v_n буде нейтралізованою, якщо існує механізм захисту, який успішно протидіє атаці

$$\forall p_i \in P : S(v_n, p_i) = 0, \quad (2)$$

а так як механізми захисту визначаються вимогою (1), то для побудови ефективного міжмережевого екрану веб застосунку потрібно визначити вимоги, що і розробляються в роботі. Також для перевірки правильності висунутих вимог і, як наслідок, коректності реалізованих механізмів захисту в міжмережевому екрані веб застосунку під час виконання роботи реалізовано інструмент для тестування.

На рис. 2 зображено послідовність аналізу основних національних, вендерних та державних стандартів, які прямо чи опосередковано містять інформацію про вимоги до міжмережевих екранів взагалі й до міжмережевих екранів веб застосунків, зокрема.

Рисунок 2 – Послідовність аналізу нормативних документів та найкращих практик для формування вимог

До першої групи віднесено міжнародні стандарти серії ISO/IEC 27000 [4], які встановлюють вимоги й настанови до забезпечення інформаційної безпеки організацій. Стандартом ISO/IEC 27001 визначаються вимоги до процесів розроблення системи управління інформаційною безпекою [5], але він є загальним і призначеним для застосування всіма організаціями, незалежно від їх типу, розміру і характеру. Цим документом не встановлюються технічні деталі, тому необхідне доповнення елементами управління інформаційною безпекою з ISO/IEC 27002 [6] для оброблення ризиків, пов'язаних з втратою конфіденційності, цілісності та доступності інформації. Стандартом ISO/IEC 27032 [7] визначаються порядок збереження цих властивостей інформації в кіберпросторі. В центрі уваги цього документу лежить вирішення питання безпеки в глобальній мережі Інтернет і надання технічних настанов для оброблення ризиків безпеки.

Наступним документом є ISO/IEC 27033 [8]. Метою ISO/IEC 27033 є надання детальної настанови по аспектах безпеки управління, експлуатації та використання інформаційних систем в мережі і їх взаємозв'язку. ISO/IEC 27033 містить докладний посібник щодо реалізацій елементів управління інформаційною безпекою, які введені в ISO/IEC 27002.

В розділі ISO/IEC 27033-4 описано, що шлюзами забезпечення інформаційної безпеки повинен здійснюватися контроль мережевого трафіку за допомогою:

1. Фільтрування пакетів.
2. Стандартного аналізування мережевих пакетів.
3. Проксі програм (міжмережевих екранів прикладного рівня).
4. Трансляції мережевих адрес (англ. Network Address Translation, NAT).
5. Аналізу контенту та фільтрації мережевого трафіку.

ISO/IEC 27035 [9] в своєму керівництві з планування та підготовки до реагування на інциденти містить 8 основних положень, одним з яких є надання інформації системі реагування щодо подій безпеки. У ISO/IEC 15408 [10] представлені критерії для оцінки механізмів безпеки програмно-технічного рівня. Цей стандарт визначає функціональні вимоги безпеки та адекватності реалізації функцій безпеки.

Серед вітчизняних нормативно-правових документів можна виділити 4 основні документи, що стосуються забезпечення інформаційної безпеки в глобальній мережі Інтернет.

НД ТЗІ 2.5-004-99 [11] надає методологічну базу для визначення вимог з захисту інформації в комп'ютерних системах від несанкціонованого доступу, створення захищених комп'ютерних систем і засобів захисту від несанкціонованого доступу, оцінки захищеності інформації в комп'ютерних системах і їх придатності для обробки критичної інформації.

Цим документом визначається:

1. Порівняльна шкала для оцінювання надійності механізмів захисту інформації від несанкціонованого доступу, реалізованих в комп'ютерних системах.
2. База для розроблення комп'ютерних систем, в яких мають бути реалізовані функції захисту інформації.

НД ТЗІ 2.5-005-99 [12] встановлює принципи класифікації автоматизованих систем і стандартних функціональних профілів захищеності інформації, що оброблюється, від несанкціонованого доступу.

НД ТЗІ 2.5-010-03 [13] визначає й описує вимоги до технічних та організаційних заходів щодо захисту інформації веб сторінки в глобальній мережі Інтернет. Згідно з визначеними НД ТЗІ 2.5-004-99 специфікаціями він встановлює мінімально необхідний перелік послуг безпеки інформації та рівнів їх реалізації у КЗЗ інформації веб сторінки від несанкціонованого доступу. Мета цього нормативного документу – надання нормативно-методологічної бази для розроблення КЗЗ від несанкціонованого доступу до інформації веб сторінки під час створення КСЗІ, спираючись на НД ТЗІ 3.7-003-05 [14]. Зокрема, в ньому зазначається, що функціонування веб сторінки забезпечується автоматизованою системою (АС), за допомогою якої здійснюється актуалізація розміщених на веб сторінці інформаційних ресурсів та керування доступом до них. Оскільки КСЗІ визначається сукупністю організаційних і інженерно-технічних заходів, а також програмно-апаратних засобів, які забезпечують захист інформації, то одним з таких програмно-апаратних засобів може виступати міжмережевий екран веб застосунків.

