ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра інженерії програмного забезпечення

Пояснювальна записка
до магістерської роботи
на ступінь вищої освіти магістр

на тему: «**РОЗРОБКА КОМПЛЕКСНОЇ МЕТОДИКИ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ WEB-ДОДАТКІВ**»

Виконав: студент 6 курсу, групи ПДМ-61
спеціальності: 121 Інженерія програмного забезпечення
(шифр і назва спеціальності)

Вітусевич Є.С.
(прізвище та ініціали)

Керівник Негоденко О.В.
(прізвище та ініціали)

Рецензент_____
(прізвище та ініціали)

Нормоконтроль_____
(прізвище та ініціали)

Київ – 2022

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра Інженерії програмного забезпечення
Ступінь вищої освіти -«Магістр»
Спеціальність підготовки – 121 «Інженерія програмного забезпечення»

ЗАТВЕРДЖУЮ
Завідувач кафедри
Інженерії програмного забезпечення
_____Негоденко О.В.
"____" _____2022 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТА

Вітусевичу Євгенію Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи: «Розробка комплексної методики виявлення вразливостей WEB-додатків»

Керівник роботи: Негоденко О.В., к.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом закладу вищої освіти від « 11 » жовтня 2021 року №.170
2. Строк подання студентом роботи _____
3. Вхідні дані до роботи
Евристично-аналітичні методи пошуку вразливостей;
Науково-технічна література з питань, пов'язаних з методиками виявлення вразливостей WEB-додатків;

4. Зміст розрахунково-пояснювальної записки(перелік питань, які потрібно розробити).
4.1 Аналіз захищеності WEB-додатків.
4.2 Аналіз існуючих вразливостей WEB-додатків.
4.3 Аналіз нормативного забезпечення в галузі інформаційної безпеки.
4.4 Розробка комплексної методики.

5. Перелік демонстраційного матеріалу (назва основних слайдів)

5.1 Мета, об’єкт та предмет дослідження.

5.2 Актуальність роботи.

5.3 Евристично-аналітичний метод виявлення загроз.

5.4 Система аналізу DPI.

5.5 Використання системи аналізу DPI.

5.6 Спрощена аналітична модель.

5.7 Математичне обгрунтування.

5.8 Результати моделювання.

5. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури		Виконано
2	Аналіз захищеності WEB-додатків		Виконано
3	Аналіз існуючих вразливостей WEB-додатків		Виконано
4	Аналіз нормативного забезпечення в галузі інформаційної безпеки		Виконано
5	Розробка комплексної методики пошуку вразливостей		Виконано
6	Вступ, висновки, реферат		Виконано
7	Розробка обов‘язкових демонстраційних матеріалів		Виконано
8	Попередній захист роботи		
9	Здача роботи		

Студент _____ Вітусевич Є.С.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Негоденко О.В.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Текстова частина магістерської роботи 83 с., 12 рис., 4 табл., 29 джерел.

Об'єкт дослідження – методи та засоби захисту WEB-додатків від зловмисників.

Предмет дослідження – методика виявлення вразливостей WEB-додатків з використанням евристичних методів та системного аналізу.

Мета роботи – удосконалення існуючих процесів виявлення вразливостей WEB-додатків з використанням евристичних методів та системного аналізу.

Методи дослідження – методи теорії ймовірності, математичної статистики, математичне імітаційне моделювання та евристично-аналітичні методи.

У роботі проведено аналіз захищеності WEB-додатків. Наведено статистику найбільш розповсюджених вразливостей зі списку OWASP та проаналізовано результати досліджень повнофункціональних WEB-додатків, для яких у 2020 році проведено аналіз із найповнішим покриттям.

Здійснено аналіз існуючих вразливостей та подано узагальнені дані стосовно їх розповсюдженості.

Проаналізовано нормативне забезпечення та оглянуто міжнародні стандарти в галузі оцінювання інформаційної безпеки, взято до уваги існуючі методи оцінювання та управління ризиками інформаційної системи.

Запропоновано метод посилення рівня захищеності WEB-додатків за допомогою використання IPS та Firewall в якості базової системи захисту в комбінації з евристичним методом пошуку вразливостей та технологією системного аналізу DPI, яка дозволяє на найвищих рівнях моделі OSI працювати з захищеними даними. На відміну від брандмауерів, Deep Packet Inspection аналізує не лише заголовки пакетів, але і повний вміст трафіку на рівнях моделі OSI з другого і вище.

Застосувавши комплексне рішення, яке запропоноване в магістерській роботі, можна звести до мінімуму ризики пов’язані з компрометацією роботи системи.

Галузь використання – пошук вразливостей WEB-додатків.

ПОШУК ВРАЗЛИВОСТЕЙ WEB-ДОДАТКІВ, ЕВРИСТИЧНО-АНАЛІТИЧНІ МЕТОДИ, DPI, WEB-ДОДАТОК, IPS, FIREWALL

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

(Computer Emergency Response Team) – спеціалізований структурний підрозділ Державного центру кіберзахисту.

CERT – UA (Computer Emergency Response Team – Ukraine) – команда реагування на комп’ютерні надзвичайні події в Україні.

FIRST (Forum of Incident Response and Security Teams) – форум команд реагування на надзвичайні події.

FTP (File Transfer Protocol) – протокол передачі файлів по мережі.

HTTP (Hypertext Transfer Protocol) – протокол передачі даних.

ID (Identifier) – унікальна ознака об'єкта.

IP (Internet Protocol) – інтернет протокол.

ISO (International Organization for Standardization) – міжнародна організація, що займається випуском стандартів.

LDAP (Lightweight Directory Access Protocol) – мережевий протокол прикладного рівня для надсилання запитів та модифікації даних служби каталогів через TCP/IP.

NIST (National Institute of Standards and Technology) – національний орган зі стандартизації у США.

OWASP (Open Web Application Security Project) – це відкритий проект забезпечення безпеки WEB-додатків.

XSS (Cross – site Scripting) – міжсайтове виконання сценаріїв ДСТУ – державний стандарт України НД ТЗІ – нормативний документ системи технічного захисту інформації.

QoS (Quality of service) – набір методів для управління ресурсами пакетних мереж.

Модель OSI — абстрактна мережева модель для комунікацій і розробки мережевих протоколів.

ВСТУП

Сьогодні інтернет є невідкладною складовою життя ледь не кожного з нас. З його допомогою люди можуть збирати та аналізувати необхідну інформацію, проводити час переглядаючи фільми, граючи в ігри, читаючи книги та спілкуючись між собою.

WEB-ресурсів стає дедалі більше. На жаль не всі з них є безпечними для користування. Відсутність базових налаштувань безпеки сприяють розповсюдженню різноманітних загроз. WEB-сайти можуть містити віруси або ж бути уразливими до хакерських атак. Внаслідок чого може бути викрадена та скомпрометована важлива інформація користувачів. Тому розробникам слід приділяти увагу безпеці розроблюваного продукту, а власникам продукту пам'ятати про це.

Рівень захищеності WEB-додатків продовжує постійно зростати, проте все ще залишається на доволі низькому рівні. В 9 з 10 WEB-додатків зловмисники можуть проводити атаки на користувачів. В тому числі – перенаправляти клієнтів на підконтрольний їм ресурс, викрадати дані за допомогою фішингових атак та заражати комп'ютер шкідливим програмним забезпеченням. Несанкіонований доступ до WEB-додатку можливий на 39% сайтів. Загроза втрати важливих даних присутня в 68% WEB-додатків.

Є безліч компаній готових платити фахівцям для дослідження вузьких місць їхніх продуктів з метою усунення вразливостей. Попри великий попит на подібних спеціалістів – кадрів недостатньо, а вартість послуг може бути досить значною, внаслідок чого лише невелика частина компаній здатні виділяти ресурси для підтримки безпеки програмного забезпечення у належному стані.

Обґрунтування вибору теми та її актуальність: З метою оптимізації та спрощення проведення операцій виявлення вразливостей WEB-додатків було прийнято рішення розробити комплексну методику виявлення проблем. За

допомогою розроблюваної методики можна швидко кваліфікувати вид загрози, передбачити можливі витоки інформації та зробити усе можливе аби цього не сталося.

Тому розробка комплексного рішення проблеми є доцільною і залишається актуальною науковою роботою, адже від захисту процесів, інформації та діяльності в кіберпросторі залежить дуже багато ніж просто втрата інформації.

Наукова новизна роботи полягає в розробці методики, яка в комплексі буде використовувати евристично-аналітичні методи виявлення загроз покладаючись на систему аналізу пакетів DPI на найвищих рівнях OSI та Firewall разом з IPS для забезпечення базового захисту.

Метою роботи є удосконалення існуючих процесів виявлення вразливостей WEB-додатків з використанням евристичних методів та системного аналізу.

Об'єкт дослідження – методи та засоби захисту WEB-додатків від зловмисників.

Предмет дослідження – методика виявлення вразливостей WEB-додатків з використанням евристичних методів та системного аналізу.

Методи дослідження – методи теорії ймовірності, математичної статистики, математичне імітаційне моделювання та евристично-аналітичні методи.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

- проаналізувати діючі міжнародні стандарти та рекомендовані практики у галузі управління інцидентами інформаційної безпеки;
- дослідити сучасні проблеми захисту WEB-додатків;
- проаналізувати існуючі WEB вразливості, методи та засоби захисту WEB-додатків;
- розробити методику виявлення вразливостей WEB-додатків.

1. АНАЛІЗ ЗАХИЩЕНОСТІ WEB-ДОДАТКІВ

1.1 Аналіз захищеності

З 2020 року значно (на 17% у порівнянні з 2019 роком) знизилася доля веб-додатків, котрі містять вразливості високого рівня ризику. Число критичних критично небезпечних вразливостей, котре в середньому припадає на один WEB-додаток, знизилося у порівнянні з минулим роком майже у півтора рази, рис. 1.1.

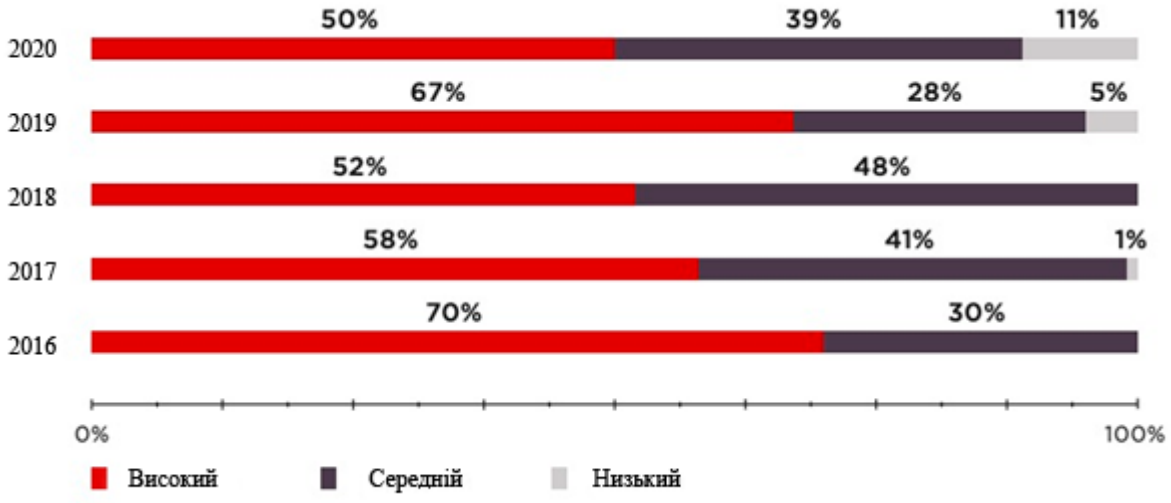

Рисунок 1.1 – Долі вразливих ресурсів в залежності від максимального ступеня ризику вразливостей

Аналізуючи дані за останні п’ять років, бачимо закономірне зниження долі сайтів, що містять критичні вразливості та загальне підвищення рівня захисту.

Рівень захищеності WEB-додатків визначається експертами за результатами проведених перевірок та залежить від потенційно можливого впливу на систему з урахуванням специфіки оброблюваної в ній інформації [1]. Топ десять найбільш розповсюджених вразливостей можна побачити на рис. 1.2.

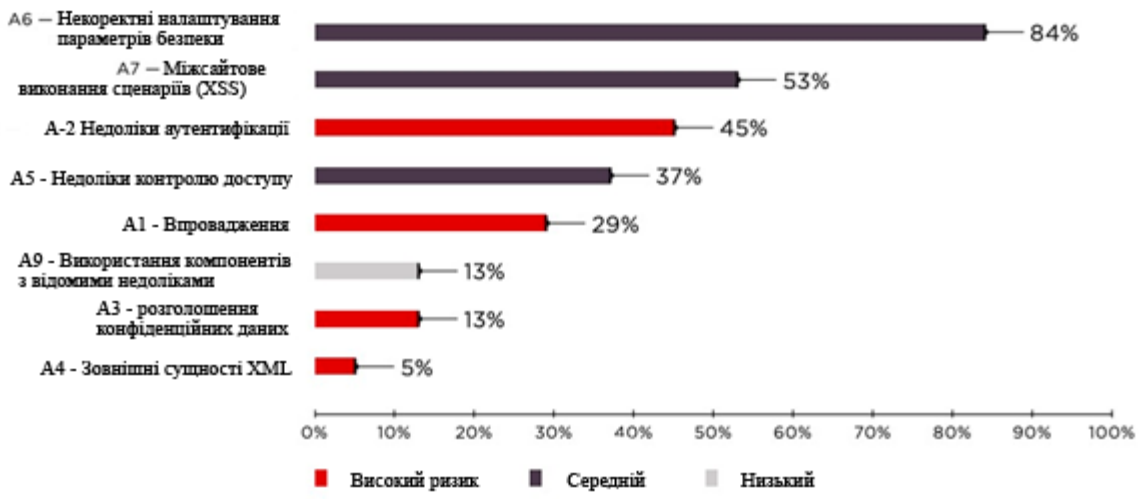

Рисунок 1.2 – Найбільш розповсюджені вразливості зі списку OWASP Top 10 (доля додатків)

Найчастіше за інших в 2020 році в веб-додатках зустрічалися вразливості пов'язані з невірними параметрами безпеки (Security Misconfiguration). Так, в кожному п'ятому проаналізованому додатку були виявлені вразливості, що дозволяють проводити атаку на сесію, в тому числі відсутність флагів HttpOnly та Secure в конфіденційних кукі параметрах. За допомогою цих недоліків хакери можуть проводити міжсайтові атаки (Cross-Site Scripting, XSS), щоб перехватити ідентифікатор сесії користувача та від його імені виконувати різноманітні дії в додатку.

В 45% веб-додатків були виявлені недоліки автентифікації. Майже третина виявлених вразливостей з цієї категорії – це невірне обмеження кількості невдалих спроб автентифікації. В результаті експлуатації цієї вразливості злочинці можуть підібрати дані користувача і таким чином отримати доступ до веб-додатка. Так, наприклад, для одного додатку знадобилося всього 100 спроб для того, щоб успішно увійти в систему з правами адміністратора.

Більшість атак на автентифікацію пов'язано з використанням виключно паролів. Раніше вважалося, що потреба у зміні пароля та його складності є гарним

способом для боротьби з подібними атаками, однак як стало зрозуміло пізніше, подібні дії лише сприяють використанню ненадійних паролів користувачами. Згідно останнім рекомендаціям, організаціям слід використовувати багатофакторну автентифікацію. Рис. 1.3 демонструє вразливості, що пов’язані з недоліками автентифікації.

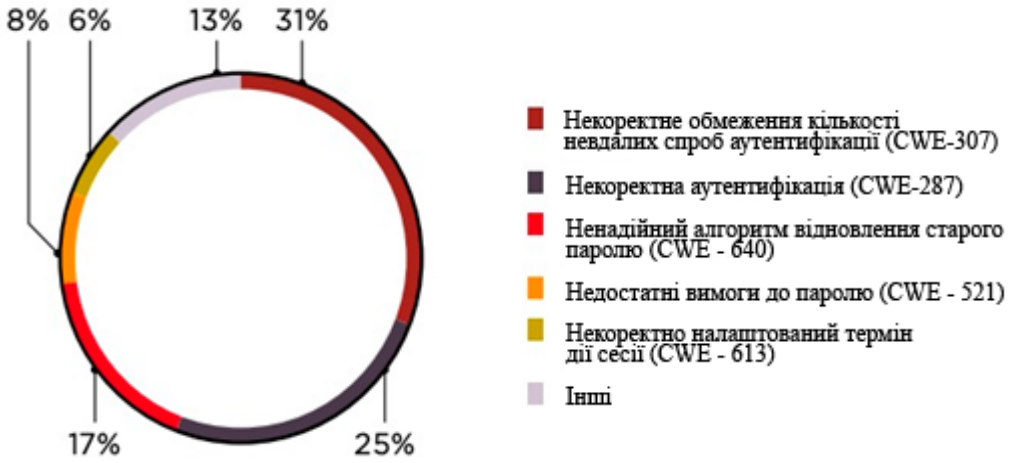

Рисунок 1.3 – Вразливості, пов’язані з недоліками автентифікації.

Недоліки контролю доступу в 2020 році зустрічалися в кожному третьому додатку. Обхід обмежень доступу зазвичай приводить до несанкціонованого розголошення, зміні або знищенню даних. Так, наприклад, в одному з проектів небезпечна авторизація дозволяла змінювати профіль будь-якого користувача додатку. Спеціалісти Positive Technologies дізналися логін адміністратора ресурсу, в його профілі змінили адресу електронної пошти на власну, а потім через стандартну процедуру відновлення пароля отримали доступ до сайту з правами адміністратора.

Кількість вразливостей, пов’язаних з автентифікацією та авторизацією, як правило, можна мінімізувати, якщо при розробці WEB-додатку дотримуватися практик безпечного програмування.

Окрім вразливостей зі списку TOP 10-2017, OWASP виділяє ряд недоліків, наявність яких рекомендується перевіряти. Третина веб-додатків виявилися вразливими для атак типу Clickjacking (містили вразливості пов’язані з невірним відображенням важливої інформації інтерфейсом користувача) і стільки ж для атаки пов’язаної з підробкою міжсайтового запиту. В ході CSRF-атаки зловмисники за допомогою спеціально зформованих сценаріїв можуть виконувати дії від імені користувача, авторизованого в уразливому WEB-додатку.

