

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ОДЕСЬКИЙ ДЕРЖАВНИЙ ЕКОЛОГІЧНИЙ УНІВЕРСИТЕТ

Факультет Магістерської підготовки

Кафедра Інформаційних технологій

**МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА**

на тему: «Дослідження методів забезпечення захищеності веб-ресурсів»

Виконав студент 2 курсу групи

МІС-18 спеціальності 122

Комп'ютерні науки

Гросу Лілія Василівна

Керівник д.т.н., проф.

Казакова Н.Ф.

Консультант

Рецензент д.т.н., проф.

Положаєнко С.А

## ЗМІСТ

Перелік скорочень .....	7
Вступ.....	8
1 Аналіз уразливостей WEB-ресурсів.....	11
1.1 Статистичне дослідження найбільш поширених уразливостей WEB-ресурсів.....	11
Висновки до розділу 1 .....	18
2 Аналіз нормативного забезпечення в галузі інформаційної безпеки .....	19
2.1 Аналіз міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки .....	25
2.2 Аналіз сучасних стандартів в галузі управління інформаційною безпекою систем .....	27
2.3 Аналіз існуючих методів оцінювання та управління ризиками інформаційної системи.....	34
2.4 Оцінка відповідності сучасних WEB-серверів вітчизняним нормативним документам в галузі захисту інформації .....	35
Висновки до розділу 2 .....	43
3 Проблематика захисту WEB-сервісів .....	45
3.1 Аналіз актуальних атак на WEB-ресурси.....	46
Висновки до розділу 3 .....	50
4 Аналіз методів та засобів захисту WEB-ресурсів.....	51
4.1 Аналіз методів тестування web-додатків.....	51
4.2 Комплекс засобів захисту Web-сервісів.....	55
Висновки до розділу 4.....	60
5 Посилення рівня захищеності WEB за допомогою DPI.....	62
Висновки до розділу 5 .....	71
Висновки .....	73
Перелік джерел посилання .....	76

## ПЕРЕЛІК СКОРОЧЕНЬ

АС	– автоматизована система;
ЕОМ	– електронно-обчислювальна машина;
ЗІ	– захист інформації
ІС	– інформаційна система
ІБ	– інформаційна безпека
ІТ	– інформаційні технології
ІзОД	– інформація з обмеженим доступом;
КЗЗ	– комплекс засобів захисту;
КСЗІ	– комплексна система захисту інформації;
НД ТЗІ	– нормативний документ системи технічного захисту інформації;
НСД	– несанкціонований доступ;
ОС	– обчислювальна система;
ПЕОМ	– персональна електронно-обчислювальна машина;
ПЗ	– програмне забезпечення;
СУІБ	– система управління інформаційною безпекою
СЗІ	– система захисту інформації
ТЗІ	– технічний захист інформації
CISRT	– Critical Incident Stress Response Team
ENISA	– European Union Agency for Network and Information Security
NIST	– National Institute of Standards and Technology
SLA	– Service Level Agreement

## ВСТУП

Кількість організацій, які застосовують веб-технології для підвищення продуктивності роботи і залучення нових клієнтів, зростає з кожним роком. До таких організацій належать, як комерційні компанії різних форм власності, так і органи державної влади і місцевого самоуправління. Безсумнівно, інтернет-сервіси несуть з собою безліч переваг, але є й зворотна сторона медалі – з ростом числа додатків збільшується і кількість кіберзагроз. Так, компанія Symantec в своєму звіті Global Internet Security Threat Report (ISTR) вказує, що кіберзлочинці при зломі веб-сайтів зазвичай використовують вразливості веб-додатків, що працюють на сервері, або експлуатують деякі вразливості операційної системи, на якій працюють ці додатки. Наприклад, за допомогою атак типу XSS хакер може перенаправити запити користувачів на шкідливі веб-сторінки, а за допомогою SQL-ін'єкцій – витягувати з баз даних сайту різну конфіденційну інформацію. У відповідь на масові зломи систем безпеки був створений консорціум OWASP – Open Web Application Security Project, це відкритий проект забезпечення безпеки веб-додатків. Однак і зловмисники, і фахівці в області кібербезпеки продовжують знаходити вразливості в веб-додатках, які можуть привести до серйозних втрат з боку бізнесу. Основною причиною більшості взломів в веб-додатках є написаний розробниками програмний код. Розробники можуть допускати помилки при написанні коду або не усвідомлювати всю важливість використання прийомів безпечного програмування – все це призводить до появи вразливостей в додатках.

Безсумнівно, захист веб-інфраструктури потрібний для будь-якої компанії. Однак з безлічі категорій захисних рішень – Firewall, IPS / IDS, NGFW (Next Generation Firewall), WAF (Web-Application Firewall) тільки Web Application Firewall здатні забезпечити комплексний захист веб-додатків від відомих і невідомих загроз, а також забезпечити відповідність вимогам регуляторів, наприклад, PCI DSS. Ні класичний Firewall, ні IPS / IDS не зможуть забезпечити адекватного захисту веб-додатків.

За даними щорічного дослідження корпоративних ризиків «Барометр ризиків Allianz 2016», яке було складено на основі опитування більш ніж 820 ризик-менеджерів і страхових експертів з 44 країн, вперше в ТОП-3 корпоративних ризиків увійшли кіберзлочини. Вони ж вказуються як найбільш значний ризик для підприємств в довгостроковій перспективі наступних 10 років. Згідно з прогнозами дослідницької компанії Cybersecurity Ventures, до 2021 року збиток від кібершахрайства збільшиться вдвічі у порівнянні з 2015 роком і досягне \$ 6 трлн. Основною метою кіберзлочинців традиційно є різні фінансові організації, в першу чергу – банки, а також майданчики електронної комерції. При цьому, згідно з даними звіту Trend Micro Incorporated за перше півріччя 2016 року, однією з найбільш значущих загроз у фінансовій галузі як і раніше залишаються банківські трояни. Вкрадена троянами інформація використовується правопорушниками для проведення шахрайських транзакцій або продається на підпільних сайтах. Більш того, в результаті подібних шкідливих дій фінансові організації змушені нести витрати на компенсацію збитків, які понесли їх клієнти в результаті кібератак. Дуже часто основною точкою злому організації стає саме веб-додаток. Загроза злому веб-додатків залишається однією з найсерйозніших проблем для веб-ресурсів будь-якої спрямованості. Відчути себе хакером сьогодні може навіть людина, слабо підготовлена технічно – методи злому і необхідні інструменти доступні у відкритому вигляді і легко можуть бути знайдені за допомогою звичайних пошуковиків.

У результаті зростають не тільки кількість атак на веб-ресурси, але й економічні наслідки таких атак. Останнім часом вразливість веб-ресурсів до атак отримала політичний вимір унаслідок як поширення гібридних війн у світі, так і зростання терористичних загроз.

Таким чином, удосконалення методів і систем захисту веб-ресурсів від атак залишається актуально науковою проблемою, особливо з урахуванням постійного вдосконалення методів та інструментів атак і появи нових методів та інструментів. Удосконалення методів захисту веб-ресурсів від атак є також

важливою в практичному застосуванні задачею внаслідок зростаючих економічних, соціальних і політичних наслідків від зловмисних дій.

**Метою роботи** є підвищення рівня оцінки захищеності Web-ресурсів, за рахунок удосконалення методів та засобів виявлення потенційних загроз на підставі огляду сучасного стану та перспективних методів оцінки загроз інформаційним ресурсам та світових практик впровадження систем управління інформаційною безпекою.

**Об'єкт дослідження** – методи та засоби оцінки захисту Web-ресурсів від несанкціонованого доступу.

**Предмет дослідження** – законодавчі та нормативні акти, технології та програмні засоби тестування в галузі інформаційної безпеки та захисту Web-ресурсів.

**Метод дослідження** – аналітичний з використанням комп'ютерних технологій.

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 ресурсів;
- проаналізувати існуючі WEB уразливості;
- провести аналіз методів та засобів захисту web ресурсів.

## **1 АНАЛІЗ УРАЗЛИВОСТЕЙ WEB-РЕСУРСІВ**

Захист веб-ресурсів залишається одним із важливих напрямків інформаційної безпеки. Щороку кількість веб-ресурсів збільшується, зростає також кількість конфіденційної інформації, яка локалізується на серверах віддаленого доступу (особливо із використанням хмарних технологій).

У результаті цього зростають не тільки кількість атак на веб-ресурси, але й економічні наслідки таких атак. Останнім часом вразливість веб-ресурсів до атак отримала політичний вимір унаслідок як поширення гібридних війн у світі, так і зростання терористичних загроз.

Таким чином, удосконалення методів і систем захисту веб-ресурсів від атак залишається актуально науковою проблемою, особливо з урахуванням постійного вдосконалення методів та інструментів атак і появи нових методів та інструментів. Удосконалення методів захисту веб-ресурсів від атак є також важливою в практичному застосуванні задачею внаслідок зростаючих економічних, соціальних і політичних наслідків від зловмисних дій.

### **1.1 Статистичне дослідження найбільш поширених уразливостей WEB-ресурсів**

Фахівцями компанії Positive Technologies було проведено дослідження найбільш поширених уразливостей веб-ресурсів, яке дало наступні результати (рис. 1.1).

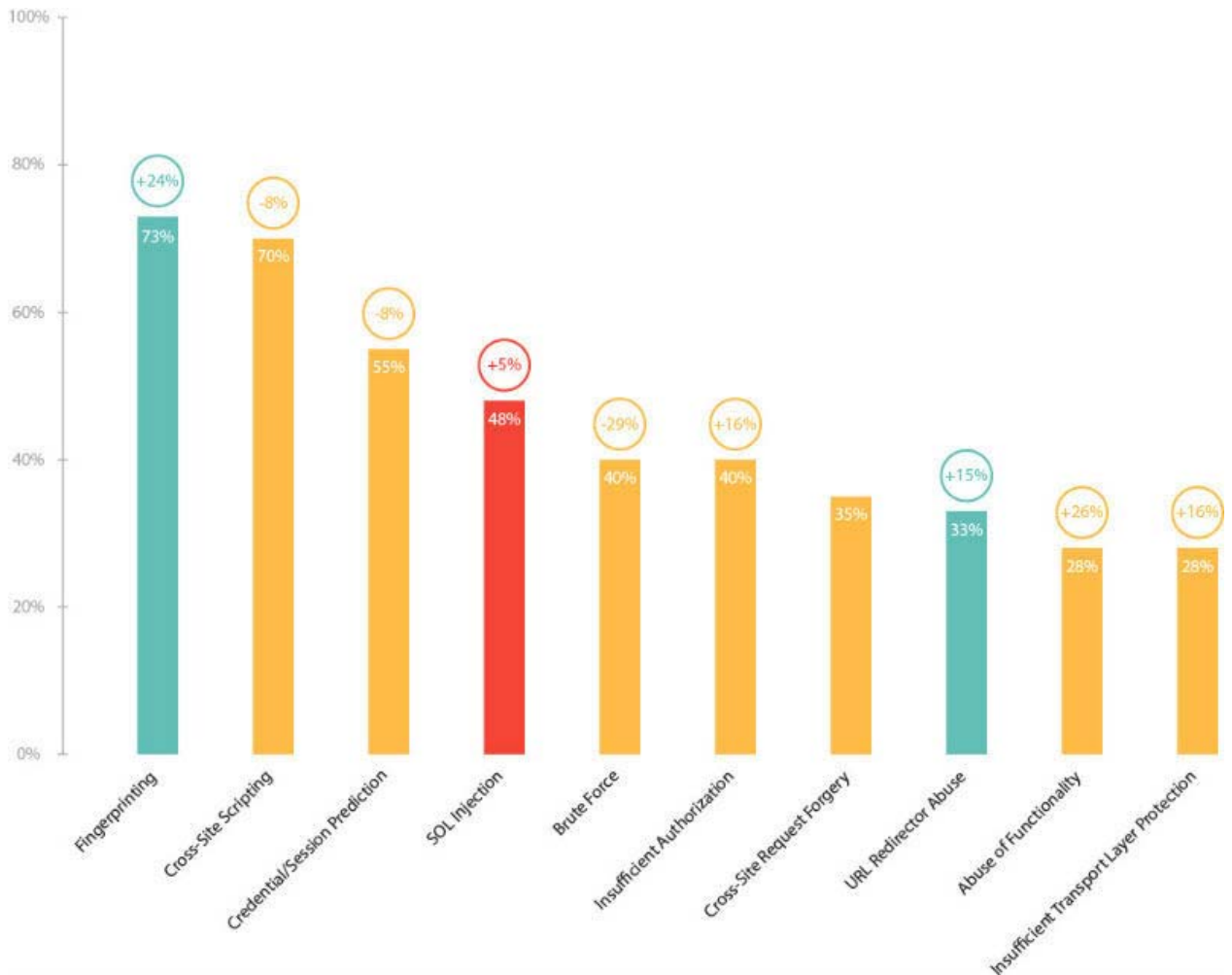


Рисунок 1.1 – Поширеність різних типів уразливостей

### Джерела та методика

В цілому фахівцями компанії Positive Technologies було проаналізовано близько 300 веб-додатків. З них виділено 40 систем, для яких проводився поглиблений аналіз з найбільш повним покриттям перевірок. У статистику увійшли тільки дані про зовнішні веб-додатки, доступні з глобальної мережі Інтернет. Оцінка захищеності проводилася методами чорного, сірого і білого ящика з використанням автоматизованих допоміжних засобів. Виявлені уразливості класифікувалися відповідно відповідним загрозам по системі WASC TC v. 2, ступінь ризику уразливостей оцінювалася за CVSS v. До статистики увійшли тільки проблеми, пов'язані з помилками в коді і конфігурації веб-додатків.



Досліджувані веб-додатки належали компаніям, які представляють різні галузі: електронна комерція (30%), фінанси і банки (22%), промисловість (17%), інформаційні технології (15%) і телекомунікації (13%); також у дослідженні брало участь одна державна установа.

Більшість веб-додатків, які ввійшли у вибірку, розроблені на базі PHP (58%) і ASP.NET (25%). Найбільш поширеним веб-сервером в дослідженні цього року став Nginx (37% веб-додатків), за ним йдуть Apache (26%) і IIS (24%). Більшість ресурсів представляли собою продуктивні системи (85%), проте досліджувалися також і тестові майданчики, що знаходяться в процесі розробки або прийняття в експлуатацію.

Всі 40 досліджених веб-додатків містять ті чи інші уразливості, загальним числом 1194. При цьому 68% систем містять уразливості високого ступеня ризику. Даний показник вище торішнього (62%). Крім того, в 2013 році в середньому на кожне веб-додаток доводилося 15,6 уразливостей, а в 2014 році це число зросло майже в два рази — до 29,9. Більшість виявлених уразливостей (89%) викликані помилками в програмному коді, і лише 11% недоліків пов'язані з некоректною конфігурацією веб-додатків.

