КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА
ФАКУЛЬТЕТ РАДІОФІЗИКИ, ЕЛЕКТРОНІКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ

Кафедра радіотехніки та радіоелектронних систем

«На правах рукопису»

Робота допущена до захисту в ЕК
рішенням кафедри радіотехніки та радіоелектронних систем
від ___ червня 2024 року, протокол № ___.
Завідувач кафедри доктор фіз.-мат. наук, професор
Ігор АНІСІМОВ

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА
на тему:
"Захист web-сайту для недержавних компаній: аналіз загроз
та розробка ефективних стратегій кібербезпеки"

Виконав:
студент 4-го курсу
денної форми навчання
спеціальності 172 - Телекомунікації та радіотехніка
ОПП «Інформаційна безпека телекомунікаційних систем і мереж»
Рижко Дмитро Олександрович

Науковий керівник:
кандидат військових наук, доцент
Добвня Сергій Якович

Рецензент:
Доктор технічних наук, старший науковий співробітник
Владимирський Олександр Альбертович

Засвідчую, що у цій бакалаврській роботі
немає запозичень з праць інших авторів без
відповідних посилань
Студент Рижко Дмитро Олександрович

Київ-2024

ЗМІСТ

РЕФЕРАТ

Дипломна робота: ст. 36, 4. табл., 16 джерел.

Ключові слова – SWIFT, FTA, МЕТЕЛИК

Об’єкт дослідження - захист web-сайтів для недержавних компаній, включаючи аналіз потенційних загроз кібербезпеці.

Мета роботи - розробити ефективні стратегії кібербезпеки для захисту -web-сайтів недержавних компаній в Україні, враховуючи їх особливості та обмежені ресурси.

1. Проаналізовано актуальні кіберзагрози в Україні, враховуючи контекст кібер-війни.
2. Оцінено вразливості типових -web-сайтів недержавних компаній.
3. Запропоновано комплексні стратегії захисту, включаючи технічні, організаційні та соціальні заходи.
4. Оцінено ефективність запропонованих стратегій та надано практичні рекомендації.

Результати роботи мають практичне значення для недержавних компаній - підвищення рівня кібербезпеки web-сайтів.

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ

КА-2 - базова адміністративна конфіденційність;

ДР-1 - квоти;

НЦ-1 - КЗЗ з контролем цілісності;

SWIFT - Structured what-if technique (Що?, якщо?);

ПЗ – Програмне-забезпечення;

FTA – Fault Tree Analysis;

ETA – Event Tree Analysis;

Dos/DDoS – Distributed Denial-of-service;

SQL – Structured query language;

КЗЗ – комплекс засобів захисту;

ВСТУП

Тема дипломної роботи "Захист web-сайту для недержавних компаній: аналіз загроз та розробка ефективних стратегій кібербезпеки" є вкрай актуальною в сучасних умовах. В епоху швидкого розвитку інформаційних технологій та збільшення кількості кіберзагроз, забезпечення належного рівня захисту -web-сайтів стає одним із пріоритетних завдань для недержавних компаній в Україні.

Метою роботи є розробка ефективних стратегій кібербезпеки для захисту -web-сайтів недержавних компаній в Україні, враховуючи їхні особливості та обмежені ресурси.

Об’єктом дослідження є захист web-сайтів недержавних компаній, включаючи аналіз потенційних загроз кібербезпеці. У процесі виконання роботи було здійснено наступні завдання:

1. Проаналізовано актуальні кіберзагрози в Україні, враховуючи контекст кібер-війни.

2. Оцінено вразливості типових web-сайтів недержавних компаній.

3. Запропоновано комплексні стратегії захисту, включаючи технічні, організаційні та соціальні заходи.

4. Оцінено ефективність запропонованих стратегій та надано практичні рекомендації.

Використано такі технології та методи, як Fault Tree Analysis (FTA), Structured What-If Technique (SWIFT), КА-2 (базова адміністративна конфіденційність), ДР-1 (квоти), НЦ-1 (комплекс засобів захисту з контролем цілісності), та комплекс засобів захисту (КЗЗ). Завдяки застосуванню цих методів, результати моєї роботи допоможуть недержавним компаніям підвищити рівень кібербезпеки своїх web-сайтів, що сприятиме їхній стійкості перед можливими кіберзагрозами.

1. АНАЛІЗ ЗАГРОЗ БЕЗПЕЦІ WEB-САЙТІВ НЕДЕРЖАВНИХ КОМПАНІЙ

У цьому розділі проведено детальний аналіз сучасних загроз, з якими стикаються -webсайти недержавних компаній. Розглянуті як загальні типи кібератак (технічні, організаційні, соціальні), так і специфічні загрози, характерні саме для недержавного сектору (наприклад, атаки на репутацію, витік даних про донорів чи бенефіціарів).

Наведено:

1. Класифікація загроз;
2. Аналіз вразливостей;
3. Моделювання сценаріїв атак;
4. Оцінка ризиків.

На підставі цього та [1-16] зроблено всебічний огляд загроз, з якими стикаються web-сайти недержавних компаній та їх вразливості.

Це є основою для розробки ефективних стратегій кібербезпеки у наступному розділі.

1.1. МЕТОДИ ВИЯВЛЕННЯ ТА АНАЛІЗУ ВРАЗЛИВОСТЕЙ WEB-САЙТУ

Виявлення та аналіз вразливостей web-сайту є ключовим етапом у розробці ефективних стратегій кібербезпеки. Цей розділ присвячений опису методів, які були використані для ідентифікації та аналізу вразливостей web-сайтів недержавних компаній [1-5]. Застосовані методи включають аналізування за схемою «краватка-метелик», SWIFT (Структурований метод «Що? Якщо?») та аналізування дерева подій (FTA). В дипломній роботі використовувалися три різни методи аналізів web-атак.

Аналіз застосування методів наведено на рисунках 1.1, 1.2 та в таблиці 1. Детальна інформація та опис наведено в Додатку А.

Факторами, які виявляються у дереві, можуть бути події, пов'язані з відмовою компонентів інформаційної системи, помилками людини або будь-якими іншими відповідними подіями, які призводять до небажаної події.

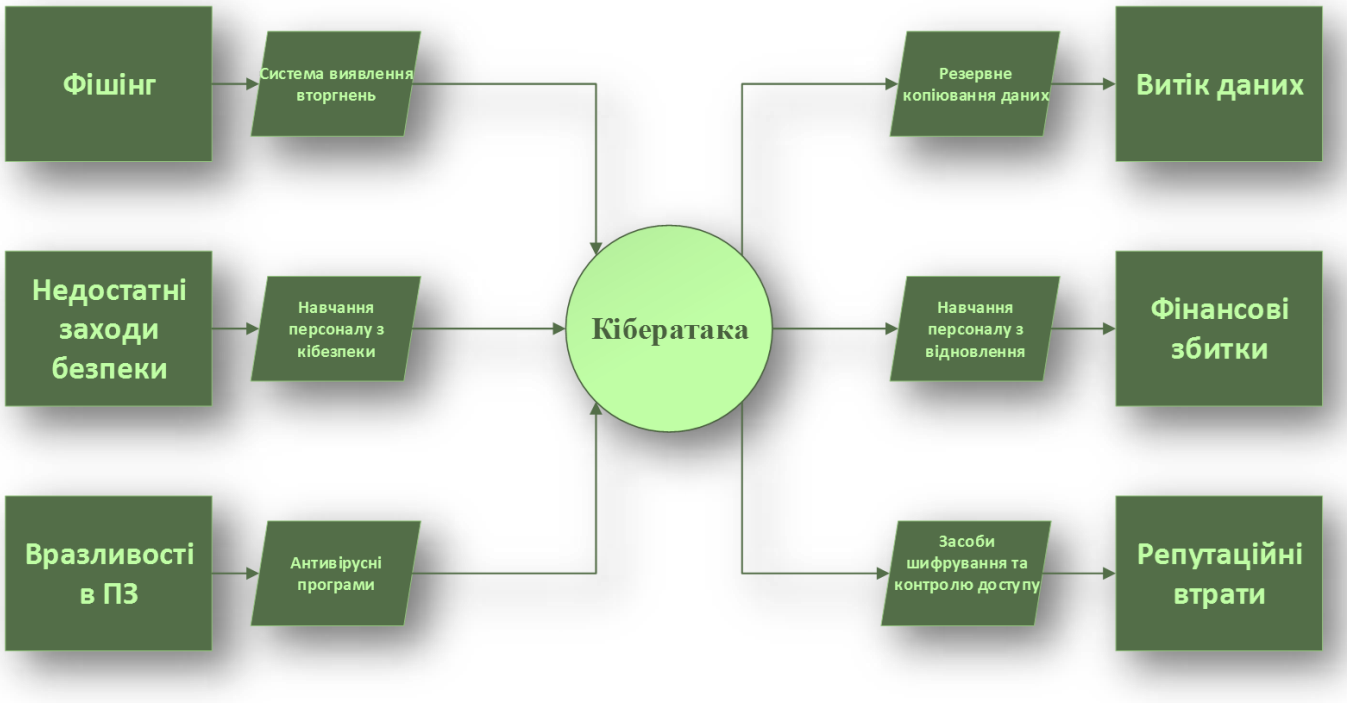


Рисунок 1.1 – приклад застосування FTA для аналізу кібератак

Аналізування кібератак за допомогою методу “краватка-метелик” наведено на рис.1.2.