В ході атак типу Clickjacking користувач, як правило, вже знаходиться на сайті зловмисника, на якому користувач може скористатися рекламним банером чи цікавим посиланням. Поверх цих банерів або ж посилань хакер реалізовує невидимий HTML-фрейм вразливого сайту. Коли користувач тисне по кнопці відбувається дія на уразливому сайті, наприклад відбувається накрутка лайків, голосів тощо. Одним із способів захисту від цього типу атак є використання HTTP заголовка X-Frame-Options. Рис. 1.4 демонструє вразивості, що не увійшли до топ десять.

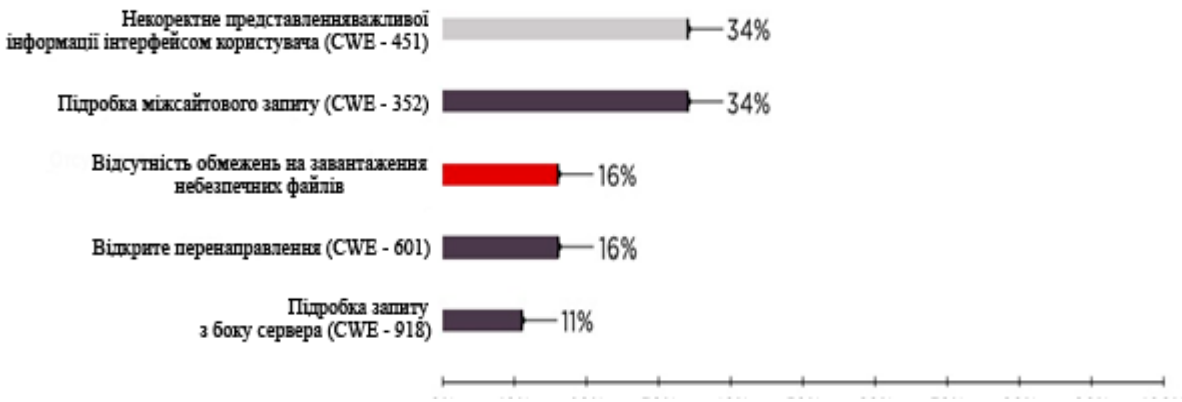

Рисунок 1.4 – Вразливості, що не увійшли в OWASP TOP 10

1.2 Аналіз загроз

Як і в 2019 році, в 2020 році для 9 з 10 веб-додатків актуальна загроза атаки на клієнтів. Як і раніше, суттєву роль при цьому грає «Міжсайтове виконання сценаріїв».

У результаті експлуатації вразливостей зловмисник може заразити комп'ютери користувачів шкідливим програмним забезпеченням, проводити фішингові атаки, наприклад для отримання учбових даних, а також виконувати дії від імені користувача. Під час отримання загальних рекомендацій щодо захисту варто відмітити, що всі дані, які надходять із сторін користувача та потім відображаються в браузері, включаючи заголовки HTTP-запрошення, такі як User-Agent, Referer, - повинні проходити попередню обробку. Потенційно небезпечні символи, які можуть бути використані при форматуванні HTML-сторінок, повинні бути замінені на їх еквіваленти, котрі не являються символами форматування. Крім того, рекомендується використовувати сучасні мережеві екрани рівня додатків (брандмауери веб-додатків), оскільки вони намагаються блокувати міжсайтове виконання сценаріїв. На рис. 1.5 можна побачити топ п’ять найбільш розповсюджених загроз.

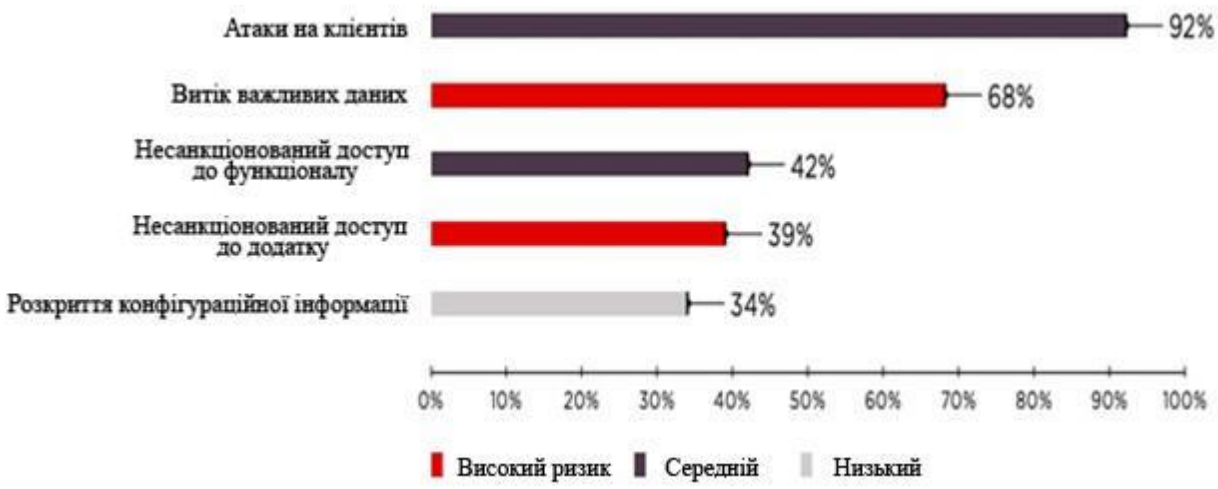

Рисунок 1.5 – Топ п’ять найбільш розповсюджених загроз

Витік важливої інформації є другою за актуальністю загрозою безпеці сайту. Таким чином, майже половина витоків (47%) загрожувала особистим даним, а 31% - обліковим даним користувача. Як показує проведений аналіз кіберінцидентів у 2020

році, саме крадіжка інформації є пріоритетною метою зловмисників при атаках на юридичні особи.

Результати дослідження свідчать про те, що на сьогоднішній день не всі компанії готові забезпечити надійний захист персональних даних.

У 16% веб-додатків були знайдені критично небезпечні уразливості, що дозволяють отримати контроль не тільки над додатком, а й над операційною системою сервера. Рис. 1.6 демонструє статистику розголошених даних.

Рисунок 1.6 – Статистика розголошених даних

Зловмисник, який отримав контроль над веб-додатком може, наприклад, впровадити в його код JavaScript код і продовжити атаку вже на користувачів сайту. Подібні вставки можуть використовуватися для крадіжки як облікових і персональних даних, так і даних банківських карт. У 2018-2019 роках серед атак на приватних осіб найбільш небезпечними виявилися саме атаки з використанням JavaScript вставок. Для того, щоб їх виявити, потрібно проводити аналіз захищеності методом білого ящика.

У разі цілеспрямованої атаки на організацію уразливості веб-додатків можуть допомогти зловмисникам отримати дані про внутрішні мережі компанії - про структуру сегментів мережі, вибір потрібного порту, сервісах тощо. У ряді випадків порушники навіть можуть отримати доступ до внутрішніх ресурсів та конфіденційної інформації, що там зберігається.

Зловмисники можуть збирати викрадені дані в спеціальні бази, а потім використовувати їх в свої цілях для атаки на веб ресурси. Від подібних атак в травні 2019 постраждало півмільйона клієнтів двох інтернет-магазинів.

1.3 Інструментальний аналіз захищеності коду

При проведенні інструментального обстеження веб сайтів в першу чергу використовуються сканери безпеки (а в більшості випадків ними і обмежуються), котрі дозволяють шляхом здійснення перевірок досліджуваного об'єкта виявити його схильність до різноманітних вразливостей.

Інструментальне обстеження є найбільш простим і, як наслідок, найбільш поширеним способом проведення аналізу захищеності. За простоту даного способу доводиться розплачуватися помилками "другого роду". Такі помилки виникають, коли частина вразливостей, яким піддається досліджуваний додаток, не встановлені в процесі його аналізу. Подібна ситуація обумовлена в першу чергу функціональними обмеженнями автоматизованих засобів.

Незважаючи на деякі обмеження аналізу захищеності, що виконується таким способом, використання сертифікованих сканерів безпеки задовольняє вимогам стандарту PCI DSS (Payment Card Industry Data Security Standard). Даний стандарт описує вимоги до забезпечення інформаційної безпеки для компаній, що працюють з міжнародними платіжними системами, і починаючи з 2007 р стандарт є обов'язковим до виконання як для міжнародних, так і для українських організацій.

1.4 Ручний аналіз захищеності

У порівнянні з попереднім способом ручний спосіб пошуку вразливостей в веб сайтах дозволяє виявити більше число вразливостей та провести перевірки, які неможливо було виконати при проведенні інструментального обстеження. Однак варто зазначити, що на його виконання може бути витрачено набагато більше часу, ніж при проведенні аналогічних робіт з використанням інструментальних засобів.

Даний спосіб часто застосовується в тому випадку, коли неможливо або вкрай важко провести інструментальне сканування. Прикладом подібних web-сайтів можуть бути ресурси, які використовують продуману модель захисту від вразливостей типу "Підробка HTTP-запитів" (подібний захист запобігає обробку запитів, які надходять в обхід логіки навігації програми). На практиці подібні ресурси зустрічаються переважно в банківському секторі. В цьому випадку єдиним способом віддаленого аналізу захищеності веб сайту як раз і є виконання всіх перевірок вручну.

Консалтингові компанії в області інформаційної безпеки (системні інтегратори), які прагнуть надати послуги з оцінки захищеності інформаційних систем на високому рівні, при проведенні робіт з аналізу захищеності намагаються об'єднати обидва способи - інструментальний і частково ручний. Таким чином можливо отримати найбільш об'єктивну оцінку захищеності додатку з мінімальними тимчасовими витратами на його проведення.

1.5 Аналіз вихідного коду

Даний спосіб дозволяє виявити всі уразливості, яким піддається веб сайт. Але в силу своєї складності подібний аналіз може займати досить багато часу, що пропорційно складності стилю програмування, який використовується при написанні сайту, і обсягом аналізованого коду.

На практиці аналіз вихідного коду використовується в повному обсязі переважно для окремих модулів або функцій веб сайту.

Виділяють наступні методи аналізу захищеності веб додатків.

Метод "чорного ящика". Принцип "чорного ящика" полягає в проведенні робіт по оцінці захищеності веб сайту без попереднього отримання будь-якої інформації з боку замовника про досліджуваний додаток. Даний метод застосовується, коли необхідно оцінити захищеність сайту з позицій зловмисника з мінімальним рівнем знань про досліджувану систему. В основному подібні дослідження здійснюються в рамках проведення робіт з тестування на проникнення, тобто моделювання дій реального зловмисника щодо інформаційної системи клієнта.

Всі дослідження можуть проходити як з попередженням обслуговуючого персоналу про планові роботи, так і без нього. У другому випадку існує можливість оцінити, за який час після початку дослідження веб сайту буде зафіксовано інцидент, а також адекватність дій, котрі робляться для мінімізації впливу на додаток в реальних умовах (імітація дій реального зловмисника).

Метод "сірого ящика". Це найбільш поширена практика проведення робіт з аналізу захищеності додатків. Його принцип полягає в проведенні робіт по оцінці захищеності з наданням всієї необхідної інформації про додаток виконавцю, окрім безпосереднього доступу до самого сервера, на якому функціонує веб сайт. Зазвичай виконавцю надаються такі дані: структура каталогів веб сайту, необхідні дані для можливості авторизованого підключення в додатку, вихідний код деяких файлів або функцій тощо.

Метод "білого ящика". Цей метод дозволяє домогтися максимальної ефективності від проведення аналізу захищеності. Принцип "білого ящика" має на увазі передачу всього інтернет-вузла виконавцю.

В даному випадку у фахівців з боку виконавця існує можливість відстежити, яким чином додаток реагує на будь-який запит, що передається до нього. Це найбільш

продуктивний метод проведення аналізу захищеності веб сайту, який дозволяє виявити найбільше число вразливостей.

Досвід показує, що більшість вразливостей сайтів пов’язані з помилками в коді WEB-додатку. І це спонукає надати спеціалістам вихідний код для проведення аналізу захищеності, або ж самостійно використовувати аналізатор коду в рамках процесу безпечної розробки. Майже 82% вразливостей пов’язані з кодовою базою додатків.

Так в рамках робіт з аналізу захищеності одного WEB-додатку експерти Positive Technologies змогли прочитати вихідний код одного з скриптів і виявили фрагмент, який дозволяв віддалено виконувати код. Використовуючи цю вразливість, будь-який зловмисник міг отримати контроль над сервером, переглядати важливу інформацію, редагувати і видаляти дані на сторінках ресурсу, а також повністю вивести сайт з ладу. Примітно, що поряд з цим фрагментом стояв коментар розробника: «Що це?». Ймовірно, цей артефакт був забутий іншим розробником при налагодженні програми, а пізніше його колеги не вважали питання важливим і не стали вникати в сенс і призначення цих рядків коду.

Аналіз захищеності методом білого ящику виконується декількома спеціалістами одночасно, щоб не впустити жодної деталі і виявити якомога більше недоліків. Крім того, даний вид робіт включає як ручний аналіз коду, так і аналіз з використанням засобів автоматизації. Автоматизований пошук вразливостей прискорює процес тестування, але потребує ручної перевірки для виключення випадкових спрацювань, а ручний аналіз коду займає більше часу, проте гарантує, що виявлені загрози актуальні.

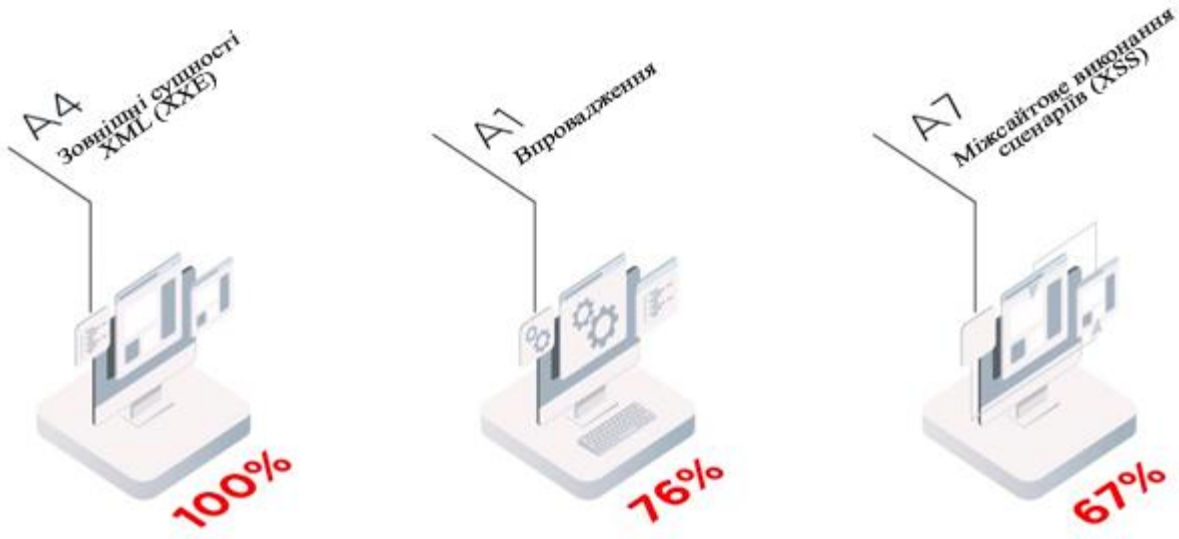

Рисунок 1.7 – Доля вразливостей, виявлених методом білого ящику

1.6 Організація процесу аналізу захищеності веб сайту

Необхідно зрозуміти, яку мету переслідує планований процес аналізу, потім визначити область дослідження і, керуючись стратегією управління інформаційною безпекою в компанії і припустимо бюджетом, сформувати необхідні перевірки з аналізу захищеності додатку.

Якщо мета аналізу захищеності веб сайту полягає в демонстрації проникнення, демонстрації порушення штатного режиму його роботи або демонстрації компрометації чутливої інформації в ньому, тоді роботи варто організувати за принципом "чорного ящика" без обмежень по проведеним перевіркам з боку виконавців консалтингової компанії, що надає подібні послуги . Результати такого дослідження наочно демонструють керівництву компанії-замовника поточний стан інформаційної безпеки. У разі низького рівня захищеності досліджуваних об'єктів подібні роботи наочно продемонструють реалізовані загрози інформаційної безпеки з боку зовнішнього порушника (хакера). Наслідком цього може стати виділення

додаткового бюджету відділу інформаційної безпеки з метою мінімізації ризиків, пов'язаних з реалізацією виявлених загроз.

Коли мета аналізу захищеності веб сайту полягає в істотному підвищенні рівня безпеки цього ресурсу і при цьому на прийняття рішень тисне обмежений бюджет, найбільш оптимально буде організувати процес аналізу ресурсу методом "сірого ящика" з використанням інструментального підходу до його обстеження з частковими ручними перевірками фахівцями консалтингової компанії. Такий підхід оптимальний у співвідношенні ціни і якості послуг, що надаються.

Який би варіант проведення обстеження не був би обраний, вкрай важливо створити резервні копії ресурсу до початку проведення подібних робіт з метою мінімізації небажаних наслідків, які можуть мати місце в силу присутності різних критичних вразливостей в інформаційній системі.

Таким чином, при організації процесу аналізу захищеності веб сайтів важливо визначити:

- мету проведеного дослідження;
- область дослідження;
- можливі обмеження при проведенні дослідження;
- необхідні методи і допустимі перевірки при проведенні дослідження.

Потім можна побудувати наступний технологічний процес аналізу захищеності:

- провести резервне копіювання об'єктів дослідження;
- провести аналіз захищеності інформаційних систем;
- усунути уразливості, якщо вони були виявлені (можливо, змінити процеси системи управління інформаційною безпекою або акцентувати увагу на недоліках, які до цього часу не були помічені);
- повторно провести аналіз захищеності і переконатися в коректності усунення виявлених вразливостей.