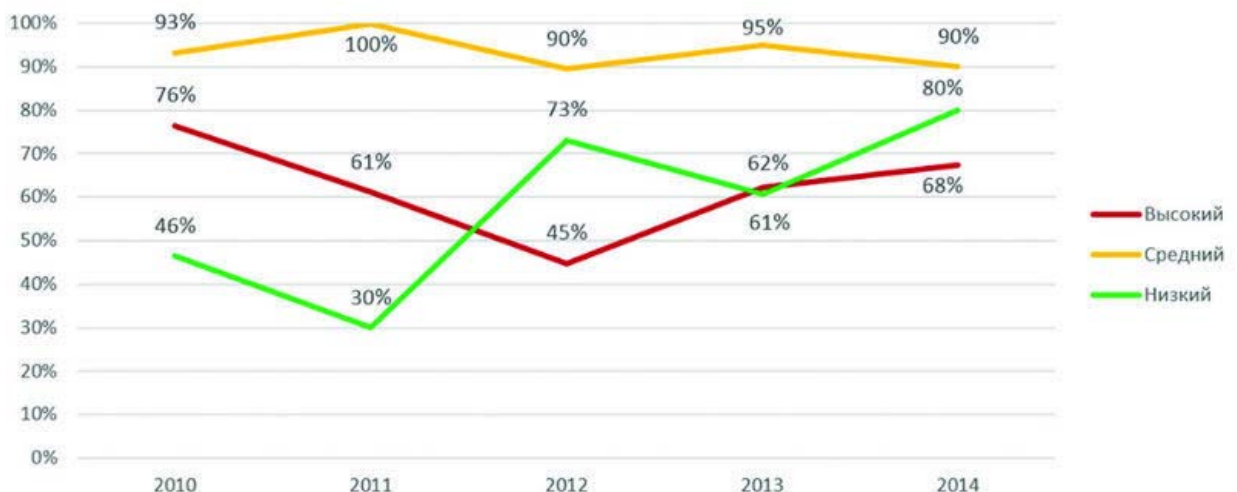


Рисунок 1.2 – Частки уразливих сайтів в залежності від ступеня ризику уразливостей

Найбільше поширення (73% систем) отримала вразливість низького рівня ризику «Ідентифікація програмного забезпечення» (Fingerprinting). Друге місце (70%) займає найбільш поширена в 2013 році вразливість «Міжсайтового виконання сценаріїв» (Cross-Site Scripting, XSS). В результаті експлуатації даної помилки в кодї зловмисник може організувати атаку на користувачів веб-додатки, наприклад, з метою отримання доступу в особистий кабінет.

Більше половини веб-сайтів містять уразливості, пов'язані з використанням передбачуваних значень ідентифікаторів користувачів і сесій (Credential/Session Prediction). Критично небезпечна уразливість «Впровадження операторів SQL» (SQL Injection) піднялася з 6-го місця на 4-е, тепер вона виявляється майже в половині веб-додатків (48%). Експлуатація цієї проблеми може призвести до отримання несанкціонованого доступу до інформації, що зберігається в базах даних додатків; крім того, часто можливий розвиток атаки аж до отримання повного контролю над сервером.

Як і у попередні періоди, найбільш уразливими виявилися програми на PHP: 81% систем, написаних цією мовою, містять критично небезпечні уразливості (в 2013 році було 76%). Зате для ресурсів на основі ASP.NET цей показник зменшився з 55 до 44%. Кожен веб-додаток на PHP в середньому містить 11 критично небезпечних уразливостей. Для ASP.NET даний показник склав 8,4, але в даному випадку на статистику сильно вплинула одна система, що містила 60 уразливостей високого ступеня ризику: в інших додатках на основі ASP.NET середнє число уразливостей склало лише 2.

Також можна відзначити, що частка ресурсів на PHP, схильних до уразливості «Міжсайтового виконання сценаріїв», значно вище (95%), ніж відповідна частка ресурсів на ASP.NET (44%). Це може бути пов'язано з тим, що в ASP.NET існують вбудовані базові механізми захисту від атак цього типу (Request Validation).

PHP	Доля сайтів, %	ASP.NET	Доля сайтів, %	Другие	Доля сайтів, %
Cross-Site Scripting	95	Fingerprinting	78	Fingerprinting	67
Fingerprinting	76	Cross-Site Scripting	44	Credential/Session Prediction	67
SQL Injection	67	Insufficient Authorization	44	Cross-Site Scripting	50
Credential/Session Prediction	62	Brute Force	44	Brute Force	50
Abuse of Functionality	48	SQL Injection	33	Insufficient Authorization	33
Insufficient Authorization	43	Credential/Session Prediction	33	SQL Injection	33
Cross-Site Request Forgery	43	XML External Entities	33	Cross-Site Request Forgery	33
URL Redirector Abuse	43	Abuse of Functionality	22	URL Redirector Abuse	33
Brute Force	38	Insufficient Transport Layer Protection	22	Information Leakage	33
Information Leakage	33	Path Traversal	22	Denial of Service	33

Рисунок 1.3 – Найбільш поширені уразливості (по засобам розробки)

### Уразливості по серверам

86% досліджених веб-додатків під управлінням сервера Nginx містять уразливості високого рівня ризику. Частка вразливих ресурсів на базі Microsoft IIS значно знизилася порівняно з 2013 роком і склала 44% замість 71%. Кількість уразливих сайтів під Apache зросла на 10% і склало 70%.

Найпоширенішою помилкою адміністрування веб-серверів є «Ідентифікація програмного забезпечення» (Fingerprinting). Зокрема, дана уразливість зустрічається на 8 з 10 веб-ресурсів під управлінням Apache. Це пов'язано з тим, що стандартна конфігурація досліджуваних серверів передбачає розкриття інформації про версії веб-сервера в повідомленнях про помилки (наприклад, при зверненні до неіснуючого ресурсу).

### Уразливості по галузях

Лідером за кількістю систем з уразливими високого рівня ризику опинилася банківська галузь (89%). Це може бути пов'язано з тим, що більшість

досліджених ресурсів не були системами ДБО або іншими системами, де обробляються дані про фінансові транзакції, тому банки приділяли меншу увагу забезпеченню захисту даних додатків. Також високий відсоток веб-додатків, схильних до критично небезпечні уразливості, зазначається для телекомунікаційної галузі (80%). Далі йдуть промисловість (71%) та інформаційні технології (67%). В електронній комерції частка систем з уразливими високого рівня ризику теж досить висока — 42%.

За середньою кількістю уразливостей на одну систему найменш захищеними виявилися сайти промислових підприємств, де на один додаток припадає 18 критично небезпечних уразливостей. Варто зазначити, що згадане раніше додаток, в якому було виявлено 60 критично небезпечних уразливостей, відносилося до промислового сектору. Без його урахування відповідний показник по даному сектору економіки становить 13,1 уразливості високого ступеня ризику на систему, що збігається з показником для банківської галузі.

У 2014 році уразливості високого рівня ризику «Впровадження операторів SQL», «Впровадження сутностей XML» і «Вихід за межі призначеного каталогу» зустрічалися частіше, ніж інші недоліки. Як і в 2013 році, критично небезпечна уразливість «Впровадження операторів SQL» була виявлена в веб-додатках всіх досліджуваних галузей економіки.

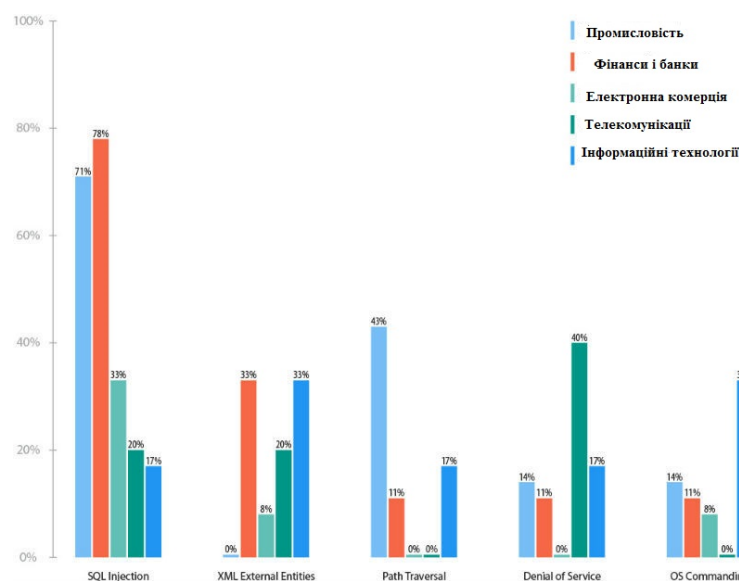


Рисунок 1.4 – Частки уразливих сайтів з різних галузей економіки

## **Уразливості на продуктивних і тестових сайтах**

У 71% продуктивних веб-ресурсів були виявлені критично небезпечні уразливості, для тестових майданчиків даний показник становить 50%. Середня кількість уразливостей високого ступеня ризику, виявлених у тестових системах (12,8), майже в два рази вище порівняно з продуктивними, де виявлено в середньому по 7 критично небезпечних уразливостей. Однак при цьому в продуктивних системах в середньому виявлено більше уразливостей середнього рівня ризику (20,6 проти 14,3 для тестових).

Подібна ситуація з захищеністю систем, що вже знаходяться в експлуатації, наочно свідчить про необхідність впровадження процесів забезпечення безпеки на всіх стадіях життєвого циклу додатків (SSDLC).

## **Порівняння методів тестування**

В ході досліджень захищеності фахівці Positive Technologies порівняли результати тестування методом білого ящика (з використанням внутрішніх даних про системи, включаючи аналіз вихідних кодів) з результатами тестування методами чорного і сірого ящика (коли аналіз проводиться з привілеями, ідентичними привілеїв потенційного зловмисника). Частка сайтів, що містять уразливості високого і середнього рівня ризику, виявилася приблизно однакова для цих методів тестування. Можна зробити висновок, що відсутність у атакуючого доступу до вихідного коду не робить веб-додатки захищеними.

З іншого боку, аналіз вихідних кодів, на додаток до аналізу методами чорного і сірого ящика дозволяє виявити більше уразливостей для кожного додатка. Зокрема, тестування методом білого ящика в середньому знаходить в 3,5 рази більше уразливостей середнього ступеня ризику в порівнянні з методами чорного і сірого ящика. Інший яскравий приклад: в кожному ресурсі, дослідженому методами чорного і сірого ящика, в середньому було виявлено по 4 уразливості типу «Міжсайтового виконання сценаріїв» — зате метод білого ящика дозволив виявити в середньому по 29 уразливостей даного типу.

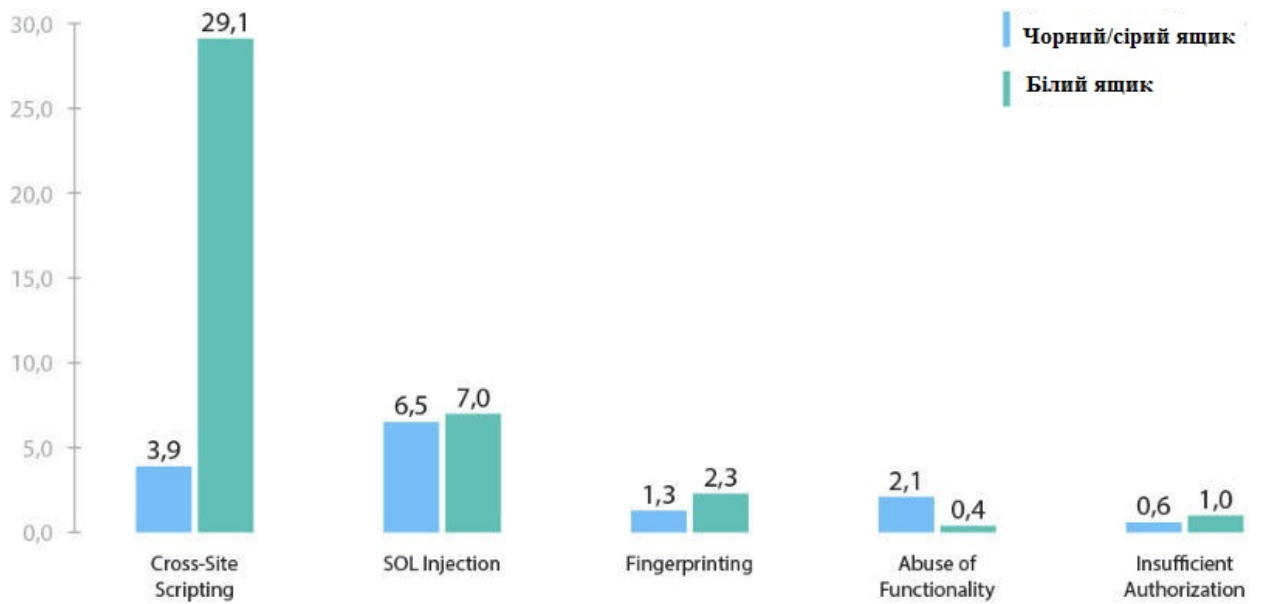


Рисунок 1.5 – Середня кількість виявлених уразливостей певного типу на одну систему за методом тестування)

## Висновки до розділу 1

В першому розділі проведено статистичне дослідження найбільш поширених уразливостей веб-ресурсів. Досліджені веб-додатки належали компаніям, які представляють різні галузі. Проаналізовано уразливості по засобам розробки, по серверам, по галузях на продуктивних і тестових сайтах, проведено порівняння методів тестування.

В цілому, на сьогоднішній день рівень захищеності веб-додатків залишається вкрай низьким. Незважаючи на це, системи виявлення та запобігання вторгнень рівня додатків майже не використовуються: такий механізм застосовувався для захисту лише одного з усіх сайтів, розглянутих у даному дослідженні.

## 2 АНАЛІЗ НОРМАТИВНОГО ЗАБЕЗПЕЧЕННЯ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Проблемами збереження та захисту даних в інформаційних системах на даний час займається велика кількість українських та іноземних дослідників. Слід зазначити, що на державному, міжнародному та європейському рівнях проблемами захисту інформації (ЗІ) взагалі займаються такі організації як Міжнародна організація стандартизації (ISO) спільно з міжнародним електротехнічним комітетом (IEC), ENISA (European Union Agency for Network and Information Security) – європейська організація із мережевої та інформаційної безпеки, NIST (National Institute of Standards and Technology) – національний інститут стандартів та технологій Сполучених штатів Америки.

У світі розробка 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. Розробка нормативних документів з ІБ, повністю або частково присвячених керуванню інцидентами ІБ, здійснюється низькою спеціалізованих міжнародних організацій і консорціумів, таких як, наприклад: CERT, ISO, IEC, IETF, ITU-T, IEEE, OMG, SANS Institute, X/Open тощо. Значна робота щодо стандартизації питань ІБ, зокрема керування інцидентами, проводиться спеціалізованими організаціями і на національному рівні:

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

Все це дозволило сформувати розширену нормативно-методологічну базу у вигляді міжнародних, національних та галузевих стандартів, а також нормативних і керівних матеріалів, що регламентують діяльність в сфері керування інцидентами ІБ.

Проте, як свідчить сучасна практика, найважливішу роль в світі відіграють стандарти ISO, які наведені в табл. 2.1

Таблиця 2.1 – Стандарти ISO

№ п/п	Позначення документу	Назва документу	Рік
1	ISO/IEC17799	Information technology. Security techniques. Code of practice for information security management.	2000; 2005
2	ISO/IEC27001	Information technology. Security techniques. Information security management systems. Requirements.	2005; 2013
3	ISO/IEC TR 27035	Information technology. Security techniques. Information security incident management (3 Part)	2011
4	ISO/IEC 20000	ISO/IEC 20000:2005. Information technology. Service management. Part 1: Code of practice.	2011

**Стандарт ISO/IEC 17799** [1]<sup>1</sup> на сьогодні став найпоширенішим інструментом створення системи управління ІБ (СУІБ). Зауважимо, що попередня версія ISO/IEC 17799 від 2000 року офіційно прийнята в Україні як ДСТУ ISO/IEC 17799:2000. ISO/IEC 17799 – це збірка практичних рекомендацій, яка дає деталізоване керівництво щодо розробки, впровадження та оцінки заходів керування ІБ, а також загальні принципи побудови СУІБ. В цьому ж документі визначено наступні терміни, які є базовими для даного дослідження:

- *подія інформаційної безпеки* – встановлений прояв стану системи, служби або мережі, яка вказує на можливе порушення політики інформаційної безпеки або збій заходів безпеки, або невідома до даного моменту ситуація, яка може бути пов'язана з безпекою [1, п. 2.6].
- *інцидент інформаційної безпеки* – ознаками інциденту інформаційної безпеки є поодинокі або послідовні небажані або несподівані події інформаційної безпеки, які мають значну вірогідність компрометації ділових операцій і загрожують інформаційній безпеці [1, п. 2.7].

Розділ 13 ISO/IEC 17799 присвячено керуванню інцидентами ІБ. В ньому розглянуто наступні питання:

<sup>1</sup> [1] ISO/IEC 17799:2005. Information technology. Security techniques. Code of practice for information security management.