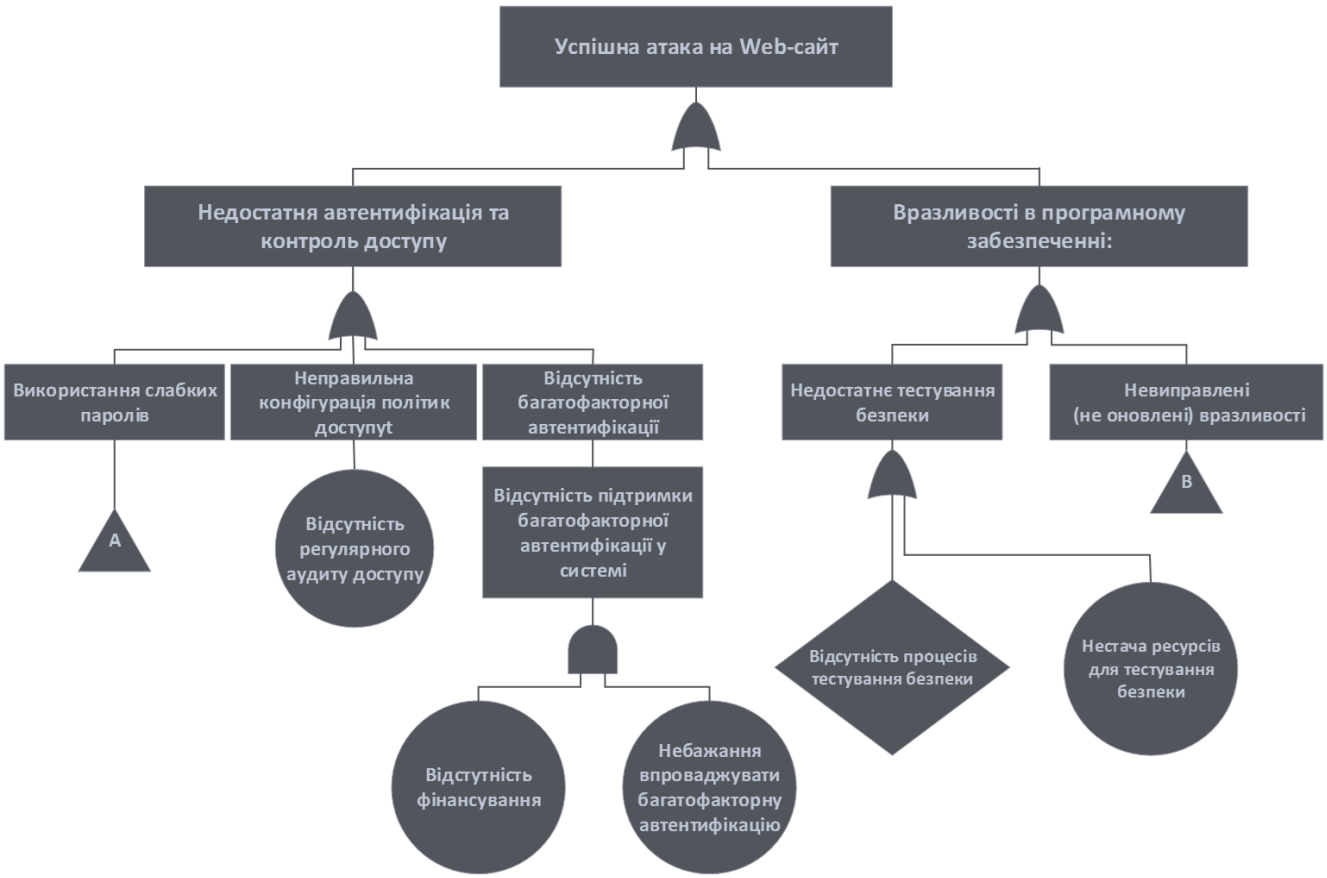


Рисунок 1.2. Застосування методу "краватка-метелик" щодо успішної атаки на web-сайт

Також застосовується метод SWIFT (Structured What If Technique). Характеристика цих методів наведена в таблиці 1.1.

Таблиця 1.1

Тип методу загального оцінювання ризику	**Опис**	**Важливість впливних чинників**			**Уможливлює отримання кількісних вихідних даних**
		Ресурси та можливості	**Характер і ступінь невизначеності**	**Складність**	

Аналізування за схемою «краватка-метелик»	Простий схематичний спосіб описування й аналізування варіантів розвитку ризику, починаючи з небезпечних чинників та закінчуючи наслідками, з критичним перевірянням засобів контролювання. Його можна розглядати як поєднання логіки дерева відмов, що уможливлює аналізування причини події (графічно поданої у формі «краватки-метелика») і дерева подій, що уможливлює аналізування наслідків.	Середня	Висока	Середня	Так
SWIFT (Структорований метод “Що? Якщо?”)	Система спонукання групи експертів до ідентифікації ризиків. Зазвичай використовують на засіданнях тематичних робочих груп за участі координатора. Зазвичай пов'язана з аналізуванням ризику та методом оцінювання ризику.	Середня	Середня	Будь-яка	Ні
Аналізування дерева подій	Використання індуктивного мислення для переведення ймовірностей першопочаткових подій у можливі результати	Середня	Середня	Середня	Так

Використання різних методів дає змогу провести комплексну оцінку кібератак та їх наслідків - оцінити вразливості WEB-сайту.

1.2. ОЦІНКА РИЗИКІВ ТА ПОТЕНЦІЙНИХ ЗБИТКІВ ВІД КІБЕРАТАК

Оцінка ризиків проведена на підставі матеріалів наведених у [6-12].

У таблиці 1.3 представлені потенційні збитки від кібератак на web-сайти недержавних компаній, включаючи фінансові, репутаційні, операційні та юридичні збитки, з описом кожного типу збитків та прикладами їх проявів.

Таблиця 1.3

Тип збитків	**Опис**	**Приклади**
Фінансові	Прямі та непрямі фінансові втрати, пов'язані з кібератакою.	Крадіжка коштів, вимагання викупу, втрата клієнтів, витрати на відновлення роботи.
Репутаційні	Втрата довіри до організації та негативний вплив на її імідж.	Негативні публікації в ЗМІ, відмова донорів та партнерів від співпраці.
Операційні	Порушення нормальної роботи організації та її web-сайту.	Переривання роботи web-сайту, втрата даних, необхідність відновлення систем.
Юридичні	Штрафи та судові позови, пов'язані з порушенням законодавства та витоком даних.	Штрафи за порушення GDPR, судові позови від постраждалих клієнтів.

У таблиці 1.4 представлені особливості оцінки ризиків кібератак для недержавних компаній, включаючи обмежені ресурси, специфіку даних та залежність від репутації, з описом кожної особливості.

Таблиця 1.4

Особливость	Опис
Обмежені ресурси	Недостатність фінансових та людських ресурсів для впровадження комплексних систем захисту.
Специфіка даних	Обробка особливо чутливих даних (медичні, персональні), що вимагає підвищеного рівня захисту.
Залежність від репутації	Репутація є критично важливою для діяльності недержавних компаній, тому атаки на неї можуть бути особливо небезпечними.

На рисунку 1.3 показано розподіл причин інцидентів інформаційної безпеки.

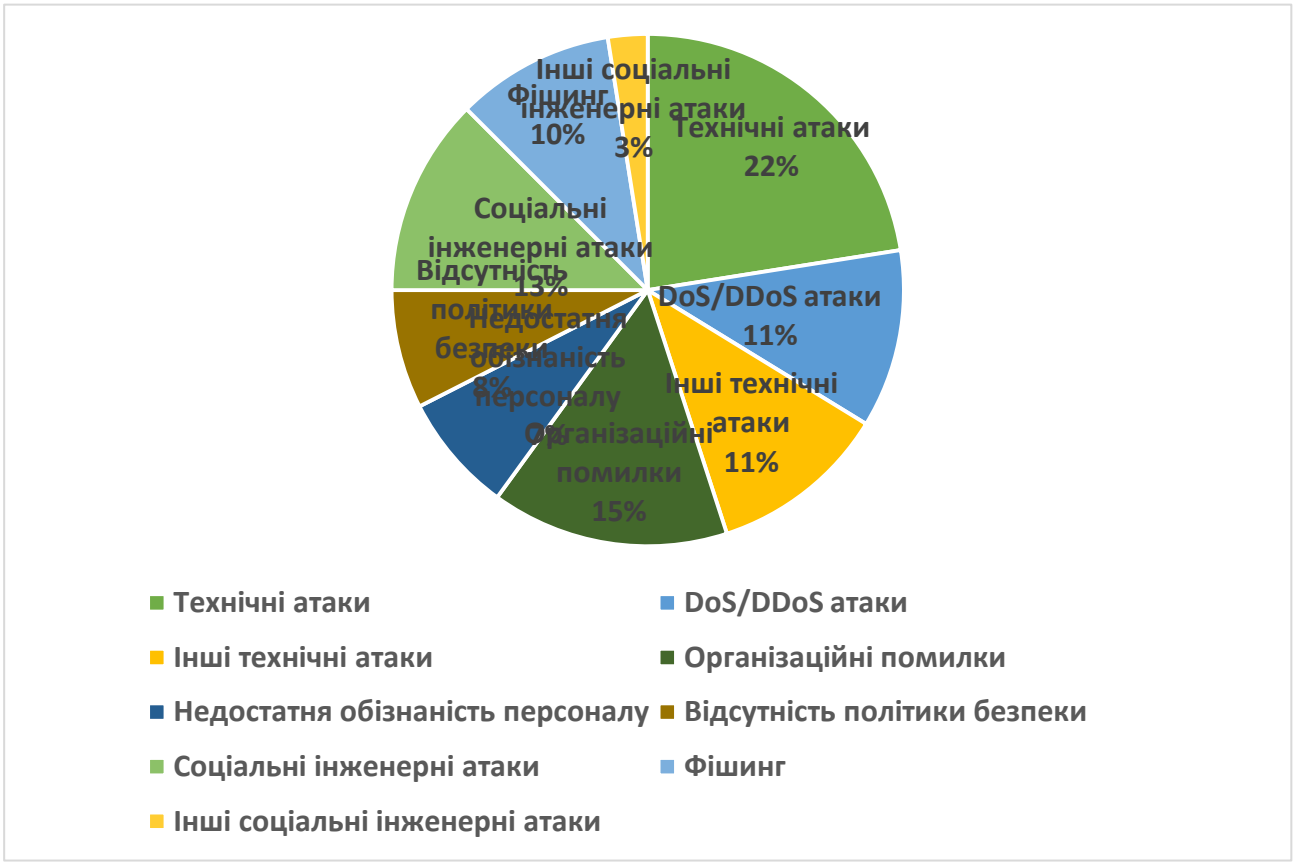


Рисунок 1.3. Розподіл кібер-атак на WEB – сайти в Україні

Найбільш поширеною причиною є відсутність політики безпеки (85%), яка включає недостатню обізнаність персоналу (7%). Далі йдуть технічні атаки (22%), організаційні помилки (15%) та соціальна інженерія (16%). Серед технічних атак найчастіше зустрічаються DoS/DDoS атаки (11%), а серед соціальної інженерії – фішинг (10%).