Доброю практикою системи управління інформаційною безпекою є використання "превентивних" підходів, тому аналіз захищеності, в першу чергу

додатків, що обробляють критичні для бізнесу дані, повинен бути частиною загальної стратегії побудови такої системи.

Висновки

Підбиваючи підсумки, варто відмітити, що рівень захищеності більшості веб-додатків продовжує залишатися на досить низькому рівні [26]. На кожному другому сайті присутні вразливості високого рівня ризику. Загалом можна констатувати, що з кожним роком постійно знижується доля веб-додатків, котрі містять критичні вразливості. Число вразливостей, яке в середньому приходиться на один додаток, знизилося в порівнянні з 2019 роком в півтора рази. Подібна тенденція також є в тому, що компанії, починають серйозніше відноситися до захисту веб-додатків.

Підтримання високого рівня захищеності WEB-додатків – непростий процес. Найбільш ефективно налаштувати його можна, дотримуючись декількох головних правил:

- виправлення виявлених вразливостей якомога раніше;
- автоматизація процесів, де це можливо.

Для їх виконання, окрім проведення аналізу захищеності WEB-додатків, компанії варто приділити увагу до підготовки програмістів методам безпечної розробки та використання інструментів для автоматизованого аналізу вихідного коду. Це дозволить скоротити кількість помилок і вразливостей ще на етапі розробки. Крім того, для захисту від атаки на WEB-додатки завжди варто застосовувати попереджувальні заходи захисту, такі як міжмережевий екран рівня програм (брандмауер веб-додатків, WAF). Використання WAF дозволить знизити відповідні риски. При цьому WAF не повинен виявляти та запобігати відомим атакам на рівні додатків та бізнес-логіки, а також виявляти експлуатацію вразливостей нульового дня, запобігати атакам на користувачів, аналізувати та порівнювати безліч подій для виявлення можливих атак.

2. АНАЛІЗ ПОШИРЕНИХ ВРАЗЛИВОСТЕЙ WEB-ДОДАТКІВ

В даному розділі буде розглянуто теоретичні основи та класифікацію вразливостей і атак. Класифікація є спільною спробою зібрати та організувати загрози безпеці для веб-серверів. Члени Web Application Security Consortium створили цей проект для розробки та просування стандартної термінології, яка використовується для опису цих проблем. Це дозволить розробникам додатків, експертам з безпеки, постачальникам програмного забезпечення та аудиторам взаємодіяти однією мовою.

У багатьох організаціях веб-додатки використовуються як критична система, яка щодня обробляє мільйони доларів транзакцій. Однак справжню цінність веб-сайту слід оцінювати відповідно до потреб кожної організації. Важливість речей у певній кількості форм неможливо уявити.

Уразливості веб-додатків вже давно становлять загрозу для користувачів. Після виявлення вразливості для здійснення атаки використовується один із кількох методів.

Розділ містить добірку відомих категорій атак, які загрожують WEB-додаткам. Кожна категорія атаки має стандартну назву та описує її основні характеристики. Класи організовані за ієрархією.

2.1 Аутентифікація (Authentication)

Цей розділ присвячено опису атак, що розповсюджені серед зловмисників, щоб перевіряти ідентифікатори обраного ними користувача, служби або програми. Розділяють 3 фактори (механізми), що висвічують автентифікацію:

- те, що у нас є;
- те, що ми знаємо;
- те, що ми є.

Ось опис атак, Що дають змогу обійти чи використати вразливі точки в факторі автентифікації, котрий підлягає реалізації WEB-сервером.

2.1.1 Підбір (Brute Force)

Для вгадування імені, паролю, номеру кредитки, ключа шифру чи інших даних майбутньої жертви аферисти використовують автоматичний хід спроб та похибок – **підбір.**

Вирізняють 2 види підбору:

- прямий - підбір різних варіантів паролю під однойменного користувача;
- зворотній - підбір різних імен користувачів при незмінному паролі. При існуванні мільйонів облікових записів в системі вірогідність того, що декілька осіб використало однаковий пароль вкрай висока.

Деякі системи пропускають використання слабких паролів чи шифрів. У висновку користувач обирає щось легке до запам’ятовування чи щось із запропонованого словника. Користуючись підбором даних з цього ж словника злодій, комбінуючи, підбере необхідний під користувача пароль. Атака вважатиметься вдалою, коли він матиме доступ до облікового запису.

Такою технікою спроб та похибок користуються, щоб підібрати ключ шифрування. При використанні ключа недостатнього обсягу, злодій у змозі одержати потрібний, якщо спробує інші вірогідні комбінації.

Підбір дуже популярний та високоефективний, проте, в залежності від випадку, може тривати годину, день або ж, навіть, рік.

2.1.2 Недостатня аутентифікація (Insufficient Authentication)

Якщо веб-сервер дає дозвіл зловмиснику на отримання доступу до користувацьких даних на сервері або ж до його функцій то автентифікація вважається недостатньою. Виразним прикладом критичних систем є WEB-інтерфейс адміністрування.

За специфікою програм, такі складники можуть бути доступними за недостатньої автентифікації. Для уникнення використання автентифікації для деяких ресурсів вони маскуються іншою адресою. Основні сторінки на сервері чи інші загальнодоступні ресурси не міститимуть посилань на дану адресу . Зловмисник може не знати URL-адресу, проте знайти доступ до неї через WEB.

Потрібний URL буде знайденим завдяки перебору файлів та директорій типу «/admin/», за використання сповіщень щодо помилок, звітів використаних посилань чи методом примітивної вичитки документів. Ресурс користувача повинен бути захищений у відповідності до його вагомості та функцій.

2.1.3 Небезпечне відновлення паролів (Weak Password Recovery Validation)

Така небезпека трапляється, якщо сервер дає дозвіл несанкціонованому отриманню, відновленню та модифікації паролів користувача.

Веб-сервер майже завжди пропонує запам’ятати логін та пароль при реєстрації на сайті. Лише користувачу має бути відомий пароль і чітко ним пам’ятатись.

Через деякий час, пароль забувають, адже середньостатистична людина користується декількома сайтами одночасно, а багато з них вимагають автентифікацію. Тому, можливість відновлення паролю – необхідність, яку допускає WEB-сервер.

Система може допомогти користувачу згадати зареєстрований пароль. При реєстрації можна скористатись функцією «секретне запитання». В ній необхідно обрати одне з наведених запитань або ж придумати своє та надати на нього відповідь. Таким чином, коли користувач не зможе пригадати пароль – він скористається цією функцією відповівши на своє запитання. Якщо відповідь буде правильною доступ до сайту надається, в іншому випадку ні. Інші функції вбачають за собою надсилання даних для зміни паролю на прив’язаний до сайту мобільний номер або електронну адресу.

2.2 Авторизація (Authorization)

Існують атаки зосереджені на методах аналізу сервером необхідних дозволів у користувача, служби або програми для входу та будь-якої діяльності на сайті. Деякі ресурси дають дозвіл лише окремим користувачам на одержання доступу до наповнення контентом та функціювання програм. Інші користувачі мають бути обмежені в доступі. Користуючись різними технологіями, злодій здатен укріпити свої привілеї для отримання доступу до автентичних даних.

2.2.1 Передбачуване значення ідентифікатора сесії (Credential/Session Prediction)

Передбачуване значення ідентифікатора сесії дає можливість перехопити користувацькі сесії. Таку атаку можливо виконати завдяки передбаченню або вгадуванню особливого коду сесії. Формат багатьох серверів допускає автентифікацію особи з першого звернення та надалі відстежувати його дії. Щоб це стало можливим користувач повинен вказати ім’я та пароль у відповідних полях. Повторно передавати щоразу дані користувачу не буде потреби, так як сервер згенерує особливий ідентифікатор, що буде присвоєний користувачу. Подальші спроби скористатись сервером міститимуть сесійний ідентифікатор - доказ, що автентифікація вдало пройдена. В разі передбачення або вгадування зловмисником особистого коду користувача, може бути проведена атака.

2.2.2 Відсутність тайм-ауту сесії (Insufficient Session Expiration)

Для зловмисника ідентифікатор сесії та облікові дані більш легкодоступні якщо для них відсутній тайм-аут. Таким чином, він може використати вкрадені застарілі дані щоб авторизуватись. Так як протокол HTTP не контролює сесію, то WEB-сервер, здебільшого, використовує ідентифікатор сесії щоб визначити запит користувача. Тому, кожен ідентифікатор повинен бути конфіденційним. Тоді вдасться запобігти

багаторазового доступу користувачів до одного профіля. Вкрадений ідентифікатор можуть використати, щоб отримати доступ до персональних даних та проведення шахраями фінансових транзакцій. При відсутності тайм-ауту збільшена вірогідність успіху аферистських атак. Зловмисник, що отримав ідентифікатор, скористається мережевим аналізатором або механізм відтворення сценаріїв між сайтами. Варто наголосити, що тайм-аут не стане в нагоді, якщо зловмисник негайно використає ідентифікатор. Обмежений час допомагає тільки при більш пізніх спробах користування ідентифікатором.

В ситуації, коли користувач отримав доступ до сервера в публічному місці з загального комп'ютера (в бібліотеці, інтернет-кафе, тощо) відсутність тайм-аут сесії дозволить зловмисникам використати історію браузера щоб переглянути сторінки користувача.

Значимо для користувача тайм-аут збільшує шанси підбору власного ідентифікатора. Також, при підвищенні даного параметра – збільшиться кількість відкритих сесій одночасно, а це, в свою чергу, збільшує вірогідність вдалого підбору.

2.2.3 Фіксація сесії (Session Fixation)

Користуючись цим методом, зловмисники застосовують до ідентифікатора сесії користувача дане значення. В залежності від функціонування механізму сервера, є кілька методів фіксації ідентифікатора сесії. В таких випадках використовують атаку у вигляді втілення міжсайтових сценаріїв, а також підготування сайту за допомоги завчасного HTTP запиту. Зафіксувавши значення ідентифікатора зловмисник вичікує момент, коли власник даних увійде в систему. Коли користувач виконає вхід, зловмиснику залишиться використати сесійний ідентифікатор, щоб отримати системний доступ від чужого імені.

Виділяють 2 типи систем для управління сесіями через ідентифікатори:

- дозволяючий - браузер має змогу показувати будь-який ідентифікатор. Тобто при використанні цих систем, зловмисники можуть обрати будь-який ідентифікатор сесії;
- суворий - обробляються лише ідентифікатори, генеровані сервером. З цими системами зловмисник мусить підтримувати «сесію-заглушку» та час від часу перевіряти з'єднання з сервером щоб уникнути закриття сесії завдяки тайм-ауту.

Не використавши активний захист від фіксування сесії, ці атаки можуть бути використані проти будь-якого сервера, автентифікації користувачів за допомогою ідентифікатора сесії. Здебільшого WEB-сервери зберігають ID в Cookie, проте ця інформація також може висвічуватись в прихованому полі форми або URL.

Статистично системи, що мають у використанні Cookie - найбільш уразливі. Здебільшого відомі сьогодні варіанти фіксування сесії напрямлені якраз на значення Cookie.

2.3 Атаки на клієнтів (Client-side Attacks)

Відвідуючи сайт користувач і сервер, відносно, встановлюють довірчі стосунки як технологічні, так і психологічні. Користувач бажає, щоб сайт надав йому достовірну інформацію. Також, користувач точно не очікує атаку зі сторони сайту. Користуючись цією довірою, аферист використовує різноманітні методики щоб атакувати клієнта сервера.

2.3.1 Підміна вмісту (Content Spoofing)

Користуючись цим методом, зловмисники змушують користувача повірити, що необхідна сторінка генерована веб-сервером, а не з іншого джерела.

Декотрі веб-сторінки створювались за використання динамічного джерела HTML-коду. Наприклад, місцезнаходження фрейму може бути переданим

параметром URL «http://for.example/page?frame_src=http://for.example/filev2.html». Атакуючі можуть підмінити значення параметру «frame_src» на «frame_src = http://attacker.example/spoofv2.html». Коли відображатиметься остаточна сторінка, в адресному рядку браузера для користувача буде відображено адресу сервера «for.example», проте аналогічно на сторінці буде присутній вміст з зовнішніх джерел, завантажених з сервера зловмисника «attacker.example», замаскований як легальний.

Підмінене посилання надсилають по електронній пошті, в мессенджерах публікуються на дошках оголошень, тощо. Користувач може бути впевнений, що переглядає достовірну інформацію з сервера, на яку його направили, проте насправді це може бути фішинговий сайт спеціально генерований зловмисником по сторонньому посиланню.

Отже, відбувається спотворення (дефейс) сайту «http://for.example» по сторону користувача, так як вміст сервера було добавлено з сервера «http://attacker.example». Цей вид атаки можуть використовувати задля проектування хибних сторінок, типу форми для вводу паролю, прес-реліз, тощо.

2.3.2 Міжсайтові скрипти (Cross-site Scripting, XSS)

Міжсайтові скрипти дають змогу зловмиснику транслювати серверу код, котрий виконуватиметься через браузер користувача. Такий код створюється на таких мовах як HTML / Java Script, проте можуть використовуватись і такими як VBScript, ActiveX, Java, Flash, та іншими, що підтримує браузер.

Направлений код виконуватиметься в контексті безпеки незахищеного сервера. Завдяки привілеям, код отримає змогу зчитувати, змінювати та передавати стороннім користувачам персональні дані. Крадіжка Cookie призводить до скомпрометованості облікового. Браузер скоріш за все буде направлений на другий сервер, а в іншому випадку здійсниться підміна його вмісту. У висновку завдяки чітко спланованій атаці аферист зможе використати браузер користувача для огляду інформації на сайті під

іменем атакованого. Код також може використовуватись злочинцем в заголовках HTTP запиту, URL, полях форм, тощо.

Є дві типові атаки, які призводять до міжсайтових виконань сценаріїв:

- збережені (постійні) – код передається та повертається в різних HTTP-запитах;
- відображені (непостійні) - код передається та повертається в діапазоні одного HTTP-запиту.

Для використання непостійної атаки користувач повинен перейти за посиланням генерованим зловмисником. Під час завантаження сайту код, вписаний до URL або ж заголовок запиту передається клієнту і використовується в його браузері. При передачі коду серверу його збереження навіть на короткий проміжок часу робить сайт вразливим. Найпопулярнішою цільовою аудиторією таких атак являються різні форуми, пошта з веб-інтерфейсом та чат-обговорення. Щоб потрапити на атаку досить просто відвідати незахищений сайт.

2.3.3 Розщеплення HTTP-запиту (HTTP Response Splitting)

За цим методом зловмисники надсилають серверу спеціально згенерований запит, на котрий приходить модифікована відповідь у вигляді двох різних. Дубльовану відповідь повноцінно контролюють зловмисники. Це дає їм можливість підробити відповідь сервера.

В розщепленні HTTP-запиту приймають участь хоча б 3 сторони:

- вразливий WEB-сервер;
- користувач;
- ініціатор атаки.

Можливою атака стане як тільки сервер поверне дані, що надавались користувачем. Здебільшого таке спостерігається, коли користувача перенаправляють на другу сторінку або якщо дані були збережені в Cookie.

Підґрунтям для розщеплення HTTP-запиту являється вписування символів переведення рядка (CR і LF) так, щоб згенерувати дві HTTP-транзакції, хоча в реальності відбуватиметься лише одна. Щоб завершити першу транзакцію та сформувати другу після пари питань та відповідей повністю контрольованих зловмисником та абсолютно непрогнозовану логікою програми використовують переклад рядка.

Після вдалої реалізації такої атаки аферист може піти на такі дії як:

- заміна даних кешу сервера посередника. Декотрі кешуючі сервери посередники (Squid 2.4, Apache Proxy 2.0, NetCache 5.2,тощо), зберігають на жорсткому диску підроблену злочинцем відповідь та на наступні запити користувачів за даною адресою завертають кешовану інформацію. Через це відбувається заміна сторінок сервера зі сторони клієнта. Також, інформація з Cookie користувача може бути перенаправлена або змінена. Таким же ж способом може атакований індивідуальний кеш браузера користувача;
- міжсайтове виконання сценаріїв;
- міжкористувацька атака за схемою: користувач - сторінка - її тимчасова підміна. Реалізуючи такий метод атакуючий не посилає додаткові запити але використовує той факт, що декотрі сервери посередники розділяють одне TCP-з'єднання до сервера різними користувачами. Як висновок - інший користувач одержить генеровану злочинцем сторінку у відповідь. Також атакуючий може виконувати різні операції з файлами Cookie користувача;
- перехопити сторінки, які вміщують персональні дані особи. Так аферист отримає відповідь з серверу замість користувача і загалом отримає доступ до персональних даних.

2.4 Виконання команд (Command Execution)

Цей вид атаки спрямований на виконанні команди(коду) на веб-сервері. Кожен сервер по суті використовує дані, надані користувачем під час обробки запитів. Таку інформацію використовують для генерування команд, що використовують для створення динамічного вмісту. Аферист має змогу змінювати виконавчі коди, якщо для їх розробки не враховувались вимоги безпеки.

2.4.1 Атака форматування рядків (Format String Attack)

Для атаки цим способом перезаписується область пам’яті через форматування символів. Таким чином змінюється шлях програмного виконання. Дані стають незахищеними, якщо користувач застосує їх як аргументи функцій для форматування рядків, а саме: printf, fprintf setproctitle, syslog sprintf, тощо. Коли зловмисник передасть додатком рядок, який містить форматуючі символи («% f», «% n» «% p»,, тощо.), то в нього з’явиться можливість:

- зчитувати значення з стека;
- виконувати довільне кодування на сервері;
- викликати програмні збої.

2.4.2 Впровадження операторів LDAP (LDAP Injection)

Ця атака спрямована на веб-сервери, які створюють запит до LDAP користуючись даними, що вводились користувачем. Спрощений протокол для доступу в служби каталогу - Lightweight Directory Access Protocol (LDAP) – це відкритий протокол, що використовується для створення запитів та управління службами даного каталогу сумісними з стандартом X.500. LDAP функціонує над транспортними протоколами Internet (TCP / UDP). WEB-додаток здатен застосовувати персональні дані користувача задля створення запитів протоколом LDAP в генерації

динамічних WEB-сторінок. Зловмисник має можливість атакувати модифікуючи LDAP-запит, коли верифікація користувача не проходить правильно.