Національний інститут стандартів і технологій (англ. National Institute of Standards and Technology, NIST) в своєму документі [15] описав широкий список атак, націлених на веб застосунки. Також визначено, що традиційних засобів недостатньо для захисту, так як неможливо заборонити роботу протоколів HTTP/HTTPS. Водночас зазначено, що WAF повинен функціонувати в системі обміну інформацією через мережу Інтернет. Однак не висунуто жодних вимог до міжмережевого екрану веб застосунків.

Асоціація аудиту і контролю інформаційних систем (англ. Information Systems Audit and Control Association, ISACA) [16] є міжнародною професійною організацією, орієнтованою на управління інформаційними технологіями (IT), Основним її завданням є розробка і формалізація єдиних ефективних підходів до оцінки та управління IT-процесами та IT-системами. Щодо міжмережевих екранів ISACA визначила 2 категорії критеріїв, а саме: "загальні критерії", "критерії захисту та попередження веб атак".

До загальних критеріїв, яким має відповідати міжмережевий екран веб застосунків, належать [16]:

1. Проходження ним тестування і демонстрація політики безпеки.
2. Не порушення ним роботи дозволених служб та застосунків.
3. Повинен зберігати цілісність та конфіденційність даних.
4. Повинен підтримувати автентифікацію.

Щодо захисту і попередження міжмережевий екран повинен протидіяти наступним атакам на веб застосунки:

1. Переповнення буферу.
2. Міжсайтовий скриптинг.
3. Підробка запитів та валідації.
4. Відмова в обслуговуванні.
5. Сезонна недієздатність.
6. Неправильне кодування доступу та автентифікації.

Федеральний офіс інформаційної безпеки в Німеччині (англ. Bundesamt für Sicherheit in der Informationstechnik, BSI) в своєму документі [17] вимагає забезпечення фільтрації протоколів більш високого рівня за допомогою WAF. Так як HTTP-протокол передає дані, то аналіз атак на рівні застосунків за допомогою WAF забезпечить виявлення атак раніше, ніж вони потраплять на веб сервер.

Фільтрацію атак в WAF зазвичай може бути зроблено двома способами [17]:

1. Дані перевіряються на наявність відомих моделей атак, які повинні регулярно оновлюватися.
2. Для досягнення надійного рівня захисту, окрім стандартного програмного забезпечення слід використовувати власні правила фільтрації.

Проте, цей документ не описує вимоги до самого WAF.

Ґрунтуючись на висунутих вимогах (2) й проведеному аналізі основних національних, вендерних та державних стандартів сформовано наступні вимоги до WAF:

1. WAF не повинен порушувати роботу служб, що дозволені визначеною політикою безпеки.
2. WAF не повинен змінювати або видаляти вміст даних, що дозволені визначеною політикою безпеки.
3. WAF повинен підтримувати наступні режими роботи:
    1) прозорий міст;
    2) прозорий зворотний проксі-сервер;
    3) зворотний проксі-сервер;
    4) пасивна робота (аналіз логів/записів трафіку);
4. WAF повинен підтримувати наступні варіанти встановлення:
    1) у вигляді віртуальної машини;
    2) у вигляді апаратного комплексу;
    3) у вигляді хмарного сервісу;
5. WAF повинен підтримувати SSL\TLS-термінації з’єднання.
6. WAF повинен підтримувати роботу клієнтських сертифікатів.
7. WAF повинен підтримувати роботу з веб стандартами відмінними від HTTP/HTTPS (Web Sockets, XML, JSON).
8. WAF повинен підтримувати окремі типи блокування.
9. WAF повинен здійснювати сигнатурний аналіз.
10. WAF повинен здійснювати поведінковий і репутаційний аналіз.
11. WAF повинен бути здатним до інтеграції.
12. WAF повинен вести журнал подій безпеки.
13. WAF повинен захищати ідентифікатори сесій.
14. WAF повинен підтримувати користувацькі правила.

15. WAF повинен перевіряти HTTP-транзакції на відповідність RFC.
16. WAF повинен підтримувати відмовостійкість.
17. WAF повинен захищати від наступних атак:
    1) ін’єкції (SQL, OS, NoSQL, LDAP, XML);
    2) підроблена автентифікація;
    3) незахищеність важливих даних (кредитні карти, рахунки);
    4) зовнішній доступ через;
    5) невірно налаштований контроль доступу користувачів;
    6) невірна конфігурація політики безпеки;
    7) міжсайтовий скриптинг;
    8) небезпечна десеріалізація (віддалене виконання коду);
    9) використання компонентів з відомими вразливостями;
    10) вразливості процесів реєстрації та моніторингу.

Вимоги поділяються на 2 підгрупи: системні вимоги (пункти 1-14) та вимоги до механізмів запобігання мережевим атакам (пункти 15-17).