Інші категорії, такі як інші технічні та соціальні інженерні атаки, складають по 3% та 11% відповідно.

В цілому можна зробити висновок, що більшість інцидентів безпеки пов'язані з людським фактором та недоліками в організації процесів безпеки, а не лише з технічними вразливостями.

2. РОЗРОБКА ЕФЕКТИВНИХ СТРАТЕГІЙ КІБЕРБЕЗПЕКИ WEBСАЙТІВ ТА АНАЛІЗ ІСНУЮЧІХ СТРАТЕГІЙ КІБЕРБЕЗПЕКИ

В даному розділі здійснено аналіз 3-х стратегій кібербезпекі відповідно до вимог НД ТЗІ 2.5-010-03.

КА-2 - надає адміністратору безпеки можливість контролювати доступ до інформації, розподіляючи її від захищених об'єктів до користувачів.

ДР-1 - дозволяє контролювати використання користувачами послуг та ресурсів автоматизованої системи (АС).

НЦ-1 - визначає здатність КЗЗ WEB-сторінки захищати себе та гарантувати свою спроможність керувати захищеними об'єктами.

На основі цих трьох стратегій можливо розробити комплексну стратегію забезпечення інформаційної безпеки WEB -сторонки. Ця стратегія включатиме наступні ключові елементи (**КСЗІБВ**):

1. **Контроль доступу та розмежування прав:**
    - Визначення ролей та відповідальностей користувачів.
    - Встановлення чітких правил доступу до інформації залежно від ролі користувача.
    - Надання адміністратору безпеки можливості гнучко керувати правами доступу.
    - Регулярний перегляд та оновлення прав доступу відповідно до змін в організаційній структурі та завданнях користувачів.
2. **Забезпечення цілісності системи:**
    - Впровадження механізмів контролю цілісності компонентів КЗЗ (контрольні суми, цифрові підписи тощо).
    - Регулярне оновлення компонентів КЗЗ та програмного забезпечення.

- Моніторинг стану системи та виявлення потенційних порушень цілісності.
- Розробка процедур реагування на інциденти та відновлення цілісності системи.

3. **Захист веб-сторінки:**
   - Використання сучасних технологій захисту від веб-атак (WAF, фільтрація трафіку, захист від DDoS-атак).
   - Регулярне сканування веб-сторінки на наявність вразливостей.
   - Впровадження механізмів захисту від несанкціонованого доступу до адміністративної частини веб-сторінки.
   - Захист від витоку конфіденційних даних через веб-інтерфейс.
4. **Управління обчислювальними ресурсами:**
   - Встановлення обмежень на використання ресурсів для користувачів та процесів.
   - Моніторинг використання ресурсів та виявлення аномальної активності.
   - Оптимізація роботи веб-сторінки для ефективного використання ресурсів.
5. **Аудит та моніторинг:**
   - Ведення журналів подій безпеки та доступу до ресурсів.
   - Регулярний аналіз журналів для виявлення підозрілої активності.
   - Створення системи оповіщення про інциденти безпеки.

Ця стратегія дозволяє забезпечити комплексний захист веб-сторінки, враховуючи різні аспекти інформаційної безпеки: конфіденційність, цілісність та доступність.

2.1. ТЕХНІЧНІ ЗАХОДИ ЗАХИСТУ (БРАНДМАУЕРИ, СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ, ШИФРУВАННЯ).

2.1. Принципи побудови комплексних систем захисту web-сайтів.

Практичні аспекти побудови комплексної системи захисту web-сайту недержавної компанії розглядаються на прикладі – благодійного фонду "Допомога дітям".

Аналіз потреб та ризиків

Першим кроком є аналіз потреб та ризиків фонду. Web-сайт фонду містить інформацію про проекти, звіти про діяльність, форму для онлайн-пожертв та особисті дані благодійників. Основні ризики включають:

- **Фінансові:** крадіжка коштів з рахунків фонду, шахрайство з онлайн-пожертвами.
- **Репутаційні:** дефейс сайту, поширення неправдивої інформації, DDoS-атаки.
- **Витік даних:** несанкціонований доступ до персональних даних благодійників.

Розробка комплексної системи захисту

На основі аналізу ризиків розробляється комплексна система захисту, що включає наступні елементи:

- **Технічні заходи:**
  - **Брандмауер:** для захисту від несанкціонованого доступу до мережі.
  - **Система виявлення вторгнень (IDS):** для виявлення підозрілої активності та атак.
  - **Антивірусне та антишпигунське програмне забезпечення:** для захисту від шкідливого ПЗ.
  - **Система фільтрації web-трафіку:** для блокування шкідливих сайтів та контенту.
  - **Система захисту від DDoS-атак:** для забезпечення доступності сайту під час атак.
  - **Шифрування даних:** для захисту конфіденційності даних, що передаються через сайт.
  - **Регулярне оновлення програмного забезпечення:** для виправлення вразливостей.

- **Резервне копіювання даних:** для відновлення даних у разі їх втрати або пошкодження.

- **Організаційні заходи:**
- **Розробка політики безпеки:** документ, що визначає правила та процедури щодо використання інформаційних систем та захисту даних.
- **Навчання персоналу:** регулярне проведення тренінгів з кібербезпеки для співробітників фонду.
- **Обмеження доступу до даних:** надання доступу до конфіденційних даних лише уповноваженим особам.
- **Аудит безпеки:** регулярна перевірка ефективності системи захисту та виявлення потенційних проблем.

- **Соціальні заходи:**
- **Інформування користувачів:** розміщення на сайті інформації про безпечне використання інтернету та захист від фішингу.
- **Співпраця з правоохоронними органами:** повідомлення про виявлені кібератаки.

Впровадження та підтримка системи захисту

Після розробки система захисту впроваджується на webсайті фонду. Важливо забезпечити її регулярну підтримку та оновлення, оскільки загрози кібербезпеки постійно змінюються.

Практичне застосування технічних заходів захисту на прикладі webсайту недержавної організації

Для ілюстрації практичного застосування технічних заходів захисту, розглянемо приклад webсайту недержавної організації "Екологічна ініціатива", яка займається захистом довкілля та проводить онлайн-кампанії зі збору коштів.

Брандмауер (Firewall):

- **Застосування:** Встановлення апаратного або програмного брандмауера для контролю вхідного та вихідного трафіку.

- **Практичний приклад:** Налаштування брандмауера для блокування доступу до адміністративної панелі сайту з усіх IP-адрес, крім тих, що використовуються співробітниками організації. Блокування портів, які не використовуються web-сервером.

Система виявлення та запобігання вторгненням (IDS/IPS):

- **Застосування:** Впровадження IDS/IPS для моніторингу мережевого трафіку та виявлення підозрілої активності.
- **Практичний приклад:** Налаштування IDS/IPS для виявлення спроб SQL-ін'єкцій, XSS-атак, сканування портів та інших типових атак на web-додатки. Автоматичне блокування IP-адрес, з яких здійснюються атаки.

Шифрування (Encryption):

- **Застосування:** Використання протоколу HTTPS для шифрування трафіку між web-сервером та браузерами користувачів.
- **Практичний приклад:** Отримання SSL-сертифіката та налаштування web-сервера на підтримку HTTPS. Це забезпечить захист конфіденційних даних користувачів (наприклад, даних платіжних карток при онлайн-пожертвах) від перехоплення.

Web-application firewall (WAF):

- **Застосування:** Встановлення WAF для захисту web-додатків від специфічних атак.
- **Практичний приклад:** Налаштування WAF для блокування SQL-ін'єкцій, XSS-атак, атак на основі файлових включень та інших відомих вразливостей web-додатків.

Системи захисту від DDoS-атак:

- **Застосування:** Використання спеціалізованих сервісів або рішень для захисту від DDoS-атак.
- **Практичний приклад:** Підключення до хмарного сервісу захисту від DDoS-атак, який фільтруватиме трафік та блокуватиме підозрілі запити.

Системи управління вразливостями:

- **Застосування:** Використання автоматизованих інструментів для виявлення та виправлення вразливостей у програмному забезпеченні web-сервера та web-додатків.
- **Практичний приклад:** Регулярне сканування web-сайту за допомогою сканерів вразливостей (наприклад, Nessus, OpenVAS) та встановлення оновлень безпеки для виявлених вразливостей.