- Повідомлення про події і слабкі місця ІБ [1, п. 13.1]<sup>1</sup>. Виявлення користувачами подій і слабких місць ІБ, пов'язаних з інформаційними системами, має гарантувати можливість ухвалення своєчасних корегуючих дій.
- Має бути впроваджений формальний порядок повідомлення про події і порядок ескалації. Всіх співробітників, контрагентів і користувачів третіх сторін слід поінформувати про порядок повідомлення щодо різних типів подій і слабких місць, які можуть мати вплив на безпеку активів організації. Дані особи зобов'язані негайно повідомляти про будь-які події і слабкі місця ІБ, використовуючи певну точку контакту.

Відповідно до розроблених регламентів, про події ІБ потрібно повідомляти за допомогою прийнятних каналів керування настільки швидко, наскільки це можливо. Також необхідно затвердити формальний порядок повідомлення про події ІБ, разом з порядком реагування на інциденти. В цих порядках потрібно описати дії, що мають бути здійснені при отриманні повідомлення про подію ІБ. Необхідно встановити точку контакту для повідомлень про події ІБ.

Далі, потрібно забезпечити обізнаність всієї організації про дану точку контакту, її постійну доступність і здатність адекватно і своєчасно реагувати.

Приклади подій та інцидентів ІБ:

- втрата обслуговування, устаткування або засобів обслуговування;
- системні збої або перевантаження;
- людські помилки;
- невідповідність політикам або керівництву; порушення заходів фізичної безпеки;
- некеровані системні зміни;
- збої програмного або апаратного забезпечення;
- порушення доступу.

---

<sup>1</sup> [1] ISO/IEC 17799:2005. Information technology. Security techniques. Code of practice for information security management.

**Стандарт ISO/IEC 27001 [2]<sup>1</sup>** конкретно звертає увагу на необхідність створення процедури керування інцидентами ІБ. В рамках даного стандарту висуваються загальні вимоги щодо побудови СКІБ, що відносяться у тому числі і до процесів керування інцидентами ІБ. Згідно з ISO/IEC 27001 для обробки подій і інцидентів ІБ необхідно організувати процес реагування на інциденти. Основними завданнями процесу реагування на інциденти ІБ є:

- координація реагування на інцидент ІБ;
- підтвердження/спростування факту виникнення інциденту ІБ;
- забезпечення збереження і цілісності доказів виникнення інциденту ІБ, створення умов для накопичення і зберігання точної інформації про інциденти ІБ, що мали місце, про корисні рекомендації;
- мінімізація порушень порядку роботи і пошкодження даних ІТ-системи, відновлення в найкоротші терміни працездатності компанії при її порушенні в результаті інциденту;
- мінімізація наслідків порушення конфіденційності, цілісності і доступності інформації ІТ-систем;
- захист прав компанії, встановлених законом; створення умов для порушення цивільної або кримінальної справи проти зловмисників;
- захист репутації компанії і її ресурсів;
- швидке виявлення і/або попередження подібних інцидентів в майбутньому;
- навчання персоналу компанії діям до виявлення, усунення наслідків і запобігання інцидентам ІБ.

В рамках ISO/IEC 27001 висуваються наступні вимоги до процесу реагування на інциденти ІБ, які повністю відповідають вищезгаданому рекомендаціям щодо керування інцидентами ІБ у ISO/IEC17799.

Задачам керування інцидентами ІБ присвячено технічний звіт.

---

<sup>1</sup> [2] ISO/IEC 27001:2005. Information technology. Security techniques. Information security management systems. Requirements.

**ISO/IEC TR 27035** [3]<sup>1</sup>. Стандарт ISO / IEC 27035:2011 "Інформаційні технології. Методи забезпечення безпеки. Управління інцидентами інформаційної безпеки" надає практичне керівництво з виявлення, реєстрації та оцінки випадків порушення інформаційної безпеки і уразливостей.

Його призначення – допомога організаціям реагувати на інциденти інформаційної безпеки, зокрема, вводити відповідні інструменти контролю для їх запобігання і скорочення, а також відновлення, і, таким чином, витягувати уроки і покращувати загальний підхід.

Інтеграція системи управління інцидентами інформаційної безпеки дає ряд переваг:

- підвищення загального рівня інформаційної безпеки;
- зменшення негативних наслідків для бізнесу;
- посилення акценту на попередженні інцидентів інформаційної безпеки, призначення пріоритетів і зборі даних;
- поліпшення якості результатів оцінки та управління ризиків інформаційної безпеки;
- поліпшення інформованості в області інформаційної безпеки і допомогу в підготовці матеріалів для навчання;
- надання додаткової інформації для політики інформаційної безпеки та супутньої документації.

Новий стандарт ISO/ IEC 27035 пропонує перевірені рішення в області процесів і методів забезпечення ефективного управління інцидентами інформаційної безпеки.

**ISO/IEC 27035:2011** замінює технічний звіт ISO/IEC TR 18044:2004 і узгоджений з загальними принципами, встановленими в ISO / IEC 27001:2005 "Інформаційні технології. Методи забезпечення безпеки. Системи менеджменту інформаційної безпеки. Вимоги".

---

<sup>1</sup> [3] ISO/IEC TR 27035:2011. Information technology – Security techniques – Information security incident management.

Він може застосовуватися в будь-якій організації, незалежно від її розміру. Стандарт поширюється на широкий діапазон інцидентів інформаційної безпеки, навмисних або випадкових, викликаних технічними або фізичними причинами.

Процедура керування IT-інцидентами регулюється стандартом **ISO/IEC 20000** [4]<sup>1</sup>, який описує систему керування IT-сервісами та процедуру керування інцидентами, але також розглядає IT-інциденти. Сама процедура керування інцидентами IT дуже близька до процедури керування інцидентами ІБ з тією різницею, що в останньому випадку більший акцент робиться на його розслідування, збір доказів, покарання винних.

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

- виконання вимог безпеки, закріплених в SLA (Service Level Agreement) та інших вимогах зовнішніх і внутрішніх угод, законодавчих актів і встановлених правил;
- забезпечення базового рівня ІБ, незалежного від зовнішніх вимог.

Вхідними даними для процесу служать SLA, що містять вимоги безпеки, за можливості, доповнені документами, що визначають політику організації в цій області, а також інші зовнішні вимоги. Процес також одержує важливу інформацію, що відноситься до проблем безпеки, з інших процесів, наприклад про інциденти, пов'язані з ІБ.

**CMU/SEI-2004-TR-015** (Defining incident management processes for CISRT) [5]<sup>2</sup>. Цей документ описує методологію планування, впровадження, оцінки і поліпшення процесів управління інцидентами. Основний наголос робиться на організації роботи CISRT (Critical Incident Stress Response Team) – групи або підрозділів, які забезпечують сервіс і підтримку запобігання,

---

<sup>1</sup> [4] ISO/IEC 20000:2011. Information technology. Service management. Part 2: Code of practice.

<sup>2</sup> [5] 5. 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.

обробки і реакції на інциденти інформаційної безпеки. Вводиться ряд критеріїв, на підставі яких можна оцінювати ефективність даних сервісів, приводяться докладні процесні карти.

**NIST SP 800-61** (Computer security incident handling guide) [5]<sup>1</sup>. Тут наведена збірка "кращих практик" щодо побудови процесів управління інцидентами і реакції на них. Детально розбираються питання реакції на різні типи загроз, такі як розповсюдження шкідливого програмного забезпечення, несанкціонований доступ та ін.

З метою визначення найбільш перспективних напрямків та тенденцій у світовому законодавстві, в наступному підрозділі більш детально опишемо деякі особливості міжнародних законодавчих актів за вищевказаним напрямком.

## **2.1 Аналіз міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки**

В останні кілька років у світі спостерігається тенденція до стандартизації складових систем управління в організаціях. Ініціатива виходить як на державному рівні, так і на рівні окремо взятих галузей. Серед нормативних актів, що підштовхують організації перебудовувати свою систему інформаційної безпеки (ІБ) та отримали найбільше поширення і популярність, можна відзначити акт Sarbanes-Oxley та угоду з банківського нагляду Basel II.

Sarbanes-Oxley був прийнятий в США з метою контролю за фінансовою звітністю організацій, і в даний час застосовується переважно в цій країні. Стандарт використовують, головним чином, ті компанії, що виходять зі своїми акціями на американські біржі. З боку заходів, які вживаються такими компаніями з точки зору вдосконалення системи ІБ, це передбачає запровадження

---

<sup>1</sup> [5] 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.

контролю цілісності, захист від несанкціонованого доступу (НСД), шифрування даних і т.д.

Угода Basel II має більш широку географію розповсюдження: його положення застосовуються в країнах Євросоюзу, США, Японії та ін. Основною метою, сприяти досягненню якої покликаний цей документ, є контроль банківських ризиків. Оцінка ризиків є зараз одним з актуальних напрямків у сфері регулювання банківської діяльності. Головним чином це стосується операційних ризиків, які несуть банки [6]<sup>1</sup>. Серед найбільш значущих з них є ризики ІБ, такі як неадекватні або помилкові дії персоналу та внутрішні процеси.

У загальному випадку можна виділити наступні складові управління ризиками:

- моніторинг та оцінювання організаційних ризиків функціонування системи;
- моніторинг та оцінювання ризиків технічних засобів;
- прийняття рішення з управління ризиками на основі наявних оцінок;
- проведення безпосередньої роботи з управління ризиками [7]<sup>2</sup>.

Поступово відходить у минуле підхід, коли окремі вимоги нормативних актів та окремі проблеми інформаційної безпеки вирішуються в порядку виникнення. Багато компаній сьогодні приходять до того, що система захисту інформаційних ресурсів повинна будуватися, виходячи із загальноприйнятих норм і з урахуванням напрацьованих практик. Це допомагає уникнути розбудови інфраструктури інформаційної системи (ІС) в «авральному режимі» під будь-які вимоги і знижує рівень незапланованих витрат на обслуговування системи (у тому числі і ризик витрат, пов'язаних з втратою або крадіжкою інформації).

---

<sup>1</sup> [6] 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.

<sup>2</sup> [7] ГОСТ Р ИСО/МЭК 17799-2005.

## 2.2 Аналіз сучасних стандартів в галузі управління інформаційною безпекою систем

Сімейство Міжнародних Стандартів на Системи Управління Інформаційною Безпекою 27000 розробляється ISO/IEC JTC 1/SC 27. Це сімейство включає в себе Міжнародні стандарти, що визначають вимоги до системи управління інформаційної безпеки (СУІБ), управління ризиками, метрики і вимірювання, а також керівництво з впровадження.

Для цього сімейства стандартів використовується послідовна схема нумерації, 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 описує загальну методологію підходу до забезпечення ІБ в організації і акцентує увагу на найбільш критичних складових ІС. Він охоплює елементи управління системою ІБ, актуальні для всіх без винятку сфер бізнесу, такі як: політика ІБ, розподіл відповідальності за ІБ, проведення навчання в цій області, звітність по інцидентах, захист від вірусів, забезпечення безперервності роботи, контроль копіювання ліцензійного програмного забезпечення (ПЗ), захист архівної документації та захист персональних даних. Цей стандарт дає компанії інструмент, що дозволяє управляти конфіденційністю, цілісністю і збереженням такого важливого активу компанії як інформація. Елементи управління системою ІБ розділені в стандарті по декількох груп, і включають в себе розділи:

- політика безпеки – підтримка політики у сфері ІБ з боку керівництва підприємства;
- інфраструктура системи безпеки – створення організаційної структури, яка буде забезпечувати працездатність системи ІБ в організації;



- класифікація ресурсів і управління – пріоритезація інформаційних ресурсів за ступенем їх цінності і розподіл відповідальності за них;
- співробітники – зниження ризику людських помилок, крадіжки і неправильного використання устаткування (навчання співробітників та відстеження інцидентів);
- фізична і зовнішня безпека – запобігання НСД та порушення роботи ІС організації;
- управління мережами і комп'ютерними ресурсами – забезпечення безпечного функціонування комп'ютерів та мереж;
- управління доступом – управління доступом до бізнес-інформації;
- розвиток та обслуговування системи – виконання вимог безпеки при створенні або розвитку інформаційної системи організації, підтримку безпеки додатків і даних;
- забезпечення безперервності бізнесу – план дій у разі надзвичайних обставин для забезпечення безперервності роботи організації;
- відповідність вимогам законодавства – виконання вимог відповідного громадянського та кримінального законодавства, включаючи закони про авторські права і захист даних.

Стандарт складається з двох частин: в першій частині описані механізми контролю (всього їх 127), необхідні для побудови СУІБ. Ця частина використовується в якості основи для проведення аудиту СУІБ в організації. У другій частині стандарту описуються ті критерії, по яких проводиться сертифікація СУІБ. Виходячи з ідеології стандарту ключовим елементом СУІБ є система управління ризиками, найважливішою частиною яких є аналіз цих ризиків з метою визначення, які ресурси від яких загроз необхідно захищати, а також якою мірою ресурси потребують захисту. Проведення аналізу ризиків дозволяє організації оцінити можливі збитки в кількісних і якісних показниках. Цей міжнародний стандарт був підготовлений для того, щоб надати модель для створення, впровадження, експлуатації, постійного контролю, аналізу, підтримання в робочому стані і поліпшення СУІБ. Передбачається, що прийняття

СУІБ є стратегічним для організації [8]<sup>1</sup>. Стандарт приймає процесний підхід для створення, впровадження, експлуатації, постійного контролю, аналізу, підтримання в робочому стані і поліпшення СУІБ організації.

Організація для того, щоб задовольнити вимоги даного стандарту, повинна зробити наступне: визначити область програми і межі СУІБ в термінах характеристик бізнесу, її місця розташування, активів і технологій, також включаючи подробиці та обґрунтування будь-яких винятків з області застосування; визначити політику щодо СУІБ в термінах характеристик бізнесу, організації, її місця розташування, активів і технологій; захистом інформації, враховувати законодавчі, нормативні вимоги, визначати стратегії управління інформаційними ризиками; визначити підхід до оцінки ризику в організації; виявити ризики; проаналізувати ризик та оцінити значущість ризику; виявити та оцінити можливості для обробки ризиків; вибрати цілі та засоби керування для обробки ризику. Стандарт рекомендує проводити постійний контроль результативності СУІБ, аналіз цілей управління, беручи до уваги результати аудиту та статистику виникнення порушень.

У відповідності з стандартом ISO/IEC 27001 документація, яка визначає управління інформаційними ризиками організації, повинна включати в себе: документовану заяву про політику та цілі СУІБ; область програми СУІБ; процедури і засоби управління на підтримку СУІБ; опис методології оцінки ризиків; звіт про оцінки ризиків; план обробки ризиків [8]. В стандарті наголошується відповідальність керівництва в організації управління інформаційними ризиками. У розділі розглядаються види зобов'язань керівництва, деякі принципи менеджменту ресурсів і забезпечення необхідного рівня компетентності персоналу. Стандарт розглядає основні цілі та принципи проведення аудиту захищеності організації від загроз в інформаційній сфері, а також аналіз СУІБ з точки зору керівництва. У стандарті зазначено основні вхідні і вихідні дані для внутрішнього аудиту. В якості важливих результатів аудиту можна

---

<sup>1</sup> [8] ГОСТ Р ИСО/МЭК 27001.

виділити оновлення оцінки ризиків для організації та відповідно зміну методів управління ними. Заключна частина стандарту присвячена принципу постійного поліпшення в СУІБ.

Стандарт Великобританії BS 7799 присвячений УІБ організації. Цей стандарт є одним з найбільш авторитетних в світі. На його базі розроблено міжнародний стандарт ISO/IEC 17799, котрий згодом еволюціонував в ISO/IEC 27002. Третя частина даного стандарту присвячена питанням управління інформаційними ризиками.

Стандарт BS 7799-3:2006 гармонізований з ISO/IEC 17799:2005 щодо прикладів по компонентах системи захисту. Стандарт допускає використання будь-яких стратегій організації оцінки ризиків, зокрема викладених у ISO 13335-3.