Після встановлення вимог до WAF постає питання щодо розробки методики перевірки відповідності реалізованих міжмережевих екранів веб застосунків цим вимогам. Для досягнення даної мети, методика тестування міжмережевого екрану веб застосунків на відповідність розробленим вимогам формувалась шляхом аналізу і синтезу методик OWASP, OSSTMM. Як наслідок, пропонується розділити процес тестування міжмережевого екрану веб застосунків на дві фази:

1. Перевірка системних вимог (відповідає за перевірку перших 14 пунктів вимог до WAF).
2. Перевірка механізмів запобігання мережевим атакам (відповідає за перевірку роботи механізмів захисту WAF):
    1) перевірка протокольних аномалій (порушення специфікації протоколу HTTP);
    2) перевірка структурних аномалій в запитах та відповідях (синтаксис параметрів, можливі ін’єкції через параметри заголовків, DDOS-атаки, небезпечні типи підключення);
    3) перевірка поведінкових аномалій (порушення політики генерації та зберігання токенів, захоплення сесії, атаки підбору);
    4) перевірка аномалій в сценаріях (перевірка сценаріїв веб застосунку, порушення прав доступу користувачів до ресурсу);
    5) перевірка аномалій компонентів веб застосунку (вразливі версії програмного забезпечення та протоколів шифрування);
    6) перевірка аномалій на стороні клієнта (атаки типу Man-in-the-middle та Man-in-the-browser).

Перевірка системних вимог відбувається шляхом перевірки функціональних можливостей, заявлених вендором щодо міжмережевого екрану веб застосунку. Ці функції повинні надавати максимальний набір можливостей та налаштовуватись офіцером безпеки.

Запобігання мережевим атакам за допомогою WAF повинно відбуваєтьсяся автоматично і потребувати мінімального втручання адміністратора щодо налаштування. Тестування ж відбувається шляхом здійснення всіх можливих атак, зазначених в пунктах 15-17 вимог. Такі дії можна реалізувати за допомогою спеціальних утиліт для тестування або за допомогою розробленої авторами програми WebAnalyzer.

Для реалізації компонента захисту, який відповідає встановленим вимогам було розгорнуто локальну мережу з відповідними кінцевими та проміжними пристроями, зображеними на рис. 3: веб-сервер з вразливими веб застосунками, міжмережевий екран веб застосунку, кінцевий пристрій, який здійснює запити.

Незахищений веб сервер реалізовано на базі дистрибутиву Ubuntu – BeeBox, так як він містить вразливі застосунок за всіма категоріями OWASP TOP 10. Серед найпоширеніших реалізацій міжмережевого екрану веб застосунку з відкритим кодом розглянуті такі рішення:

NAXSI, IronBee, WebKnight, Shadow Daemon та ModSecurity. У якості WAF використано ModSecurity module на базі веб серверу NGINX Open Source в режимі зворотного проксі, так як це єдине рішення, яке відповідає зазначеним вище функціональним вимогам. Встановлено динамічний конектор шляхом компіляції його вихідного коду з вихідним кодом веб сервера. Після чого модуль ModSecurity скомпільовано у якості додаткового компонента веб серверу NGINX. Цим досягається модульність архітектури міжмережевого екрану веб застосунку. Під час налаштування використовувались офіційні документи компанії NGINX [18] та інших ресурсів [19], [20], але основну частину складають авторські налаштування.

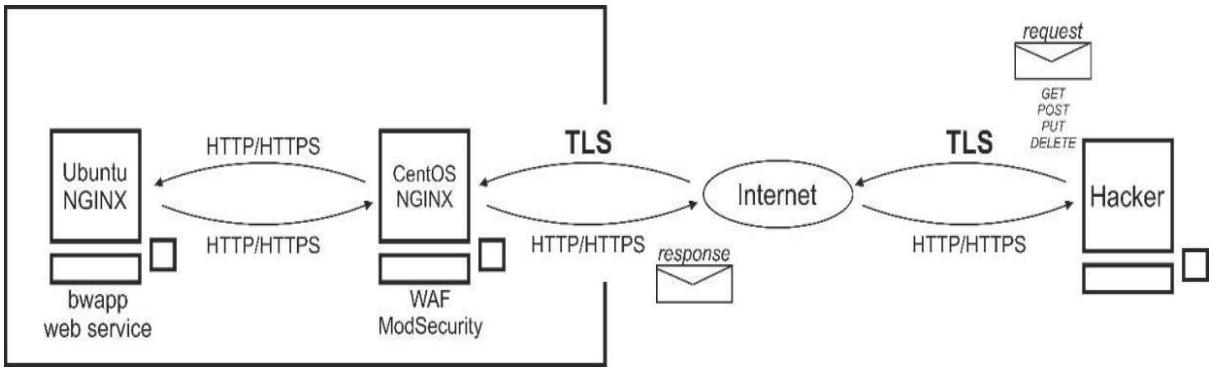

Рисунок 3 – Структурна схема розгорнутої мережі
(IP-адреса BeeBox: 192.168.200.128, IP-адреса NGINX: 192.168.200.39,
IP-адреса Windows 10: 192.168.200.1, IP-адреса Kali Linux 2.0: 192.168.200.40)

Програма WebAnalyzer, написана мовою програмування Python 3.7.2 й реалізує прив'язку до терміналу дистрибутивів Linux та є кросплатформною. WebAnalyzer має графічний інтерфейс з одним полем вводу для URL-адреси та кнопкою запуску. Після початку роботи створюється два файли в теці "reports" в кореневому каталозі програми зі звітами про сканування.