Антивірусне та антишпигунське програмне забезпечення:

- **Застосування:** Встановлення та регулярне оновлення антивірусного та антишпигунського ПЗ на сервері, де розміщено web-сайт.
- **Практичний приклад:** Використання антивірусного ПЗ для сканування файлів на сервері та виявлення шкідливого коду.

Системи резервного копіювання:

- **Застосування:** Регулярне створення резервних копій даних web-сайту та бази даних.
- **Практичний приклад:** Налаштування автоматичного резервного копіювання на віддалений сервер або хмарне сховище. Це дозволить відновити дані у разі їх втрати або пошкодження внаслідок кібератаки.

2.2. ОРГАНІЗАЦІЙНІ ЗАХОДИ (ПОЛІТИКИ БЕЗПЕКИ, НАВЧАННЯ ПЕРСОНАЛУ, РЕЗЕРВНЕ КОПІЮВАННЯ).

Організаційні заходи захисту web-сайтів є невід'ємною частиною комплексної стратегії кібербезпеки. Вони спрямовані на створення безпечного середовища для роботи з інформаційними системами та даними, а також на підвищення обізнаності та відповідальності персоналу щодо питань кібербезпеки.

Політики безпеки

Політики безпеки –в додатку А наведено терміналогію.

Практичний приклад: Розробка політики безпеки для недержавної організації "Екологічна ініціатива" може включати наступні пункти:

- **Управління паролями:** Вимоги до складності паролів, регулярна зміна паролів, заборона використання однакових паролів для різних систем.
- **Управління доступом:** Надання доступу до конфіденційних даних лише уповноваженим особам, використання двофакторної аутентифікації.
- **Обробка інцидентів:** Процедура повідомлення про інциденти безпеки, розслідування інцидентів, вжиття заходів щодо їх усунення.
- **Управління вразливостями:** Регулярне сканування webсайту на наявність вразливостей, встановлення оновлень безпеки.
- **Захист даних:** Шифрування конфіденційних даних, обмеження доступу до даних, резервне копіювання.

Навчання персоналу

Навіть найдосконаліші технічні засоби захисту не будуть ефективними, якщо персонал не знає, як їх використовувати та як розпізнавати потенційні загрози. Тому навчання персоналу є важливим елементом організаційних заходів захисту.

Практичний приклад: Проведення регулярних тренінгів для співробітників компанії n з таких тем:

- **Основи кібербезпеки:** типи кібератак, соціальна інженерія, фішинг.
- **Безпечне використання паролів:** створення надійних паролів, правила зберігання та використання паролів.
- **Безпечна робота з електронною поштою:** розпізнавання фішингових листів, обережне відкриття вкладень.
- **Безпечне використання Інтернету:** захист від шкідливого ПЗ, безпечне використання Wi-Fi.
- **Дії у разі кібератаки:** кому повідомляти про інцидент, як діяти для мінімізації наслідків.

Резервне копіювання

Резервне копіювання даних є важливим заходом захисту, який дозволяє відновити дані у разі їх втрати або пошкодження внаслідок кібератаки, збою обладнання або інших непередбачуваних ситуацій.

Практичний приклад: Впровадження системи автоматичного резервного копіювання даних webсайту n на віддалений сервер або хмарне сховище. Регулярна перевірка цілісності резервних копій та їх відновлення у тестовому середовищі.

2.3. РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВИБОРУ ТА ВПРОВАДЖЕННЯ ЗАСОБІВ ЗАХИСТУ.

Вибір та впровадження засобів захисту web-сайту є відповідальним та складним завданням, яке вимагає врахування багатьох факторів [11-13]. Не існує універсального рішення, яке підвиде для всіх організацій, тому важливо розробити індивідуальний підхід, що враховує специфіку діяльності, бюджет та рівень ризику.

Перелік рекомендації щодо розробки, вибору та впровадження засобів захисту від кібератак наведено у додатку А.

ВИСНОВКИ

В результаті виконання кваліфікаційної бакалаврської роботи є – класифікація, показники сучасних загроз кібербезпеці та рекомендації щодо їхнього подолання.

Аналіз виявив, що найбільш поширеними загрозами для web-сайтів недержавних компаній в Україні є технічні атаки, такі як DoS/DDoS, організаційні помилки, та соціальні інженерні атаки, зокрема фішинг. Кількість інцидентів у цих категоріях складає відповідно 450, 300 та 250 випадків на рік.

Особливо важливим є той факт, що недержавні компанії часто не мають достатніх ресурсів та політик для ефективного захисту своїх web-сайтів.

Для підвищення рівня кібербезпеки були розроблені наступні рекомендації:

1. Технічні заходи:

- Встановлення брандмауерів та систем виявлення вторгнень.

- Використання засобів шифрування для захисту даних.

- Регулярне оновлення програмного забезпечення та проведення тестувань на вразливості.

2. Організаційні заходи:

- Розробка та впровадження політик безпеки.

- Проведення навчання персоналу з питань кібербезпеки.

- Впровадження систем резервного копіювання даних.

3. Соціальні заходи:

- Підвищення обізнаності персоналу щодо соціальної інженерії.

- Розробка протоколів для реагування на інциденти фішингу.

Загалом, впровадження комплексного підходу до кібербезпеки, що включає технічні, організаційні та соціальні заходи, є ключовим для забезпечення надійного захисту web-сайтів недержавних компаній в Україні. Це допоможе не лише знизити ризики успішних кібератак, але й мінімізувати потенційні збитки від них.

Отже, результатами даної роботи є обґрунтування ефективних стратегій захисту web-сайтів, що враховують специфіку та обмежені ресурси недержавних компаній, сприяючи підвищенню їхньої стійкості до кіберзагроз.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Інформаційні системи в менеджменті / А.Є. Батюк, З.П. Двуліт, К.М. Обельовська, І.М. Огороднік, Л.П. Фабрі. – Львів: «Інтелект-Захід», 2004. – С. 343–384.
2. Міжнародний стандарт «ISO/IEC 27001 Third edition 2022-10 Information security, cybersecurity and privacy protection — Information security management systems — Requirements» - Режим доступу: https://www.iso.org/standard/27001
3. Литвинюк А.А. Основи інформаційної безпеки. Комплексна система захисту інформації: структура, встановлення та підтримка функціонування // А.А. Литвинюк. – [Електронний ресурс]. – Режим доступу: http://www.cvk.gov.ua/visnyk/pdf/2008_4/visnik_st_08.pdf
4. Стаття «Система економічної безпеки підприємства та її методологічні засади» [Електронний ресурс] – Режим доступу: https://studopedia.su/8_58207_sistema-ekonomichnoi-bezpeki-pidpriiemstva-ta-iimetodologichni-zasadi.html
5. Стаття «Методика оцінювання захищеності інформаційних систем за допомогою СУІБ «Матриця».» [Електронний ресурс] – Режим доступу: http://www.epos.ua/view.php/about_pubs_archive
6. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем. Стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
7. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу.
8. НД ТЗІ 3.7-003-2023 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі.
9. Г.Ф. Конахович та інші. Захист інформації в телекомунікаційних системах: Навчальний посібник. – К.: НАУ, 2009.-380 с.

10. Основи інформаційної безпеки. Лужецький В.А., Кожухівський А.Д., Войтович О.П. Навчальний посібник. – Вінниця: ВНТУ, 2009. – 268 с.
11. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем.-К.: Видавнича група BHV, 2009 – 608с.:іл.
12. Педагогічний програмний засіб (ППЗ) «Телекомунікаційні системи та мережі. Структура й основні функції. Том 1». Автори: Поповський В.В, Лемешко О.В.; Ковальчук В.К.; Плотніков М.Д.; Картушин Ю.П.; Попонін О.М.; Агєєв Д.В.; Сабурова С.О., Олійник В.Ф., Персиков А.В.; Лошаков В.А. Селіванов К.О. Друге видання. Виправлено та доповнено. 2018.
13. Голев Д.В. Методики оцінки інформаційної захищеності телекомунікацій : навч. посіб. / Голев Д.В., Кононович В.Г., Хомич С.В.; за ред. чл.-кор. МАЗ В.Г. Кононовича. - Одеса: ОНАЗ ім. О.С. Попова, 2013. - 218 с.
14. Герасимов Б.М., Домарев В.В. Вибір оптимального варіанту системи захисту інформації на основі застосування методів нечіткої багатокритеріальної оптимізації// Захист інформації. №3.
15. Висоцька Е., Давиденко А. Сучасний стан методології аналізу ризиків при забезпеченні інформаційної безпеки комп’ютерної системи // Правове. нормативне та метрологічне забезпечення системи захисту інформації в Україні.

Додаток А.

Детальний опис методів аналізу кібератак

Аналізування дерева відмов (FTA)

FTA - це метод, який дозволяє визначити та проаналізувати фактори, що можуть призвести до небажаної події. Ці фактори виявляються дедуктивним шляхом, організовуються логічно та представляються графічно у вигляді деревоподібної діаграми (див. рисунок 1.1), яка показує причинні фактори та їх логічні зв'язки з небажаною подією.

Дерево відмов можна використовувати для якісного аналізу, щоб визначити потенційні причини та шляхи виникнення відмови (завершальної події), або для кількісного аналізу, щоб обчислити ймовірність завершальної події, знаючи ймовірності причинних подій.

Цей метод можна застосовувати на етапі проєктування системи, щоб визначити потенційні причини відмов і, виходячи з цього, зробити вибір між варіантами проєктування. Його також можна застосовувати на етапі функціонування, щоб визначити, як можуть виникати найсуттєвіші відмови, і відносну важливість настання різних завершальних подій. Дерево відмов можна також використовувати для аналізу відмови, що вже виникла, щоб схематично відобразити, як різні події разом спричинили відмову.