Стандарт BS 7799-3 містить вступну частину, розділи з оцінки ризиків, обробці ризиків, безперервних дій з управління ризиками, а також має додаток з прикладами активів, погроз, уразливостей, методів оцінки ризиків. Стандарт дотримується самого загального поняття ризику, під яким розуміють комбінацію ймовірності події і його наслідків. Управління ризиків сформульовано як скоординовані безперервні дії з управління та контролю ризиків в організації.

Оцінка ризиків – перший етап в управлінні системи ІБ, призначеної для ідентифікації джерел ризиків і визначення його рівня значущості. Оцінку розбивають на аналіз ризиків та оцінювання ризиків. У рамках аналізу проводиться інвентаризація та катетеризація ресурсів, що захищаються, з'ясовуються нормативні, технічні, договірні вимоги до ресурсів в сфері ІБ. а потім, з урахуванням цих вимог, визначається вартість ресурсів. Наступним етапом аналізу ризиків є складання переліку значущих загроз та уразливостей для кожного ресурсу та обчислення ймовірності їх реалізації. Стандарт допускає двояке тлумачення поняття загрози ІБ: як умова реалізації вразливості ресурсу, і, як загальне, потенційна подія, здатна призвести до компрометації ресурсу. Оцінювання ризику проводиться шляхом його обчислення і порівняння з заданою шкалою. Обчислення ризику полягає в множенні ймовірності

компрометації ресурсу на значення величини збитку, пов'язаного з його компрометацією. BS 7799-3 допускає використання як кількісних, так і якісних методів оцінки ризиків, але, на жаль, в документі немає обґрунтування та рекомендацій по вибору математичного і методичного апарату оцінки ризиків ІБ. Додаток до стандарту містить єдиний приклад, який умовно можна віднести до якісного методу оцінки. Даний приклад використовує трьох-і п'ятибальні оціночні шкали:

- оцінюються рівні вартості ідентифікованого ресурсу за п'ятибальною шкалою: «незначний», «низький», «середній », «високий», «дуже високий»;
- оцінюються рівні можливості загрози за трибальною шкалою: «низький», «середній », «високий»;
- оцінюються рівні ймовірності вразливості: «низький», «середній », «високий»;
- за заданою таблицею розраховуються рівні ризику;
- проводиться ранжування інцидентів за рівнем ризику.

Після того як ризик оцінений, повинно бути ухвалено рішення щодо його обробки – точніше, вибору та реалізації заходів та засобів з мінімізації ризику. Крім оціненого рівня ризику, при прийнятті рішення можуть бути враховані витрати на впровадження та супровід механізмів безпеки, політика керівництва, простота реалізації, думка експертів та ін.

У результаті обробки ризику залишається так званий залишковий ризик, щодо якого приймається рішення про завершення етапу відпрацювання ризику. На жаль, в стандарті BS 7799-3 нічого не сказано про ефективність заходів, засобів і сервісів, які можуть бути використані при обробці ризику.

Розділ 7 BS 7799-3 «Безперервна діяльність з управління ризиками» відповідає на наступні дві фази менеджменту системи: контроль ризику та оптимізація ризику. Для контролю ризику рекомендуються технічні заходи (моніторинг, аналіз системних журналів та виконання перевірок), аналіз з боку керівництва, незалежні внутрішні аудити ІБ. Фаза оптимізації ризику містить

переоцінку ризику і, відповідно, перегляд політик, керівництва з управління ризиками, корегування та оновлення механізмів забезпечення безпеки.

Процедури контролю ризиків і оптимізації, включаючи використання політик, заходів і засобів безпеки, ідентифікацію ресурсів, загроз та вразливостей, документування, гармонізовані з ISO/IEC 27001 та 27002. Відмінною рисою стандарту є принцип обізнаності про процеси оцінки, відпрацювання, контролю та оптимізації ризиків в організації. На кожному етапі управління ризиками передбачено інформування всіх учасників процесу управління безпекою, а також фіксування подій СУІБ. Стандарт перераховує обов'язки і задає вимоги до категорії осіб, що безпосередньо беруть участь при управлінні ризиками, а саме: експертам з оцінки ризиків, менеджерам з безпеки, менеджерам ризиків безпеки, а також власникам ресурсів і навіть керівництву організації [9]<sup>1</sup>.

Основними видами інформаційних активів, які зачіпаються при управлінні інформаційними ризиками, відповідно до документа, є: процеси та служби інформаційної системи; програмне забезпечення; технічні засоби; людські ресурси; нематеріальні ресурси – репутація, імідж організації, а також інші нематеріальні фактори, що впливають на ведення бізнесу.

Наведений у стандарті метод оцінки ризиків є універсальним, але при цьому не передбачає використання якоїсь певної методології оцінки ризиків. Це породжує певну неоднозначність у виборі методів управління ризиками.

В основі наведеного в стандарті методу оцінки зазвичай лежать зважені якісні оцінки. Природно, такий метод не позбавлений недоліків, а саме:

- проблеми завдання масштабу при побудові якісних шкал;
- проблеми адекватності експертної оцінки;
- неможливості визначити, які параметри системи і якою мірою впливають на загальний рівень ризику.

---

<sup>1</sup> [9] Марков А. Нормативный вакуум информационной безопасности / А. Марков, В. Цирлов // Открытые системы. – 2007. – №8.

Це ускладнює управління ризиками та говорить про актуальність розробки універсальної методології оцінки та управління інформаційними ризиками, яка б дозволяла спільно використовувати аналітичні та якісні методи.

### **2.3 Аналіз існуючих методів оцінювання та управління ризиками інформаційної системи**

Як показує огляд інформаційних джерел, у галузі оцінки та управління інформаційними ризиками на даний момент переважають експертні методи їх оцінки. Це обумовлено, перш за все, відсутністю узагальнених статистичних даних по реалізації загроз в інформаційній сфері для систем. Часто доводиться використовувати достовірну статистику спільно з експертними оцінками. Експертні оцінки зазвичай є оцінки ймовірності настання подій, а також приблизні значення збитку відповідні цим подіям. На основі цих даних проводиться розрахунок ризику системи. Таким чином, для управління ризиками оцінка суб'єктивної ймовірності є ключовим моментом [10]<sup>1</sup>.

Застосування методів експертної оцінки має очевидні недоліки, такі, як їх суб'єктивність, великі похибки при використанні їх в аналітичних розрахунках.

Необхідно відзначити також існуючі кількісні методи, що призначені для оцінок ризику. Вони зазвичай використовують накопичену статистику і оперують з ймовірностями, отриманими в результаті статистичних розрахунків [11]<sup>2</sup>. Недоліком таких методів є необхідність накопичення досить великих обсягів статистичних даних для отримання точних прогнозів щодо рівня ризику [12]<sup>3</sup>.

---

<sup>1</sup> [10] Петренко С.А. Управление информационными рисками: Экономически оправданная безопасность / С.А. Петренко, С.В. Симонов. – М.: АйТи-Пресс, 2004. – 381 с.

<sup>2</sup> [11] 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.

<sup>3</sup> [12] 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.

Застосування згаданих нормативних актів передбачає, як правило, часткову зміну ІТ-інфраструктури організації і, в тому числі, перебудову системи ІБ як частини цієї інфраструктури, а також зміну підходу до її побудови [12]<sup>1</sup>, [13]<sup>2</sup>. Вплив даних нормативних актів на формування СУІБ компаній має непрямий характер, але підштовхує керівництво замислитися про те, наскільки дії і засоби, що застосовуються в цілях захисту інформації, адекватні та ефективні. Будь-який стандарт робить компанію більш прозорою для взаємодіючих з нею контрагентів, так як повідомляє про те, що параметри в цій організації відповідають певним нормативам – перевірено та підтверджено авторитетним джерелом. Це може відноситися до якості продукції, методів управління, і, в тому числі, до системи ІБ.

#### **2.4 Оцінка відповідності сучасних WEB-серверів вітчизняним нормативним документам в галузі захисту інформації**

Що стосується державного регулювання захисту Web-ресурсів в Україні, то це питання обмежується нормативними документами технічного захисту інформації розробленими Державною службою спеціального зв'язку та захисту інформації, основним з яких в даному випадку є НД ТЗІ 2.5-010-03 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу» [14]<sup>3</sup>.

Згідно з визначеними НД ТЗІ 2.5-004-99 специфікаціями він встановлює мінімально необхідний перелік послуг безпеки інформації та рівнів їх

---

<sup>1</sup> [12] 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.

<sup>2</sup> [13] 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

<sup>3</sup> [14] НД ТЗІ 2.5-010-03 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу»

реалізації у комплексах засобів захисту інформації WEB-сторінки від несанкціонованого доступу.

Мета цього НД ТЗІ – надання нормативно-методологічної бази для розроблення комплексу засобів захисту від несанкціонованого доступу до інформації WEB-сторінки під час створення комплексної системи захисту інформації.

Цей НД ТЗІ призначений для суб'єктів відносин (власників або розпорядників WEB-сторінки, операторів (провайдерів), користувачів), діяльність яких пов'язана з розробкою та експлуатацією WEB-сторінки, розробників комплексної системи захисту інформації та постачальників окремих її компонентів, а також для фізичних та юридичних осіб, які здійснюють оцінку захищеності WEB-сторінки на відповідність вимогам ТЗІ.

Встановлені цим НД ТЗІ вимоги є обов'язковими для виконання державними органами, Збройними Силами України, іншими військовими формуваннями, утвореними відповідно до законів України, Радою Міністрів Автономної республіки Крим та органами місцевого самоврядування, а також підприємствами, установами та організаціями (далі – установи) усіх форм власності під час захисту інформації, що належить до державних інформаційних ресурсів на WEB-сторінках.

Для захисту інших видів інформації власники WEB-сторінок користуються цим НД ТЗІ на власний розсуд.

У цьому НД ТЗІ використовуються терміни та визначення, що відповідають встановленим ДСТУ 2226 та НД ТЗІ 1.1-003.

Інші терміни, ужиті в цьому НД ТЗІ, мають такі значення:

Інтернет (мережа Інтернет) – сукупність мереж та обчислювальних засобів, які використовують стек протоколів TCP/IP (Transport Control Protocol/Internet Protocol), спільний простір імен та адрес для забезпечення доступу до інформаційних ресурсів мережі будь-якій особі;

Оператор (провайдер, provider) – юридична або фізична особа, яка надає користувачам доступ до мережі Інтернет;



Броузер (browser) – програмне забезпечення, що надає інтерфейс для доступу до інформації WEB-сторінок та їх перегляду;

Робоча станція (клієнт мережі) – окрема (персональна) ЕОМ або віддалений термінал мережі, з яких користувачі отримують доступ до ресурсів мережі Інтернет;

Сервер (server) – об'єкт комп'ютерної системи (програмний або програмно-апаратний засіб), що надає послуги іншим об'єктам за їх запитом;

WEB-сервер – сервер, який обслуговує запити користувачів (клієнтів) згідно з протоколом HTTP (Hyper Text Transfer Protocol), забезпечує актуалізацію, збереження інформації WEB-сторінки, зв'язок з іншими серверами;

WEB-сторінка (WEB-сайт) – мережевий інформаційний ресурс, що надається користувачу у вигляді HTML-документу і має у мережі свою унікальну адресу;

HTML-документ – файл текстової або нетекстової природи (звук, відео, зображення), створений за допомогою мови гіпертекстової розмітки HTML (Hyper Text Mark-up Language);

Посилання (гіпертекстове посилання) – адреса іншого мережевого інформаційного ресурсу у форматі URL (Universal Resource Location), який тематично, логічно або будь-яким іншим способом пов'язаний з документом, у якому це посилання визначене.

Відповідно до цього НД ТЗІ, СЗІ повинна забезпечувати реалізацію вимог із захисту цілісності та доступності розміщеної на WEB-сторінці загальнодоступної інформації, а також конфіденційності та цілісності технологічної інформації WEB-сторінки.

Технологія оброблення інформації повинна відповідати вимогам політики безпеки інформації, визначеної для КС, що забезпечує функціонування WEB-сторінки.

Вимоги щодо забезпечення цілісності загальнодоступної інформації WEB-сторінки та конфіденційності й цілісності технологічної інформації вимагають застосування технологій, що забезпечують реалізацію

контрольованого і санкціонованого доступу до інформації та заборону неконтрольованої й несанкціонованої її модифікації.

Технологія оброблення інформації повинна бути здатною реалізовувати можливість виявлення спроб несанкціонованого доступу до інформації WEB-сторінки та процесів, які з цією інформацією пов'язані, а також забезпечити реєстрацію в системному журналі визначених політикою відповідної послуги безпеки подій (як НСД, так і авторизованих звернень).

У процесі еволюції технологій і систем захисту інформації (СЗІ) виникла необхідність уніфікувати вимоги до їх створення та забезпечити деяку стандартизацію. Одним з найважливіших підсумків цієї роботи став міжнародний стандарт ISO/IEC 15408, так звані «Загальні критерії», що отримав визнання в багатьох країнах світу. Паралельно з критеріями захищеності, що оперують в якості мети оцінки сукупності програмно-апаратних засобів, розвивався напрямок стандартизації в частині менеджменту ІБ, результатом чого стало затвердження міжнародного стандарту ISO/IEC 27001 [15]<sup>1</sup>. Впровадження системи управління інформаційною безпекою (СУІБ) відповідно до цього стандарту дозволяє правильно організувати процес захисту інформаційних ресурсів (ІР) та управління ризиками для цих ресурсів.

Україна на цьому шляху обрала власний вектор розвитку, розробивши серію нормативних документів (НД) системи технічного захисту інформації (ТЗІ) та фактично не приєднавшись до загальносвітового процесу стандартизації в частині менеджменту ІБ [16]<sup>2</sup>. Так, й донині ключовим серед НД ТЗІ є документ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних систем від несанкціонованого доступу». Документ ґрунтується на

---

<sup>1</sup> [15] ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements. [Електрон. ресурс]: – Режим доступу: <http://www.itgovernance.co.uk/standards.arx>.

<sup>2</sup> [16] Гавриленко О.В. Відповідність національної нормативної бази у сфері технічного захисту інформації міжнародним стандартам: зіставлення документів, шляхи гармонізації. Матеріали XVII Міжнародної науково-практичної конференції «Безпека інформації у інформаційно-телекомунікаційних системах», м.Київ, 2015.

«Канадських критеріях захищеності» 1993 року [17]<sup>1</sup> та регламентує створення на об'єктах інформаційної діяльності (ОІД) комплексних систем захисту інформації (КСЗІ). При цьому власне визначення КСЗІ, як взаємозалежної сукупності організаційних та інженерно-технічних заходів, засобів і методів захисту інформації наводиться в Законі України «Про захист інформації в інформаційно-телекомунікаційних системах» [18]<sup>2</sup>. Статус державного стандарту в частині менеджменту ІБ у нашій країні отримала при цьому тільки перша версія ISO/IEC 27001. Питання практичної застосовності цього документу залишається актуальним, але, тим не менш, слід зауважити, що зазначений стандарт у вигляді вимог СОУ Н НБУ 65.1 СУІБ 1.0: 2010 [19], [20]<sup>3</sup> нині є обов'язковим у банківській сфері.

Отже, на цей момент в Україні одночасно існують дві парадигми систем захисту: КСЗІ і СУІБ в банківській сфері.

Головними групами інцидентів, які можуть призвести до припинення обслуговування клієнтів або розголошенню їх персональних даних згідно схеми, запропонованої Конвенцією Ради Європи 2001 року по боротьбі з кіберзлочинністю, є:

- 1) інциденти, спрямовані проти конфіденційності, цілісності й доступності комп'ютерних даних і систем;
- 2) шахрайство та підробки, пов'язані з використанням ПЕОМ;

---

<sup>1</sup> [17] НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу». [Електрон. ресурс]: – Режим доступу: [http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art\\_id=40386&cat\\_id=38835](http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40386&cat_id=38835).