Показати працездатність налаштування WAF можна шляхом тестування вразливого веб серверу, виконавши наприклад SQL ін'єкцію. Спочатку тестування відбувається без, а потім з увімкненим WAF. На рис. 4 на розроблений для тестування веб додаток за адресою 192.168.200.128/bWAPP/sqli3.php проведено атаку, де передбачена чутливість до SQL ін'єкцій. В поле Login введено *'or 1=1* -- , а в поле "Password" будь-яке значення.

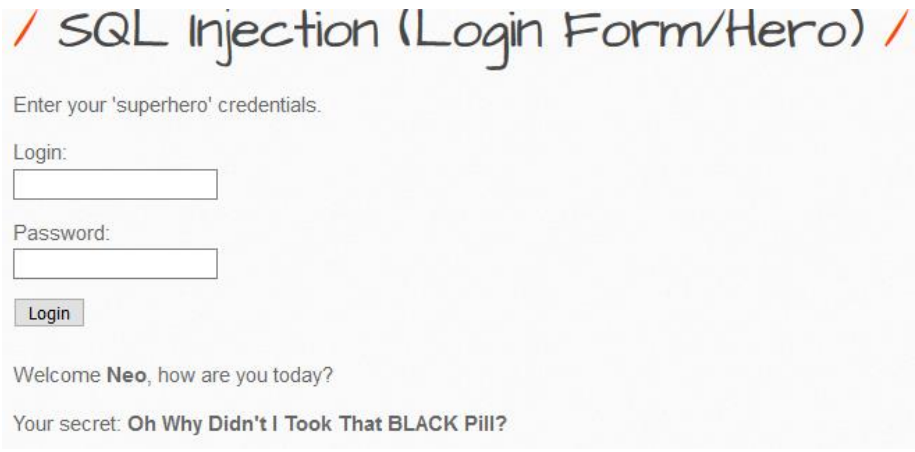

Рисунок 4 – Результат проведення SQL ін'єкції

Результатом даної операції є отримання доступу до облікового запису користувача без знань логіну та пароля. На рис. 5 зображені результати проведення аналогічних дій через зворотній проксі-сервер, які не дали жодних дієвих результатів.

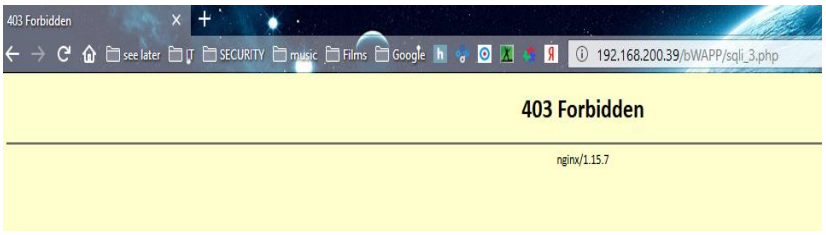

Рисунок 5 – Результат проведення SQL ін’єкції через проксі-сервер

Переконавшись в коректній роботі міжмережевого екрану веб застосунку на найпростіші атаці нижче продемонстровано результат перевірки розробленого WAF на вразливості, які зазначені у розроблених вимогах до WAF за допомогою програми WebAnalyzer. На рис. 6 показано результат роботи програми при скануванні безпосередньо вразливого веб серверу, де у файлі зліва записані всі можливі вразливості, а у файл справа – всі альтернативні приховані адреси для доступу.