Етапи розробки дерева відмов:

1. Визначення завершальної події: Визначається подія, яка буде аналізуватися. Це може бути відмова або більш загальний негативний результат. Якщо аналізується результат, дерево може включати розділ щодо пом'якшення наслідків фактичної відмови.

2. Визначення безпосередніх причин: Починаючи з завершальної події, визначаються можливі безпосередні причини або види відмов, що призводять до неї.

3. Аналіз причин: Кожна з цих причин (кожен вид відмови) аналізується, щоб зрозуміти, як вона може виникати.

4. Поетапне визначення небажаного функціонування: Проводиться поетапне визначення небажаного функціонування системи, послідовно спускаючись до нижчих рівнів, доки подальше аналізування не стане недоцільним. У технічних системах це може бути рівень відмови компонента. Події та причинні фактори на найнижчому рівні називаються базовими подіями.

5. Обчислення ймовірності завершальної події: За можливості надання ймовірностей базовим подіям, можна обчислити ймовірність завершальної події.

Для обґрунтованості кількісного аналізу необхідно показати, що для кожного логічного елемента всі вхідні дані є необхідними та достатніми для спричинення результуючої події.

6. Спрощення дерева відмов: У межах кількісного аналізу може знадобитися спрощення дерева відмов за допомогою булевої алгебри, щоб врахувати дублювання видів відмов.

7. Ідентифікація мінімальних перерізів: Поряд з отриманням кількісної оцінки ймовірності головної події, можна ідентифікувати мінімальні перерізи, які утворюють окремі шляхи до головної події, та обчислити їхній вплив.

8. Використання програмного забезпечення: Для складних дерев відмов, для належного опрацювання обчислень за наявності повторних подій та для обчислення мінімальних перерізів, необхідне програмне забезпечення. Програмні засоби забезпечують узгодженість, правильність та можливість перевірки.

Результати аналізу дерева відмов включають:

- Графічне представлення того, як може відбутися кінцева подія, з відображенням взаємопов'язаних шляхів, якими можуть виникати дві або більше одночасних подій.
- Перелік мінімальних перерізів (окремих шляхів до відмови) з імовірністю (за наявності даних) виникнення кожного з них.
- Імовірність кінцевої події.

Переваги FTA:

- Структурований підхід: FTA пропонує організований та систематичний спосіб аналізу різних факторів, включаючи людські помилки та фізичні явища.
- Фокус на наслідках: Метод "зверху вниз" дозволяє зосередитися на наслідках відмов, які безпосередньо пов'язані з кінцевою подією.
- Аналіз складних систем: FTA особливо корисний для аналізу систем з численними зв'язками та взаємодіями.
- Візуалізація: Графічне представлення полегшує розуміння поведінки системи та її внутрішніх факторів.
- Ідентифікація прихованих шляхів відмови: Логічний аналіз дерев відмов допомагає виявити неочевидні комбінації подій, що призводять до кінцевої події.

Обмеження FTA:

- Невизначеність даних: Обчислення ймовірності кінцевої події залежать від точності ймовірностей базових подій, що може призводити до високої невизначеності результатів.
- Незалежні події: У деяких випадках причинні події можуть бути не пов'язані між собою, що ускладнює визначення всіх значущих шляхів до кінцевої події.
- Статична модель: FTA не враховує часові залежності між подіями.
- Бінарні стани: Метод працює лише з двома станами: "несправність" або "справність".
- Труднощі з людським фактором: Включення людських помилок у FTA може бути складним завданням, особливо якщо їх ступінь або якість важко визначити.
- Ігнорування "ефекту доміно": FTA не враховує можливість ланцюгових реакцій або умовних відмов.

Метод «краватка-метелик».

Опис методу наведено на рисунку 1.2.

Аналіз діаграми "краватка-метелик" - це простий спосіб схематичного опису та аналізу шляхів ризику, від причин до наслідків. Цей метод можна розглядати як поєднання дерева відмов (для аналізу причин) і дерева подій (для аналізу наслідків), але з акцентом на бар'єрах, які стоять між причинами та ризиком, а також між ризиком та наслідками. Діаграми "краватка-метелик" можна будувати на основі дерев відмов та подій, але частіше їх створюють безпосередньо після мозкового штурму.

Аналіз за допомогою діаграми "краватка-метелик" використовується для візуалізації ризику, показуючи можливі причини та наслідки. Він застосовується, коли ситуація не є настільки складною, щоб вимагати повного аналізу дерева відмов, або коли основний акцент робиться на забезпеченні наявності бар'єрів або засобів контролю для кожного шляху відмови. Такий аналіз корисний, коли існують чіткі та незалежні шляхи, що ведуть до відмови.

Діаграма "краватка-метелик" часто легша для розуміння, ніж дерево відмов або дерево подій, тому може бути корисним інструментом для обміну інформацією, коли аналіз проводиться з використанням більш складних методів.

Для проведення аналізу ризику необхідно чітко розуміти його причини та наслідки, а також бар'єри та засоби контролю, які можуть запобігти ризику, зменшити його або посилити.

Процедура аналізу діаграми "краватка-метелик" починається з визначення конкретного ризику, який необхідно проаналізувати. Цей ризик зображується у вигляді центрального вузла діаграми "краватка-метелик".

a) Почніть з визначення конкретного ризику, який потрібно проаналізувати. Цей ризик буде представлений у вигляді центрального вузла в діаграмі "краватка-метелик".

b) Перерахуйте причини події, залежно від джерел ризику (або небезпечних факторів у контексті безпеки).

c) Визначте, як кожне джерело ризику призводить до критичної події.

d) Для кожної причини та події намалюйте лінії, щоб сформувати ліву частину "краватки-метелика". Також можна визначити та додати до діаграми будь-які фактори, що посилюють ситуацію.

e) Бар'єри, які слід розглянути на шляху кожної причини, що призводить до небажаних наслідків, можна показати як вертикальні смуги, що перетинають лінії. Якщо є фактори, що посилюють ситуацію, також можна показати бар'єри для посилення. Цей підхід можна використовувати для позитивних наслідків, для яких вертикальні смуги представляють "засоби контролю", які сприяють настанню події.

f) У правій частині "краватки-метелика" визначте різні потенційні наслідки ризику та намалюйте лінії, що радіально розходяться від події ризику до кожного потенційного наслідку.

g) Бар'єри наслідків зображуються як смуги, що перетинають радіальні лінії. Цей підхід можна використовувати для позитивних наслідків, для яких вертикальні смуги представляють "засоби контролю", які сприяють виникненню наслідків.

h) Функції управління для підтримки ефективності засобів контролю (наприклад, навчання та інспекційний контроль) показуються під "краваткою-метеликом", пов'язуючи їх з відповідним засобом контролю.

Можливі певні рівні кількісного представлення для діаграми "краватка-метелик" у випадку, коли шляхи є незалежними, ймовірність конкретного наслідку або результату є відомою, а ефективність засобу контролю може бути кількісно оцінена. Однак у багатьох ситуаціях шляхи та бар'єри не є незалежними, а засоби контролю можуть бути процедурними, а їхня ефективність, внаслідок цього,

нечітко вираженою. Часто кількісне подання доцільніше здійснювати з використанням FTA та ETA.

Вихідні дані - це проста діаграма, що показує основні шляхи ризику та встановлені бар'єри, щоб запобігти небажаним наслідкам або пом'якшити їх, а також стимулювати або сприяти бажаним наслідкам.

Переваги аналізу діаграми «краватка-метелик»:

- Простий для розуміння та забезпечує чітке графічне зображення проблеми.
- Зосереджує увагу на засобах контролю, які вважаються впровадженими для запобігання та пом'якшення, а також на їх ефективності.
- Можливість застосування до бажаних наслідків.
- Не вимагає високого рівня професійної компетентності для застосування.

Обмеження:

- Не дозволяє відобразити випадки одночасного впливу кількох причин на виникнення наслідків (тобто, коли в дереві відмов, що зображує ліву частину "краватки-метелика", застосовано логічний елемент "І").
- Може надмірно спрощувати складні ситуації, особливо у разі кількісного подання.

Метод SWIFT (Structured What If Technique) був розроблений як спрощений варіант HAZOP.

Це системне дослідження, яке проводить група експертів, використовуючи набір навідних слів або фраз, щоб стимулювати ідентифікацію ризиків. Координатор і група використовують стандартні фрази типу "що трапиться, якщо..." у поєднанні з навідними фразами, щоб дослідити, як на систему, технічний об'єкт, організацію чи процедуру впливатимуть відхилення від нормального функціонування та поведінки. Методика SWIFT, на відміну від методики HAZOP, зазвичай застосовується на рівні систем з нижчим рівнем деталізації.

Хоча методика SWIFT спочатку була розроблена для дослідження небезпечних факторів на підприємствах хімічної та нафтохімічної промисловості, зараз її широко застосовують до систем, технічних об'єктів, процедур і організацій загалом. Зокрема, її застосовують для дослідження наслідків будь-яких змін, а також ризиків, які через це можуть виникнути чи зазнати змін.

Перед початком дослідження необхідно ретельно визначити систему, процедуру, технічний об'єкт і/або зміну. Зовнішнє та внутрішнє середовище визначає координатор за допомогою опитувань, а також вивченням документів, планів і креслень. Зазвичай, досліджуваний об'єкт, ситуацію чи систему розбивають на вузли чи ключові елементи, щоб полегшити процес аналізування, але це рідко відбувається на рівні деталізації, необхідному для HAZOP.