Запит від LDAP виконуватиметься на тому ж рівні, на якому робить складник програми, що виконує запит (веб-сервер, сервер СУБД, тощо). Тобто зловмисник отримує ті ж можливості, на які має право складник програми. Метод використання даної вразливості майже не відрізняється від уведення SQL операторів.

2.4.3 Впровадження операторів SQL (SQL Injection)

Ця атака направлена на веб-сервери, котрі формують SQL запити до серверів СУБД опираючись на дані введені користувачем.

SQL(Structured Query Language) - мова запитів спеціалізована на програмуванні, котре дає змогу створити запит на сервери СУБД. Багато серверів використовують її у варіантах, уніфікованих ISO та ANSI. В більшості нинішніх СУБД є можливість використання діалекту SQL, специфічні для даної реалізації (PL SQL в Oracle, T-SQL в Microsoft SQL Server, тощо). Деякі веб-додатки користуються даними, переданими користувачем, задля створення динамічних веб-сторінок.

У випадку, коли інформація, отримана від користувача, не верифікується правильно, зловмисник здобуває можливість змінювати запит в SQL-сервер, який відправиться додатком. Запит виконається з тим самим рівнем переваг, з якими функціонує складник програми, котрий втілює запит (WEB-сервер, СУБД сервер , тощо). У висновку зловмисник здатен одержати повноцінний контроль над СУБД сервером, а також його ОП. Експлуатації LDAP Injection вкрай подібна до SQL Injection.

2.4.4 Впровадження серверних розширень (SSI Injection)

Даний клас атак дозволяє атакуючому передавати код, що буде виконаний на WEB-сервері. Незахищеність, яка призводить до змоги виконання таких нападів,

здебільшого відбуваються через відсутність перевірки персональних даних, що вказувались користувачем до збереження.

Задля генерації сторінки HTML сервер може здійснювати сценарії, типу SSI (Server-site Includes). У деяких ситуаціях вихідний код сторінок генерується на основі даних, наданих користувачем.

Зловмисник отримає змогу виконувати команди ОП або доповнити її забороненим вмістом при подальших відтвореннях, якщо передасть серверу оператори SSI.

2.5 Розголошення інформації (Information Disclosure)

Ця атака направлена на заволодіння інформації WEB-додатку. Користуючись цими вразливостями, атакуючий визначить використані форми розповсюдження (дистрибутиви) ПЗ, встановлені оновлення, номери версій сервера і користувача. Просочена інформація може містити розташування резервних копій та тимчасових файлів. В більшості випадків таким відомостям не надається увага користувача. Багато серверів дають доступ до надмірної кількості даних, проте варто організувати мінімізацію обсягу додаткової інформації. Від обсягу інформації, якою володіє зловмисник залежать його шанси на компрометацію системи.

2.5.1 Індексування директорій (Directory Indexing)

Надавання списків файлів до директорії - нормальна поведінка WEB-сервера, коли сторінка, що висвітлюється по замовченню (home.html / index.html / default.htm) неявна.

Якщо користувачем надіслано запит основної сторінки сайту, а він здебільшого вказує доменне ім’я серверу - сервер перегляне головну папку, знайде там файл, котрий застосовується по замовченню та базуючись на ньому згенерує відповідь.

Якщо такого файлу нема, то у відповідь користувачу повернеться список файлів з директорії сервера.

Аналогічно виконаються команди «dir» (Windows) або «ls» (Unix) на сервері та форматування наслідків у HTML.

Таким чином аферист має змогу одержати доступ до інформації, не призначеної бути доступною. Систематично адміністрація покладається на «безпеку через приховування», адже якщо гіперпосилання на файл відсутнє, то він типу недоступний. Нинішні сканери вразливості типу Nikto, здатні швидко додавати документи та тексти до сканованих списків в залежності від наслідків запитів. Користуючись інформацією з отриманого списку директорій або / robots.txt сканер можливо знайде непомітний вміст або ж інакші файли.

Так, ззовні вроді безпечний індекс директорій призведе до втрати вагомої інформації, котра надалі використовуватиметься для системних атак.

2.5.2 Витік інформації (Information Leakage)

Такі уразливості проявляються в обставинах, коли сервер опубліковує вагому інформацію, до прикладу, примітки розробників чи сповіщення про похибки, що дасть змогу скомпрометувати систему. Важливі, на розсуд атакуючого дані можуть знаходитися в сповіщеннях про помилки, коментарях HTML або бути у відкритому доступі. Існує неабияка кількість обставин, за котрих може просочитися інформація. З втратою вагомих даних можуть виникнути ризики різноманітного ступеня, чому й потрібно мінімізувати обсяг доступної інформації.

Аналіз доступних даних дає змогу аферисту провернути розвідку і одержати бачення щодо структури директорій сервера, які використовуються в заголовках ключових процесів і програм сервера та SQL запитах,.

Здебільшого розробники програми лишають примітки в HTML коді сценаріїв і сторінках для спрощення пошуку погрішностей і допомоги. Такі дані можуть бути як

простим описом подробиць поведінки програми, так і, в гірших випадках, іменами користувачів та паролями, що використовуються для налагодження.

Просочена інформація з серверу може виявитись персональними даними користувачів. Наприклад номери водійських посвідчень, паспортів, ІПН, тощо, а ще буденна інформація типу балансу особового рахунку чи історія платежів.

Деякі атаки переходять з області захисту WEB-додатків в область фізичної безпеки. Просочення даних, за таких умов, часто трапляється, якщо браузером відображена інформація, що не мала доступно показуватись навіть користувачем. До прикладу, можна привести номери кредитних карток, паролі користувача, тощо.

2.5.3 Зворотний шлях в директоріях (Path Traversal)

Така методика атаки цілеспрямована на заволодінні доступом до документів, папок і команд, що перебувають поза базою директорії WEB-сервера. Аферист проводить маніпуляції з URL-параметрами задля отримання доступу до тек аби реалізувати команди з файлової системи веб-сервера. До схожих атак чутливий любий пристрій, що використовує WEB-інтерфейс.

Безліч WEB-серверів лімітують доступ користувача деяким фрагментом документальної системи, названої «CGI root» або «web document root». Дані директорії включають документи, призначені лише користувачу та програмі, задля одержання доступу до функціонувань WEB-додатків.

Багато атак, що використовують зворотній напрям, започатковані на введенні в URL знаків «../», для зміни розташування ресурсу, що оброблятиметься сервером. Так як здебільшого WEB-сервери фільтрують цю черговість, то атакуючий скористається альтернативним кодуванням для надання символів та переходу по директоріях. Сучасні методики включають використовування альтернативного кодування типу Unicode («..% u2216 «або» ..% c0% af «), та застосування зворотного слеша (« .. \ «) в Windows-серверах, символів URL-Encode («% 2e% 2e % 2f «) або ж подвійне кодування URL-Encode («..% 255c»).

Якщо WEB-сервер обмежить хід до документів якимось каталогом, ця уразливість зможе проявлятися в CGI-програмах або сценаріях. Змога користування зворотним шляхом в каталогах доволі частенько з'являється в додатках, котрі застосовують механізми шаблонів або завантажують текст сторінок з документів на сервері. Цим варіаном кібер-атаки аферист видозмінює ім'я документу, який передається як параметр CGI-програми або сценарію серверу. Як результат - зловмисник зможе дістати вихідний код для сценаріїв. Нерідко до ім'я необхідного документу додають спеціальні символи, наприклад «% 00», задля обходу фільтрів.

2.5.4 Передбачуване розміщення ресурсів (Predictable Resource Location)

Передбачуване розміщення ресурсів дає змогу отримувати зловмисником доступ до скритих файлів або функціональних можливостей. Завдяки підбору він може здобути доступ до інформації, не призначеної до публічного огляду. Тимчасові документи, файли конфігурації, дані резервних копій часто стають метою похожих атак. Здебільшого підбір можна оптимізувати використавши стандартну угоду щодо імен файлів та директорій сервера. Отримані аферистом файли часто містять дані про дизайн платформи, бази даних, шляхи до директорій, імена машин або паролі. Приховані файли теж можуть включати уразливості, яких нема в головному додатку.

2.6 Логічні атаки (Logical Attacks)

Цей вид атаки цілеспрямований на використання функцій програм або закономірності їх функціонування. Логіка програми являється гіпотетичним процесом функціонування програм за виконання конкретних дій. До прикладу - відновлення паролів, реєстрація облікових даних, аукціони, перерахування в системі електронної комерції. Інколи додаток вимагає у користувача чітке виконання декількох покрокових дій задля виконання конкретного завдання. Атакуючий може оминути або використати такі механізми для своїх цілей.

2.6.1 Зловживання функціональними можливостями (Abuse of Functionality)

Цей вид атаки використовують для обходу механізмів розмежування доступу до WEB-функцій. Деякі компоненти WEB-додатків, залучаючи функції забезпечення безпеки, можуть використатись для цього. Наявна вразливість в хоча б одному з вторинних складових системи призведе до компрометації цілого додатку. Від самого додатку залежать рівень ризику та потенційні перспективи зловмисника в разі атаки.

Функціональні можливості досить часто використовуються додатково з інакшими атаками як зворотний шлях в директоріях, тощо. За наявності вразливості типу міжсайтового виконання сценаріїв в HTML-чаті аферист може використати функціонал чатів для розсилання URL, який використовує вразливість, всім поточним користувачам.

Загалом, всі види атак на комп'ютерну систему є зловживанням функціональними резервами. Найбільше це стосується атак, спрямованих на веб-додатки, котрі не потребують видозміни функцій програм.

2.6.2 Відмова в обслуговуванні (Denial of Service)

Цей вид атак спрямовують на сприяння недоступності веб-сервера. Здебільшого такі атаки, спрямовують на відмову в сервісі сайту, здійснюються саме до мережі, проте можуть бути націлені і на прикладні системи. Скориставшись функціями веб-додатків, аферист черпає критичні ресурси систем, або користується вразливістю, щоб призвести до збою функцій систем. Здебільшого DoS атака спрямована на використання критичних ресурсів систем, таких як оперативна пам'ять, обчислювальна потужність, пропускна здатність каналів зв'язку або дисковий простір. Коли хоча б один з ресурсів буде максимально завантаженим - додаток повністю стане недоступним. Атака може бути направлена на один з компонентів веб-додатку, як сервер СУБД, сервер автентифікації, тощо. На відміну від мережевих атак, які потребують значні ресурси зловмисника, прикладну атаку легше реалізувати.

2.6.3 Недостатня перевірка процесу (Insufficient Process Validation)

Вразливості даного виду трапляються, якщо сервер недостатньо перевіряється на послідовність виконування операцій програм. Коли сесії користувача та програм не контролюються відповідним чином, додаток може стати вразливим для шахраїв. В ході доступу до декотрих функцій програм передбачається, що користувач здійснить алгоритм дій в необхідному порядку. Коли декотрі дії виконуються не чітко або не по алгоритму, вибиває помилку, яка призводить до порушення цілісності. Прикладом схожих функцій є відновлення паролів, створення облікового запису, переклади, підтвердження покупок, тощо. Здебільшого дані процеси складаються з чіткого алгоритму дій. Щоб забезпечити коректну роботу схожих функцій WEB-додаток мусить детально відслідковувати становище сесії користувач та її відповідність вжитим операціям. У багатьох випадках це здійснюють напрямом фіксування стану сесії в Cookie чи прихованому полі форми HTML. Проте так як ці дані можуть змінитись користувачем, то обов’язково повинна проводитись перевірка потрібних даних на сервері. Якщо це не відбудеться, зловмисник отримає змогу оминути алгоритм і, в наслідку – логіку програми.

2.7 Узагальнені дані

Узагальнені результати за розподілом виявлених вразливостей за допомогою детального аналізу WEB-додатків і при автоматичному скануванні представлено в табл. 2.1.

Таблиця 2.1 – Узагальнена статистика вразливостей WEB-додатків

Тип уразливості	**Автоматичне сканування**		**Детальний аналіз**	
	% вразливостей	**% вразливих сайтів**	**% вразливостей**	**% вразливих сайтів**
Cross-Site Scripting	30,08	50,10	41,75	61,01
Information Leakage	29,82	97,19	12,50	16,94
SQL Injection	7,95	15,50	17,69	67,79
Brute Force	0,01	0,06	3,54	18,64
Path Traversal	0,23	0,70	4,95	11,86
HTTP Response Splitting	0,84	2,07	2,59	5,08
Predictable Resource Location	0	0	3,54	18,64
Insufficient Authentication	0	0	2,36	15,25
Abuse of functionality	0	0	1,65	6,77
Insufficient Process Validation	0	0	1,18	5,08
Insufficient Transport Layer Protection	11,18	53,25	0,94	3,38
Insufficient Session Expiration	0	0	0,71	5,08
Remote File Inclusion	0,22	0,44	0,71	3,38

Продовження таблиці 2.1 – Узагальнена статистика вразливостей WEB-додатків

Credential/Session Prediction	0	0	0,47	3,38
Insufficient Anti-automation	0	0	0,47	3,38
OS Commanding	0,08	0,06	0,47	3,38
Mail Command Injection	0	0	0,24	1,69
Session Fixation	0	0	0,24	1,69

Висновки

В даному розділі було описано атаки, направлені на методи, що використовуються WEB-сервером для визначення необхідних дозволів у користувача чи служби для проведення операцій. Більшість WEB-ресурсів мають обмеження на доступ до вмісту або функцій програмного забезпечення. Використовуючи різні технології, зловмисник може підвищити свої привілеї і отримати доступ до захищених ресурсів. При розробці методики потрібно врахувати існуючий досвід виявлення вразливостей.

3. АНАЛІЗ НОРМАТИВНОГО ЗАБЕЗПЕЧЕННЯ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У всьому світі безперервно проводиться розробка керівництв, стандартів, технічних звітів та рекомендацій в галузі ІБ (інформаційної безпеки). Публікують проекти і можливі шаблони, присвячені аспектам інформаційної безпеки на різноманітних стадіях погодження і затвердження. Розроблення нормативних актів з ІБ, повноцінно або в певній мірі присвячене керівництву над інцидентами ІБ, здійснюється низкою спеціалізованих інтернаціональних асоціацій та консорціумів (наприклад: IEC, CERT, IEEE, ISO, IETF, ITU-T, OMG, SANS Institute, X/Open тощо). Спеціалізованими структурами проводиться вагома робота щодо стандартизації факторів ІБ та керування інцидентами проводиться на національному рівні в:

- Німеччині та Великобританії – BSI ;
- США – NIST, CMU/SEI.

Це все дозволило організувати широку методологічно- нормативну базу у вигляді інтернаціональних, галузевих і національних стандартів, а ще керівних і нормативних матеріалів, що впорядковують діяльність в галузі правління випадками ІБ. Сучасна практика запевняє,, що найвагомішу роль на планеті відіграють стандарти ISO, що зображені в табл. 3.1.

Таблиця 3.1 – ISO стандарти

Позначення документу	**Назва документу**	**Рік**
ISO/IEC17799	Information technology. Security techniques. Code of practice fori nformation security management.	2000; 2005

Продовження таблиці 3.1 – ISO стандарти

ISO/IEC27001	Information technology. Security techniques. Information security management systems. Requirements.	2005; 2013
ISO/IEC TR27035	Information technology. Security techniques. Information security incident management (3 Part)	2011
ISO/IEC 20000	ISO/IEC 20000:2005. Information technology. Service management. Part 1: Code of practice.	2011

Стандарт ISO/IEC 17799 для сьогодення став найпопулярнішим знаряддям відтворення системи управління ІБ (СУІБ). Колишня версія ISO/IEC 17799 від 2000-го року юридично прийнята в Україні у вигляді ДСТУ ISO/IEC 17799:2000. ISO/IEC 17799 – зібрання організованих рекомендацій, що надає детальне керівництво для розробки, запровадження та аналізу заходів правління ІБ, а ще загальні положення доктрини СУІБ. Цим документом також встановлено наступні поняття, котрі являються базовими для цього дослідження:

- подія ІБ – установлений вираз стану системи, мережі або служби, котрий вказує на альтернативне порушення політики ІБ або збій заходів безпеки, або на невідому до цього моменту ситуацію, що може повпливати на безпеку [1, п. 2.6];
- інцидент ІБ – особливостями інциденту ІБ являються окремі або послідовні нежадані або неочікувані події ІБ, що мають високу ймовірність компрометації дипломатичних операцій і загрожують ІБ [1, п. 2.7].

Розділ 13 ISO/IEC 17799 присвячено управлінню інцидентами ІБ. В ньому розглядають такі питання:

- сповіщення про події і вразливі точки ІБ [1, п. 13.1]. Вияв користувачами подій і вразливих точок ІБ, пов’язаних з інформаційними системами, повинні запевнити можливість схвалення вчасних коригуючих дій;
- повинен бути впровадженим прямий порядок сповіщення про події та порядок ескалації. Всі співробітники, контрагенти та користувачі третіх сторін повинні бути проінформовані з приводу порядку сповіщення про різні типи подій і вражені точки, котрі матимуть вплив на безпеку цінності організації. Ці особи повинні негайно повідомити щодо будь-яких подій і слабких місць ІБ, використавши конкретну точку контактування.

У відповідності до регламентів, щодо подій ІБ необхідно повідомляти з допомогою допустимих каналів правління так швидко, як це можливо. Також потрібно утвердити алгоритм сповіщення про події ІБ, разом з алгоритмом реагування на події. В даних алгоритмах необхідно відобразити дії, що повинні здійснитись після отримання сповіщення про подію інформаційної безпеки. Потрібно постановити точку комунікації для сповіщень про події ІБ.

Далі, необхідно ознайомити всю організацію з даною точкою комунікації, інформацією про її стабільну доступність і спроможність адекватно і вчасно реагувати.

Приклади інцидентів та подій ІБ:

- утрата обслуговування, обладнання або засобів обслуговування;
- систематичні помилки або перевантаження систем;
- людські помилки;
- несумісність політики або керівництва;
- недотримання заходів фіз. безпеки;
- некеровані систематичні переміни;
- помилки апаратного або програмного забезпечення;
- порушення доступу.