<sup>2</sup> [18] Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 року № 80/94-ВР, Відомості Верховної Ради України (ВВР), 1994, № 31. – с.286

<sup>3</sup> [19] СОУ Н НБУ 65.1 СУІБ 1.0:2010. Настанова. Методи захисту в банківській діяльності. Система управління інформаційною безпекою. [Електрон. ресурс]: – Режим доступу: <http://www.uk.xlibx.com/4yuridicheskie/1354389-1-sou-nbu-651-suib-10-2010-standart-organizacii-ukraini-nastanova-metodi-zahistu-bankivskiy-diyalnosti-siste.php>.

[20] НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі». [Електрон. ресурс]: – Режим доступу: [http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art\\_id=46074&cat\\_id=38835](http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=46074&cat_id=38835).

3) інциденти, пов'язані з розміщенням у мережах протиправної інформації;

4) інциденти відносно авторських і суміжних прав.

Зловмисниками такі дії реалізуються згідно діаграми, поданої на рис. 1.6 [21]<sup>1</sup>.

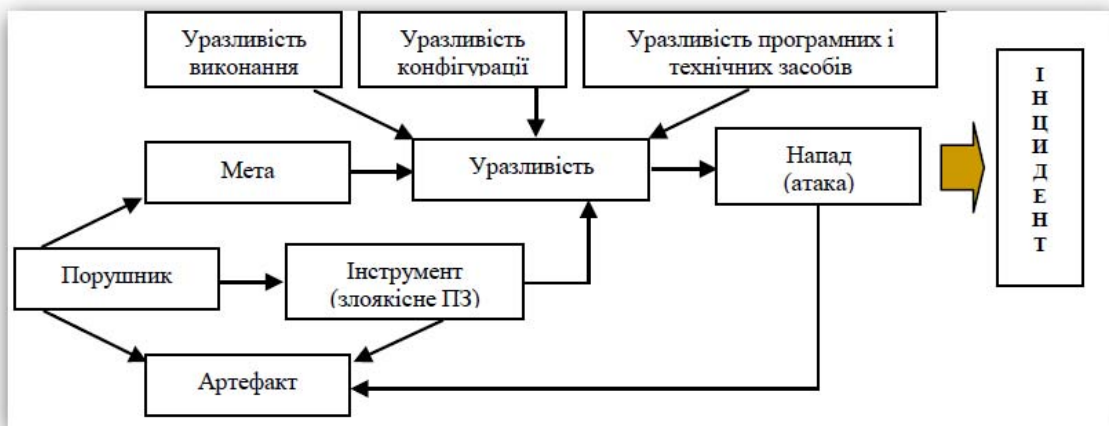


Рисунок 2.1 – Діаграма виникнення інцидентів

В умовах високої конкуренції вони неминуче можуть спричинити прямі збитки та репутаційні втрати, результати оцінки яких наведені на рис.2.2 та рис.2.3.



Рисунок 2.2 – Оцінка втрат від внутрішніх інцидентів

<sup>1</sup> [21] Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – 288 с.

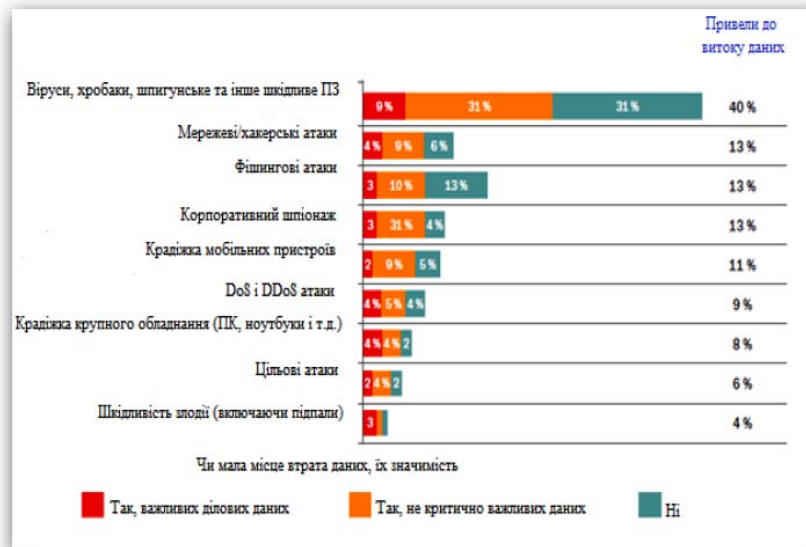


Рисунок 2.3 – Оцінка втрат від зовнішніх інцидентів

За оцінками McAfee, сукупні втрати від приведених на рис.1.7 та рис.1.8 дій можуть досягати до \$ 1 трлн. на рік. Україна від таких дій отримує у середньому збиток в розмірі \$ 200 тис. Згідно оприлюднених Лабораторією Касперського даних, за останні три роки ризик зараження через Інтернет в Україні суттєво збільшився. Цьому сприяє те, що технології реалізації атак з року в рік стають все доступнішими, а нові уразливості, в тому числі критичні, виявляються останнім часом здебільшого в самих популярних додатках, а також в ІТ-системах, обслуговуючих критичні об'єкти інфраструктури – газотранспортну систему, водопровідні мережі, електромережі й т. ін. Кількість вторгнень в ці сегменти державної економіки становить нині близько 560 тисяч на рік. Як результат за рівнем втрат у грошовому еквіваленті наша держава з 17 місця у 2012 році опустилась у 2014 на 6-ту позицію й нині входить до 10-ки країн з найбільшим ризиком зараження через Інтернет (рис.2.4).

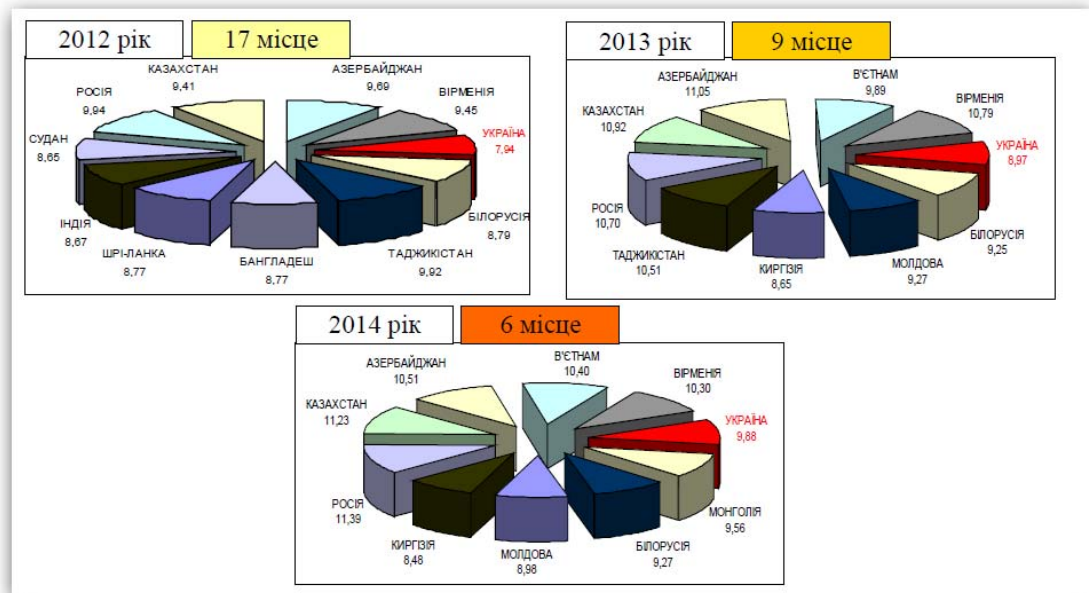


Рисунок 2.4 – Місце України у переліку країн з найбільшим ризиком зараження через Інтернет

Не зважаючи на те, що ІТ-системи об'єктів інформаційної діяльності (ОІД) будуються з урахуванням вимог щодо забезпечення найменшої уразливості до атак та унеможливлення витоку даних – перевірити їх стійкість можна тільки на практиці. Для цього застосовують, як правило, технологію проведення тестів на проникнення (пентестінгу) або інакше етичного хакінгу, яка передбачає виявлення вразливостей на ОІД та проведення контрольованих атак, спрямованих, наприклад, як на окремі інформаційні системи – CMS, CRM, ERP та інтернет клієнт-банк, так і на всю інфраструктуру ОІД в цілому – зовнішній периметр мережі (периметр ІР-адрес і Web-сайтів), бездротові мережі, внутрішню або корпоративну мережу тощо. При цьому експлуатують такі чинники, як:

- відсутність у керівництва компанії об'єктивної інформації про стан ІБ;
- нерозуміння того, якою може бути величина збитку при здійсненні хакерської атаки;
- недосконалість системи ІБ або ж відсутність комплексу заходів щодо її забезпечення.

Фактично пентестінг це ні що інше, як імітація процесу проникнення в інформаційне середовище в контрольованих рамках, або інакше – моделювання процесу банального злому з явними результатами. Його проведення дозволить: дізнатися можливості здійснення загроз безпеці інформації; оцінити наслідки спрямованої хакерської атаки; визначити уразливості в захисті інформаційної системи; оцінити ефективність засобів захисту інформації; оцінити ефективність менеджменту інформаційної безпеки; оцінити ймовірний рівень кваліфікації порушника для успішної реалізації атаки; отримати аргументи для обґрунтування подальшого вкладення ресурсів в ІБ; виробити список контрзаходів, що дозволяють знизити можливість реалізації атак. Як результат, це допоможе отримати об'єктивну інформацію про ступінь захисту ресурсів компанії та отримати, з урахуванням мотивації третьої сторони – фінансової, політичної чи моральної, реальну базу для забезпечення багаторівневої системи захисту.

## **Висновки до розділу 2**

В розділі 2 проведено аналіз нормативного забезпечення в галузі інформаційної безпеки. 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.

Означені міжнародні організації та консорціуми, які займаються розробкою нормативних документів з ІБ, присвячених керуванню інцидентами (CERT, ISO, IEC, IETF, ITU-T, IEEE, OMG, SANS Institute, X/Open).

Проведений аналіз сучасних стандартів в галузі управління інформаційною безпекою систем, а саме, розглянуті особливості застосування та призначення наступних стандартів серії ISO/IEC 27000, Стандарт BS 7799-3.

Проведений аналіз існуючих методів оцінювання та управління ризиками інформаційної системи.

Слід зазначити, 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.

Виявлено, що на цей момент в Україні одночасно існують дві парадигми систем захисту: КСЗІ і СУІБ в банківській сфері.

Головними групами інцидентів, які можуть призвести до припинення обслуговування клієнтів або розголошенню їх персональних даних згідно схеми, запропонованої Конвенцією Ради Європи 2001 року по боротьбі з кіберзлочинністю, є:

- 1) інциденти, спрямовані проти конфіденційності, цілісності й доступності комп'ютерних даних і систем;
- 2) шахрайство та підробки, пов'язані з використанням ПЕОМ;
- 3) інциденти, пов'язані з розміщенням у мережах протиправної інформації;
- 4) інциденти відносно авторських і суміжних прав.

Все це підіймає проблему захисту Web-ресурсів на якісно новий рівень.



### 3 ПРОБЛЕМАТИКА ЗАХИСТУ WEB-СЕРВІСІВ

Проблемам захисту веб-ресурсів присвячене широке коло досліджень. Наприклад, книги [22], [23]<sup>1</sup>, які повністю присвячені опису методів та інструментів атак і захисту від них. Видані з інтервалом майже в 10 років, вони наочно ілюструють зміни в підходах до захисту веб-ресурсів. Якщо в [22] стверджується про можливість забезпечення захисту від будь-яких атак на веб-ресурси, то в [23] розглянуто конкретні методи для захисту від атак. Потрібно відмітити, що методи та інструменти атак досить важко піддаються класифікації, а сама атака часто використовує технології маскуванню цих методів та інструментів.

У [24]<sup>2</sup> описано метод ідентифікації атак типу «відмова в обслуговуванні», оснований на застосуванні багатошарового персептронну, що дозволило отримати необхідну множину показників.

Розв'язання задачі детектування DDoS-атак на основі розробки спеціальної метрики є предметом статті [25]<sup>3</sup>. В роботі [26]<sup>4</sup> проаналізовано існуючі методи захисту від DDoS-атак і запропоновано новий метод, який базується на статистичному аналізі вхідного трафіка на сервері та надійній системі перевірки гіпотез.

---

<sup>1</sup> [22] Скембрейц Дж. Безопасность Web-приложений — готовые решения / Дж. Скембрейц, М. Шема. — М.: Издательский дом «Вильямс», 2003. — 384 с.

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

<sup>2</sup> [24] 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.

<sup>3</sup> [25] 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.

<sup>4</sup> [26] 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.

Розробляють також комбіновані методи захисту веб-ресурсів, основані на використанні евристичного підходу [27]<sup>1</sup>, в рамках якого виділяється аномальна поведінка, що підвищує ймовірність захисту порівняно із сигнатурним аналізом.

Перспективним також є використання моделей агента загроз для захисту веб-ресурсів від атак [28], [29]<sup>2</sup>, що дозволяє формалізувати пошук уразливостей в інформаційних системах на всіх етапах взаємодії агента загроз із веб-ресурсом.

Проблеми витоку інформації проаналізовано в [30, 31]<sup>3</sup>, де розглянуто як типові сценарії, так і методи та способи захисту від них.

У [32]<sup>4</sup> відмічено, що злам паролю залежить від наявних обчислювальних ресурсів, часу, функції, що використовується для зберігання цього пароля, а також від багатьох інших характеристик. Запропоновано загальні рамки для оцінки складності пароля й оцінки його надійності.

### 3.1 Аналіз актуальних атак на WEB-ресурси

Види атак на WEB сервіси та способи їх протидії наведені в таблиці 3.1. Найбільш популярною атакою є «Insufficient transport layer protection» —

---

<sup>1</sup> [27] Поворознюк А.И. Совершенствование защиты Web-приложений от вторжений на основе эвристического подхода / А.И. Поворознюк, М.Н. Шкарупа: сб. науч. тр. «Вестник НТУ «ХПИ». Информатика і моделювання. — 2007. — Вип. 19. — С. 145-154.

<sup>2</sup> [28] 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. Дзьобай // Научный журнал КубГАУ. — 2014. — № 101(07). — С. 1-11.

[29] Bhavani A.V. Cross-site Scripting Attacks on Android WebView / A.V. Bhavani // International Journal of Computer Science and Network. — 2013. — Vol. 2, Issue 2. — 5 p. — Режим доступу в Інтернет: <http://ijcsn.org/IJCSN-2013/2-2/IJCSN-2013-2-2-03.pdf>

<sup>3</sup> [30] Cuff P. Distributed channel synthesis / P. Cuff // IEEE. Trans. Inf. Theory. — 2013. — Vol. 59(11). — P. 7071-7096.

[31] Schieler C. Rate-distortion theory for secrecy systems / C. Schieler, P. Cuff // IEEE Trans. on Inf. Theory. — 2014. — Vol. 66(12). — P.7584-7605.

<sup>4</sup> [32] Sahin C.S. General Framework for Evaluating Password Complexity and Strength / C.S. Sahin, R. Lychev, N. Wagner. — 11 p. — Режим доступу в Інтернет: <http://arxiv.org/abs/1512.05814>

отримання даних під час передавання. Дана атака може бути виконана для 70 % ресурсів. Для виключення можливості проведення таких атак достатньо використувати протокол HTTPS.

Витік інформації («Information leakage»). Дану атаку можна виконати на 56 % ресурсів. Витік інформації з додатків виникає в результаті відмови або неправильної роботи програми, а також у разі порушення її логіки. Для виключення можливості проведення атаки необхідно ретельно тестувати програмну частину ресурсу, проводити перевірку повідомлень на стороні сервера, моніторинг оповіщень про помилки.