Інші ключові вхідні дані - це компетентність і практичний досвід членів дослідницької групи, яку треба ретельно формувати. Потрібно, щоб разом з тими, хто має практичний досвід стосовно подібних об'єктів, систем, змін або ситуацій, було представлено, за можливості, усі зацікавлені сторони.

Загальний процес такий:

a) Перед початком дослідження координатор готує належний перелік навідних фраз і слів, який може бути базований на стандартному наборі або розроблений так, щоб уможливити всебічний огляд небезпечних чинників або ризиків.

b) На робочій нараді обговорюють і погоджують зовнішнє та внутрішнє оточення, пов'язані з об'єктом, системою, зміною чи ситуацією, а також сферу застосування дослідження.

c) Координатор пропонує учасникам навести та розглянути:

- відомі ризики та небезпечні чинники;
- попередній досвід та інциденти;
- відомі та наявні засоби контролювання та захисту;
- регуляторні вимоги та обмеження.

d) Обговорення координують запитаннями, у формулюванні яких використано фразу типу «що якщо» і навідне слово чи тему. Варіанти використовуваних фраз типу «що якщо» такі: «що відбуватиметься, якщо...?», «чи може хтось чи щось...?», «чи хтось або щось вже...?». Намір — стимулювати дослідницьку групу до вивчення потенційних варіантів розвитку подій, їхніх причин, наслідків і впливів.

e) Ризики підсумовують, і група розглядає вже запроваджені засоби контролювання.

f) Група затверджує опис ризику, його причин, наслідків і передбачених засобів контролювання та складає відповідні протоколи.

g) Група розглядає адекватність і результативність засобів контролювання та погоджує виклад щодо результативності контролювання ризику. Якщо результативність незадовільна, то група глибше розглядає завдання щодо обробляння ризику, визначаючи потенційні засоби контролювання.

h) Під час обговорення ставлять конкретніші запитання типу «що якщо», щоб ідентифікувати додаткові ризики.

i) Координатор, використовуючи перелік навідних слів, відстежує хід обговорення і пропонує для обговорення в групі додаткові питання та варіанти розвитку подій.

j) Звичайною практикою є використання якісного чи напівкількісного методу загального оцінювання ризику, щоб ранжувати передбачені дії за їхньою пріоритетністю. Це загальне оцінювання ризику зазвичай провадять з урахуванням наявних засобів контролювання та їхньої результативності.

Результатом є реєстр ризиків з діями або завданнями, ранжованими за рівнем ризику. Потім ці завдання можуть бути основою плану управління ризиками.

Переваги SWIFT:

- Універсальність: може бути застосований до різноманітних технічних об'єктів, систем, ситуацій, організацій та видів діяльності.
- Мінімальна підготовка: вимагає мінімальної підготовки від членів групи.
- Швидкість: основні ризики та небезпеки швидко виявляються під час робочої сесії.
- Системна орієнтація: дозволяє зрозуміти, як система реагує на відхилення, а не лише наслідки відмов окремих компонентів.
- Поліпшення процесів: може бути використаний для виявлення можливостей для покращення процесів та систем, визначення дій, що ведуть до успіху.
- Підвищення відповідальності: залучає відповідальних осіб до обговорення, підвищуючи їхню відповідальність за управління ризиками.
- Створення реєстру ризиків: дозволяє створити реєстр ризиків та план управління ними.

- Ідентифікація ризиків: допомагає виявити ризики та небезпеки, результати яких можна використовувати для кількісного дослідження, хоча зазвичай використовується якісне або напівкількісне ранжування ризиків.

Обмеження SWIFT:

- Залежність від координатора: ефективність залежить від досвіду та кваліфікації координатора.
- Ретельна підготовка: вимагає ретельної підготовки, щоб уникнути втрати часу на робочих сесіях.
- Можливість пропуску ризиків: якщо досвід групи недостатній або система навідних фраз не всебічна, деякі ризики можуть бути не виявлені.
- Обмеження рівня деталізації: застосування методу на загальному рівні може не дозволити виявити складні, детальні або взаємопов'язані причини.

Політики безпеки – це набір правил, процедур та інструкцій, що визначають, як організація повинна захищати свої інформаційні активи. Вони включають в себе різні аспекти безпеки, такі як управління доступом, обробка інцидентів, управління вразливостями, захист даних тощо.

Рекомендації щодо вибору засобів захисту

1. **Проведіть аналіз ризиків:** Визначте, які активи є найбільш цінними для вашої організації та які загрози є найбільш ймовірними. Це допоможе визначити пріоритетні напрямки захисту та вибрати відповідні засоби.
2. **Враховуйте специфіку діяльності:** Вибирайте засоби захисту, які відповідають специфіці діяльності вашої організації. Наприклад, для недержавних організацій, що працюють з конфіденційними даними, важливим є шифрування та засоби захисту від витоку даних.
3. **Оцінюйте вартість та ефективність:** Порівнюйте різні засоби захисту за їх вартістю, функціональністю та ефективністю. Вибирайте ті, які забезпечують найкраще співвідношення ціна/якість.
4. **Звертайтеся до фахівців:** Якщо у вас немає достатнього досвіду у сфері кібербезпеки, зверніться до спеціалістів, які допоможуть вам вибрати та налаштувати засоби захисту.

Рекомендації щодо впровадження засобів захисту

1. **Розробіть план впровадження:** Визначте послідовність дій, відповідальних осіб та терміни виконання.
2. **Проведіть навчання персоналу:** Ознайомите співробітників з новими засобами захисту та правилами їх використання.
3. **Тестуйте систему захисту:** Регулярно проводьте тестування на проникнення та інші перевірки, щоб переконатися в ефективності системи захисту.
4. **Оновлюйте програмне забезпечення:** Встановлюйте оновлення безпеки для всіх компонентів системи захисту.
5. **Моніторе безпеку:** Постійно відстежуйте стан безпеки web-сайту та реагуйте на виявлені інциденти.

Додаток Б

Детальний опис показників безпеки

Політика адміністративної конфіденційності стосується:

- Усіх користувачів, крім винятків, визначених у пункті 6.3.1 "a".
- Об'єктів, що містять технологічну інформацію комплексної системи захисту інформації (КСЗІ) та інформацію щодо управління автоматизованою системою (АС).
- Системного та функціонального програмного забезпечення, що використовується для оновлення, захисту загальнодоступної інформації, підтримки веб-сторінок та доступу до периферійних пристроїв (принтерів, накопичувачів тощо).

КЗЗ повинен:

- Розмежовувати доступ на основі атрибутів доступу користувача та об'єкта.
- Надавати доступ до загальнодоступної інформації всім категоріям користувачів.
- Дозволяти адміністратору безпеки призначати атрибути доступу користувачам та процесам до захищених об'єктів на основі аналізу їхніх функціональних та службових обов'язків.
- Надавати лише адміністратору безпеки права доступу до технологічної інформації КСЗІ та процесів її оновлення, супроводу та аналізу.
- Надавати доступ до процесів адміністрування та забезпечення функціонування АС лише користувачам з відповідними повноваженнями.
- Обробляти запити на зміну прав доступу тільки від адміністратора безпеки.
- Встановлювати права доступу до кожного захищеного об'єкта під час його створення або ініціалізації.

Комплекс засобів захисту (КЗЗ) повинен відповідати рівню ДР-1.

Ця послуга дозволяє контролювати використання користувачами послуг та ресурсів автоматизованої системи (АС). Політика використання ресурсів, що реалізується КЗЗ, стосується:

- користувачів загальнодоступної інформації;
- адміністратора безпеки та користувачів, яким надано повноваження щодо управління АС;
- файлової системи;
- системного та функціонального програмного забезпечення;
- технологічної інформації щодо управління АС;
- окремих периферійних пристроїв (принтерів, накопичувачів інформації тощо);
- обчислювальних ресурсів АС.

Вона передбачає можливість встановлення обмежень на їх використання.

Обмеження щодо використання окремим користувачем та/або процесом обсягів обчислювальних ресурсів АС або кількості об'єктів встановлюються адміністратором безпеки або користувачами, яким надано повноваження щодо управління АС. Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від зазначених користувачів.

Спроби користувачів перевищити встановлені обмеження на використання ресурсів повинні реєструватися в системному журналі.

КЗЗ повинен реалізовувати рівень НДЦ-1.

Ця послуга визначає здатність КЗЗ WEB-сторінки захищати себе та гарантувати свою спроможність керувати захищеними об'єктами.

Політика цілісності КЗЗ повинна визначати склад КЗЗ, механізми контролю цілісності його компонентів та порядок їх використання.

Політика цілісності КЗЗ стосується: адміністратора безпеки, окремих компонентів системного та функціонального програмного забезпечення, які задіяні для реалізації механізмів КЗЗ, засобів захисту інформації, а також технологічної інформації КСЗІ, і забезпечує взаємодію зазначених об'єктів.

Політика реалізації послуги повинна гарантувати, що всі послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ. Якщо існують обмеження, недотримання яких може призвести до надання послуг в обхід інтерфейсу КЗЗ і порушення цілісності КЗЗ, то такі обмеження повинні бути описані і задокументовані. До користувачів має бути доведено порядок їх роботи з дотриманням цих обмежень, а КЗЗ повинен надавати адміністратору можливість здійснення контролю за цим порядком.

КЗЗ повинен повідомляти адміністратора безпеки про порушення цілісності будь-якого компонента КЗЗ. WEB-сторінка під час цього має бути переведена до стану, в якому доступ до неї користувачів, крім адміністратора безпеки, заборонено. Повернення до нормального режиму функціонування може бути здійснено тільки адміністратором після відновлення відповідності цього компонента еталону.

Комплекс засобів захисту (КЗЗ) веб-сторінки повинен забезпечувати власний захист та цілісність, а також контроль доступу до захищених об'єктів (рівень НДЦ-1).