Стандарт ISO/IEC 27001 [3] звертає увагу на потребу створення процедур керівництва інцидентами ІБ. Даний стандарт висуває загальні вимоги щодо побудови СКІБ, які відносяться також до процесів правління інцидентами ІБ. Опираючись на ISO/IEC 27001 обробку подій і інцидентів ІБ необхідно зорганізувати як процес реагування на ці інциденти.

Основні завдання процесу реагування на інциденти ІБ:

- координування реакції на інцидент ІБ;
- аргументування/спростовування факту виникнення події ІБ;
- забезпечення зберігання і цільності доказів прояву інциденту ІБ, створення відповідних умов накопичення і збереження конкретної інформації щодо інцидентів ІБ, які мали місце, та про корисні рекомендації;
- мінімізація недотримань циклу роботи та ушкодження даних ІТ систем, поновлення в найшвидші строки працездатності організації при її порушенні в через інцидент;
- мінімізація результатів недотримання конфіденційності, доступності та цілісності інформації ІТ-систем;
- захист прав організації, встановлених законодавством;
- створення певних умов для недотримання кримінальної чи цивільної справи проти аферистів;
- захист репутації установи та її ресурсів;
- динамічне виявлення та запобігання схожих інцидентів у майбутньому;
- організація навчання персоналу установи дій для виявлення, усунення результатів та запобігання інцидентам ІБ.

По ISO/IEC 27001 висувають такі вимоги до процесів реакції на інциденти ІБ, котрі повністю відповідають розглянутим вище рекомендаціям по керуванню інцидентами інформаційної безпеки у ISO/IEC17799.

Задачам по керуванню інцидентами ІБ присвятили технічний звіт.

ISO/IEC TR 27035 [4]. Стандарт ISO / IEC 27035:2011 «Інформаційні технології. Методи забезпечення безпеки. Управління інцидентами інформаційної безпеки» подає організоване керівництво з вияву, реєстрації та оцінки епізодів порушень ІБ та незахищеності.

Його ціль – допомогти організаціям вчасно реагувати на події ІБ, а також застосовувати відповідний інструмент контролю задля їхнього запобігання і зменшення, а ще відновлення, і, завдяки цьому, навчатись ситуативно та модернізувати загальний підхід.

Інтеграція систем правління подіями ІБ дає такі переваги:

- збільшення загального рівня ІБ;
- скорочення негативних впливів на бізнес;
- збагачення знань задля попередження подій ІБ, встановлення пріоритетів та збір даних;
- покращення результатів оцінки і управління ризиків ІБ;
- покращення інформування про область ІБ та допомога в підготовці навчальних матеріалів;
- надавання допоміжної інформації про політику ІБ та супровідної документації. Оновлений стандарт ISO/ IEC 27035 радить перевірені вирішення в області процесів і методів задля забезпечення ефективнішого управління подіями ІБ.

ISO/IEC 27035:2011 заміняє технічний звіт ISO/IEC TR 18044:2004 і погоджений з загальними правилами, встановленими в ISO / IEC 27001:2005 «Інформаційні технології. Методи забезпечення безпеки. Системи менеджменту інформаційної безпеки. Вимоги».

Стандарт може застосуватися в любій конторі, не залежно від її величини. Він поширює свою дію на великий діапазон випадків ІБ, зумисних чи невмисних, спричинених технічними чи фізичними проявами.

Процедура правління ІТ-інцидентами врегульовується стандартом **ISO/IEC 20000** [5], що відображає систему керування ІТ-сервісами і процедуру правління випадками, а також досліджує ІТ-інциденти. Сама процедура ІТ дуже наближена до процедури ІБ з різницею тільки в тому, що в ІБ більше робиться акцент на розслідування, збір доказів, покарання винуватих.

З позицій ISO/IEC 20000 процес керування ІБ має два цілеутворюючі значення:

- здійснення правил безпеки, закріплених в SLA (Service Level Agreement) і інших угод зовнішніх і внутрішніх домовленостей, законодавчих актів та встановлених правил;
- забезпечення базового показнику ІБ, в незалежності від зовнішніх потреб.

SLA –вихідні дані для процесу, що містять правила безпеки, по-можливості, підкріплені документами, котрі характеризують політику компанії в цій галузі та інші зовнішні канони. Процес теж отримує вагому інформацію, щодо проблем безпеки та інших процесів, наприклад, про події, пов’язані з ІБ.

CMU/SEI-2004-TR-015 (Defining incident management processes for CISRT) [6]. Даний документ окреслює методи планування, введення, аналізу та покращення процесів правління подіями. Основний акцент роблять на організації роботи CISRT (Critical Incident Stress Response Team) – групи або підрозділів, що убезпечують обслуговування і сприяння запобіганню, обробці та реакції на події ІБ. Вставляється ряд критеріїв, на основі котрих можна буде аналізувати ефективність цих сервісів.

NIST SP 800-61 (Computer security incident handling guide) [6]. Тут показана колекція «кращих практик» для організації процесів правління подіями та реакції на них. Детально розбирають питання реакцій на різноманітні види загроз типу поширювання шкідливого програмного забезпечення, несхвалений доступ та ін.

Задля визначення найбільш багатообіцяючих напрямів і тенденцій у всесвітньому законодавстві, у наступному підрозділі детальніше описано декотрі ознаки інтернаціональних законодавств.

3.1 Аналіз міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки

За останні роки у світі спостерігалась тенденція до стандартизації систем управління в компаніях. Ініціатива проявляється і на державному рівні, і на рівні окремих галузей посеред нормативних актів, які спонукують компанії перебудувати власну систему ІБ. Вони отримали найбільшу популярність - акт Sarbanes-Oxley та угода з банківського нагляду Basel II.

Sarbanes-Oxley був прийнятий в США задля контролю фінансової звітності компаній та на даний час використовується здебільшого в цій країні. Стандарт використовують ті організації, котрі виходять з власними акціями на американські біржі. Це передумова для запровадження контролю цілісності, захисту несанкціонованого доступу (НСД) та шифрування даних, тощо.

Угода Basel II більш широко розповсюджена: його канони застосовують в Євросоюзі, Японії, США та ін. Основна мета сприяти досягненню якої націлений документ - контроль банківських ризиків. Аналіз ризиків – один із найактуальніших напрямів в області регулювання банківської діяльності. Загалом це торкається операційних ризиків, що несуть банки [7]. Серед найбільш вагомих з них є ризики ІБ, такі як недостеменні або неточні дії персоналу і внутрішні процеси.

Можна виділити декілька складових управління ризиками:

- моніторинг і аналіз організаційних ризиків діяльності системи;
- моніторинг та аналіз ризиків технічних прийомів;
- прийняття рішення з керівництва ризиками на основі наявного аналізу;
- проведення особистої роботи з керівництва ризиками [8].

Поволі підхід, коли поодинокі канони нормативних актів і окремі проблеми ІБ вирішуються після виникнення, віддаляється у минуле. Немало організацій нині дійшли висновку, що порядок захисту інформаційних ресурсів повинен базуватися на загальноприйнятих нормах з врахуванням напрацьованих ситуацій. Цей метод

допомагає обійти розбудову інфраструктури ІС в «авральному режимі» під любі вимоги та зменшує незаплановані затрат на обслуговування систем.

3.2 Аналіз сучасних стандартів в галузі управління інформаційною безпекою системи

Сімейство Міжнародних Стандартів на Системи Управління ІБ 27000 розробляється документом ISO/IEC JTC 1/SC 27. До сімейства входять Міжнародні стандарти, що встановлюють вимоги до системи управління інформаційної безпеки (СУІБ), керівництво ризиками, метрики, вимірювання, а ще керівництво з запровадження.

До даного сімейства норм використовується послідовна схема нумерування, починаючи з 27000 і далі. ISO 27000 ISO/IEC 27000:2009 Information technology. Security techniques. Information security management systems. Overview and vocabulary (Визначення і основні принципи). Випущений в липні 2009 р.

ISO 27001 ISO/IEC 27001:2005/BS 7799-2:2005 Information technology. Security techniques. Information security management systems. Requirements Інформаційні технології (Методи забезпечення безпеки. Системи управління інформаційною безпекою. Вимоги). Випущений в жовтні 2005 р.

ISO 27002 ISO/IEC 27002:2005, BS 7799-1:2005, BS ISO/IEC 17799:2005 Information technology. Security techniques. Code of practice for information security management (Інформаційні технології. Методи забезпечення безпеки. Практичні правила управління інформаційною безпекою (УІБ)). Випущений в червні 2005 р.

ISO 27003 ISO/IEC 27003:2010 Information Technology – Security Techniques – Information Security Management Systems Implementation Guidance (Керівництво з впровадження СУІБ). Випущений в січні 2010 р.

ISO 27004 ISO/IEC 27004:2009 Information technology. Security techniques. Information security management. Measurement (Вимірювання ефективності СУІБ). Випущений в січні 2010 р.

ISO 27005 ISO/IEC 27005:2008 Information technology. Security techniques. Information security risk management (Інформаційні технології. Методи забезпечення безпеки. Управління ризиками ІБ). Випущений в червні 2008 р.

ISO 27006 ISO/IEC 27006:2007 Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems (Інформаційні технології. Методи забезпечення безпеки. Вимоги до органів аудиту та сертифікації СУІБ). Випущений в березні 2007 р.

ISO 27007 Керівництво для аудитора СУІБ (в розробці).

ISO 27011 ISO/IEC 27011:2008 Information technology. Security techniques. Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 (Керівництво з управління ІБ для телекомунікацій). Випущений в травні 2009 р.

ISO 27033-1 ISO/IEC 27033-1:2009 Information technology. Security techniques. Network security. Overview and concept (Основні концепції управління мережевою безпекою). Випущений в січні 2010 р.

Стандарт ISO/IEC 27001:2005 відображає загальну методику підходу для забезпечення ІБ в компанії та підкреслює увагу на найкритичніших складових ІС. Цей стандарт включає елементи правління системою ІБ, так необхідні всім сферам бізнесу, такі як: політика інформаційної безпеки, організація навчання в даній області, поділ відповідальності за ІБ, , звітність про події, забезпечення циклічної роботи, захист від вірусів, захист архівів, контролювання копіювання ліцензійного ПЗ та захист персональних даних. Даний стандарт дає організації знаряддя, яке дозволить керувати конфіденційністю, цілісністю і збереженням такого важливого активу компанії як інформація. Елементи управління системою ІБ поділені в стандарті по декілька груп, і включають такі розділи:

- політика безпеки – допомога політиці в сфері ІБ керівництвом підприємства;
- інфраструктура систем безпеки –організаційний підрозділ, який буде убезпечувати працездатність системи Ш в компанії;
- систематизація ресурсів і управління – пріоритетність інформаційних систем за ступенем їхньої значущості та поділ відповідальності за них;
- працівники – зменшення ризиків людських похибок, крадіжок і неправильного користування устаткуванням завдяки навчанню працівників та відстеженню подій;
- фізична і зовнішня безпека – запобігання НСД та недотримання роботи ІС компанії;
- керування мережами і серверними ресурсами – представлення безпечного функціоналу комп'ютерів і мереж;
- керування доступом – керування доступом до корпоративної інформації;
- розвиток і обслуговування систем – виконування правил безпеки при відтворенні чи розвитку ІС компанії, направлений на підтримку безпеки додатків і серверних даних;
- забезпечення циклічності бізнесу – план дій в надзвичайних обставинах для забезпечення циклічності роботи компанії;
- відповідність канонам законодавства – виконання правил відповідного громадянського і кримінального законодавства, включаючи такі закони як про авторські права та захист персональних даних.

Стандарт поділяється на дві частини: в першій - описано механізми контролю (всього 127), що потрібні для будови СУІБ. Дана частина використовується як базис для проведення аудитів СУІБ в компанії. В іншій частині описують критерії, за якими відбувається сертифікація СУІБ. За ідеологією стандарту, ключовий елемент СУІБ - система керування ризиками, найвагомішою частиною яких є оцінка ризиків для визначення, які саме ресурси та від яких небезпек потрібно захищати, а ще в якій мірі ресурси вимагають цього захисту. Проведення оцінки ризиків дозволяє компанії

оцінювати імовірні збитки в числових і якісних покажчиках. Цей інтернаціональний стандарт був заготовлений для надання моделі для виготовлення, введення, використання, постійного інспектування, оцінки, підтримання робочого стану та покращення СУІБ. Очікуватиметься, що прийняття 30 СУІБ є стратегічним для компанії[9]. Компанія, щоб вдовольнити побажання цього стандарту, мусить зробити такі кроки: встановити область програми та межі СУІБ в терміни характеристик для бізнесу, її місця знаходження, активи і технології, і, включаючи деталі та обґрунтування всіх винятків в колі використання; встановити політику щодо СУІБ в строках рекомендацій бізнесу, компанії, її місце розташування, цінностей та технологій; обороною інформації, врахувати законодавчі та нормативні канони, розкривати стратегії правління інформаційними ризиками; встановити підхід для аналізу ризику в компанії; встановити ризики; поцінити ризик та проаналізувати значущість ризику; виразити та проаналізувати перспективи обробки ризиків; обрати мету та способи керівництва для обробки небезпеки. Стандарт рекомендує робити стабільний контроль рентабельності СУІБ, аналіз цілей правління, зважаючи на результати аудиту та статистичні виникнення порушень.

Відповідно до стандарту ISO/IEC 27001 документи, що характеризують правління інформаційними ризиками компанії, має складатись з: документованої заяви про політику і мету СУІБ; область використання програми СУІБ; процедури і прийоми управління для підтримки СУІБ; опис методів аналізу ризиків; звітність про аналіз ризиків; програма обробки ризиків [9]. В даному розділі розглядаються типи зобов’язань правління, деякі положення менеджменту активів і забезпеченість необхідним рівнем компетенції персоналу. Стандарт досліджує головні цілі і правила проведення аудиту захищення компанії від загроз в інформативній сфері, а також оцінка СУІБ і сторони керівництва. У цьому стандарті вказано ключові вхідну та вихідну інформацію задля внутрішнього аудиту. Як важливі результати аудиту можна відокремити оновлення аналізу ризиків для компанії та відповідно заміну методів

правління ними. Підсумкова частина стандарту посвячена девізу постійного покращення в СУІБ.

Стандарт Великобританії BS 7799 присвячений УІБ організації. Даний стандарт - один з найавторитетніших у всьому світі. Базуючись на ньому розроблено інтернаціональний стандарт ISO/IEC 17799, котрий з часом еволюціонував у ISO/IEC 27002. Третя частина цього стандарту присвячується питанням керування інформаційними небезпеками.

Стандарт BS 7799-3:2006 гармонізований з ISO/IEC 17799:2005 щодо прикладів компонентів систем безпеки. Цей стандарт допускає використовування любих стратегій компанії аналізу ризиків, зокрема наведених у ISO 13335-3.

Стандарт BS 7799-3 вміщає вступ, розділи з аналізу ризиків, обробки ризиків, циклічні дії з керування ризиками, а ще має доповнення з зразками активів, загроз, вразливостей, методів аналізу ризиків. Стандарт додержується самого основного поняття ризику, під яким вбачають комбінації ймовірностей подій і їх наслідків. Керівництво ризиків сформовано як координовані циклічні дії з правління та контролю ризиків в компанії.

Оцінка ризиків – найперший етап в керівництві системи ІБ, призначеної для впізнавання джерел цих ризиків та визначення їх рівня значимості. Оцінку поділяється на аналіз ризиків та оцінку ризиків. В межах аналізу проводять інвентаризацію і катетеризацію активів, котрі захищаються, визначаються нормативні, технічні, договірні побажання до активів в сфері ІБ. А далі, за врахування даних побажань, відзначається цінність ресурсів. Черговий фазис аналізу ризиків - складання переліку значимих небезпек та вразливостей для всіх ресурсів та розрахунок імовірності їх реалізації. Стандарт припускає подвійне тлумачення значення загрози ІБ:

- як умова реалізації вразливості ресурсу;
- потенційна подія, здатна призвести до компрометації ресурсу.

Оцінка ризиків відтворюється шляхом обчислення і зіставлення з заданою шкалою. Обрахунок ризику полягає в множенні ймовірності 32 компрометації ресурсу на значення обсягу збитку, пов'язаного з його компрометацією. BS 7799-3 припускає застосовування кількісних та якісних методів оцінки ризиків. Доповнення до стандарту містить лиш один приклад, котрий символічно можна підпорядкувати до якісного методу оцінки.

Цей приклад використовує 3 і 5-ти бальні оціночні шкали:

- оцінюються типові ціни конкретного ресурсу за п'ятибальною шкалою: «незначний», «низька», «середня », «висока», «дуже висока»;
- оцінюються рівні ймовірності небезпеки за трибальною шкалою: «низька», «середня », «висока»;
- оцінюються однакові імовірності уразливості: «низька», «середня », «висока»;
- за доданою таблицею розраховуються рівні ризику;
- проводиться ранжування подій за рівнем ризику.

Після оцінки ризику, має бути схвалено рішення про його обробку –вибір та реалізацію заходів та способів мінімізації ризику. Окрім оціненого ризику, для прийняття рішення повинні бути враховані затрати на введення та використання механізмів безпеки, політики управління, простоти реалізації, думки експертів, тощо.

Результатом обробки ризику лишається залишковий ризик, щодо котрого вирішуватиметься доля завершення етапу відпрацювання ризику. Нажаль, в стандарті BS 7799-3 нема інформації щодо ефективності заходів, засобів та сервісів, що можуть використовуватись для обробки ризику.

Розділ 7 BS 7799-3 «Безперервна діяльність з управління ризиками» дає відповідь на такі дві етапи менеджменту системи як: контроль ризику та його оптимізація. Задля його контролю рекомендують технічні заходи (виконання перевірок, моніторинг та аналіз системних журналів), аналіз зі сторони управління та незалежні внутрішні аудити ІБ. Етап оптимізації ризику вміщає 33 переоцінки ризику

і, звісно, перегляд політик, коректування і оновлення механізмів підтримки безпеки, керівництва по управлінню ризиками.