Таблиця 3.1 – Види WEB атак та способи їх протидії

№ за/п	Вид атаки	Вразливість веб-ресурсів, %	Протидія
1	Insufficient transport layer protection	70 %	Використання протоколу HTTPS.
2	Information leakage	56 %	Тестування програмної частини ресурсу, перевірка повідомлень на стороні сервера, моніторинг оповіщень про помилки
3	Cross-site scripting	47 %	Очищення та валідація вхідних даних
4	Brute force	29 %	Використання паролів високої складності, налаштування сервера на аналіз вхідних запитів
5	Content spoofing	26 %	Відмовитися від використання фреймів і не передавати в параметрах абсолютні або локальні шляхи до файлів
6	Cross-site request forgery	24 %	Перевірка вхідних даних з форм
7	URL redirector abuse	16 %	Валідація вхідних даних
8	Predictable resource location	15 %	Контроль доступу до файлів сервера

Атаку «Cross-site scripting» — міжсайтове використання сценаріїв, можливо виконати на 47 % ресурсів. Атака дозволяє передати JavaScript-код на виконання в браузер користувача. Атаки такого роду часто також називають HTML-ін'єкціями, адже механізм їхнього впровадження дуже схожий із SQL-ін'єкціями, але на відміну від останніх, впроваджуваний код виконується в браузері користувача. Для захисту від цього виду атак необхідно проводити очищення та валідацію вхідних даних.

Генерацію великої кількості запитів, або підбір паролів («Brute force») можливо виконати на 29 % ресурсів. Для захисту необхідно забезпечити використання паролів високої складності, налаштування сервера на аналіз вхідних запитів.

Атака «Content spoofing» — підміна даних через заміну контенту сторінок можлива для 26 % ресурсів. Використовуючи цю техніку, зловмисник змушує користувача повірити, що сторінка згенерована веб-сервером, а не передана із зовнішнього джерела. Для захисту від даного виду атак потрібно відмовитися від використання фреймів і, найголовніше, ніколи не передавати в параметрах абсолютні або локальні шляхи до файлів.

Вид атак на відвідувачів веб-сайтів, який використовує недоліки протоколу HTTP — «Cross-site request forgery». Якщо жертва заходить на сайт, створений зловмисником, браузер таємно відправляє запит на інший сервер (наприклад, на сервер платіжної системи), який здійснює якусь шкідливу операцію (наприклад, переказ грошей на рахунок зловмисника). Дану атаку можливо виконати на 24 % ресурсів. Для захисту необхідно проводити перевірку вхідних даних з форм, наприклад шляхом додавання унікального прихованого поля.

Перенаправлення на інші сайти через підміну початкових посилань («URL redirector abuse»). Цей вид вразливостей, також як і багато інших перерахованих вище, є різновидом помилок перевірки вхідних даних і можлива на 16 % ресурсів. Вирішенням є валідація вхідних даних.

Ще однією популярною атакою є «Predictable resource location» — знаходження прихованого функціоналу та даних. Доступна на 15 % ресурсів і вирішується шляхом контролю доступу до файлів сервера.

Починаючи з 2010 року: більша частина атак використовує: SQL-ін'єкції – 17.9%, XSS – 13.7%, DDoS – 6.2%, розкриття інформації – 4.6%, передбачуваність інформаційного ресурсу – 4.4%, Brute force – 3.9%, вгадування сесій – 3.2%. Інші – CSRF, фішинг, шкідливе ПЗ, викрадення DNS, викрадення облікових записів і т. д. [36]<sup>1</sup>. З кожним роком статистика атак змінюється, так у 2014 році найпопулярнішою була атака «Cross-site scripting», а в 2013 — Витік інформації («Information leakage»).

На лютий 2016 р. лідируючим стало викрадення даних (12%), а ін'єкції досягли аж 10,7%. Збільшилась кількість спрямованих атак (9,3%) і шкідливе програмне забезпечення (6,7%). Атаки типу DDoS значно менше використовуються, як і спотворення веб-сайтів (4%) [37]<sup>2</sup>. На березень 2016 р. викрадення даних стало номером один серед відомих векторів атак з 20,7% (було 12%). Ін'єкції продовжують лідирувати з 9,8% (у лютому було 10,7%), такий же відсоток спрямованих атак (було 9,3%). DDoS трохи більше використовувалось (7,6%), поширення шкідливого ПЗ через рекламу (5,4%). Спотворення сайтів та шкідливе ПЗ 3,3%.

Виходячи з наведених даних, можна зробити висновки про те, що для захисту від більшості популярних видів атак достатньо належним чином перевіряти вхідні дані. Також рекомендовано використовувати шифрований протокол HTTPS та будувати програмний додаток ресурсу на одному з відомих програмних каркасів (Framework), в якому вбудовані механізми перевірки, шифрування та валідації. Найкращим методом захисту від атак на мережеві

---

<sup>1</sup> [36] Web Application Security Statistics [Електронний ресурс] – Режим доступу до ресурсу: <http://projects.webappsec.org/f/wasc-wafec-v1.0.pdf>

<sup>2</sup> [37] HACKMAGEDDON – статистика інформаційної безпеки [Електронний ресурс] – Режим доступу до ресурсу: <http://www.hackmageddon.com>

служби, наприклад, DoS та DDoS є використання хмарних технологій і перевірених конфігурацій серверів.

Як свідчать статистичні результати [33]<sup>1</sup> та запропоновані методи, які орієнтовані на захист від конкретного типу атаки, зловмисна дія на веб-ресурс відбувається, як правило, із використанням відразу декількох різних типів атак. Тому задачею системи менеджменту інформаційної безпеки є розробка ефективної стратегії протидії атакам зловмисників за умови, що вони використовують комбіновані типи атак. Рівень ефективності при цьому визначається замовником веб-ресурсу і задається він специфікою ведення бізнесу підприємством (чи діяльністю організації), параметрами, що характеризують специфіку інформації та баз даних, які належать до конфіденційних і рядом інших параметрів і характеристик. Розробка такої стратегії захисту веб-ресурсу є нетривіальною задачею.

### **Висновки до розділу 3**

В розділі 3 проведений аналіз проблем захисту WEB сервісів. З кожним роком доля уразливих WEB сервісів зростає. Для захисту від більшості популярних видів атак достатньо належним чином перевіряти вхідні дані. Також рекомендовано використовувати шифрований протокол HTTPS та будувати програмний додаток ресурсу на одному з відомих програмних каркасів (Framework), в якому вбудовані механізми перевірки, шифрування та валідації. Найкращим методом захисту від атак на мережеві служби, наприклад, DoS та DDoS є використання хмарних технологій і перевірених конфігурацій серверів.

---

<sup>1</sup> [33] Website Security Statistics Report: 2015. — WhiteHat Security, 2015. — 30 p. — Режим доступу в Інтернет: <https://info.whitehatsec.com/Website-Stats-Report-2015.html>

## 4 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ WEB-РЕСУРСІВ

### 4.1 Аналіз методів тестування web-додатків

Тестування безпеки – це стратегія тестування, яка використовується для перевірки безпеки системи, а також для аналізу ризиків, пов'язаних із забезпеченням цілісного підходу до захисту програми, атак хакерів, вірусів, несанкціонованого доступу до конфіденційних даних. Дане випробування направлено на діагностику шляхів злому системи, оцінку захищеності веб-додатків або сайту, а також аналіз ризиків, пов'язаних з підходом до захисту від зловмисників, доступу до конфіденційних даних. Базуючись на принципах конфіденційності, доступності та цілісності, тестування безпеки сприяє забезпеченню збереження даних, облікових записів, доступів і підключень користувачів.

Загальна стратегія безпеки ґрунтується на трьох основних принципах: конфіденційність, цілісність, доступність. Конфіденційність – це приховування певних ресурсів або інформації. Під конфіденційністю можна розуміти обмеження доступу до ресурсу деякої категорії користувачів, або іншими словами, за яких умов користувач авторизований отримати доступ до цього ресурсу.

Існує два основних критерії при визначенні поняття цілісності.

Довіра. Очікується, що ресурс буде змінений тільки відповідним способом певною групою користувачів.

Пошкодження і відновлення. У разі коли дані пошкоджуються або неправильно змінюються авторизованим або авторизованим користувачем. Доступність є вимогою про те, що ресурси повинні бути доступні авторизованому користувачеві, внутрішньому об'єкту або пристрою. Як правило, чим більш критичний ресурс тим вище рівень доступності повинен бути.

Виділяються три підходи до виявлення вразливості веб-додатків: тестування методом чорного, сірого та білого ящиків. Різниця між ними визначається тими ресурсами, які доступні під час тестування.

Перший тип, тестування за принципом «білого ящика», передбачає наявність доступу до будь-яких ресурсів, в першу чергу до вихідних кодів, а також технічних завдань і всілякої документації.

Другий тип, тестування за принципом «чорного ящика», навпаки не вимагає ніяких знань про внутрішній устрій програми, необхідна лише можливість взаємодії з нею. Прикладом такого тестування є зовнішній аудит веб-додатків із закритим вихідним кодом.

Нарешті, третій тип, тестування за принципом «сірого ящика», має на увазі, що в розпорядженні у фахівця знаходиться виконуваний файл і, можливо, якась базова документація. Далі кожен тип буде розглянуто більш докладно.

#### **4.1.1 Принцип «білого ящика»**

Аудит вихідного коду. Аудит вихідного коду може бути виконаний або вручну, або з використанням засобів автоматизації. З урахуванням того, що сучасні програми можуть досягати обсягу в сотні тисяч рядків програмного коду, повністю ручний аналіз представляється недостатньо ефективним. Засоби автоматизації здатні позбавити аналітика від необхідності ретельно вивчати кожен рядок коду програми, проте вони виявляють лише потенційно вразливі або підозрілі ділянки. Кожна така ділянка повинна бути згодом розглянута вручну. Не існує методу виявлення уразливостей, який був однозначно краще за інших. Для отримання найкращих результатів необхідно використовувати всі можливі підходи.

Тестування методом «білого ящика» має суттєву перевагу – це покриття коду. Оскільки вихідні коди доступні, то можуть бути проаналізовані на предмет наявності потенційних уразливостей.



До недоліків даного методу можна віднести складність, адже існуючі інструменти неідеальні і видають велику кількість помилкових спрацьовувань. Тому звіт, сформований в результаті роботи програми, повинен бути ретельно вивчений компетентним фахівцем. Враховуючи обсяг коду, який містять сучасні програми, такі звіти можуть досягати величезної довжини.

#### **4.1.2 Принцип «чорного ящика»**

Під принципом «чорного ящика» мається на увазі, що аналітик може лише спостерігати за поведінкою додатків, тобто контролювати вхідні дані, що надходять в програму, і аналізувати вихідні дані, але не має уявлення про її внутрішню структуру. Зазвичай така ситуація виникає в процесі аудиту віддалених веб-додатків.

Ручне тестування. Розглянемо приклад веб-додатків. У цьому випадку при ручному тестуванні дослідник за допомогою звичайного інтернет-браузера переміщається по сторінках додатків, підставляючи в поля введення і параметри запитів спеціальні символи, наприклад, символ одинарної лапки для виявлення потенційно уразливих до SQL-ін'єкцій сценаріїв.

В даний час ручне тестування без використання засобів автоматизації вважається неефективним.

Автоматизоване тестування (фаззінг). Незважаючи на те, що в основі фаззінга лежить метод грубої сили, недолік при такому підході компенсується його простотою і ефективністю. По суті фаззінг – це передача для обробки досліджуваному додатком великої кількості випадкових вхідних даних і аналіз результатів його роботи.

Варто відзначити, що існують більш розвинені фаззери, які генерують неповністю випадкові вхідні дані, а спираються на специфікації досліджуваних протоколів і форматів файлів. Такі інструменти можна також віднести також категорії методів «сірого ящика».

До переваг тестування за принципом «чорного ящика» відносять:

**Доступність.** Даний метод можна застосовувати в будь-яких ситуаціях і він може бути корисний навіть у тому випадку, якщо доступні вихідні коди програми.

**Універсальність.** Так як підхід не спирається на будь-які відомості про конкретний програмний продукт, інструмент, створений, наприклад, для оцінки безпеки одного веб-сервера, може використовуватися і для будь-якого іншого.

**Простота.** На самому елементарному рівні фаззінг не вимагає ніяких знань про внутрішню структуру програми. Зрозуміло, однак, що найбільш складні помилки таким способом виявити практично неможливо.

Даний метод тестування має і ряд недоліків.

**Покриття.** Одне з найбільш складних питань, яке необхідно вирішити в процесі фаззінга, це коли необхідно припинити тестування і наскільки воно ефективно.

**Примітивність.** Фаззінг погано справляється з виявленням складних уразливостей, таких, які займають кілька етапів щоб помістити програму в певний стан і з нього викликати помилку. Такі вразливості як правило виявляють за допомогою аналізу вихідного коду.

### **4.1.3 Принцип «сірого ящика»**

Тестування за принципом «сірого ящика» являє собою комбінацію методів, що використовуються при тестуванні за принципом «чорного ящика», а також технологій і прийомів реверс розробки. Цінність вихідного коду в процесі пошуку уразливостей полягає в тому, що він представляє логіку роботи програми в зрозумілому для дослідника поданні.. Основна мета аналізу – визначення внутрішньої логіки роботи захищеного додатки. Не існує інструмента, що дозволив би отримати оригінальний вихідний код з захищеного файлу (обфускація). Однак, за допомогою засобів реверс розробки можливо

представити програму у вигляді, який доступний для сприйняття, хоча це не повноцінний вихідний код.

Даний метод успадковує одну з переваг тестування за принципом «чорного ящика» – доступність. Ще одною істотною перевагою є покриття коду. Інформація, отримана в результаті реверс аналізу, здатна істотно поліпшити якість вхідних даних, які генеруються фаззером.

Великим недоліком даного методу є його складність. Серед розглянутих технологій пошуку вразливостей дана пред'являє найвищі вимоги до кваліфікації аналітика.

## **4.2 Комплекс засобів захисту Web-сервісів**

Для захисту від WEB-атак класичним пристроєм є Web Application Firewall. Міжмережний екран веб-додатків (Web Application Firewall) 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 веб-серверами.

В набір функцій WAF зазвичай входять такі типові механізми захисту:

- валідація протоколу;
- сигнатурний аналіз;
- захист сесій та cookie;
- блокування витоку даних;
- розпізнавання атак (з негативної моделі, атаки на додатки, мережу, веб-сервер і атаки на ОС);
- можливість створення власних правил захисту;
- машинне навчання.

### **4.2.1 Вимоги до сучасного Web Application Firewall**

Загальні вимоги до сучасного Web Application Firewall:

- системні компоненти WAF повинні відповідати вимогам PCI DSS;
- можливість реагування на загрози, описані в OWASP Top 10;
- інспектування запитів і відповідей відповідно до політики безпеки;
- журнал роботи подій;
- запобігання витоку даних – інспекція відповідей сервера на наявність критичних даних;
- інспектування всього вмісту веб-сторінок, включаючи HTML, DHTML і CSS, а також протоколів доставки вмісту (HTTP / HTTPS);
- інспектування будь-якого протоколу або конструкції даних, що використовуються для передачі даних веб-додатків;
- захист від загроз, спрямованих безпосередньо на WAF;
- підтримка SSL/TLS-термінації з'єднання;
- запобігання або виявлення підробки ідентифікатора сесії;
- автоматичне оновлення сигнатур атак і застосування їх;
- підтримка пристроєм клієнтських SSL-сертифікатів;
- підтримка апаратного зберігання ключів (FIPS).

З наведеного (Таблиця 3.1) зробимо висновок про недоліки системи, а саме про нездатність WAF протистояти деяким видам атак.

Таблиця 3.1 – Ефективність WAF відносно різних типів атак

<b>Типи атак</b>	<b>Чи блокує такі атаки WAF</b>
Атаки направлені на викрадання даних	Блокує
Ін'єкції	Блокує
Цілеспрямована атака	Може блокувати, а може і ні, в залежності від атаки
DDoS	Може бачити активність в мережі і зменшувати кількість запитів до ресурсу за певний час. але фактично не блокує
Ураження шкідливим ПЗ	Може блокувати, а може і ні, в залежності від атаки
Атаки на компоненти з відомими вразливостями	Може блокувати, а може і ні, в залежності від атаки
XSS	Блокує

Типи атак	Чи блокує такі атаки WAF
SYN-flood	Не блокує
Атаки, спрямовані на викрадання сесії користувача	Блокує
TCP-flood	Не блокує
UDP-flood	Не блокує
CSRF	Блокує

Даних загальних функцій WAF недостатньо для повного захисту інтернет-ресурсів, так, як WAF не захищає від атак низького рівня, таких, як, наприклад DDoS, SYN-flood, TCP-flood, UDP-flood. Таким чином виникає потреба в додатковому захисті, а саме в створенні комплексу для покращення системи безпеки захисту веб-ресурсів.