Політика цілісності КЗЗ визначає:

- склад КЗЗ;
- механізми контролю цілісності його компонентів (адміністратор безпеки, програмне забезпечення, засоби захисту інформації, технологічна інформація КСЗІ);
- порядок використання цих механізмів.

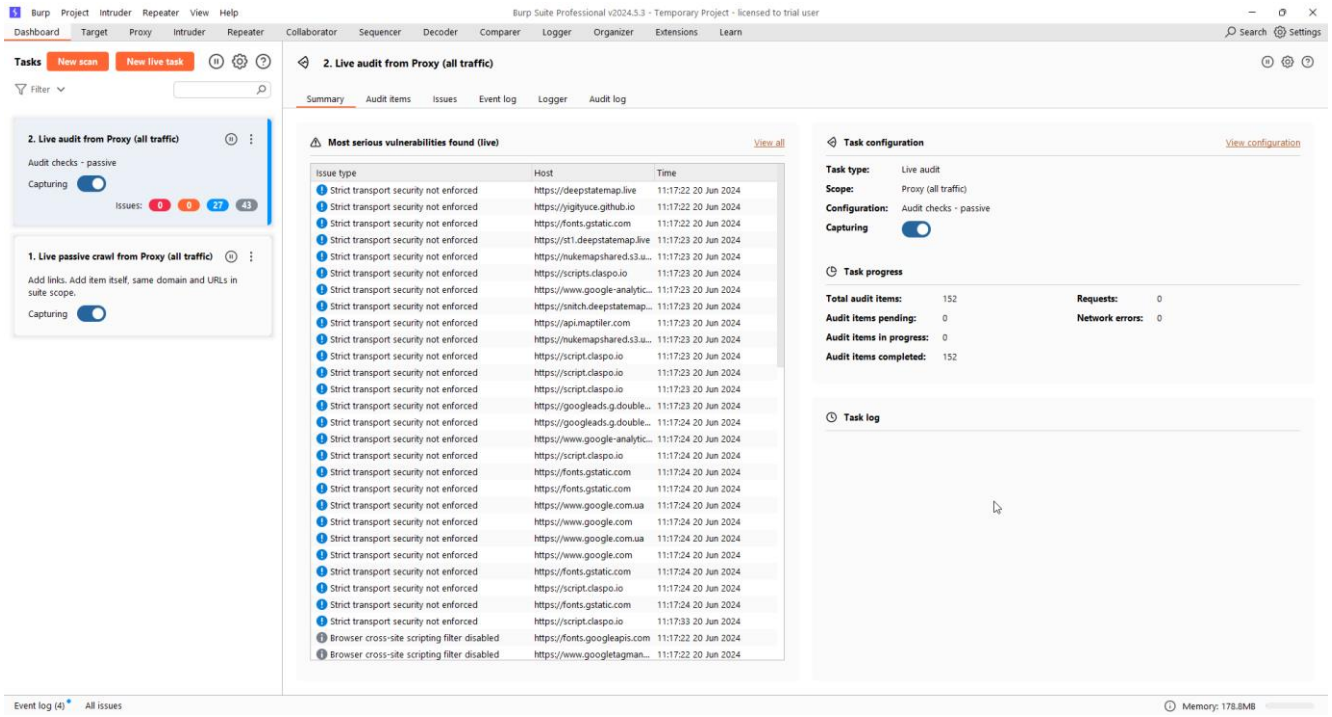
Політика реалізації послуг:

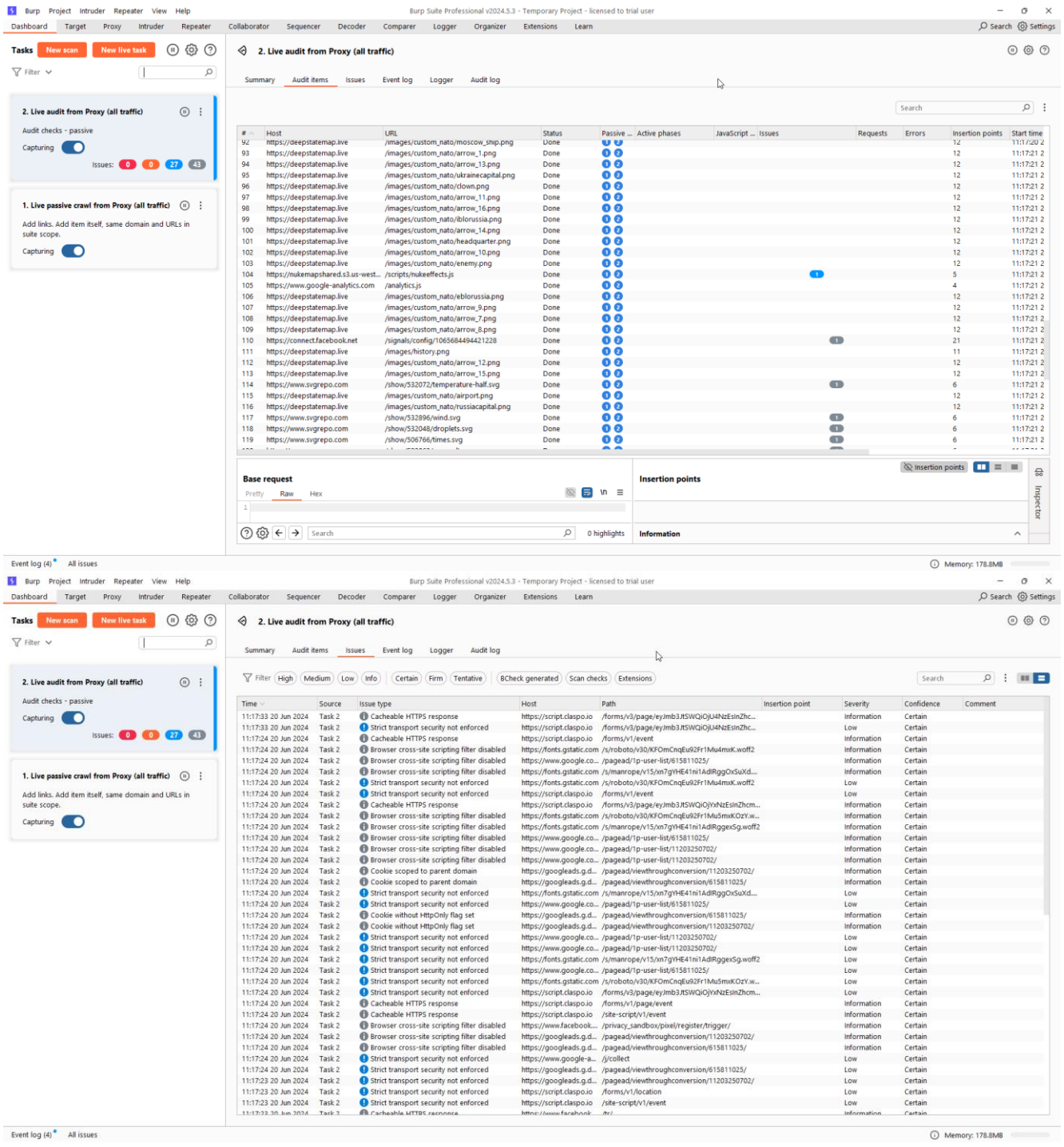
- гарантує доступ до послуг безпеки лише через інтерфейс КЗЗ;
- контролює всі запити на доступ до захищених об'єктів;
- описує та документує обмеження, недотримання яких може призвести до порушення цілісності КЗЗ;
- інформує користувачів про порядок роботи з дотриманням обмежень;
- надає адміністратору можливість контролю за дотриманням порядку.

У разі порушення цілісності компонента КЗЗ:

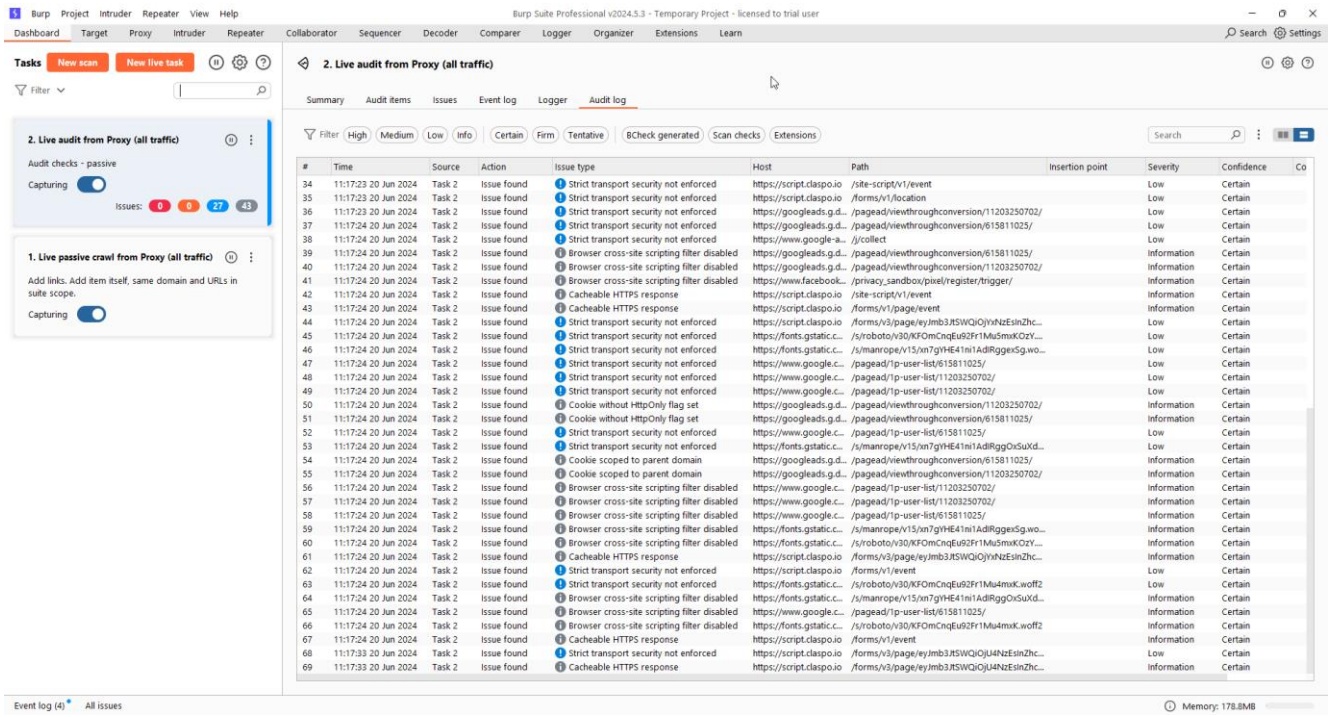
- адміністратор безпеки отримує повідомлення;
- доступ до WEB-сторінки для всіх користувачів, крім адміністратора безпеки, забороняється;
- повернення до нормального режиму можливе тільки після відновлення відповідності компонента еталону адміністратором.