Процедури інспектування ризиків і оптимізація включає використання політик, засобів та заходів безпеки, ідентифікування активів, загроз та небезпек, звітність гармонізованість з ISO/IEC 27001 та 27002. Несхожою рисою стандарту являється принцип ерудиції про ходи оцінки, відробітку, інспектування та оптимізації ризиків в компанії. На всіх етапах управління ризиками передбачається інформування всіх учасників процесу керівництва безпекою, а також фіксація подій СУІБ. Стандарт перелічує обов'язки і задає побажання до категорій осіб, які безпосередньо участь при управлінні ризиками, а саме: менеджерам з безпеки, експертам з оцінки ризиків, власникам ресурсів, керівництву компанії та менеджерам ризиків безпеки[10].

Основні види інформаційних ресурсів, що беруть участь при правлінні інформаційними ризиками, відповідно до документа - це служби та процеси інформаційної системи; технічні засоби; людські ресурси; програмне забезпечення; нематеріальні активи як імідж організації, репутація, а також інші нематеріальні цінності, які мають на ведення бізнесу.

Метод оцінки ризиків, наведений у стандарті є універсальним, але не завбачає використання конкретної методики оцінки ризиків. Це зароджує деяку розбіжність у виборі методів керування ризиками.

В основі цього методу оцінки лежать зважені якісні оцінки. Звісно, такий метод містить недоліки, а саме:

- проблему задання масштабу при будові якісних шкал;
- проблеми коректності експертної оцінки;
- неможливості визначити, які саме виміри системи і як впливають на валовий рівень ризику.

Таким чином ускладняється керування ризиками, що говорить про необхідність створення універсальної методики оцінки та керування інформаційними ризиками, яка дозволила б одночасно використовувати аналітичні та якісні методи.

3.3 Аналіз існуючих методів оцінювання та управління ризиками інформаційної системи

Огляд інформаційних джерел показує, що в галузі оцінки та керування інформаційними ризиками на сьогодні здебільшого використовуються експертні методи оцінки. Це зумовлено відсутністю типових статистичних даних щодо реалізації небезпек у інформаційній галузі для систем. Часто приходиться використовувати правдиву статистику разом з експертними оцінками. Зазвичай експертна оцінка - оцінка імовірності спричинення подій та приблизні дані збитку, що відповідають цим подіям. По цим даним і проводять обчислення ризику системи. Таким чином, для керування ризиками оцінка індивідуальної вірогідності - ключовий момент [11].

Застосовування методики експертної оцінки проявляє явні недоліки - суб'єктивність та надто великі похибки для застосовування їх в аналітичних розрахунках.

Потрібно вирізнити теж присутні кількісні методи, що використовуються при оцінках ризику. Вони генерують накопичену статистику та працюють на основі ймовірностей, що були отримані як результат статистичних розрахунків [12]. Недоліком – потреба накопичення доволі великого обсягу статистичних даних задля отримання адекватних прогнозів про рівень ризику [13].

Застосовування названих нормативних актів передбачає часткову зміну IT-інфраструктури компаній, з урахуванням, перебудову системи ІБ як елементу цієї інфраструктури та пертурбацію підходу до її побудови [13], [14].

Дані нормативних актів на формування СУІБ організацій мають опосередкований вплив але підштовхують управління задуматись наскільки дії і засоби, котрі використовуються для захисту інформації, ефективні та адекватні. Любий стандарт робить організацію прозорішою для співпрацюючих з нею контрагентів, бо заявляє, що виміри в цій компанії відповідають нормативам –

перевірені та підтверджені авторитетними джерелами. Це відноситься до методів управління, якості продукції, системи ІБ, тощо.

Висновки

У розділі проведено аналітику нормативного забезпечення у сфері безпеки інформації. Установлено, що вивченням проблем захисту та збереження даних в ІС сьогодні займається величезна кількість як українських, так і іноземних науковців. На світовому ринку розробки та вдосконалення стандартів, технічних звітів, управлінь та рекомендацій у сфері ІБ проводяться безперестанку; цілеспрямовано публікуються проекти та версії стандартів, присвячених різним аспектам ІБ на тих чи інших стадіях узгодження та затвердження.

Вказані міжнародні компанії та консорціуми, що займаються розробленням нормативних документів з ІБ, присвячених управлінню інцидентами (CERT, ISO, IEC, IETF, ITU-T, IEEE, OMG, SANS Institute, X/Open).

Проведено аналітику популярних стандартів у сфері керування ІБС, а точніше, розглянуто особливості використання та призначення наступних стандартів серії ISO/IEC 27000, Стандарт BS 7799-3.

Проведено аналітику наявних методів оцінки та керування ризиками ІС.

Варто зауважити, що використання означених у розділі нормативних документів призведе, до потреби модернізації ІТ-інфраструктури компанії, а також перебудови системи ІБ на основі змінених підходів як вагомого компоненту цієї інфраструктури.

4. РОЗРОБКА КОМПЛЕКСНОЇ МЕТОДИКИ

Проблемам захисту веб-додатків присвячене величезне коло досліджень. Наприклад, книги, [15, 16], які описують методи та інструменти атак, а також захист від них. Якщо в [15] констатується можливість забезпечення захисту від будь-яких атак на веб-додатки, то в [16] розглянуто конкретні методи захисту. Така різниця в подачі матеріалу досить симптоматична та є результатом того, що методи та інструменти атак важко піддаються класифікації, а сама атака часто використовує технології маскування цих методів та інструментів.

Вирішенню задачі визначення DDoS-атак на основі розробки спеціальної метрики присвячена стаття [18]. В роботі [19] проаналізовано існуючі методи захисту від DDoS-атак та запропоновано новий метод, який базується на статистичному аналізі вхідного трафіка на сервері та надійній системі перевірки гіпотез.

В матеріалі [17] описується метод визначення атак типу «відмова в обслуговуванні», що базується на застосуванні багатошарового персептрону та дозволяє отримати необхідну множину показників.

Виділяють також комбіновані методи захисту WEB-додатків, засновані на використанні евристичного підходу [20], в межах якого виділяється аномальна поведінка споживача, що підвищує ймовірність захисту порівняно із сигнатурним аналізом.

Нині в перспективі також є використання моделей агента загроз для захисту веб-додатків від атак [21, 22], що допомагає формалізувати пошук вразливостей в інформаційних системах на всіх етапах взаємодії агента загроз із веб-додатком.

Проблеми витоку інформації розглянуто в матеріалах [23, 24], де проаналізовано типові сценарії, методи та способи захисту від них.

В [15] стверджується, що злам паролю залежить від існуючих обчислювальних ресурсів, часу та функцій, котрі використовуються для зберігання паролю, а також від

безлічі інших характеристик. Пропонуються загальні поняття оцінки складності та надійності пароля.

Згідно статистичних результатів та запропонованих методів, які орієнтовані на захист від конкретного типу атаки, негативна дія на WEB-додаток відбувається, як правило, із використанням одразу декількох типів атак. Тому задачею системи інформаційної безпеки є розробка ефективної методики протидії атакам зловмисників за умови, що вони використовують комбіновані типи атак. Рівень ефективності в такому випадку визначається замовником WEB-додатку і задається специфікою ведення бізнесу підприємством (або діяльністю організації), параметрами, що характеризують специфіку інформації та баз даних, що належать до конфіденційних і рядом інших параметрів та характеристик. Розробка подібної стратегії захисту WEB-додатку є нетривіальною задачею.

4.1 Використання Firewall та IPS систем в якості базової системи захисту

Щоб покращити роботу системи безпеки веб-ресурсів потрібно створити захист від атаки низького рівня. Щоб втілити цю ідею можемо скористатись системами Firewall та IPS. Firewall формує доступність портів та надає мінімальний захист. IPS відстежуватиме атаку низького рівня і відреагує на трансформації потоків трафіку.

Система протидії вторгнень (Intrusion Prevention System) – це система, що дає змогу розпізнати признаки вторгнення в систему, виявляє і запобігає атаки. В ході аналізу система використовує різноманітні методи вияву атак – поведінковий, сигнатурний та ідентифікацію відхилень в протоколах [17] .

Всі види IPS-технологій стандартно здійснюють такі функції:

- IPS припиняють вплив атаки;
- блокують зловмисний фрагмент, а неураженій частині дозволяють проникнути в систему;

- повідомляють адміністраторів безпеки в разі спостереження в системі важливих подій;
- реагують на події, перероблюючи осередок безпеки для зірвання атаки;
- формують звіти.

Основні положення IPS та види подій, що найчастіше виявляються:

- розвідка та атака прикладного рівню типу переповнення буферу, підбір паролю або передача шкідливих програм. Більшість мережевих IPS аналізують протоколи додатків;
- розвідка і атака транспортного рівня типу сканування портів, , SYN-floods та непростої фрагментації пакетів. Найчастіше аналізуються протоколи транспортного рівня – UDP та TCP;
- розвідка та атака мережевого рівня у вигляді підміни IP-адреси та ненормальних значень заголовку IP;
- несподіваний запуск додатків, наприклад, хости можуть виконувати несхвалені дії;
- недотримання політики - несе за собою використання заборонених протоколів.

Міжмережевий екран (Firewall) – система мережевої безпеки, що стежить та проводить контроль за вхідними та вихідними трафіками на основі завчасно визначених норм безпеки. Міжмережевий екран, зазвичай, встановлює бар'єр між захищеною внутрішньою мережею і зовнішньою незахищеною мережею. Основною його метою є захист внутрішньої мережі або окремих її вузлів від несанкціонованого доступу. Firewall контролює доступ до мережевих ресурсів з підмогою позитивної моделі керування (до внутрішньої мережі попадає лише санкціонований трафік, а весь інший -заборонений).

Firewall ділиться на 2 категорії:

- Firewall мережевого рівня - дозволяє або забороняє трафік, опираючись на адреси джерел IP-адрес або портів;

– Firewall прикладного рівня – займається аналізом протоколів прикладного рівня, одночасно спостерігаючи за активністю протоколу у відношенні до конкретного профілю та дозволяють або забороняють трафік, опираючись на відхилення від профілю.

Типові функції Firewall:

– контроль доступу до вузлів в мережі;
– фільтрація доступу до незахищених служб;
– контроль порядку доступу до мережі;
– запобігання спроба доступу з зовнішньої та внутрішньої мережі;
– перешкоджання отриманню конфіденційної інформації з внутрішньої захищеної мережі. Таблиця 4.1 зображує як саме в моделі OSI працюють всі систем.

Таблиця 4.1 – Робота систем комплексу на моделі OSI

Рівень моделі OSI	**Firewall**	**Intrusion Prevention System**	**WEB Application Firewall**
2	+		
3	+	+	
4	+	+	
5		+	+
6		+	+
7			+

Отже, комплексно, системи захищатимуть WEB-ресурси на всіх рівнях моделі OSI.

Застосовування комплексної системи захисту WEB-ресурсів у Firewall, IPS чи WAF забезпечує на 30% кращу ефективність, аніж застосування простого WAF. Застосовування новітніх високопродуктивних IPS та Firewall дозволяє блокувати

доступ шкідливим файлам у домашню мережу та забезпечити додаткову безпеку від ризиків спрямованих атак на ІТ-ресурси. Даний комплекс дасть змогу підвищити захищеність любого інтернет-ресурсу та зменшити загрузку адміністраторів ІТ-систем, а також забезпечити ефективнішу обробку справжніх користувачів інтернет-ресурсів.

4.2 Посилення рівня захищеності WEB-додатку за допомогою евристично-аналітичного підходу

Далі піде мова про удосконалений метод захисту WEB-додатку, який відмінний від аналогічних одночасним здійсненням системного, статистичного та евристичного аналізу вразливостей ресурсу, що дасть виконати якісний вияв та захист від зловмисників, котрі використовують кілька типів атак. Метод захисту можна подати у такій формі (структура методу схематично подана на рис. 4.1).

Крок 1. Створюється множина N характеристик WEB-додатку, яка містить в собі бази даних та знань, які необхідно захистити, а ще характеристики, котрі описують існуючі системи захисту. Це можуть бути інтегровані в хмарні сховища, ліцензійні програми, що використовуються тощо. Також до такої множини відносяться характеристики, котрі визначають своєрідні методи та технології взаємодій з користувачами WEB-додатків.

Крок 2. Множина N характеристик перейде до систем менеджменту ІБ WEB-додатку, що виконує аналітику наявних вразливостей та обробляє ряд заходів захисту WEB-додатку. Функції, що описується на етапах 3-5, виконуються в одночасному режимі з достатньою кількістю ресурсів або у покроковому режимі, якщо ресурсів надто мало.

Крок 3. Виконується системна аналітика вразливостей WEB-додатку до атак. Задачею такого аналізу буде пошук множини T цілей задля атак та множини цілей TP задля захисту WEB-додатку; аналіз обмеження програмного, технічного та

інформаційного характеру; аналітика альтернатив; відбір ефективних критеріїв С захисту WEB-додатку; розроблення характеристик для впровадження; синтез моделі для системи захисту.

Крок 4. Виконується евристична аналітика вразливостей ресурсу. Тут можуть бути вжиті нейронні класифікатори [20], онтології [28], експертні методи [29], тощо. Цей крок необхідний, адже робота WEB-додатку з користувачами не достатньо формалізована, отже до неї частіше всього нереально знайти правильні моделі чи методи достеменного опису. Також на цьому етапі виконується аналітика поведінки зловмисників та прогноз різних атак, котрі вони можуть застосовувати. Необхідно завбачати, що процентний розподіл використаних аферистами атак постійно змінюється, а реалізація статистично достовірного прогнозування таких змін [23], поки-що, нездійсниме.

Крок 5. Виконується аналітика збору статистичних даних, для поточного стану вразливостей WEB-додатку з використанням наявних баз даних, що носять загальну характеристику [26]. Загалом виділяють декілька найуживаніших видів кібератак на веб-додаток, при яких використовуються методи протидії, котрі можна використати до декількох видів атак. До прикладу, в таблиці видно, для атак «Cross-site request forgery» та «URL redirector abuse» методи протидії ґрунтуються на вхідних даних.

Крок 6. В результаті здійснення аналізу у етапах 3-5 система менеджменту ІБ утворює задля веб-додатку сукупність заходів (погоджених поміж собою методів та інструментів) для захищеності необхідного ресурсу.

Крок 7. Відтворюється автентифікація пропонованої системи захисту веб-додатку від атак. Для заданої дії може бути використана уже наявне та розроблене тестове ПЗ, задіяні фахівці з кібербезпеки тощо. У разі вияву неналежного захисту WEB-додатку, що виражатиметься в невідповідній характеристиці захисту множинних критеріїв С, розроблених на етапі 2, фази 1-6 повторюються.

Крок 8. Коли досягнутий заданий рівень захисту, система даного WEB-додатку зафіксується та впровадиться.

При потребі, цей метод повторюється циклічно.

Рисунок 4.1 – Метод формування системи захисту WEB-додатку

4.3 Використання системи аналізу DPI

В якості системи аналізу WEB-додатку можна скористатись DPI (DEEP PACKET INSPECTION).

DPI - найефективніша система аналізу інтернет-трафіку, що дозволяє на максимальних рівнях моделі OSI орудувати даними для захисту систем, рис. 4.2.

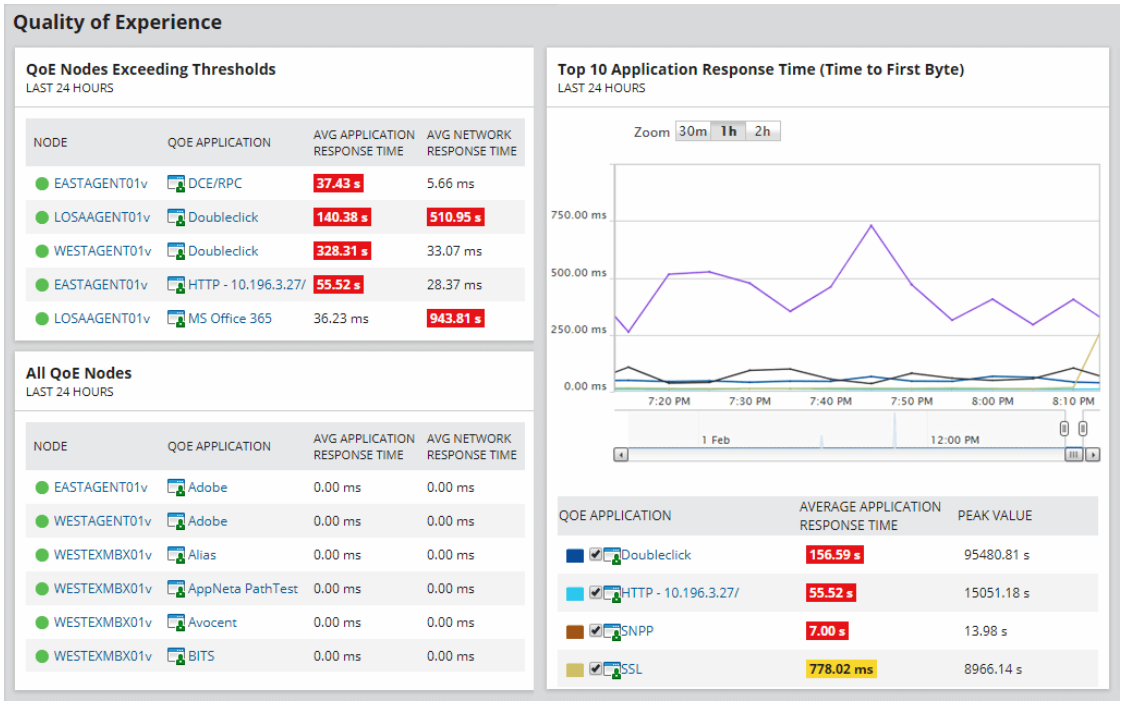

Рисунок 4.2 – Графічний інтерфес системи аналізу DPI

Необхідно не лише відзначати події але й притягати порушників до відповідальності. Персональні дані, що залишаються під час роботи з веб-сервісами представлені у вигляді таблиці 4.2.