#### 4.2.2 Використання IPS систем та Firewall

Для покращення роботи системи безпеки веб-ресурсів необхідно створити захист від атак низького рівня. Для цього можна використати системи IPS та Firewall. Firewall буде формувати доступ до портів та забезпечувати мінімальний захист, IPS буде відстежувати атаки низького рівня та реагувати на зміни потоків трафіку.

Intrusion Prevention System (система протидії вторгнень) – система, яка розпізнає ознаки вторгнення, виявляє атаки і запобігає їм. Під час аналізу використовуються різні методи виявлення атак – сигнатурний, поведінковий і ідентифікація аномалій в протоколах [24]<sup>1</sup>.

Також, всі види IPS технологій, як правило, виконують наступні функції:

- IPS зупиняє саму атаку.
- Блокує зловмисну частину, дозволяючи неураженій частині проникати до системи.

<sup>1</sup> [24] 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.

- Повідомляють адміністраторів безпеки у разі важливих подій, що спостерігаються у системі
- Реагують на інциденти, змінюючи середу безпеки для зривання атаки.
- Створюють звіти.

Загальні вимоги до IPS та типи подій, які найбільш часто виявляються:

- Дослідження і атаки прикладного рівня (наприклад, переповнення буфера, підбір пароля, передача шкідливих програм). Більшість мережевих IPS аналізують протоколи додатків.
- Дослідження і атаки транспортного рівня (наприклад, сканування портів, незвичайна фрагментація пакетів, SYN floods). Найбільш часто аналізуються протоколи транспортного рівня – TCP і UDP.
- Дослідження і атаки мережевого рівня (наприклад, підміна IP-адреси, ненормальні значення заголовка IP).
- Неочікувана робота додатків (наприклад, хости виконують несанкціоновані дії).
- Порушення політики (наприклад, використання заборонених протоколів).

Firewall (міжмережний екран) – система мережної безпеки, яка відстежує і контролює вхідний і вихідний трафік на основі заздалегідь визначених правил безпеки. Міжмережний 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. Міжмережний екран контролює доступ до ресурсів мережі за допомогою позитивної моделі управління (у внутрішню мережу потрапляє тільки дозволений правилами трафік, весь інший трафік заборонений).

Загалом міжмережні екрани діляться на дві категорії:

- Міжмережні екрани мережного рівня дозволяють чи забороняють трафік, базуючись на адресах джерела IP і адресах чи портах призначення IP.
- Міжмережні екрани прикладного рівня аналізують протоколи

прикладного рівня, спостерігаючи за активністю протоколу по відношенню до визначеного профілю і дозволяють чи забороняють трафік, базуючись на відхиленнях від профілю.

Типові функції Firewall:

- Контроль доступу до вузлів в мережі
- Фільтрація доступу до незахищених служб
- Контроль порядку доступу до мережі
- Запобігає спробам доступу з зовнішньої і з внутрішньої мережі
- Перешкоджання отримання закритої інформації із внутрішньої захищеної мережі. Таблиця 3.2 зображує на якому рівні моделі OSI працює кожна з систем.

Таблиця 4.2 – Робота систем комплексу на моделі OSI

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

Таким чином, в комплексі, системи будуть захищати інтернет-ресурси на всіх рівнях моделі OSI.

На рисунку 4.1 зображена схема запропонованої інтеграції систем. WAF впроваджується в систему в режимі зворотнього проксі-сервера перед захищеними веб-серверами. IPS впроваджується в комплекс в режимі Transparent. Отримуючи запити, допущені Firewall, IPS аналізує протоколи і зупиняє певні види атак, надалі дані передаються до WAF, де обробляються і також блокуються атаки функціоналу WAF.

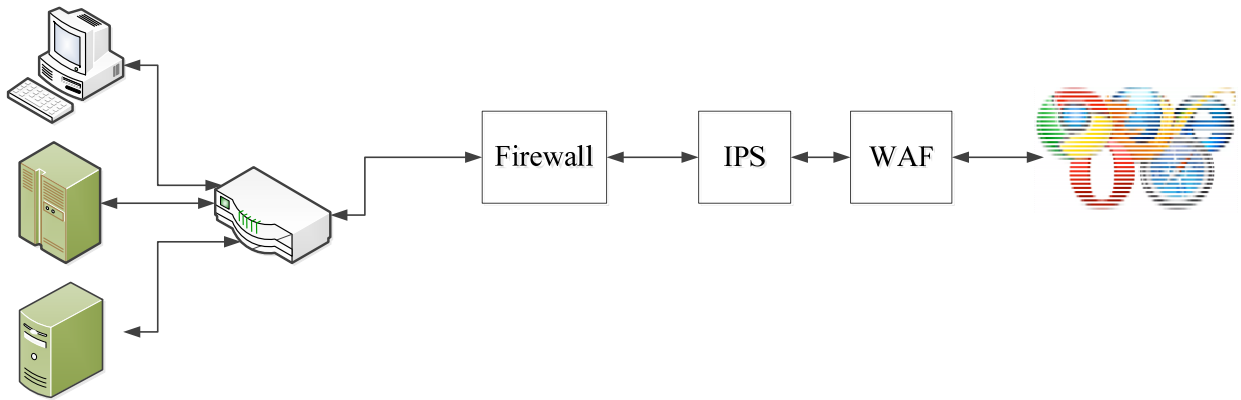


Рисунок 4.1 — Схема інтеграції систем з Web Application Firewall

Відповіді веб-сервера знову повертаються до WAF, де перевіряються на наявність витоку даних. Після перевірки, дані ідуть до користувача.

Використання даної комплексної системи захисту інтернет-ресурсів у складі Firewall, IPS та WAF забезпечує на 30% більшу ефективність ніж використання звичайного WAF. Використання сучасних високопродуктивних Firewall та IPS дозволить блокувати потрапляння шкідливих файлів у внутрішню захищену мережу, забезпечить додаткову безпеку і зменшить ризики цілеспрямованих атак на ІТ-ресурси. Даний комплекс дозволить збільшити захищеність будь-якого інтернет-ресурсу, зменшити навантаження на адміністраторів ІТ-систем, та забезпечити більш ефективну обробку легітимних користувачів інтернет-ресурсів.

#### Висновки до розділу 4

В розділі 4 проведений аналіз методів та засобів захисту WEB сервісів. Виділяються три підходи до виявлення вразливості веб-додатків: тестування методом чорного, сірого та білого ящиків. Різниця між ними визначається тими ресурсами, які доступні під час тестування. 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 веб-серверами. Але цього не достатньо, тому в роботі пропонується комплексне рішення, яке включає WAF, IPS та FIREWALL, тобто захист на всіх рівнях моделі OSI.

## 5 ПОСИЛЕННЯ РІВНЯ ЗАХИЩЕНОСТІ WEB ЗА ДОПОМОГОЮ DPI

Найефективнішою системою аналізу мережевого трафіку являється DEEP PACKET INSPECTION, яка дозволяє на найвищих рівнях моделі OSI працювати з даними для захисту систем. Потрібно не тільки констатувати інциденти а і притягувати до відповідальності порушників. Ідентифікаційну інформацію, яка «залишається» під час роботи з WEB сервісами представлена у вигляді таблиці 5.1

Таблиця 5.1 – Ідентифікаційна інформація користувача WEB

«Ідентифікатор»	Зміст ідентифікуючих даних	Спосіб анонімізації
IP-адреса	Як мінімум інформація про провайдера та країну користувача	VPN, Proxu, SSH, Tor, I2P, P2P- анонімайзери
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 підключенні до публічної Wi-Fi 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 неузgodженої активності в анонімному сеансі

Ще одним випадком деанонізації користувача є передавання програмним забезпеченням, зокрема оглядачами (браузерами), різного роду даних, що зазвичай передбачено специфікацією до програмного продукту.

Типовий оглядач містить наступні функціональні компоненти і технологічні категорії:

- cookies – це текстові файли з деякими даними, що їх зберігають прикладні програми для різних задач, наприклад, аутентифікації. Розкриття анонімного клієнта настає, якщо він спочатку відвідав ресурс через відкритий сеанс, браузер зберіг cookies, а потім користувач з'єднався через анонімний сеанс. В результаті серверу доступно співставлення cookies і, як наслідок, деанонізація клієнта;
- Flash, Java – плагіни, що ґрунтуються на цих технологіях, завантажуються від імені користувача як окреме програмне забезпечення та можуть працювати в обхід проксі, зберігати свої cookies й інші налаштування;
- відбиток (fingerprint) браузера – оглядач представляє серверу десятки категорій даних, що дає змогу сформувати унікальний цифровий відбиток браузера, за яким його можна ідентифікувати серед багатьох інших навіть в анонімному сеансі (найчастіше застосовується з метою цільової реклами);
- скрипти JavaScript – код, що виконується на стороні клієнта, здатен накопичувати для сервера ідентифікуючу інформацію, а також, за умови вразливості цільового для користувача ресурсу, створює умови для проведення успішних атак на інформаційний ресурс;
- http-referrer – за допомогою цього http-заголовку цільовий для користувача веб-сайт може визначити, ким було сформовано трафік.

Вирішенням цієї проблеми є налаштування параметрів безпеки оглядача, включаючи блокування кожної із наведених категорій ідентифікації даних, та відмова під час анонімного сеансу від неперевіреного програмного забезпечення.

Система Deep Packet Inspection (DPI, також complete packet inspection і Information eXtraction або IX) — технологія накопичення статистичних даних, перевірки і фільтрації мережевих пакетів по їх вмісту. 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. Deep Packet Inspection здатна виявляти і блокувати віруси, фільтрувати інформацію, що не задовольняє заданим критеріям, виконує глибокий аналіз усіх пакетів, що проходять через неї. Система DPI здійснює так званий поведінковий аналіз трафіку, який дозволяє розпізнати додатки, що не використовують для обміну даними заздалегідь відомі заголовки і структури даних.

За допомогою DPI спецслужби можуть вести спостереження за мережевою активністю того або іншого користувача та аналізувати VPN, HTTPS трафік. Система DPI може зібрати різну інформацію, не порушуючи особистих прав користувача

DPI може захистити від:

- Спам-ботів (виявляються на основі аналізу SMTP трафіку).
- DoS і DDoS-атак (виявляються за аномаліями трафіку).
- Зараження вірусами (виявляється за сигнатурами).

Захист від спаму реалізується шляхом блокування відправника, коли з однієї адреси генерується надмірно велика кількість SMTP -запитів.

Система DPI дозволяє захиститися від TCP SYN Flood і Fragmented UDP Flood.

Атака SYN flood викликає підвищену витрату ресурсів системи, оскільки на кожний SYN-пакет, що входить, система повинна зарезервувати певні ресурси в пам'яті або згенерувати велику кількість пакетів, що призводить до її відмови.

DPI виявляє перевищення порогу SYN-запитів, та замість сайту відповідає на них.

Fragmented UDP Flood атака здійснюється фрагментованими udp-пакетами, зазвичай невеликого розміру, на обробку і аналіз яких витрачається багато ресурсів.

DPI відкидає неактуальні для сайту протоколи або обмежує їх по смузі пропускання (для веб-сайту залишаються тільки протоколи HTTP і HTTPS).

Для опису роботи системи DPI необхідно заглибитися в питання архітектури, але воно досить складне і заслуговує окремого розгляду. У рамках даної роботи представимо DPI у вигляді етапів роботи з пакетами, показаними на (рис. 4.1): прийом мережевою картою і фільтрація пакетів, виділення потоків трафіку, вилучення даних пакету (0,3% часу роботи процесора) і завантаження сигнатур з БД (7,6% часу роботи процесора), обробка даних алгоритмами (8,7% часу роботи процесора) і порівняння з сигнатурами (83% часу роботи процесора).

Комбінатор рішень дає алгоритмам початкові дані і вибирає найбільш достовірне рішення. Далі відбувається співвідношення пакету з певним потоком трафіку. У [33]<sup>1</sup> була проведена оцінка відсоткового відношення необхідного часу роботи процесора для виконання цих етапів, яка показала, що 83% займає етап порівняння даних пакету з сигнатурами.

Якщо на етапі виділення потоків пакет належить існуючому потоку даних, то він передається на апаратний фільтр.

Зазвичай на етапі аналізу даних пакету алгоритмами обробки спочатку проводиться аналіз 2-4-го рівнів і заголовків тунелів, далі відбувається порівняння інформації 5-7-го рівнів з базою сигнатур додатків (що містить більше 1000 прикладів).

---

<sup>1</sup> [33] Website Security Statistics Report: 2015. — WhiteHat Security, 2015. — 30 p. — Режим доступу в Інтернет: <https://info.whitehatsec.com/Website-Stats-Report-2015.html>



Рисунок 5.1 – Аналіз пакетів DPI з використанням комбінатора рішень

Для нового виявленого потоку призначена політика виконується на апаратному фільтрі, в якому (режим розвантаження) не ведеться аналіз 5-7-го рівнів, але робиться підрахунок трафіку для заданого застосування [25]<sup>1</sup>.

Окрім режиму аналізу пакетів, що надходять в даний момент, DPI -системи можуть працювати в режимі навчання, в якому аналізуються приклади різномірних помічених потоків трафіку. Режим навчання має наступні етапи: захоплення пакетів, зчитування міток істинних значень потоків трафіку, отримання сигнатур і запис в базу даних (БД).

Для систем DPI важливо забезпечити задану тривалість обробки пакетів і її стабільність. Також складним завданням виступає підтримка стабільності імовірно-тимчасових характеристик в умовах роботи на граничній продуктивності.

Зазвичай аналіз і вилучення необхідної інформації вимагають значних обчислювальних ресурсів. Чим вони вищі, тим менше буде тривалість обробки пакетів, а значить, менше буде величина затримки проходження нового потоку даних через систему DPI. Крім того, робота апаратного фільтру також вносить певну затримку при проходженні пакетів. Якщо навантаження на систему DPI

<sup>1</sup> [25] Фаткиєва Р.Р. Разработка метрик для обнаружения атак на основе анализа сетевого трафика / Р.Р. Фаткиєва // Вестник Бурятского государственного университета. — 2013. — Vol. 9. — С. 81-86.

почне перевищувати певний поріг, то це приведе до збільшення затримки, втрати пакетів і в крайньому випадку – до пропуску трафіку без його аналізу.

Щоб оцінити доцільність застосування технології DPI для забезпечення QoS, необхідно розробити її математичну модель. Для побудови простої математичної моделі, що представляє систему масового обслуговування (СМО), треба ще раз спростити етапи обробки трафіку системою DPI. Допустимо, що сервер аналізу трафіку використовує тільки перший пакет потоку, що поступає з апаратного фільтру, і по ньому визначає необхідну політику і передає далі на апаратний фільтр. Позначимо середню затримку пакету при аналізі як  $T_1$ . Проте в деяких випадках сервер аналізу трафіку посилає запит на необхідну політику до сервера ухвалення рішень про застосування політики. У такому разі середня затримка ( $T_2$ ) буде сумою затримок в чергах і затримок обробки на сервері ухвалення рішень і сервера аналізу трафіка.

В якості першої системи масового обслуговування (СМО<sub>1</sub>) позначимо багатопроцесорний сервер аналізу трафіку з чотирма опрацьовувачами. За класифікацією Кендалла M/M/V означає систему з пуассонівським вхідним потоком заявок, експоненціальним законом розподілу часу обслуговування і V – опрацьовувачами. Припущення, що сумарний вхідний потік на сервер аналізу трафіку пуассонівський, засноване на його великому числі незалежних стаціонарних потоків. Наступна СМО<sub>2</sub> – це сервер ухвалення рішень про застосування політики з одним опрацьовувачем (M/M/1). Аналогічно, використовуючи теорему Берка, можна зробити висновок, що потік, який поступає на сервер ухвалення рішень теж пуассонівський, але відрізняється від початкового з ймовірністю настання випадку звернення до цього сервера. Позначимо інтенсивність простого потоку, що входить, через  $\lambda$ .