Результати тестування WEB- сайтів.




Burp Project Intruder Repeater View Help
Burp Suite Professional v2024.5.3 - Temporary Project - licensed to trial user
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks New scan New live task
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing
Issues: 0 0 27 43
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing
Summary Audit items Issues Event log Logger Audit log
Host URL Status Passive ... Active phases JavaScript ... Issues Requests Errors Insertion points Start time
Base request
Pretty Raw Hex
Insertion points
Information
Inspector
Event log (4) All issues
Memory: 178.8MB

Burp Project Intruder Repeater View Help
Burp Suite Professional v2024.5.3 - Temporary Project - licensed to trial user
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks New scan New live task
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing
Issues: 0 0 27 43
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing
Summary Audit items Issues Event log Logger Audit log
Filter High Medium Low Info Certain Firm Tentative BCheck generated Scan checks Extensions
Time Source Issue type Host Path Insertion point Severity Confidence Comment
Event log (4) All issues
Memory: 178.8MB


Burp Project Intruder Repeater View Help
Burp Suite Professional v2024.5.3 - Temporary Project - licensed to trial user
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks New scan New live task
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing
Issues: 0 0 27 43
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing
2. Live audit from Proxy (all traffic)
Summary Audit items Issues Event log Logger Audit log
Filter High Medium Low Info Certain Firm Tentative BCheck generated Scan checks Extensions
Search
Time Source Action Issue type Host Path Insertion point Severity Confidence
34 11:17:23 20 Jun 2024 Task 2 Issue found Strict transport security not enforced https://script.claspo.io /site-script/v1/event Low Certain
35 11:17:23 20 Jun 2024 Task 2 Issue found Strict transport security not enforced https://script.claspo.io /forms/v1/location Low Certain
36 11:17:23 20 Jun 2024 Task 2 Issue found Strict transport security not enforced https://googleads.g.d... /pagead/viewthroughconversion/11203250702/ Low Certain
37 11:17:24 20 Jun 2024 Task 2 Issue found Strict transport security not enforced https://googleads.g.d... /pagead/viewthroughconversion/615811025/ Low Certain
38 11:17:24 20 Jun 2024 Task 2 Issue found Strict transport security not enforced https://www.google-a... /j/collect Low Certain
39 11:17:24 20 Jun 2024 Task 2 Issue found Browser cross-site scripting filter disabled https://googleads.g.d... /pagead/viewthroughconversion/615811025/ Information Certain
40 11:17:24 20 Jun 2024 Task 2 Issue found Browser cross-site scripting filter disabled https://googleads.g.d... /pagead/viewthroughconversion/11203250702/ Information Certain
41 11:17:24 20 Jun 2024 Task 2 Issue found Browser cross-site scripting filter disabled https://www.facebook... /privacy_sandbox/pixel/register/trigger/ Information Certain
42 11:17:24 20 Jun 2024 Task 2 Issue found Cacheable HTTPS response https://script.claspo.io /site-script/v1/event Information Certain
43 11:17:24 20 Jun 2024 Task 2 Issue found Cacheable HTTPS response https://script.claspo.io /forms/v1/page/event Information Certain
44 11:17:24 20 Jun 2024 Task 2 Issue found Strict transport security not enforced https://script.claspo.io /forms/v3/page/eyJmb3JtSWQiOjYxNzEsInZhc... Low Certain
45 11:17:24 20 Jun 2024 Task 2 Issue found Strict transport security not enforced https://fonts.gstatic.c... /s/roboto/v30/KFOmCnqEu92Fr1Mu5mxKOzY.... Low Certain
46 11:17:24 20 Jun 2024 Task 2 Issue found Strict transport security not enforced https://fonts.gstatic.c... /s/manrope/v15/xn7gYHE41ni1AdIRggexSg.wo... Low Certain
47 11:17:24 20 Jun 2024 Task 2 Issue found Strict transport security not enforced https://www.google.c... /pagead/1p-user-list/615811025/ Low Certain
48 11:17:24 20 Jun 2024 Task 2 Issue found Strict transport security not enforced https://www.google.c... /pagead/1p-user-list/11203250702/ Low Certain
49 11:17:24 20 Jun 2024 Task 2 Issue found Strict transport security not enforced https://www.google.c... /pagead/1p-user-list/11203250702/ Low Certain
50 11:17:24 20 Jun 2024 Task 2 Issue found Cookie without HttpOnly flag set https://googleads.g.d... /pagead/viewthroughconversion/11203250702/ Information Certain
51 11:17:24 20 Jun 2024 Task 2 Issue found Cookie without HttpOnly flag set https://googleads.g.d... /pagead/viewthroughconversion/615811025/ Information Certain
52 11:17:24 20 Jun 2024 Task 2 Issue found Strict transport security not enforced https://www.google.c... /pagead/1p-user-list/615811025/ Low Certain
53 11:17:24 20 Jun 2024 Task 2 Issue found Strict transport security not enforced https://fonts.gstatic.c... /s/manrope/v15/xn7gYHE41ni1AdIRggOxSuXd... Low Certain
54 11:17:24 20 Jun 2024 Task 2 Issue found Cookie scoped to parent domain https://googleads.g.d... /pagead/viewthroughconversion/615811025/ Information Certain
55 11:17:24 20 Jun 2024 Task 2 Issue found Cookie scoped to parent domain https://googleads.g.d... /pagead/viewthroughconversion/11203250702/ Information Certain
56 11:17:24 20 Jun 2024 Task 2 Issue found Browser cross-site scripting filter disabled https://www.google.c... /pagead/1p-user-list/11203250702/ Information Certain
57 11:17:24 20 Jun 2024 Task 2 Issue found Browser cross-site scripting filter disabled https://www.google.c... /pagead/1p-user-list/11203250702/ Information Certain
58 11:17:24 20 Jun 2024 Task 2 Issue found Browser cross-site scripting filter disabled https://www.google.c... /pagead/1p-user-list/615811025/ Information Certain
59 11:17:24 20 Jun 2024 Task 2 Issue found Browser cross-site scripting filter disabled https://fonts.gstatic.c... /s/manrope/v15/xn7gYHE41ni1AdIRggexSg.wo... Information Certain
60 11:17:24 20 Jun 2024 Task 2 Issue found Browser cross-site scripting filter disabled https://fonts.gstatic.c... /s/roboto/v30/KFOmCnqEu92Fr1Mu5mxKOzY.... Information Certain
61 11:17:24 20 Jun 2024 Task 2 Issue found Cacheable HTTPS response https://script.claspo.io /forms/v3/page/eyJmb3JtSWQiOjYxNzEsInZhc... Information Certain
62 11:17:24 20 Jun 2024 Task 2 Issue found Strict transport security not enforced https://script.claspo.io /forms/v1/event Low Certain
63 11:17:24 20 Jun 2024 Task 2 Issue found Strict transport security not enforced https://fonts.gstatic.c... /s/roboto/v30/KFOmCnqEu92Fr1Mu4mxK.woff2 Low Certain
64 11:17:24 20 Jun 2024 Task 2 Issue found Browser cross-site scripting filter disabled https://fonts.gstatic.c... /s/manrope/v15/xn7gYHE41ni1AdIRggOxSuXd... Information Certain
65 11:17:24 20 Jun 2024 Task 2 Issue found Browser cross-site scripting filter disabled https://www.google.c... /pagead/1p-user-list/615811025/ Information Certain
66 11:17:24 20 Jun 2024 Task 2 Issue found Browser cross-site scripting filter disabled https://fonts.gstatic.c... /s/roboto/v30/KFOmCnqEu92Fr1Mu4mxK.woff2 Information Certain
67 11:17:24 20 Jun 2024 Task 2 Issue found Cacheable HTTPS response https://script.claspo.io /forms/v1/event Information Certain
68 11:17:33 20 Jun 2024 Task 2 Issue found Strict transport security not enforced https://script.claspo.io /forms/v3/page/eyJmb3JtSWQiOjU4NzEsInZhc... Low Certain
69 11:17:33 20 Jun 2024 Task 2 Issue found Cacheable HTTPS response https://script.claspo.io /forms/v3/page/eyJmb3JtSWQiOjU4NzEsInZhc... Information Certain
Event log (4) All issues
Memory: 178.8MB