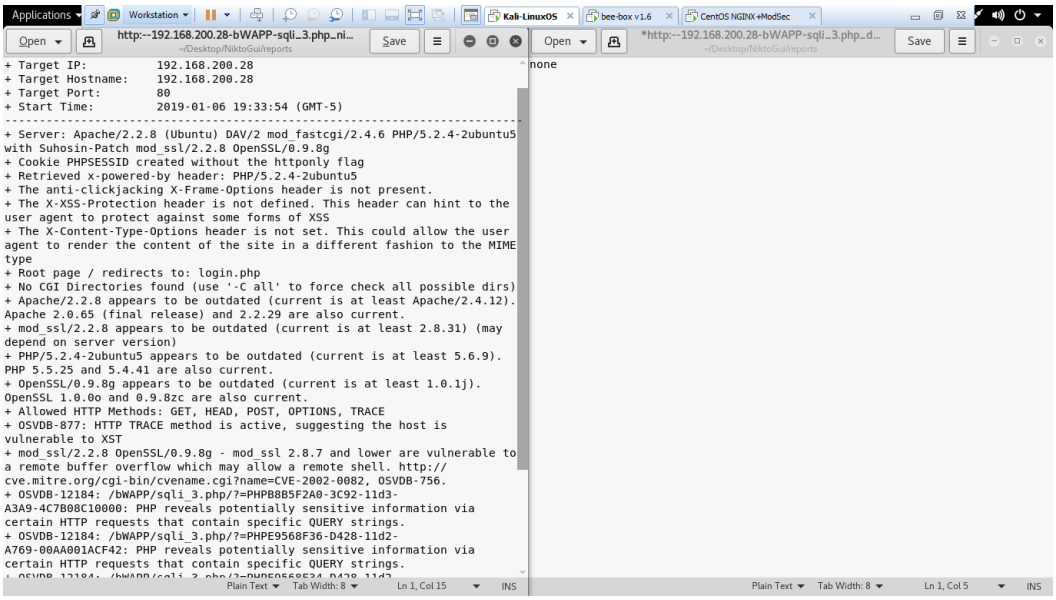

Рисунок 6 – Результат сканування

На рис. 7 в свою чергу показано результат сканування через проксі-сервер. Проаналізувавши їх, видно, що аналізатор не виявив потенційних атак, націлених на бази даних.

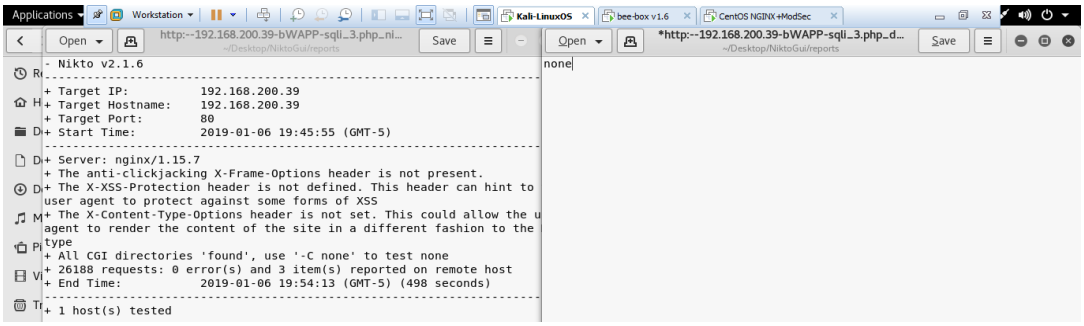

Рисунок 7– Результат сканування через проксі-сервер

Проте рекомендовані правила не захищають від усіх атак. Про це свідчить результат проведення HTML-ін’єкції з включеним міжмережевим екраном веб застосунку (див. рис. 8)

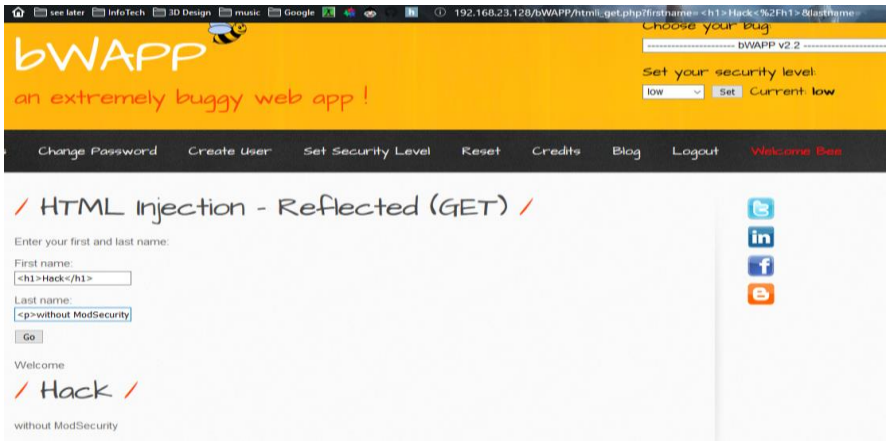

Рисунок 8 – Результат проведення HTML-ін’єкції через зворотний проксі-сервер з OWASP TOP 10 CRS

Для того, щоб міжмережевий екран веб застосунку відповідав встановленим вимогам імпортовані розроблені правила, після чого реакцією ModSecurity на аналогічну атаку є заборона доступу (див. рис. 9).