Таблиця 4.2 – Ідентифікаційна іформація користувача

Ідентифікатор	**Зміст ідентифікуючих даних**	**Способи анонімізації**
IP-адреса	Як мінімум інформація про провайдера та країну користувача	VPN, Proxy, SSH, Tor, I2P, P2P- анонімайзери

Продовження таблиці 4.2 – Ідентифікаційна інформація користувача

DNS leaks	Витоки інформації від служби доменних імен; протоколювання активності клієнта виникає, якщо програмне забезпечення відправляє DNS-запити через DNS-сервер провайдера	Використання анонімних мереж; під час роботи через VPN використання примусово статичних DNS-серверів, що належать VPN-провайдеру
MAC-адреса	При підключені до публічної WiFi точки доступу фіксується MAC-адрес мережного інтерфейсу користувача	Зміна MAC-адреси до сеансу підключення
«Профілювання»	Співставлення великого обсягу трафіку, який виходить через один вузол, із конкретним користувачем	Відмова від використання постійних схем (ланцюгів) Tor, регулярна зміна вихідних вузлів
Соціальна активність в анонімному сеансі	Розкриття особи користувача під час відвідування ним власного профілю соціальної мережі, незважаючи на засоби анонімності	Недопущення неузгодженої активності в анонімному сеансі

Звичайний браузер містить такі функціональні компоненти і технологічні категорії:

– Cookies – текстові документи з певними даними, які зберігаються прикладними програмами для різних задач типу автентифікації. Розкриття анонімності користувача наступає, коли він спершу побував на ресурсі через відкритий сеанс, оглядач зберіг Cookies, а потім клієнт під’єднався

через анонімний хост. У висновку серверу доступні співставлення Cookies і, зрештою, наступає деанонімізація користувача;

- Flash, Java. На цих технологіях ґрунтуються плагіни, що грузяться від імені клієнта як окреме ПЗ та може функціонувати оминаючи проксі, зберігати свої Cookies та інакші налаштування;
- відбиток (fingerprint) оглядача. Браузер презентує серверу десятки категорій даних, а це дає змогу створити особливий цифровий відбиток оглядача, по якому його можливо впізнати серед сотні інакших навіть у анонімному сеансі (частіше всього використовується для проведення цільової реклами);
- скрипти JavaScript – код, що генерується зі сторони користувача та здатен нагромаджувати для сервера персональну інформацію і навіть при вразливості цільового для клієнта ресурсу, продукує умови для відтворення вдалих атак на інформаційний ресурс;
- http-referrer. З використанням цього http-заголовку необхідний користувачу веб-сайт може встановити, ким саме було сформовано трафік.

Рішенням такої проблеми буде налагодження параметрів безпеки браузера, включаючи блокування всіх наведених категорій автентифікації, та відказ під час анонімного сеансу від неперевіреного сайту.

Система (DPI), IX , Complete packet inspection та Information eXtraction — техніка для нагромадження статистичних даних, фільтрації та перевірки мережевих пакетів за їх вмістом. На відміну від брандмауерів, що аналізують лише заголовки пакетів, Deep Packet Inspection проводить аналітику повного вмісту трафіку на рівнях моделі OSI з другої фази і далі. Deep Packet Inspection вміє знаходити та блокувати віруси, відфільтровувати дані, що не задовольняють задані критерії, здійснює ґрунтовний аналіз всіх пакетів, що її проходять. Система DPI виконує поведінковий синтез трафіку, котрий дає впізнавати додатки, що не беруть для обміну даними завчасно відомі заголовки і будову даних.

З використанням DPI спеціальні служби ведуть при необхідності спостереження за активністю на сайті того або іншого користувача та аналізувати VPN і HTTPS трафік. DPI може збирати різноманітну інформацію, не порушуючи персональні права користувача DPI може захистити від:

- спам-ботів (виявляються на основі аналізу SMTP трафіку);
- DoS і DdoS-атак (виявляються за аномаліми трафіку);
- зараження вірусами (виявляється за сигнатурами).

Захист від спаму виконується через блок відправника, коли з одної адреси надходить надмірно велика кількість SMTP -запитів.

DPI дає змогу захиститися від TCP SYN Flood і Fragmented UDP Flood.

Атака SYN flood визве високу витрату ресурсів системи, так як на кожен включений SYN-пакет система повинна забронювати деякі ресурси в пам’яті або відтворити багато пакетів, що призводе до її відмови.

DPI завбачає перевищення порогу SYN-запитів, та замість WEB-додатку дає на них відповідь.

Fragmented UDP Flood – цю атаку здійснює фрагментований udp-пакет, здебільшого малого розміру, на обробку і аналіз яких втрачається немало ресурсів.

DPI відкидає непотрібні для сайту протоколи чи лімітує їх по смузі пропускання (для веб-сайту залишаються лиш протоколи HTTP і HTTPS).

В межах цієї роботи опишемо DPI у вигляді стадій роботи з пакетами, показаними на (рис. 4.3): прийом мережевою картою і фільтрація пакетів, вилучення даних пакету (0,3% часу роботи процесора) і завантаження сигнатур з БД (7,6% часу роботи процесора), виділення потоків трафіку, обробка даних алгоритмами (8,7% часу роботи процесора) і порівняння з сигнатурами (83% часу роботи процесора).

Комбінатор рішень надає алгоритмам первинні дані та вибирає найдостовірніше. Далі здійснюється пропорція пакету з певним потоком трафіку. У [27] було проведено оцінку відсоткової пропорції потрібного часу роботи процесора

задля успішного виконання цих етапів, яка продемонструвала, що 83% займає етап зіставлення даних пакету з сигнатурами.

Коли на етапі виділення потоків пакет належить до існуючого потоку даних, то він також передається на апаратний фільтр.

Здебільшого на етапі аналізів даних пакету алгоритмами обробки спершу відтворюється аналіз 2-4-го рівнів і заголовків тунелів, а далі здійснюється зіставлення інформації 5-7-го рівнів з базою сигнатур додатків (що включає >1000 прикладів).

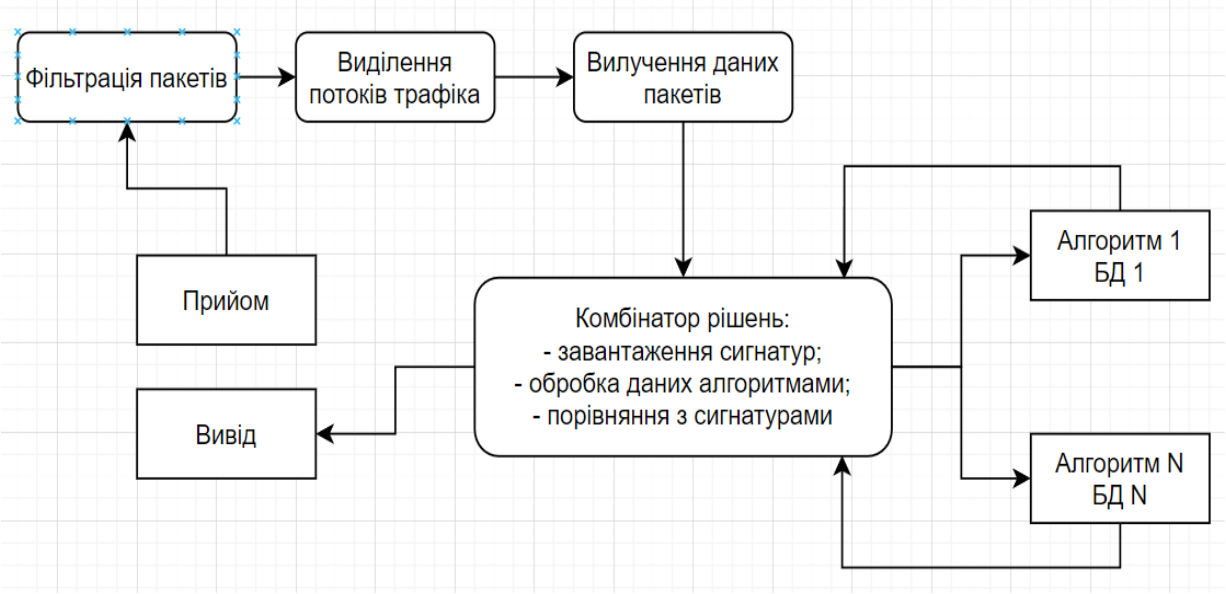

Рисунок 4.3 – Аналіз пакетів DPI з використанням комбінатора рішень

Для нового виявленого потоку назначена політика виконується на апаратному очиснику, в якому (в режимі розвантаження) не ведеться аналіз 5-7-го рівнів, проте виконується підрахунок трафіку для заданого застосовування [18].

Крім розпорядку аналізу пакетів, що прибувають в даний момент, DPI-системи здатні функціонувати в режимі навчання, в якому проаналізуються приклади неоднорідних помічених потоків трафіку. Режим навчання включає такі стадії:

захоплення пакетів, зчитування міток істинних значень потоків трафіку, отримання сигнатур та збереження в базу даних (БД).

Системі DPI вагомо організувати заданий період обробки пакетів і її стабільність. Складною виступає підтримка стабільності ймовірно тимчасових рекомендацій при умовах роботи на максимальній продуктивності.

Часто аналіз і вилучення потрібних даних вимагають величезних обчислювальних ресурсів. Чим вищі вони, тим менше триватиме обробка пакетів, а отже, меншим буде формат затримки проходу нового потоку даних крізь систему DPI. Робота апаратного очисника також додає певну затримку при проходженні пакетів. Коли навантаження на систему DPI почне перевищувати ліміт, то збільшиться затримка, втрата пакетів і, в крайньому випадку, призведе до пропуску трафіку без його аналізу.

4.4 Математичне обгрунтування

Для того щоб оцінити доцільність використання DPI як технології QoS, необхідно розробити математичну модель. Для побудови простої математичної моделі системи масового обслуговування (СМК) необхідно знову спростити етап обробки потоку системи DPI. Припустимо, що сервер аналізу трафіку використовує лише перший пакет потоку від апаратного фільтра, а отже знаходить необхідну стратегію та передає її апаратному фільтру. Припустимо, що середня затримка пакету протягом періоду аналізу дорівнює T1. Однак за особливих обставин сервер аналізу трафіку надішле запит на необхідну політику на сервер затвердження політики. У цьому випадку середня затримка (T2) буде сумою затримок черги та обробки на сервері прийняття рішень і сервері аналізу трафіку.

Позначимо багатопроцесорний сервер аналізу трафіку з чотирма процесорами як першу систему черги (СМО1). Відповідно до класифікації Кендалла, система характеристики M/M/V має застосування з вхідними потоками Пуассона,

експоненційним розподілом часу обслуговування та V-процесорами. Припущення, що загальний вхідний потік сервера аналізу трафіку є Пуассоновським, ґрунтується на його великій кількості незалежних постійних потоків. СМО2 — це розробник стратегії одного сервера (M/M/1). Відповідно, використовуючи теорему Берка, можна зробити висновок, що трафік, що надходить до сервера прийняття рішень, також є Пуассоновим, але, відмінний від початкового трафіку, існує випадок ймовірності звернення до сервера. Отже, інтенсивність простого потоку, що надходить, виражається як λ.

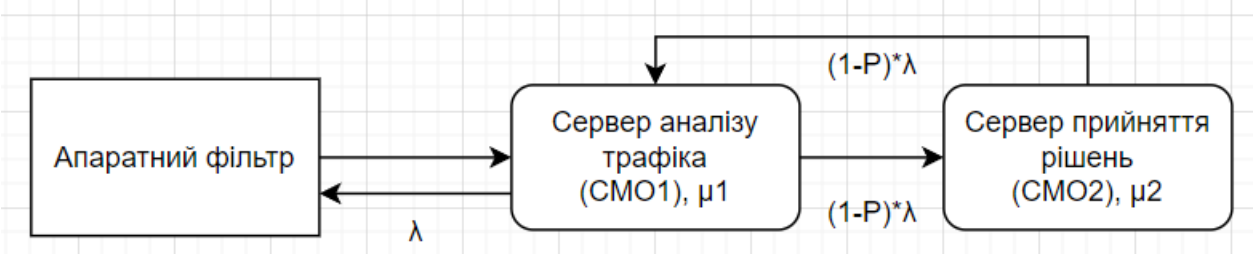

Рисунок 4.4 – Спрощена аналітична модель системи DPI

Згідно теореми Берке, що виходить із СМО2 (яка працює в стаціонарному режимі) потік буде простим з тим же параметром λ . Інтенсивність вхідного потоку на СМО2 буде рівною:

$$\lambda_{вх2} = (1 - P)\lambda \ , \tag{4.1}$$

де P – це ймовірність самостійної класифікації новоствореного потоку сервером аналізу трафіку (СМО1). Відповідно і для СМО2. Необхідно розуміти, що вимоги, що надійшли після опрацювання із СМО2, також потраплятимуть в чергу СМО1. Отже, інтенсивність вхідного потоку на СМО1 після обробки СМО2 буде рівною:

$$\lambda_{вх12} = (1 - P)\lambda \tag{4.2}$$

Загальна інтенсивність надходження пакетів на сервер в результаті аналізу трафіку (СМО1) визначається наступним виразом:

$$\lambda_{вх1} = \lambda + (1 - P)\lambda \tag{4.3}$$

Продуктивність СМО1 визначається наступним чином:

$$P_1 = \frac{\lambda + (1 - P)\lambda}{\mu 1} \ , \tag{4.4}$$

де p_1 – інтенсивність обслуговування пакетів. Ймовірність з якою система вільна (P_0), може бути отримана за формулою:

$$P_0 = \frac{1}{\frac{p_1^{n+1}}{n!\,(n - p_1)} + \sum_{n=0}^{n} \frac{{p_1}^n}{n!}} \ , \tag{4.5}$$

де n=4 – число опрацьовувачів.

Середню затримку сервера аналізу трафіку (Т1) можна підрахувати покладаючись на кількість заявок в системі (N1), залежного від середньої кількості заявок в черзі (NS):

$$NS = \frac{p_1^{n+1} p_0}{nn!\left(1 - \frac{p_1}{n}\right)^2} \tag{4.6}$$

$$N_1 = NS + p_1 \tag{4.7}$$

$$T_1 = \frac{N^1}{\lambda + (1 - P)\lambda} \tag{4.8}$$

Отже, знаючи інтенсивність з якою пакети надходять на сервер ухвалення рішень (СМО2) – λвх 2, можна охарактеризувати наступні властивості для СМО2: продуктивність (2 р) середня кількість заявок в системі (N2), середню затримку сервера ухвалення рішень (Т2), що розраховуються за формулами:

$$p_2 = \frac{(1-P)\lambda}{\mu_2} \tag{4.9}$$

$$N_2 = \frac{p_2}{1-p_2} \tag{4.10}$$

$$T_2 = \frac{N_2}{(1-P)\lambda} = \frac{1}{\mu_2\,(1-\,p_2)} \tag{4.11}$$

Загальний час, який необхідний системі DPI на опрацювання потоку і політики (Т), становить:

$$T = T_1 + P(T_1 + T_2) \tag{4.12}$$

На підставі наведених формул розрахована залежність затримки в подібній системі від інтенсивності навантаження (рис. 4.3), при обраній ймовірності звернення до сервера ухвалення рішень Р = 0,8 та інтенсивністю обслуговування заявок μ1 = 5000, μ2 = 1000 на СМО1 і 2 відповідно.

Результатом розрахунків на основі зразкової математичної моделі роботи системи DPI можна вважати те, що при збільшенні інтенсивності вхідних потоків зростає й загальний час визначення політики для кожного потоку пакетів. Отримана середня затримка системи DPI (1,2 мс без пікового завантаження, 22,8 мс з піковим завантаженням) допомагає застосовувати технологію DPI до чутливого до затримок

трафіку, згідно з вимог рекомендації Y.1541 Міжнародного союзу електрозв'язку (ITU − T) від 0,1 до 1 с.

Однак, при піковому завантаженні система показала затримку, рівну 260 мс. Беручи до уваги те, що затримка передачі пакету в мережі складається з часу на проходження відстані, часу на опрацювання пакетів маршрутизаторами, комутаторами і двох систем DPI (у мережі оператора, який надає трафік та в мережі іншого оператора, який цей трафік приймає). Певна річ, що для системи DPI затримки при обробці пакетів мають бути мінімальними, однак, не варто вважати ці результати кінцевими, так як в цій математичній моделі було зроблено чималу кількість допущень.

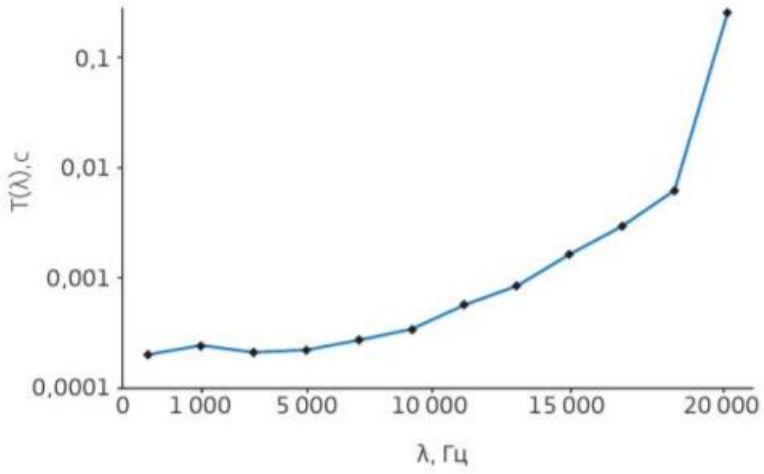

Рисунок 4.5 – Залежність затримки в системі DPI від λ

Висновки

В розділі описано комплексну методику виявлення вразливостей WEB-додатків із використанням методів евристичного аналізу та технології DPI, що дозволяє найвищому рівню моделі OSI використовувати дані для захисту системи. На відміну від брандмауерів, глибоке пакетне тестування не тільки аналізує заголовки, але й

аналізує весь вміст трафіку на другому та вищих рівнях моделі OSI. Глибоке сканування пакетів може виявляти та запобігати вірусам, відфільтровувати невідповідну інформацію та виконувати поглиблений аналіз 72 переданих пакетів. Система DPI виконує так званий поведінковий аналіз трафіку, який дозволяє визначити програми, які можуть спілкуватися без використання раніше відомих заголовків і структур даних.

Завдяки DPI спеціальні служби можуть відстежувати мережеву активність користувачів і аналізувати трафік VPN і HTTPS. Система DPI може збирати будь-яку інформацію, не порушуючи особистих прав користувача.