Отримаємо модель, показану на (рис. 5.2).



Рисунок 5.2 – Спрощена аналітична модель системи DPI

Відповідно до теореми Берке, що виходить із СМO<sub>2</sub> (що працює в стаціонарному режимі) потік буде простим з тим же параметром  $\lambda$ . Інтенсивність вхідного потоку на СМO<sub>2</sub> дорівнюватиме:

$$\lambda_{ex2} = (1 - P)\lambda, \quad (5.1)$$

де  $P$  – ймовірність самостійної класифікації нового потоку сервером аналізу трафіку (СМO<sub>1</sub>). Аналогічно для СМO<sub>2</sub>. При цьому необхідно врахувати, що вимоги, які надійшли після обробки із СМO<sub>2</sub>, також потраплятимуть в чергу СМO<sub>1</sub>.

Таким чином, інтенсивність вхідного потоку на СМO<sub>1</sub> після обробки СМO<sub>2</sub> дорівнюватиме:

$$\lambda_{ex12} = (1 - P)\lambda, \quad (5.2)$$

В результаті загальна інтенсивність надходження пакетів на сервер аналізу трафіку (СМO<sub>1</sub>) визначається виразом:

$$\lambda_{ex1} = \lambda + (1 - P)\lambda, \quad (5.3)$$



Продуктивність СМО<sub>1</sub> визначається як:

$$p_1 = \frac{\lambda + (1 - P)\lambda}{\mu 1}, \quad (5.4)$$

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

$$P_0 = \frac{1}{\frac{p_1^{n+1}}{n!(n-p_1)} + \sum_{n=0}^n \frac{p_1^n}{n!}}, \quad (5.5)$$

де  $n=4$  – число опрацьовувачів.

Середню затримку сервера аналізу трафіку ( $T_1$ ) можна отримати на основі числа заявок в системі ( $N_1$ ), залежного від середнього числа заявок в черзі (NS):

$$NS = \frac{p_1^{n+1} P_0}{nn!(1 - \frac{p_1}{n})^2}, \quad (5.6)$$

$$N_1 = NS + p_1, \quad (5.7)$$

$$T_1 = \frac{N_1}{\lambda + (1 - P)\lambda} \quad (5.8)$$

Знаючи інтенсивність надходження пакетів на сервер ухвалення рішень (СМО<sub>2</sub>) –  $\lambda_{\text{ex2}}$ , можна отримати наступні характеристики для СМО<sub>2</sub>:

продуктивність ( $p_2$ ) середнє число заявок в системі ( $N_2$ ), середню затримку сервера ухвалення рішень ( $T_2$ ), розрахунок яких проводиться за формулами:

$$p_2 = \frac{(1-P)\lambda}{\mu_2}, \quad (5.9)$$

$$N_2 = \frac{p_2}{1-p_2}, \quad (5.10)$$

$$T_2 = \frac{N_2}{(1-P)\lambda} = \frac{1}{\mu_2(1-p_2)} \quad (5.11)$$

Загальний час, необхідний системі DPI на визначення потоку і політики (T), складає:

$$T = T_1 + P(T_1 + T_2) \quad (5.12)$$

На підставі наведених вище формул визначена залежність затримки в такій системі від інтенсивності навантаження (рис. 5.3), при вибраній ймовірності звернення до сервера ухвалення рішень  $P = 0,8$  і інтенсивностями обслуговування заявок  $\mu_1 = 5000$ ,  $\mu_2 = 1000$  на СМО 1 і 2 відповідно.

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

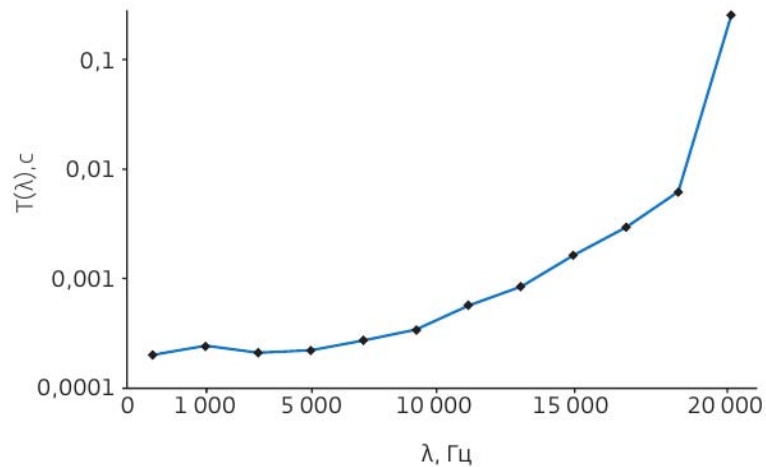


Рисунок 5.3 – Залежність затримки, яка виникає в системі DPI від  $\lambda$

Проте при піковому навантаженні система показала незадовільну затримку, рівну 260 мс. З урахуванням того, що затримка передачі пакету в мережі складається з часу на подолання відстані, часу на обробку пакетів маршрутизаторами, комутаторами і двох систем DPI (у мережі оператора, який постачає трафік, і в мережі іншого оператора, який цей трафік приймає). Зрозуміло, що для системи DPI затримки при обробці пакетів мають бути мінімальними. Проте не варто вважати ці результати остаточними, оскільки в цій математичній моделі було зроблено велику кількість допущень.

### Висновки до розділу 5

В розділі 5 розглядається питання посилення рівня захищеності WEB ресурсів за допомогою технології DPI, яка дозволяє на найвищих рівнях моделі OSI працювати з даними для захисту систем. 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. Deep Packet Inspection здатна виявляти і блокувати віруси, фільтрувати інформацію, що не задовольняє заданим критеріям, виконує глибокий аналіз усіх пакетів, що проходять через

неї. Система DPI здійснює так званий поведінковий аналіз трафіку, який дозволяє розпізнати додатки, що не використовують для обміну даними заздалегідь відомі заголовки і структури даних.

За допомогою DPI спецслужби можуть вести спостереження за мережевою активністю того або іншого користувача та аналізувати VPN, HTTPS трафік. Система DPI може зібрати різну інформацію, не порушуючи особистих прав користувача.

## ВИСНОВКИ

В першому розділі магістерської роботи проведено статистичне дослідження найбільш поширених уразливостей веб-ресурсів. Досліджені веб-додатки належали компаніям, які представляють різні галузі. Проаналізовано уразливості по засобам розробки, по серверам, по галузях на продуктивних і тестових сайтах, проведено порівняння методів тестування.

В цілому, на сьогоднішній день рівень захищеності веб-додатків залишається вкрай низьким. Незважаючи на це, системи виявлення та запобігання вторгнень рівня додатків майже не використовуються: такий механізм застосовувався для захисту лише одного з усіх сайтів, розглянутих у даному дослідженні.

В другому розділі проведено аналіз нормативного забезпечення в галузі інформаційної безпеки. 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.

Проведений аналіз сучасних стандартів в галузі управління інформаційною безпекою систем, а саме, розглянуті особливості застосування та призначення наступних стандартів серії ISO/IEC 27000, Стандарт BS 7799-3.

Проведений аналіз існуючих методів оцінювання та управління ризиками інформаційної системи.

Слід зазначити, що застосування означених в розділі нормативних актів приводить, до необхідності модернізації ІТ-інфраструктури організації і, в тому числі, перебудови системи ІБ як частини цієї інфраструктури, а також зміну підходу до її побудови.

Виявлено, що на цей момент в Україні одночасно існують дві парадигми систем захисту: КСЗІ і СУІБ в банківській сфері.

Головними групами інцидентів, які можуть призвести до припинення обслуговування клієнтів або розголошенню їх персональних даних згідно схеми, запропонованої Конвенцією Ради Європи 2001 року по боротьбі з кіберзлочинністю, є:

- 1) інциденти, спрямовані проти конфіденційності, цілісності й доступності комп'ютерних даних і систем;
- 2) шахрайство та підробки, пов'язані з використанням ПЕОМ;
- 3) інциденти, пов'язані з розміщенням у мережах протиправної інформації;
- 4) інциденти відносно авторських і суміжних прав.

Все це підіймає проблему захисту Web-ресурсів на якісно новий рівень.

В третьому розділі проведений аналіз проблем захисту WEB сервісів. З кожним роком доля уразливих WEB сервісів зростає. Для захисту від більшості популярних видів атак достатньо належним чином перевіряти вхідні дані. Також рекомендовано використовувати шифрований протокол HTTPS та будувати програмний додаток ресурсу на одному з відомих програмних каркасів (Framework), в якому вбудовані механізми перевірки, шифрування та валідації. Найкращим методом захисту від атак на мережеві служби, наприклад, DoS та DDoS є використання хмарних технологій і перевірених конфігурацій серверів.

В розділі 4 проведений аналіз методів та засобів захисту WEB сервісів. Виділяються три підходи до виявлення вразливості веб-додатків: тестування методом чорного, сірого та білого ящиків. Різниця між ними визначається тими ресурсами, які доступні під час тестування. 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 веб-серверами. Але цього не достатньо, тому в

роботі пропонується комплексне рішення, яке включає WAF, IPS та FIREWALL, тобто захист на всіх рівнях моделі OSI.

В п'ятому 5 розглядається питання посилення рівня захищеності WEB ресурсів за допомогою технології DPI, яка дозволяє на найвищих рівнях моделі OSI працювати з даними для захисту систем. 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. Deep Packet Inspection здатна виявляти і блокувати віруси, фільтрувати інформацію, що не задовольняє заданим критеріям, виконує глибокий аналіз усіх пакетів, що проходять через неї. Система DPI здійснює так званий поведінковий аналіз трафіку, який дозволяє розпізнати додатки, що не використовують для обміну даними заздалегідь відомі заголовки і структури даних.

За допомогою DPI спецслужби можуть вести спостереження за мережевою активністю того або іншого користувача та аналізувати VPN, HTTPS трафік. Система DPI може зібрати різну інформацію, не порушуючи особистих прав користувача.

Прикладів уразливостей і атак існує величезна кількість. Навіть провівши повний цикл тестування безпеки, не можна бути на 100% впевненим, що система по-справжньому безпечна. Але можна бути впевненим в тому, що відсоток несанкціонованих проникнень, крадіжок інформації і втрат даних буде в рази менше, ніж у тих хто не проводив тестування безпеки. Застосувавши комплексне рішення, яке запропоноване в дипломній роботі, можна звести до мінімуму ризики пов'язані із компрометацією системи.

## ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. ISO/IEC 17799:2005. Information technology. Security techniques. Code of practice for information security management.
2. ISO/IEC 27001:2005. Information technology. Security techniques. Information security management systems. Requirements.
3. ISO/IEC TR 27035:2011. Information technology – Security techniques – Information security incident management.
4. ISO/IEC 20000:2011. Information technology. Service management. Part 2: Code of practice.
5. 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.
6. 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.
7. ГОСТ Р ИСО/МЭК 17799-2005.
8. ГОСТ Р ИСО/МЭК 27001.
9. Марков А. Нормативный вакуум информационной безопасности / А. Марков, В. Цирлов // Открытые системы. – 2007. – №8.
10. Петренко С.А. Управление информационными рисками: Экономически оправданная безопасность / С.А. Петренко, С.В. Симонов. – М.: АйТи-Пресс, 2004. – 381 с.
11. 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.
12. 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.



13. 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

14. НД ТЗІ 2.5-010-03 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу»

15. ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems —Requirements. [Електрон. ресурс]: – Режим доступу: <http://www.itgovernance.co.uk/standards.arx>.

16. Гавриленко О.В. Відповідність національної нормативної бази у сфері технічного захисту інформації міжнародним стандартам: зіставлення документів, шляхи гармонізації. Матеріали XVII Міжнародної науково-практичної конференції «Безпека інформації у інформаційно-телекомунікаційних системах», м.Київ, 2015.

17. НД ТЗІ 2.5-004-99 “Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу”. [Електрон. ресурс]: – Режим доступу: [http://www.dsszzi.gov.ua/dstszzi/control/uk/publish/article?art\\_id=40386&cat\\_id=38835](http://www.dsszzi.gov.ua/dstszzi/control/uk/publish/article?art_id=40386&cat_id=38835).

18. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” від 5 липня 1994 року № 80/94-ВР, Відомості Верховної Ради України (ВВР), 1994, № 31. – с.286

19. СОУ Н НБУ 65.1 СУІБ 1.0:2010. Настанова. Методи захисту в банківській діяльності. Система управління інформаційною безпекою. [Електрон. ресурс]: – Режим доступу: <http://www.uk.xlibx.com/4yuridicheskie/1354389-1-sou-nbu-651-suib-10-2010-standart-organizacii-ukraini-nastanova-metodi-zahistu-bankivskiy-diyalnosti-siste.php>.

20. НД ТЗІ 3.7-003-05 “Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі”. [Електрон. ресурс]: – Режим доступу: [http://www.dsszzi.gov.ua/dstszzi/control/uk/publish/article?art\\_id=46074&cat\\_id=38835](http://www.dsszzi.gov.ua/dstszzi/control/uk/publish/article?art_id=46074&cat_id=38835).

21. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. — К.: ДУТ, 2015. — 288 с.
22. Скембрейц Дж. Безопасность Web-приложений — готовые решения / Дж. Скембрейц, М. Шема. — М.: Издательский дом «Вильямс», 2003. — 384 с.
23. Жуков Ю.В. Основы веб-хакинга: нападение и защита / Ю.В. Жуков. — СПб.: Питер, 2011. — 176 с.
24. 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.
25. 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.
26. 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.
27. Поворознюк А.И. Совершенствование защиты Web-приложений от вторжений на основе эвристического похода / А.И. Поворознюк, М.Н. Шкарупа: сб. науч. тр. «Вестник НТУ «ХПИ». Информатика і моделювання. — 2007. — Вип. 19. — С. 145-154.
28. 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. Дзьобай // Научный журнал КубГАУ. — 2014. — № 101(07). — С. 1-11.
29. Bhavani A.V. Cross-site Scripting Attacks on Android WebView / A.V. Bhavani // International Journal of Computer Science and Network. — 2013. — Vol. 2, Issue 2. — 5 p. — Режим доступа в Интернет: <http://ijcsn.org/IJCSN-2013/2-2/IJCSN-2013-2-2-03.pdf>

30. Cuff P. Distributed channel synthesis / P. Cuff // IEEE. Trans. Inf. Theory. — 2013. — Vol. 59(11). — P. 7071-7096.
31. Schieler C. Rate-distortion theory for secrecy systems / C. Schieler, P. Cuff // IEEE Trans. on Inf. Theory. — 2014. — Vol. 66(12). — P.7584-7605.
32. Sahin C.S. General Framework for Evaluating Password Complexity and Strength / C.S. Sahin, R. Lychev, N. Wagner. — 11 p. — Режим доступа в Интернет: <http://arxiv.org/abs/1512.05814>
33. Website Security Statistics Report: 2015. — WhiteHat Security, 2015. — 30 p. — Режим доступа в Интернет: <https://info.whitehatsec.com/Website-Stats-Report-2015.html>
34. Handbook on Ontologies / eds. S. Staab and R. Studer. — International Handbooks on Information Systems. — Berlin: Springer, 2009. — 832 p.
35. Новиков ДА. Теория управления организационными системами / Д.А. Новиков. — М.: Физматлит, 2007. — 584 с.
36. Web Application Security Statistics [Электронный ресурс] – Режим доступа до ресурсу: <http://projects.webappsec.org/f/wasc-wafec-v1.0.pdf>
37. HACKMAGEDDON – статистика інформаційної безпеки [Електронний ресурс] – Режим доступа до ресурсу: <http://www.hackmageddon.com>