Рисунок 9 – Результат реагування ModSecurity, після підключення додаткових правил

У свою чергу після сканування ресурсу розробленою програмою результат буде наступним (див. рис. 10):

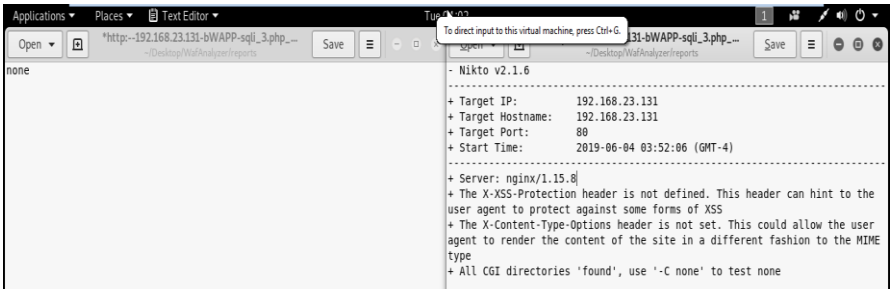

Рисунок 10 – Результати сканування після імпорту власних правил

Висновок. У роботі проаналізовано міжмережевий екран веб застосунків та необхідність визначення вимог щодо нього. З метою їхнього формування проаналізовано ряд положень основних національних, вендерних та державних стандартів та вимог. Всі вони надають нормативно-методологічну базу для розроблення КЗЗ від несанкціонованого доступу до інформації веб-сторінки під час створення КСЗІ, але не висувають вимог щодо роботи її окремих елементів, зокрема WAF.

На основі аналізу сформовано вимоги до міжмережевого екрану веб застосунків та методика його перевірки. Також показано, що рекомендовані компанією MITRE правила OWASP Top 10 CRS для міжмережевих екранів веб застосунків не забезпечують реалізацію встановлених вимог, в результаті чого додатково розроблено власні правила. З метою підтвердження отриманих теоретичних результатів у якості WAF обрано та налаштовано NGINX ModSecurity. А вже з метою перевірки налаштованого згідно з встановленими вимогами WAF NGINX ModSecurity розроблено програму WafAnalyzer.

Отримані результати можна застосовувати в підрозділах, які займаються експертизою елементів КЗЗ при побудові КСЗІ. Окрім цього перспективним напрямком продовження роботи є підґрунтя для розроблення нормативного документу у сфері ТЗІ, яким визначатимуться вимоги до міжмережевих екранів веб застосунку як компонента КСЗІ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] K. Demertzis, and L. Iliadis, "Cognitive Web Application Firewall to Critical Infrastructures Protection from Phishing Attacks", *Journal of Computations & Modelling*, vol. 9, no. 2, pp. 1-26, 2019.

[2] D. Appelt, A. Panichella, and L. Briand, "Automatically Repairing Web Application Firewalls Based on Successful SQL Injection Attacks", in *Proc. IEEE 28th International Symposium on Software Reliability Engineering (ISSRE),* Toulouse, pp. 339-350, 2017, doi: 10.1109/ISSRE. 2017.28.

[3] A. M. Hasan, D. T. Meva, A. K. Roy, and J. Doshi, "Perusal of web application security approach", in *Proc. International conference on intelligent communication and computational techniques (ICCT),* pp. 90-95, 2017, doi: 10.1109/INTELCCT.2017.8324026.

[4] International Organization for Standardization. (2018, Febr. 07). *ISO/IEC 27000, Information technology. Security techniques. Information security management systems. Overview and vocabulary. Requirements.* [Online]. Available: https://www.iso.org/ru/ standard/73906.html. Accessed on: Sept. 10, 2020.

[5] International Organization for Standardization. (2013, Okt. 1). *ISO/IEC 27001, Information technology. Information security management systems. Requirements*. [Online]. Available: https://www.iso.org/standard/54534.html. Accessed on: Sept. 10, 2020.

[6] International Organization for Standardization. (2013, Sept. 25). *ISO/IEC 27002, Information technology. Security techniques. Code of practice for information security controls. Technical Corrigendum 2*. [Online]. Available: https://www.iso.org/ru/standard/ 69379.html. Accessed on: Sept. 10, 2020.

[7] International Organization for Standardization. (2012, Jul. 16). *ISO/IEC 27032, Information technology. Security techniques. Guidelines for cybersecurity*. [Online]. Available: https://www.iso.org/ru/standard/44375.html. Accessed on: Sept. 10, 2020.

[8] International Organization for Standardization. (2015, Okt. 10). *ISO/IEC 27033-1, Information technology. Security techniques. Network security*. [Online]. Available: https://www.iso.org/ ru/standard/63461.html. Accessed on: Sept. 10, 2020.

[9] International Organization for Standardization. (2016, Okt. 28). *ISO/IEC 27035-1, Information technology. Security techniques. Information security incident management*. [Online]. Available: https://www.iso.org/ru/standard/60803.html. Accessed on: Sept. 10, 2020.

[10] International Organization for Standardization. (2009, Dec. 09). *ISO/IEC 15408, Information technology. Security techniques. Evaluation criteria for IT security*. [Online]. Available: https://www.iso.org/ru/standard/50341.html. Accessed on: Sept. 10, 2020.

[11] ДСТСЗІ СБ України. (1999, Квіт. 28). *НД ТЗІ 2.5-004-99, Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу*. [Електронний ресурс]. Доступно: https://tzi.ua. Дата звернення: Верес. 25, 2020.