Поєднання цієї комплексної системи захисту з IPS і WAF може забезпечити на 30% вищу ефективність, ніж використання традиційної WAF. Використання сучасних високопродуктивних брандмауерів та IPS дозволить запобігти потраплянню шкідливих файлів у внутрішню мережу безпеки, забезпечить додатковий захист та знизить ризик цілеспрямованих атак на WEB-додатки. Ця інтеграція покращить безпеку, зменшить навантаження на адміністраторів IT-системи та забезпечить більш ефективну обробку ресурсів для авторизованих користувачів.

ВИСНОВКИ

В результаті виконання магістерської роботи було удосконалено існуючі процеси виявлення вразливостей WEB-додатків з використанням евристичних методів та системного аналізу.

При виконанні роботи було виконано наступні задачі.

1. Проаналізовано діючі міжнародні стандарти та рекомендовані практики у галузі управління інцидентами інформаційної безпеки. Встановлено, що застосування означених в розділі нормативних актів приводить, до необхідності модернізації IT-інфраструктури організації і, в тому числі, перебудови системи ІБ як частини цієї інфраструктури, а також зміну підходу до її побудови.

2. Досліджено сучасні проблеми захисту WEB-додатків та встановлено, що проблемами збереження та захисту даних в інформаційних системах на даний час займається велика кількість українських та іноземних дослідників. У світі розробки стандартів, технічних звітів, керівництв та рекомендацій в галузі інформаційної безпеки (ІБ) проводиться безперервно; послідовно публікуються проекти і версії стандартів, присвячених тим чи іншим аспектам ІБ на різних стадіях узгодження і затвердження.

3. Проаналізовано існуючі WEB-вразливості, методи та засоби захисту WEB-додатків та встановлено, що найкращим методом захисту від атак на мережеві служби, наприклад, DoS та DDoS є використання хмарних технологій і перевірених конфігурацій серверів. Для захисту від WEB-атак класичним пристроєм є Web Application Firewall, який застосовує набір правил захисту до протоколів високого (прикладного) рівня HTTP/HTTPS, FTP/FTPS. Класичне розміщення WAF в мережі – в режимі зворотного проксі сервера перед захищеними WEB-серверами. Але цього не достатньо, тому в роботі пропонується комплексне рішення, яке включає WAF, IPS та FIREWALL, тобто захист на всіх рівнях моделі OSI.

4. Розроблено методику виявлення вразливостей WEB-додатків, яка в комплексі використовує евристично-аналітичні методи виявлення загроз покладаючись на систему аналізу пакетів DPI на найвищих рівнях OSI та Firewall разом з IPS для забезпечення базового захисту. DPI виконує так званий поведінковий аналіз трафіку, який дозволяє визначити програми, які можуть спілкуватися без використання раніше відомих заголовків і структур даних. Система захисту з IPS і WAF може забезпечити на 30% вищу ефективність, у порівнянні з використанням традиційної WAF. Використання сучасних високопродуктивних брандмауерів та IPS дозволяє запобігати потраплянню шкідливих файлів у внутрішню мережу безпеки, забезпечує додатковий захист та знижує ризик цілеспрямованих атак на WEB-додатки. Подібна інтеграція покращує безпеку, зменшує навантаження на адміністраторів IT-системи та забезпечує більш ефективну обробку ресурсів для авторизованих користувачів.

ПЕРЕЛІК ПОСИЛАНЬ

1. OWASP Top Ten. [Електрон. ресурс]: – Режим доступу: https://owasp.org/www-project-top-ten/ — Топ 10 загроз.

2. ISO/IEC 17799:2005. Information technology. Security techniques. Code of practice for information security management.

3. ISO/IEC 27001:2005. Information technology. Security techniques. Information security management systems. Requirements.

4. ISO/IEC TR 27035:2011. Information technology − Security techniques − Information security incident management.

5. ISO/IEC 20000:2011. Information technology. Service management. Part 2: Code of practice.

6. Defining Incident Management Processes for CSIRTs: A Work in Progress // CMU/SEI-2004-TR-015: ESC-TR-2004-015 Chris Alberts, Audrey Dorofee, Georgia Killcrece October 2004 Networked Systems Survivability Program.

7. Северинов А.В. Анализ угроз и рисков безопасности информации в беспроводных сетях / А.В. Северинов,В.И. Черныш //Системи управління, навігації та зв'язку. – К.: ЦНДІ НіУ, 2011. – Вип. 1(17). – С. 229-232.

8. ГОСТ Р ИСО/МЭК 17799-2005.

9. ГОСТ Р ИСО/МЭК 27001.

10. Марков А. Нормативный вакуум информационной безопасности / А. Марков, В. Цирлов // Открытые системы. – 2007. – №8.

11. Петренко С.А. Управление информационными рисками: Экономически оправданная безопасность / С.А. Петренко, С.В. Симонов. – М.: АйТиПресс, 2004. – 381 с.

12. Федотов Н.С. Оценка и нейтрализация рисков в информационных системах: метод. пос. / Н.С. Федотов, В.С. Алешин. – М.: МГТУ им. Н.Э.Баумана, 2004. – 52 с.

13. Замула О.А. Аналіз міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки / О.А. Замула, В.І. Черниш // Системи обробки інформації: зб. наук. пр. – Х.: ХУПС, 2011. – Вип. 2 (92). – С.53-56. 77.

14. Попелова И.Г. Применение и развитие современных информационных технологий в системе машиноиспытаний [Текст] /Научно-информационное обеспечение инновационного развития АПК: материалы VII Междунар. науч.-практ. конф. – М.: ФГБНУ «Росинформагротех», 2014.

15. Скембрейц Дж. — готовые решения / Дж. Скембрейц, М. Шема. — М.: Издательский дом «Вильямс», 2003. – 334 с.

16. Жуков Ю.В. Основы веб-хакинга: нападение и защита / Ю.В. Жуков. – СПб.: Питер, 2011. — 176с.

17. Сорокин С.Н. Метод обнаружения атак типа «отказ в обслуживании» на WEB-приложения / С.Н. Сорокин // Прикладная дискретная математика. — 2014. — №1 (23). — С. 55-64.

18. Фаткиева Р.Р. Разработка метрик для обнаружения атак на основе анализа сетевого трафика / Р.Р. Фаткиева // Вестник Бурятского государственного университета. — 2013. — Vol. 9. — С. 81-86.

19. Sen J. A Robust Mechanism for Defending Distributed Denial OF Service Attacks on Web Servers / J. Sen // International Journal of Network Security & Its Applications (IJNSA). — 2011, March. — Vol. 3, N 2. — P. 162–179.

20. Поворознюк А.И. Совершенствование защиты WEB-приложений от вторжений на основе звристического похода / А.И. Поворознюк, М.Н. Шкарупа: сб. науч. тр. «Вестник НТУ «ХПИ». Інформатика і моделювання. — 2007. — Вип. 19. — С. 145-154.

21. Аласенко А.В. Разработка и системный анализ математической модели угроз, модели нарушителя, процедур защиты WEB-приложений на всех этапах функционирования / А.В. Аласенко, П.И. Дзьобан // Научный журнал КубГАУ. — 2014. — № 101(07) — С. 1-11.

22. Bhavani A.B. Cross-site Scripting Attacks on Android WebView / A.B. Bhavani // International Journal of Computer Science and Network. — 2013. — Vol. 2, Issue 2. — 5 і. — Режим доступу: http://ijcsn.org/IJCSN-2013/2-2/IJCSN-2013-2-2-03.pdf.

23. Cuff P. Distributed channel synthesis / P. Cuff // IEEE. Trans. Inf. Theory. — 2013. — Vol. 59(11). — P. 7071 — 7096.

24. Schieler C. Rate-distortion theory forsecrecy systems / C. Schieler, P. Cuff // IEEE Trans. on Inf. Theory. — 2014. — Vol. 66(12). — Ц.7584–7605.

25. Sahin C.S. General Framework for Evaluating Password Complexity and Strength / C.S. Sahin, R. Lychev, N. Wagner. — 11 і. К. ГусПеу, М. Марпег. — 11 р. — Режим доступу: http://arxiv.org/abs/1512.05814.

26. Website Security Statistics Report: 2018. — WhiteHat Security, 2018. — 30 p. — Режим доступу: https://info.whitehatsec.com/Website-Stats-Report-2018.html.

27. Website Security Statistics Report: 2015. — WhiteHat Security, 2015. — 30 p. — Режим доступу в Інтернет: https://info.whitehatsec.com/Website-Stats-Report-2015.html.

28. Handbook on Ontologies / eds. S. Staab and R. Studer. — International Handbooks on Information Systems. — Berlin: Springer, 2009. — 832 p.

29. Новиков Д.А. Теория управления организационными системами / Д.А. Новиков. — М.: Физматлит, 2007. — 584 с.

ДОДАТОК А

Презентація

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра інженерії програмного забезпечення

МАГІСТЕРСЬКА РОБОТА
«РОЗРОБКА КОМПЛЕКСНОЇ МЕТОДИКИ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ WEB-ДОДАТКІВ»

Виконав: студент групи ПДМ – 61, Вітусевич Євгеній Сергійович

Керівник: , к.т.н., доц. кафедри ІПЗ, Негоденко Олена Василівна

Київ - 2022

МЕТА, ОБ'ЄКТ ТА ПРЕДМЕТ ДОСЛІДЖЕННЯ 2

Мета роботи: удосконалення існуючих процесів виявлення вразливостей WEB-додатків з використанням евристичних методів та системного аналізу.

Об'єкт дослідження: методи та засоби захисту WEB-додатків від зловмисників.

Предмет дослідження: методика виявлення вразливостей WEB-додатків з використанням евристичних методів та системного аналізу.

АКТУАЛЬНІСТЬ РОБОТИ

Недоліки існуючих процесів :

- процес виявлення вразливостей не оптимальний
- вузьконаправленність рішень;
- відсутність комплексного рішення для проведень розрахунків
- застарілі методи виявлення вразливостей

Показники для оцінки ефективності комплексного рішення :

- висока пропускна здатність виявлення вразливостей
- час витрачений на виявлення вразливостей
- кількість вразливостей, що виявляються;
- обсяг програмного коду.

ЕВРИСТИЧНО-АНАЛІТИЧНИЙ МЕТОД ВИЯВЛЕННЯ ЗАГРОЗ

Крок 1 : Створюється множина N характеристик WEB -додатку .

Крок 2 : Множина N характеристик перейде до систем менеджменту ІБ.

Крок 3 : Виконується системна аналітика вразливостей .

Крок 4 : Виконується евристична аналітика вразливостей .

Крок 5 : Виконується аналітика збору статистичних даних .

Крок 6 : система менеджменту ІБ утворює для WEB -додатку сукупність заходів захисту .

Крок 7 : Відтворюється автентифікація пропонованої системи захисту .

Крок 8 : Система фіксується та впроваджується.

Рисунок 4.1 - Метод формування системи захисту WEB-додатку

СИСТЕМА АНАЛІЗУDPI

В якості системи аналізу WEB-додатку можна скористатись

DPI (DEEP PACKET INSPECTION) .

DPI - найефективніша система аналізу інтернет- трафіку, що дозволяє на максимальних рівнях моделі OSI (абстрактна мережева модель для комунікацій і розробки мережевих протоколів) орудувати даними для захисту систем.

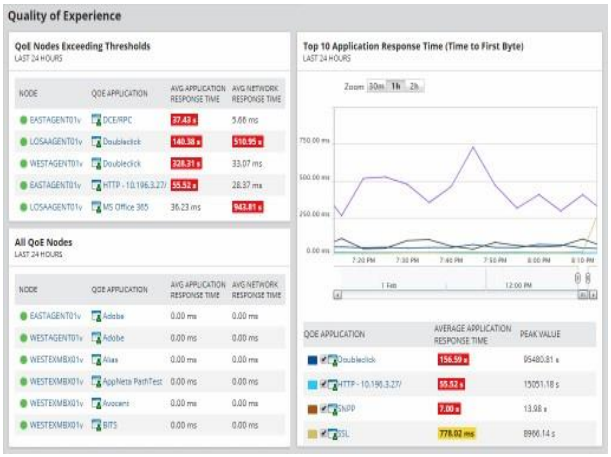

Рисунок 5.1 – Інтерфейс системи аналізуDPI

ВИКОРИСТАННЯ СИСТЕМИ АНАЛІЗУ DPI

Комбінатор рішень надає алгоритмам первинні дані та вибирає найдостовірніше . Далі здійснюється пропорція пакету з певним потоком трафіку.

Коли на етапі виділення потоків пакет належить до існуючого потоку даних, то він також передається на апаратний фільтр.

Рисунок 6.1 – Аналіз пакетів DPI з використанням комбінатора рішень

СПРОЩЕНА АНАЛІТИЧНА МОДЕЛЬ

За основу взято багатопроцесорний сервер аналізу трафіку з чотирма процесорами як першу систему черги (СМО1).

Відповідно до класифікації Кендалла, система характеристики M/M/V має застосування з вхідними потоками Пуассона, експоненційним розподілом часу обслуговування та V-процесорами. Припущення, що загальний вхідний потік сервера аналізу трафіку є Пуассоновським, ґрунтується на його великій кількості незалежних постійних потоків. СМО2 — це розробник стратегії одного сервера (M/M/1).

Рисунок 7.1 – Спрощена аналітична модель

МАТЕМАТИЧНЕ ОБГРУНТУВАННЯ

Згідно теореми Берке, що виходить із СМО2 (яка працює в стаціонарному режимі) потік буде простим з тим же параметром λ . Інтенсивність вхідного потоку на СМО2 буде рівною:

$$\lambda_{вх2} = (1 - P)\lambda \tag{8.1}$$

Інтенсивність вхідного потоку на СМО1 після обробки СМО2 буде рівною:

$$\lambda_{вх12} = (1 - P)\lambda \tag{8.2}$$

Загальна інтенсивність надходження пакетів на сервер в результаті аналізу трафіку (СМО1) визначається наступним виразом:

$$\lambda_{вх1} = \lambda + (1 - P)\lambda \tag{8.3}$$

Продуктивність СМО1 визначається наступним чином:

$$P_1 = \frac{\lambda + (1-P)\lambda}{\mu 1}, \tag{8.4}$$

де p_1 – інтенсивність обслуговування пакетів.

МАТЕМАТИЧНЕ ОБГРУНТУВАННЯ

Ймовірність з якою система вільна (P_0), може бути отримана за формулою:

$$P_0 = \frac{1}{\frac{p_1^{n+1}}{n!\,(n-p_1)} + \sum_{n=0}^{n} \frac{{p_1}^n}{n!}}\ , \tag{9.1}$$

де n=4 – число опрацьовувачів

Середню затримку сервера аналізу трафіку (T1) можна підрахувати покладаючись на кількість заявок в системі (N1), залежного від середньої кількості заявок в черзі (NS):

$$NS = \frac{p_1^{n+1} p_0}{nn! \left(1 - \frac{p_1}{n}\right)^2} \tag{9.2}$$

$$N_1 = NS + p_1 \tag{9.3}$$

$$T_1 = \frac{N^1}{\lambda + (1-P)\lambda} \tag{9.4}$$

МАТЕМАТИЧНЕ ОБГРУНТУВАННЯ

Середню затримку сервера ухвалення рішень (T2), що розраховуються за формулами:

$$p_2 = \frac{(1-P)\lambda}{\mu_2} \tag{10.1}$$

$$N_2 = \frac{p_2}{1-p_2} \tag{10.2}$$

$$T_2 = \frac{N_2}{(1-P)\lambda} = \frac{1}{\mu_2\,(1-\ p_2)} \tag{10.3}$$

Загальний час, який необхідний системі DPI на опрацювання потоку і політики (T), становить:

$$T = \ T_1 + P(T_1 + T_2) \tag{10.4}$$

РЕЗУЛЬТАТИ МОДЕЛЮВАННЯ

Результатом розрахунків на основі зразкової математичної моделі роботи системи DPI можна вважати те, що при збільшенні інтенсивності вхідних потоків зростає й загальний час визначення політики для кожного потоку пакетів. Отримана середня затримка системи DPI (1,2 мс без пікового завантаження, 22,8 мс з піковим завантаженням) допомагає застосовувати технологію DPI до чутливого до затримок трафіку, згідно з вимог рекомендації Y.1541 Міжнародного союзу електрозв'язку (ITU − T) від 0,1 до 1 с.

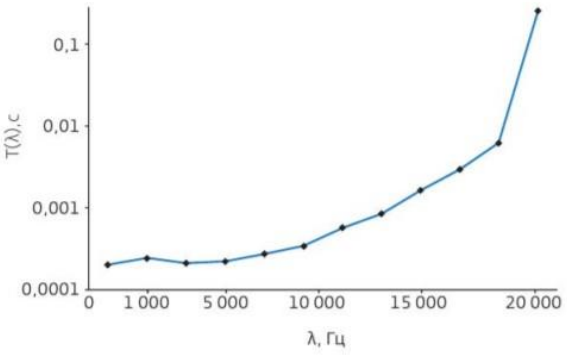

Рисунок 11.1 – Залежність затримки в системі DPI від λ

ВИСНОВКИ

1. Проаналізовано діючі міжнародні стандарти та рекомендовані практики у галузі управління інцидентами інформаційної безпеки.
2. Досліджено сучасні проблеми захисту WEB-додатків.
3. Проаналізовано існуючі WEB-вразливості, методи та засоби захисту WEB-додатків.
4. Проведено моделювання поведінки виявлення вразливостей та виконано аналіз отриманих результатів. Розроблена методика дозволяє спростити процес виявлення вразливостей та в подальшому запобігти їх розповсюдженню.

ПУБЛІКАЦІЇ ТА АПРОБАЦІЯ

Тези доповідей на конференціях:

1. Вітусевич Є. С. Розробка комплексної методики виявлення вразливостей WEB-додатків. // VII Міжнародна науково-технічна конференція студентства та молоді «Світ телекомунікації та інформатизації». – Київ: ДУТ, 2021.

Статті :

1. Вітусевич Є. С. Розробка комплексної методики виявлення вразливостей WEB-додатків. // Подано до друку в журнал «Телекомунікаційні та інформаційні технології ».

ДЯКУЮ ЗА УВАГУ!