[12] ДСТСЗІ СБ України. (1999, Квіт. 28). *НД ТЗІ 2.5-005-99, Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу*. [Електронний ресурс]. Доступно: https://tzi.ua. Дата звернення: Верес. 25, 2020.

[13] ДСТСЗІ СБ України. (2003, Квіт. 03). *НД ТЗІ 2.5-010-03, Вимоги до захисту WEB-сторінки від несанкціонованого доступу*. [Електронний ресурс]. Доступно: https://tzi.com.ua. Дата звернення: Верес. 25, 2020.

[14] ДСТСЗІ СБ України. (2005, Лист. 8). *НД ТЗІ 3.7-003, Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі*. [Електронний ресурс]. Доступно: http://www.dsszzi.gov.ua. Дата звернення: Серп. 25, 2020.

[15] National Institute of Standards and Technology. (2007, Aug. 7). *NIST Special Publication 800-95, Guide to Secure Web Services*. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-95.pdf. Accessed on: Sept. 10, 2020.

[16] ICSAlabs (2018, Feb. 23) WAF Criteria V2.1 Document V2.4, 2016. [Online]: Available: https://www.ptsecurity.com/upload/corporate/ww-en/products/documents/af/PTSecurity-PTAF-WAF-Report-180223.pdf. Accessed on: Sept. 10, 2020.

[17] BSI S 5.169 System architecture of a web application. [Online]: Available: https://enos.itcollege.ee/~valdo/bsieng/en/gstoolhtml/m/m05/m05169.html. Accessed on: Sept. 10, 2020.

[18] F. Memon, O. Garrett and M. Pleshakov, Modsecurity 3.0 & NGINX: Quick Start Guide. NGINX, Inc 2018.

[19] I. Ristic, Modsecurity handbook. Feisty Duck, 2010.

[20] Формати даних ModSecurity. Таблиця компонентів [Електронний ресурс]. Доступно: https://github.com/SpiderLabs/ModSecurity/wiki/ModSecurity-2-Data-Formats. Дата звернення: Серп. 25, 2020.

Стаття надійшла до редакції 28.09.2020.

REFERENCE

[1] K. Demertzis, and L. Iliadis, "Cognitive Web Application Firewall to Critical Infrastructures Protection from Phishing Attacks", *Journal of Computations & Modelling*, vol. 9, no. 2, pp. 1-26, 2019.

[2] D. Appelt, A. Panichella, and L. Briand, "Automatically Repairing Web Application Firewalls Based on Successful SQL Injection Attacks", in *Proc. IEEE 28th International Symposium on Software Reliability Engineering (ISSRE),* Toulouse, pp. 339-350, 2017, doi: 10.1109/ISSRE. 2017.28.

[3] A. M. Hasan, D. T. Meva, A. K. Roy, and J. Doshi, "Perusal of web application security approach", in *Proc. International conference on intelligent communication and computational techniques (ICCT),* pp. 90-95, 2017, doi: 10.1109/INTELCCT.2017.8324026.

[4] International Organization for Standardization. (2018, Febr. 07). *ISO/IEC 27000, Information technology. Security techniques. Information security management systems. Overview and vocabulary. Requirements.* [Online]. Available: https://www.iso.org/ru/ standard/73906.html. Accessed on: Sept. 10, 2020.

[5] International Organization for Standardization. (2013, Okt. 1). *ISO/IEC 27001, Information technology. Information security management systems. Requirements*. [Online]. Available: https://www.iso.org/standard/54534.html. Accessed on: Sept. 10, 2020.

[6] International Organization for Standardization. (2013, Sept. 25). *ISO/IEC 27002, Information technology. Security techniques. Code of practice for information security controls. Technical Corrigendum 2*. [Online]. Available: https://www.iso.org/ru/standard/ 69379.html. Accessed on: Sept. 10, 2020.

[7] International Organization for Standardization. (2012, Jul. 16). *ISO/IEC 27032, Information technology. Security techniques. Guidelines for cybersecurity*. [Online]. Available: https://www.iso.org/ru/standard/44375.html. Accessed on: Sept. 10, 2020.

[8] International Organization for Standardization. (2015, Okt. 10). *ISO/IEC 27033-1, Information technology. Security techniques. Network security*. [Online]. Available: https://www.iso.org/ru/standard/63461.html. Accessed on: Sept. 10, 2020.

[9] International Organization for Standardization. (2016, Okt. 28). *ISO/IEC 27035-1, Information technology. Security techniques. Information security incident management*. [Online]. Available: https://www.iso.org/ru/standard/60803.html. Accessed on: Sept. 10, 2020.
[10] International Organization for Standardization. (2009, Dec. 09). *ISO/IEC 15408, Information technology. Security techniques. Evaluation criteria for IT security*. [Online]. Available: https://www.iso.org/ru/standard/50341.html. Accessed on: Sept. 10, 2020.
[11] DSTSIP SS of Ukraine. (1999, Apr. 28). *ND TZII, 2.5-004-99 Criteria for assessing the security of information in computer systems from unauthorized access*. [Online]. Available: https://tzi.ua. Accessed on: Sept. 25, 2020.
[12] DSTSIP SS of Ukraine. (1999, Apr. 28). *ND TZII 2.5-005-99, Classification of automated systems and standard functional profiles of protection of processed information from unauthorized access*. [Online]. Available: https://tzi.ua. Accessed on: Sept. 25, 2020.
[13] DSTSIP SS of Ukraine. (2003, Apr. 03). *ND TZII 2.5-010-03, Requirements to protect the WEB-page from unauthorized access*. [Online]. Available: https://tzi.com.ua. Accessed on: Sept. 25, 2020.
[14] DSTSIP SS of Ukraine. (2005, Nov. 8). *ND TZII 3.7-003, The procedure for creating a comprehensive information security system in the information and telecommunications system*. [Online]. Available: http://www.dsszzi.gov.ua. Accessed on: Aug. 25, 2020.
[15] National Institute of Standards and Technology. (2007, Aug. 7). *NIST Special Publication 800-95, Guide to Secure Web Services*. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-95.pdf. Accessed on: Sept. 10, 2020.
[16] ICSAlabs (2018, Feb. 23) WAF Criteria V2.1 Document V2.4, 2016. [Online]: Available: https://www.ptsecurity.com/upload/corporate/ww-en/products/documents/af/PTSecurity-PTAF-WAF-Report-180223.pdf. Accessed on: Sept. 10, 2020.
[17] BSI S 5.169 System architecture of a web application. [Online]: Available: https://enos.itcollege.ee/~valdo/bsieng/en/gstoolhtml/m/m05/m05169.html. Accessed on: Sept. 10, 2020.
[18] F. Memon, O. Garrett and M. Pleshakov, Modsecurity 3.0 & NGINX: Quick Start Guide. NGINX, Inc 2018.
[19] I. Ristic, Modsecurity handbook. Feisty Duck, 2010.
[20] ModSecurity data formats. Component table [Online]. Available: https://github.com/SpiderLabs/ModSecurity/wiki/ModSecurity-2-Data-Formats. Accessed on: Aug. 25,2020.

ARTEM ZHYLIN,
DMYTRO PARFENIUK,
SERHII MITIN

REQUIREMENTS FOR WEB APPLICATIONS FIREWALLS

Domestic and foreign regulations related to the protection of web applications are analyzed. It is established that the requirements for its individual means of protection should be taken into account when developing a comprehensive information protection system. The most effective of the elements of the complex of means of protection for automated systems of class 2 and 3, on which web servers operate is the firewall of web applications, which is not required in open sources. Therefore, the development of such requirements is an urgent and urgent problem, the solution of which will simplify the development of a comprehensive information security system. Based on the relevance of the results of the work are the requirements for firewalls of web applications. One of the few open sources that allows you to implement such a component of a comprehensive information security system as the firewall of web applications is a list of rules from MITRE and the open project to ensure the security of web applications OWASP. However, these rules do not implement the developed requirements, so in addition, proposed and implemented rules for filtering

the firewalls of web applications that meet them. The technique of their check on conformity to the established requirements is formed. Based on such utilities as Metasploit FW, nikto, dirb, wafninja, a software application has been developed that implements this technique. It has a direct link to the CVE database, which allows you to detect and check for current vulnerabilities. OWASP ModSecurity is used as a security component, the source code of which is located on official repositories and operates on the basis of the nginx web server. The capabilities of ModSecurity are enhanced by a developed dynamic connector that allows you to use the firewall of web applications as a separate means of protecting information. Certain filtering rules are implemented in the developed protection tool. This satisfies the requirements for a set of security features in a comprehensive information security system such as continuous protection of computer systems and a modular structure.

Keywords: web applications, firewall, requirement, comprehensive information security system, security suite, OWASP ModSecurity.

Жилін Артем Вікторович, кандидат технічних наук, доцент кафедри кібербезпеки і застосування інформаційних систем і технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

ORCID: 0000-0002-4959-612X.

E-mail: zhylinartem@gmail.com.

Парфенюк Дмитро Миколайович, інженер, Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України, Київ, Україна.

ORCID: 0000-0002-9255-9340.

E-mail: parfeniukink@gmail.com.

Мітін Сергій Вячеславович, старший викладач кафедри кібербезпеки і застосування інформаційних систем та технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

ORCID 0000-0002-4936-2569.

E-mail: meetser@gmail.com.

Zhylin Artem, candidate of technical sciences, associate professor at the cybersecurity and application of information systems and technologies academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

Parfeniuk Dmytro, engineer, State centre of cyberdefence of State service of special communication and information protection of Ukraine, Kyiv, Ukraine.

Sergii Mitin, senior lecturer at the cybersecurity and application of information systems and technologies academic department, Institute of special communication and information protection National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv.