МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ДАЛЯ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЕЛЕКТРОНІКИ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК ТА ІНЖЕНЕРІЇ

До захисту допускається
Завідувач кафедри
_____ Скарга-Бандурова І.С.
«____»_____ 2018 р.

МАГІСТЕРСЬКА РОБОТА

НА ТЕМУ:

«СИСТЕМА ЕВРИСТИЧНОГО ВИЯВЛЕННЯ ТА ВІДБИТТЯ АТАК НА WEB-ДОДАТКИ»

Освітньо-кваліфікаційний рівень «Магістр»
Спеціальність 122 «Комп'ютерні науки та інформаційні технології»
(освітня програма «Інформаційні управляючі системи та технології (за галузями)»)

Науковий керівник роботи: _____ (підпис) Кардашук В. С. (ініціали, прізвище)

Консультант з охорони праці: _____ (підпис) Критська Я. О. (ініціали, прізвище)

Студент: _____ (підпис) Єлісєєв М. С. (ініціали, прізвище)

Група: ІУС-16 зм

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ДАЛЯ

Факультет інформаційних технологій та електроніки
Кафедра комп'ютерних наук та інженерії
Освітньо-кваліфікаційний рівень магістр
Спеціальність 122 «Комп'ютерні науки та інформаційні технології»
(освітня програма «Інформаційні управляючі системи та технології (за галузями)»)

«**ЗАТВЕРДЖУЮ**»
Завідувач кафедри
комп'ютерних наук та нженерії
д.т.н., доц. Скарга-Бандурова І.С.
_____
"____" _____ 2018 року

ЗАВДАННЯ
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Єлісєєву Максиму Сергійовичу
(прізвище, ім'я, по-батькові)

1. **Тема проекту (роботи):** «Система евристичного виявлення та відбиття атак на Web-додатки» затверджена наказом по університету № 208/48 від «18» жовтня 2017 р.

2. Строк здачі студентом закінченого проекту (роботи): 10.01.2018 р.

3. Вихідні дані проекту (роботи): матеріали переддипломної практики

4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити):

1. Огляд методів захисту інформації..
2. Дослідження методів захисту інформації та відбиття атак на WEB-додатки.
3. Розробка програмного забезпечення.
4. Порівняння методів захисту за швидкодією.
5. Охорона праці та безпека в надзвичайних ситуаціях.

5. Перелік графічного матеріалу (з точною назвою обов'язкових креслень):

не передбачено

6. Консультанти роботи, з вказівкою розділів, що до них відносяться

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
Основна частина	Кардашук В. С.		
Охорона праці та безпека в надзвичайних ситуаціях	Критська Я.О.		

7. Дата видачі завдання_____

Керівник _____ Кардашук В. С.
(підпис)

Завдання до виконання прийняв _____ Єлісєєв М. С.
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітки
1.	Отримання завдання, збір матеріалів	18.10.17- 24.10.17	
2.	Огляд літератури й обґрунтування необхідності дослідження	25.10.17 –28.10.17	
3.	Дослідження методів захисту та відбиття атак	29.10.17 – 28.11.17	
4.	Розробка програмного забезпечення	28.11.17 –05.12.17	
5.	Розробка заходів з охороні праці	05.12.17 – 19.12.17	
6.	Оформлення пояснювальної записки	19.12.17 – 08.01.18	
7.	Підготовка та подання магістерської роботи до захисту	09.01.18 – 10.01.18	

Студент _____
(підпис)

Науковий керівник _____
(підпис)

АНОТАЦІЯ

Єлісєєв М. С. Система евристичного виявлення та відбиття атак на Web-додатки.

В магістерській роботі запропоновано метод побудови евристичної системи захисту WEB-додатків, що має суттєві переваги порівняно з існуючими методами детектування і відбиття атак. До переваг систем захисту на базі запропонованого методу можна віднести здатність до виявлення нових типів атак, коли сигнатурний аналіз безсилий у силу своєї статичної природи. Розроблена система не потребує розробки і підтримки доволі не дешевої інфраструктури у мережі Internet, яка б дозволяла регулярно отримувати оновлення сигнатурних баз та повністю адаптується під особливості WEB-додатку що захищає.

Система здатна виявляти атаки, які не було виявлено на попередніх етапах сканування брандмауером та фільтром ModSecurity. При достатньому періоді навчання евристична система здатна виявляти до 40% таких атак. Розроблений метод може застосовуватися як в якості додаткової ланки захисту у вже існуючих системах запобігання вторгнень, так і в якості самостійної системи виявлення та відбиття атак.

Ключові слова: Захист, WEB-додаток, детектування, модель, алгоритм.

THE ABSTRACT

Eliseev M. S. System of heuristic detection and reflection of attacks on Web-applications.

In the thesis the method of construction of a heuristic system of protection of WEB-applications is proposed, which has significant advantages over existing methods of detecting and reflecting attacks. The advantages of security systems based on the proposed method can be attributed the ability to identify new types of attacks, when the signature analysis is powerless due to its static nature. The developed system does not require the development and maintenance of a rather inexpensive infrastructure on the Internet, which would allow regular updates of signature bases and fully adapt to the features of the protectable WEB application.

The system is capable of detecting attacks that were not detected in previous stages of firewall scanning and ModSecurity filtering. With a sufficient period of training, the heuristic system can detect up to 40% of such attacks. The developed method can be used as an additional layer of protection in existing intrusion prevention systems, as well as an independent system for detecting and responding to attacks.

Keywords: protection, WEB-application, detection, model, algorithm.

ЗМІСТ

ВСТУП

Поряд з інтенсивним розвитком обчислювальних засобів та систем передачі інформації все більш актуальною стає проблема забезпечення її безпеки. Заходи безпеки спрямовані на запобігання несанкціонованого отримання інформації, фізичного знищення або модифікації інформації, що захищається. Зарубіжні публікації останніх років показують, що можливості зловживань інформацією, що передається по каналах зв'язку, розвивалися і удосконалювалися не менш інтенсивно, ніж засоби їх попередження. У цьому випадку для захисту інформації потрібна не просто розробка приватних механізмів захисту, а організація комплексу заходів, тобто використання спеціальних засобів, методів та заходів з метою запобігання втрати інформації. У цьому сенсі сьогодні народжується нова сучасна технологія – технологія захисту інформації в комп'ютерних інформаційних системах і в мережах передачі даних. Незважаючи на дорогі методи, які вживаються, функціонування комп'ютерних інформаційних систем виявило наявність слабких місць в захисті інформації. Неминучим наслідком стали витрати і зусилля на захист інформації, що постійно збільшуються. Однак, для того, щоб прийняті заходи виявилися ефективними, необхідно визначити, що таке погроза безпеки інформації, виявити можливі канали витоку інформації та шляхи несанкціонованого доступу до захищуваних даними. Під загрозою безпеки розуміється дія або подія, що може призвести до руйнування, спотворення чи несанкціонованого використання інформаційних ресурсів, включаючи збережену, передану і оброблювану інформацію, а також програмні і апаратні засоби. Загрози прийнято ділити на випадкові, чи ненавмисні, і умисні перших можуть бути помилки в програмному забезпеченні, виходи з ладу апаратних засобів, неправильні дії користувачів або адміністрації і т. п. Умисні загрози переслідують мету нанесення шкоди користувачам і, у свою чергу, поділяються на активні і пасивні. Пасивні загрози, як правило, спрямовані на несанкціоноване використання інформаційних ресурсів, не надаючи при цьому впливу на їх функціонування. Пасивною загрозою є, наприклад, спроба отримання інформації, що циркулює в каналах зв'язку, за допомогою їх прослуховування. Активні загрози мають на меті порушення нормального процесу функціонування системи за допомогою цілеспрямованого впливу на апаратні, програмні та інформаційні ресурси.

Таким чином, актуальним є захист WEB-додатків від несанкціонованого втручання в їх роботу.

Об’єкт дослідження – процеси захисту Web-додатків та комп’ютерних систем.

Предмет дослідження – методи і засоби зниження атак на Web-додатки, скорочення часових витрат і підвищення ефективності процедури захисту в комп’ютерних системах.

Методи дослідження. Запропоновано метод побудови евристичної системи захисту

WEB-додатків на основі адаптивно-резонансної теорії, що має суттєві переваги порівняно з існуючими методами детектування і відбиття атак. До переваг систем захисту на базі запропонованого методу можна віднести здатність до виявлення нових типів атак, коли сигнатурний аналіз безсилий у силу своєї статичної природи. Розроблена система не потребує розробки і підтримки доволі не дешевої інфраструктури у мережі Internet, яка б дозволяла регулярно отримувати оновлення сигнатурних баз та повністю адаптується під особливості WEB-додатку що захищає.

Наукова новизна магістерської роботи полягає в дослідженні методів побудови системи захисту та відбиття атак на Web-додатки. На основі дослідження вироблені рекомендації щодо подальшого використання досліджених методів.

Структура і обсяг роботи.

Магістерська робота складається зі вступу, 4 розділів, висновків, переліку посилань з 47 найменувань на 3 сторінках. Загальний обсяг роботи складає 96 сторінок. Магістерська робота містить 22 рисунка, 8 таблиць.

1 ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Інформаційна безпека в Internet

Прогрес подарував людству безліч досягнень, але той же прогрес породив і масу проблем. Людський розум, розв’язуючи одні проблеми, неодмінно зіштовхується при цьому з іншими, новими, і цей процес приречений на нескінченність у своїй послідовності.

Хоча, якщо вже бути точним, нові проблеми – це всього лише обновлена форма старих. Вічна проблема – захист інформації. На різних етапах свого розвитку людство вирішувало цю проблему з властивою для даної епохи характерністю. Винахід комп'ютера й подальший бурхливий розвиток інформаційних технологій у другій половині XX століття зробили проблему захисту інформації настільки актуальною й гострою, наскільки актуальна сьогодні інформатизація для всього суспільства.

Головна тенденція, що характеризує розвиток сучасних інформаційних технологій – ріст числа комп'ютерних злочинів і пов'язаних з ними розкрадань конфіденційної й іншої інформації [1], а також матеріальних втрат. За результатами дослідження, присвяченого питанням комп'ютерних злочинів, близько 58% опитаних постраждали від комп'ютерних атак за останні 12 місяців. Приблизно 18% опитаних із цього числа заявляють, що втратили більше 80 тис. доларів у ході нападів, більше 66% понесли збитки в розмірі 50 тис. доларів. Понад 22% атак були націлені на промислові секрети або документи, що представляють інтерес насамперед для конкурентів.

Сьогодні, напевно, ніхто не зможе із упевненістю назвати точну цифру сумарних втрат від комп'ютерних злочинів, пов'язаних з несанкціонованим доступом до інформації. Це пояснюється, насамперед, небажанням постраждалих компаній обнародувати інформацію про свої втрати [2], а також тим, що не завжди втрати від розкрадання інформації можна точно оцінити в грошовому еквіваленті.

Однак за даними, опублікованим аналітичною агенцією CERT в мережі Internet, загальні втрати від несанкціонованого доступу до інформації в комп'ютерних системах в 2005 році оцінювалися в 20 мільйонів доларів, а вже в 2006 року в 53,6 мільйонів доларів.

Причин активізації комп'ютерних злочинів і пов'язаних з ними фінансових втрат досить багато. Найбільш істотні з них перераховано нижче.

1. Перехід від традиційної "паперової" технології зберігання й передачі відомостей на електронну й недостатнє при цьому розвиток технології захисту інформації в таких технологіях.

2. Об'єднання обчислювальних систем, створення глобальних мереж і розширення доступу до інформаційних ресурсів.

3. Збільшення складності програмних засобів і пов'язане з цим зменшення їхньої надійності й збільшенням вразливостей.

Будь-яке сучасне підприємство незалежно від виду діяльності й форми власності не в змозі успішно розвиватися й вести господарську діяльність без створення умов для надійного функціонування системи захисту власної інформації.

Відсутність у багатьох керівників підприємств і компаній чіткого розуміння питань захисту інформації [3] приводить до того, що їм складно повною мірою оцінити необхідність створення надійної системи захисту інформації на своєму підприємстві й тим більше складно буває визначити конкретні дії, необхідні для захисту тих або інших конфіденційних відомостей. У загальному випадку керівники підприємств ідуть по шляху створення охоронних служб, повністю ігноруючи при цьому питання інформаційної безпеки. Негативну роль при цьому відіграють і деякі засоби масової інформації, публікуючи "панічні" статті про стан справ з захисту інформації, що формують у читачів думки про неможливість у сучасних умовах забезпечити необхідний рівень захисту інформації. Можна із упевненістю стверджувати, що створення ефективної системи захисту інформації сьогодні цілком реально. Надійність захисту інформації, насамперед, буде визначатися повнотою рішення цілого комплексу завдань.

Архітектура Internet передбачає підключення до зовнішніх відкритих мереж, використання зовнішніх сервісів і надання власних сервісів для зовнішнього доступу [4], що висуває підвищені вимоги до захисту інформації.

В Internet-системах використовується підхід клієнт-сервер, а головна роль на сьогоднішній день приділяється WEB-сервісам [5]. Всі WEB-сервери повинні підтримувати традиційні засоби захисту, такі як аутентифікація й розмежування доступу. Крім того, необхідне забезпечення нових властивостей, особливо безпеки програмного середовища й на серверній, й на клієнтській сторонах.

Формування режиму інформаційної безпеки – проблема комплексна.

Заходи для її розв’язання можна розділити на чотири рівні:

– законодавчий рівень (закони, нормативні акти, стандарти й т.п.);

– адміністративний рівень (дії загального характеру, що вживає керівництво організації для посилення безпеки);

– процедурний рівень (конкретні заходи безпеки, що мають справу з людьми);

– програмно-технічний рівень (конкретні технічні міри).

Найбільш важливим рівнем є останній рівень, що містить у собі цілий комплекс апаратних, програмних і апаратно-програмних засобів захисту інформації.

Сьогодні на ринку технологій захисту комп'ютерної інформації існує велике різноманіття як програмних реалізацій систем захисту, так і концептуальних ідей побудови таких систем. Деякі з них пройшли перевірку часом, а деякі навпаки не витримали цієї перевірки. В цьому розділі описані лише ті технології, що на практиці довели свою ефективність. Також цей розділ вказує на деякі вади існуючих підходів до реалізації систем захисту інформації.

1.2 Розробка мережних аспектів політики безпеки

Політика безпеки визначається як сукупність документованих управлінських рішень, спрямованих на захист інформації й асоційованих з нею ресурсів.

При розробці й впровадженні її в життя доцільно керуватися наступними принципами:

- неможливість пройти захисні засоби;
- посилення самої слабкої ланки;
- неможливість переходу в небезпечний стан;
- мінімізація привілеїв;
- поділ обов'язків;
- ешелонованість оборони;
- розмаїтість захисних засобів;
- простота й керованість інформаційної системи;
- забезпечення загальної підтримки мір безпеки.

Кожен принцип вимагає більш детального пояснення.

Якщо в зловмисника або незадоволеного користувача з'явиться можливість минути захисні засоби, він, зрозуміло, так і зробить. Стосовно до брандмауерів даний принцип означає, що всі інформаційні потоки в мережі, що захищена, повинні проходити через брандмауер. Не повинне бути "таємних" модемних входів або тестових ліній, що йдуть в обхід екрана.

Надійність будь-якої оборони визначається самою слабкою ланкою. Зловмисник не буде боротися проти сили, він віддасть перевагу легкій перемозі над найслабкішою ланкою. Часто самою слабкою ланкою виявляється не комп'ютер або програма, а людина, і тоді проблема забезпечення інформаційної безпеки здобуває нетехнічний характер.

Принцип неможливості переходу в небезпечний стан означає, що при будь-яких обставинах, у тому числі позаштатних, захисних засіб або повністю виконує свої функції, або повністю блокує доступ.

Принцип мінімізації привілеїв пропонує виділяти користувачам і адміністраторам тільки ті права доступу, які необхідні їм для виконання службових обов'язків.

Принцип поділу обов'язків припускає такий розподіл ролей і відповідальності, при якому одна людина не може порушити критично важливий для організації процес. Це особливо важливо, щоб запобігти зловмисним або некваліфікованим діям системного адміністратора.

Принцип ешелонованості оборони пропонує не покладатися на один захисний рубіж, яким би надійним він не здавався. За засобами фізичного захисту повинні стояти програмно-технічні засоби, за ідентифікацією й аутентифікацією – керування доступом і, як останній рубіж, – протоколювання й аудит. Ешелонована оборона здатна принаймні затримати зловмисника, а наявність такого рубежу, як протоколювання й аудит, істотно ускладнює непомітне виконання злочинних дій.

Принцип розмаїтості захисних засобів рекомендує організовувати різні за своїм характером оборонні рубежі, щоб від потенційного зловмисника було потрібно оволодіння різноманітними й, по можливості, несумісними між собою навичками (наприклад умінням переборювати високу огорожу й знанням уразливостей декількох операційних систем).

Дуже важливий принцип простоти й керованості інформаційної системи в цілому й захисних засобах особливо. Тільки для простого захисного засобу можна формально або неформально довести його коректність. Тільки в простій і керованій системі можна перевірити погодженість конфігурації різних компонентів і здійснити централізоване адміністрування. В зв'язку з цим важливо відзначити інтегруючу роль WEB-сервісу, що приховує розмаїтість об'єктів, що обслуговують, і надає єдиний, наочний інтерфейс.

Принцип загальної підтримки мір безпеки – носить нетехнічний характер. Якщо користувачі й/або системні адміністратори вважають інформаційну безпеку чимсь зайвим або навіть ворожим, режим безпеки сформувати свідомо не вдасться. Треба із самого початку передбачити комплекс мір, спрямований на забезпечення лояльності персоналу, на постійне навчання, теоретичне й, головне, практичне.

Аналіз ризиків – найважливіший етап розробки політики безпеки [6]. При оцінці ризиків, яким піддані Internet-системи, потрібно враховувати ряд обставин.

1. Нові погрози стосовно старих сервісів, що випливають із можливості пасивного або активного прослуховування мережі. Пасивне прослуховування означає читання мережного трафіку, а активне – його зміна (крадіжка, дублювання або модифікацію переданих даних). Наприклад, аутентифікація окремого клієнта за допомогою пароля багаторазового використання не може вважатися надійної в мережному середовищі, незалежно від довжини пароля;

2. Нові мережні сервіси й асоційовані з ними погрози.

Як правило, в Internet-системах варто дотримуватися принципу “усе, що не дозволено, заборонене”, оскільки “зайвий” мережний сервіс може надати канал проникнення в корпоративну систему. Ту ж думку виражає положення “все незрозуміле небезпечно”.

1.3 Керування доступом шляхом фільтрації інформації

Засоби програмно-технічного рівня захисту спрямовані на забезпечення інформаційної безпеки систем, побудованих у технології Internet. На перше місце серед таких мір ставлять брандмауери [7] – засіб розмежування доступу, що служить для захисту від зовнішніх погроз і від погроз із боку користувачів інших сегментів корпоративних мереж.

Відзначимо, що боротися з погрозами, властиві мережному середовищу, засобами універсальних операційних систем не представляється можливим [8]. Універсальна ОС – це велика програма, що напевно містить, крім явних помилок, деякі особливості, які можуть бути використані для одержання нелегальних привілеїв доступу. Сучасна технологія програмування не дозволяє робити без помилок об’ємне програмне забезпечення. Крім того, адміністратор, що має справу зі складною системою, далеко не завжди може врахувати всі наслідки зроблених ним змін (як і лікар, що не може знати всіх побічних впливів ліків, що рекомендує). Нарешті, в універсальній системі з багатьма користувачами, потенційно небезпечні ситуації постійно створюються самими користувачами (слабкі й/або рідко змінювані паролі, невдало встановлені права доступу, залишений без догляду термінал та ін.).

Як було вказано вище, існує єдиний перспективний шлях пов'язаний з розробкою спеціалізованих захисних засобів, які в силу своєї простоти допускають формальну або неформальну верифікацію. Брандмауер і є таким засобом, що допускає подальшу декомпозицію, пов'язану з обслуговуванням різних мережних протоколів.

Брандмауер – це напівпрозора мембрана, що розташовується між внутрішньою мережею й зовнішнім середовищем (зовнішніми мережами або іншими сегментами корпоративної мережі) і контролює всі інформаційні потоки у внутрішню мережу та з неї (рис. 1.1). Контроль інформаційних потоків складається в їхній фільтрації, тобто у вибірковому пропущенні через екран, можливо, з виконанням деяких перетворень і повідомленням відправника про те, що його даним у пропуску відмовлено. Фільтрація здійснюється на основі набору правил, попередньо завантажених при налаштуванні брандмауеру [9].

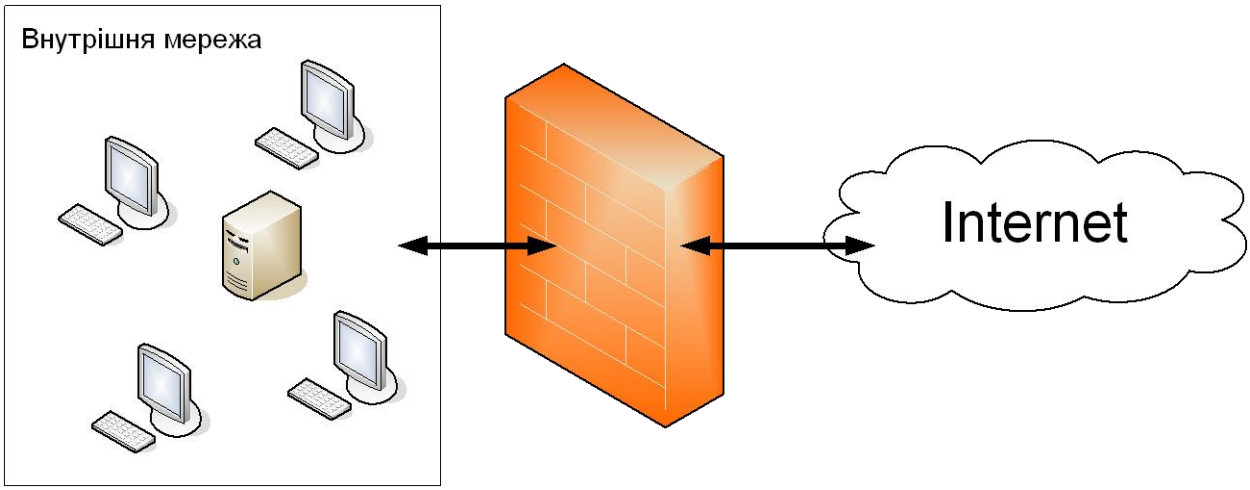


Рисунок 1.1 – Брандмауер як засіб контролю інформаційних потоків

Доцільно розділити випадки, коли екран встановлюється на границі із зовнішньою (звичайно загальнодоступною) мережею або на границі між сегментами однієї корпоративної мережі. Відповідно, можна говорити про зовнішній і внутрішній брандмауери.

Як правило, при спілкуванні із зовнішніми мережами використовують винятково сімейство протоколів TCP/IP. Тому зовнішній брандмауер повинен ураховувати специфіку цих протоколів. Для внутрішніх екранів ситуація складніше, тут варто брати до уваги крім TCP/IP принаймні протоколи SPX/IPX, що застосовуються в мережах Novell NetWare [10]. Іншими словами, від внутрішніх екранів нерідко вимагають знання багатьох протоколів.

Ситуації, коли корпоративна мережа містить лише один зовнішній канал, є, скоріше, виключенням, чим правилом [11]. Навпроти, типова ситуація, при якій корпоративна мережа складається з декількох територіально рознесених сегментів, кожний з яких підключений до мережі загального користування (рис. 1.2). У цьому випадку кожне підключення повинне захищатися своїм екраном. Точніше кажучи, можна вважати, що корпоративний зовнішній брандмауер є складовим, і потрібно вирішувати завдання погодженого адміністрування (керування й аудита) всіх компонентів.

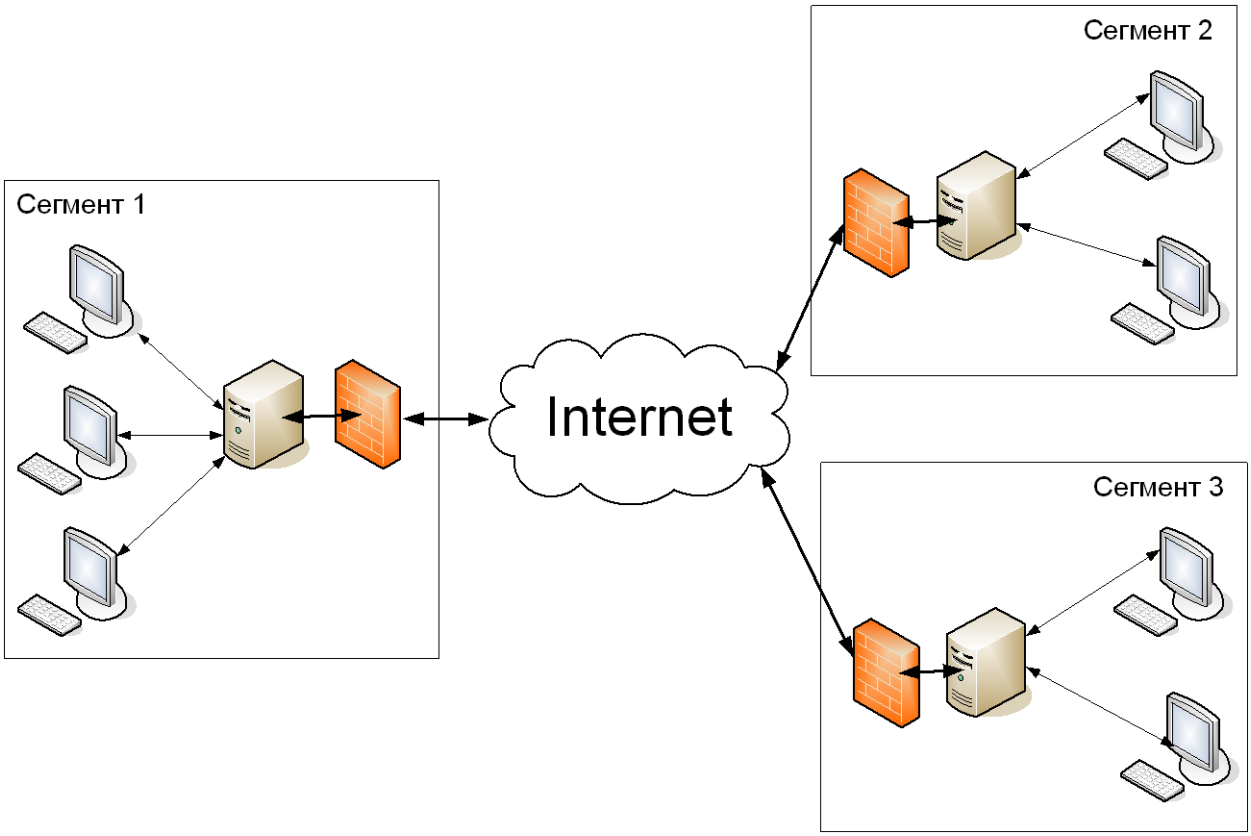


Рисунок 1.2 – Екранування корпоративної мережі

При розгляді будь-якого питання, що стосується мережних технологій, основою є еталонна модель ISO/OSI, що містить в собі сім окремих рівнів. Брандмауери також доцільно класифікувати по тому, на якому рівні проходить фільтрація – канальному, мережному, транспортному або прикладному [12]. Відповідно, можна говорити про концентратори, що екранують (рівень 2), маршрутизатори (рівень 3), про транспортне екранування (рівень 4) і про прикладні екрани (рівень 7). Існують також комплексні екрани, що аналізують інформацію на декількох рівнях.

При ухваленні рішення “пропустити/не пропустити” пакет, брандмауери можуть використати не тільки інформацію, що вміщується у потоках, що фільтруються, але й дані, отримані з оточення, наприклад поточний час та ін.

Таким чином, можливості брандмауера безпосередньо визначаються тим, яка інформація може бути використана в правилах фільтрації і якою може бути потужність наборів правил. Загалом, чим вище рівень у моделі ISO/OSI, на якому функціонує екран, тим більш змістовна інформація йому доступна й, отже, тим тонше й надійніше екран може бути сконфігурований.

У той же час фільтрація на кожному з перерахованих вище рівнів має свої переваги. Чим нижче рівень – тим фільтрація дешевше, ефективніше та прозоріше для користувачів. У

силу цих, а також деяких інших причин, у більшості випадків використаються змішані конфігурації, у яких об'єднані різнотипні екрани. Найбільш типовим є сполучення маршрутизаторів, що екранують, і прикладного брандмауера (рис. 1.3).

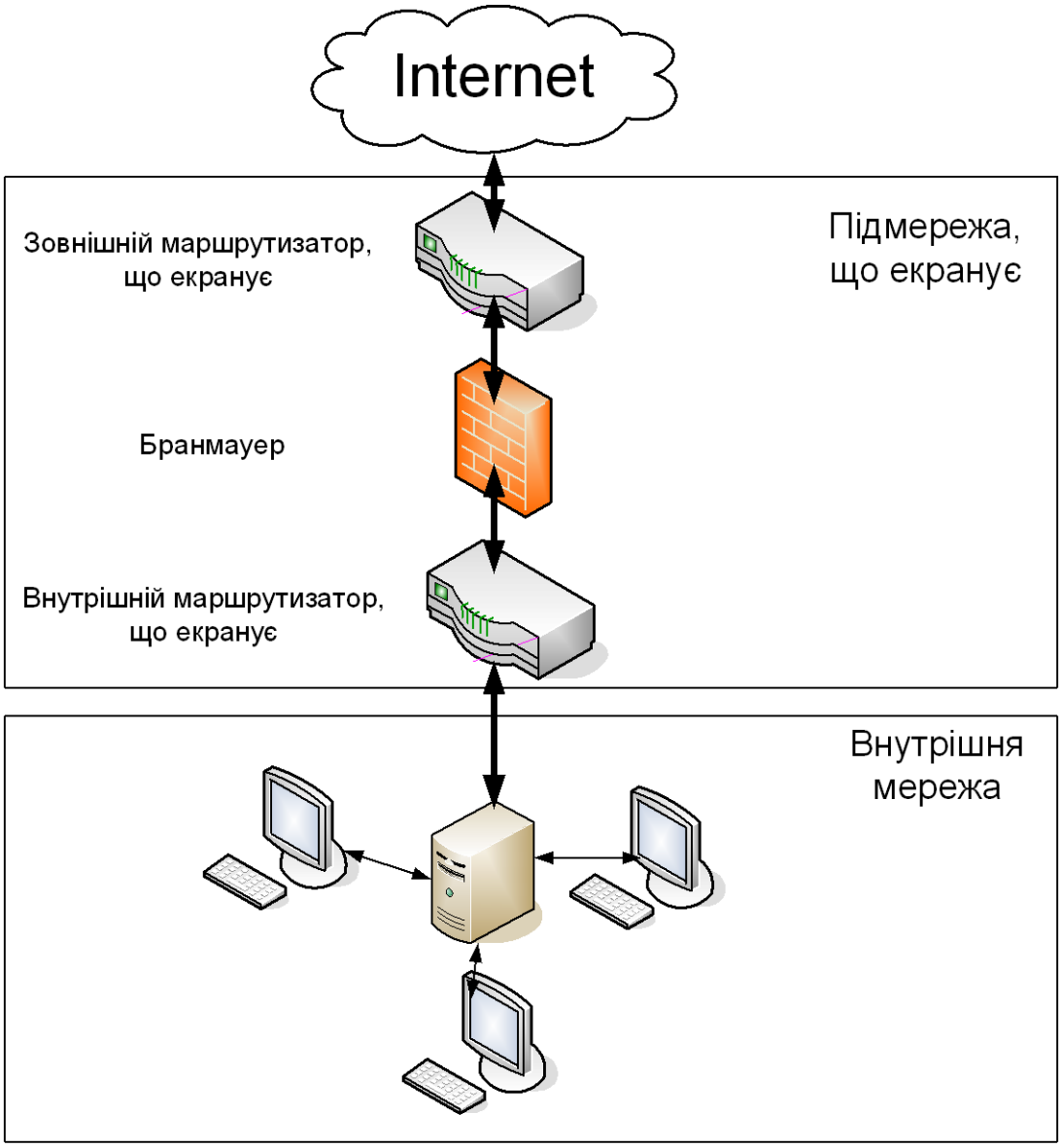


Рисунок 1.3 – Сполучення маршрутизаторів

Наведена конфігурація називається підмережою, що екранує. Як правило, сервіси, які організація надає для зовнішнього застосування (наприклад “представницький” WEB-сервер), доцільно виносити саме в підмережу, що екранує.

Крім того якість брандмауера визначається ще двома дуже важливими характеристиками – простотою застосування й власною захищеністю. У плані простоти використання першорядне значення мають наочний інтерфейс при завданні правил

фільтрації й можливість централізованого адміністрування складених конфігурацій. У свою чергу, в останньому аспекті треба виділити можливість централізованого завантаження правил фільтрації й перевірки набору правил на несуперечність. Важливий централізований збір і аналіз реєстраційної інформації, а також одержання сигналів про спроби виконання дій, заборонених політикою безпеки.

Власна захищеність брандмауера забезпечується тими ж засобами, що й захищеність універсальних систем. При виконанні централізованого адміністрування варто ще подбати про захист інформації від пасивного й активного прослуховування мережі, тобто забезпечити цілісність і конфіденційність інформації.

Треба підкреслити, що природа екранування (фільтрації), як механізму безпеки, дуже глибока. Крім блокування потоків даних, що порушують політику безпеки, брандмауер може приховувати інформацію про мережу, що захищається, тим самим ускладнюючи дії потенційних зловмисників. Так, прикладний екран може здійснювати дії від імені суб'єктів внутрішньої мережі, у результаті чого із зовнішньої мережі здається, що має місце взаємодія винятково з брандмауером (рис. 1.4). При такому підході топологія внутрішньої мережі схована від зовнішніх користувачів, тому завдання зловмисника істотно ускладнюється.

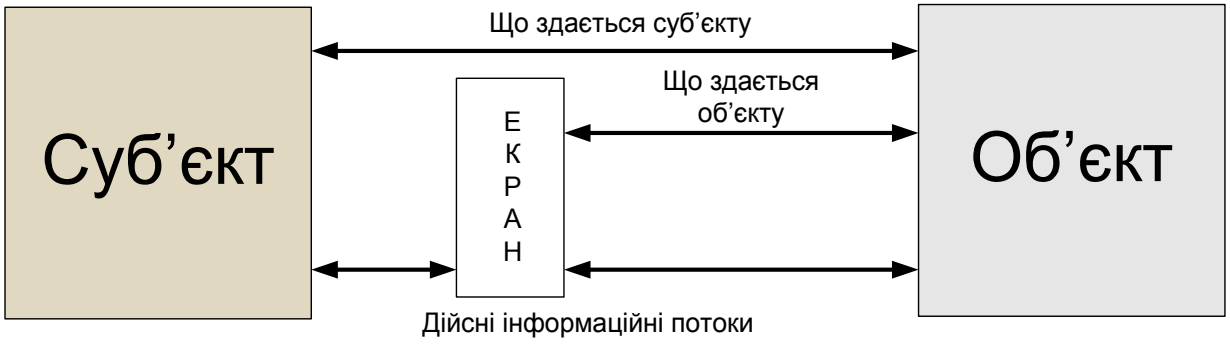


Рисунок 1.4 – Дійсні інформаційні потоки й потоки, що уявляються

Більше загальним методом приховання інформації про топологію мережі, що захитається, є трансляція “внутрішніх” мережних адрес, що одночасно вирішує проблему розширення адресного простору, виділеного організації.

Обмежуючий інтерфейс також можна розглядати як різновид екранування. На невидимий об'єкт важко нападати, особливо за допомогою фіксованого набору засобів. У цьому змісті WEB-інтерфейс має природний захист, особливо в тому випадку, коли гіпертекстові документи формуються динамічно. Кожний бачить лише те, що йому дозволено бачити і нічого більше.

Роль, WEB-сервісу, що екранує, наочно проявляється й тоді, коли цей сервіс здійснює посередницькі функції при доступі до інших ресурсів, зокрема до таблиць бази даних. Тут не тільки контролюються потоки запитів, але й приховується реальна організація баз даних.

1.4 Безпека програмного середовища

Ідея мереж з так називаними активними агентами, коли між комп'ютерами передаються не тільки пасивні, але й активні дані, що виконуються, не нова. Спочатку мета полягала в тому, щоб зменшити мережний трафік, виконуючи основну частину обробки там, де розташовані данні (наближення програм до даних). На практиці це означало переміщення програм на сервери. Класичний приклад реалізації подібного підходу – це збережені процедури в реляційних СУБД.

Для WEB-серверів аналогом збережених процедур є програми, що обслуговують загальний шлюзовий інтерфейс (Common Gateway Interface - CGI).

CGI-процедури розташовуються на серверах і звичайно використаються для динамічного створення HTML-документів. Політика безпеки організації й процедурні міри повинні визначати, хто має право розміщувати на сервері CGI-процедури. Твердий контроль тут необхідний, оскільки виконання сервером некоректної програми може привести до як завгодно важких наслідків. Розумна міра технічного характеру складається в мінімізації привілеїв користувача, від імені якого виконується WEB-сервер.

У технології Internet, якщо піклуватися про якість і виразну силу користувальницького інтерфейсу, не виникає нестача у переміщенні програм з WEB-серверів на клієнтські комп'ютери – для створення анімації (Flash, Java-аплет), виконання семантичного контролю при введенні даних (JavaScript) та ін. Взагалі, активні агенти – невід'ємна частина технології Internet.

У якому би напрямку не переміщалися програми по мережі, ці дії становлять підвищену небезпеку, тому що програма, отримана з ненадійного джерела, може містити ненавмисно внесені помилки або цілеспрямовано створений код, що несе шкоду. Такі програми потенційно загрожують всім основним аспектам інформаційної безпеки:

– доступності (програма може поглинути всі наявні ресурси);
– цілісності (програма може видалити або пошкодити дані);
– конфіденційності (програма може прочитати дані й передати їх по мережі).

Проблему ненадійних програм усвідомлювали давно, але, мабуть, тільки в рамках системи програмування Java уперше запропонована цілісна концепція її розв’язання.

Java пропонує три оборонних рубежі:

– надійність мови;
– контроль при одержанні програм;
– контроль при виконанні програм.

Втім, існує ще один, дуже важливий засіб забезпечення інформаційної безпеки – безпрецедентна відкритість Java-системи. Вихідні тексти Java-компілятора й інтерпретатора доступні для перевірки, тому існує велика ймовірність, що помилки й недоліки першими будуть виявляти чесні фахівці, а не зловмисники.

У концептуальному плані найбільші труднощі представляє контрольоване виконання програм, завантажених по мережі. Насамперед, необхідно визначити, які дії вважаються для таких програм припустимими. Якщо виходити з того, що Java – це мова для написання клієнтських частин додатків, одним з основних вимог до яких є мобільність, завантажена програма може обслуговувати тільки користувальницький інтерфейс і здійснювати мережну взаємодію із сервером. Програма не може працювати з файлами хоча б тому, що на Java-терміналі їх, скоріше всього, не буде. Більш змістовні дії повинні проводитися на серверній стороні або здійснюватися програмами, локальними для клієнтської системи.

Цікавий підхід пропонують фахівці компанії Sun Microsystems для забезпечення безпечного виконання командних файлів. Мова йде про середовище Safe-Tcl (Tool Comman Language, інструментальна командна мова). Sun запропонувала так називану коміркову модель інтерпретації командних файлів. Існує єдиний головний інтерпретатор, якому доступні всі можливості мови.

Якщо в процесі роботи додатка необхідно виконати сумнівний командний файл, породжується підлеглий командний інтерпретатор, що володіє обмеженою функціональністю (наприклад, з нього можуть бути віддалені інструменти для роботи з файлами й мережні можливості). У результаті потенційно небезпечні програми виявляються ув'язненими в осередки, що захищають користувальницькі системи від ворожих дій. Для виконання дій, які вважаються привілейованими, підлеглий інтерпретатор може звертатися із запитами до головного. Тут, мабуть, проглядається аналогія з поділом адресних просторів операційної системи й користувальницьких процесів і використанням останніми системних викликів. Подібна модель уже близько 30 років є стандартною для операційних систем.

1.5 Захист WEB-серверів

Поряд із забезпеченням безпеки програмного середовища, дуже важливим є питання про розмежування доступу до об'єктів WEB-сервісу. Для розв’язання цього питання необхідно усвідомити, що є об'єктом доступу.

В WEB-серверах об'єктами доступу виступають універсальні локатори ресурсів (URL - Uniform (Universal) Resource Locator). За цими локаторами можуть стояти різні сутності – HTML-файли, CGI-процедури, PHP-скрипти, ASP-скрипти, зображення, текстові документи та ін.

Як правило, суб'єкти доступу ідентифікуються по IP-адресах і/або іменам комп'ютерів. Крім того, може використатися парольна аутентифікація користувачів або більш складні схеми, засновані на криптографічних технологіях.

У більшості WEB-серверів права розмежовуються з точністю до каталогів (директорій) із застосуванням довільного керування доступом. Можуть надаватися права на читання HTML-файлів, виконання CGI-процедур та ін.

Для раннього виявлення спроб нелегального проникнення до WEB-серверу важливо регулярно аналізувати реєстраційну інформацію.

Зрозуміло, система, на якій функціонує WEB-сервер, повинна додержуватися універсальних рекомендацій, головної з яких є максимальне спрощення. Всі непотрібні сервіси, файли, пристрої повинні бути вилучені. Число користувачів, що мають прямий доступ до серверу, повинне бути зведене до мінімуму, а їхні привілеї - упорядковані у відповідності зі службовими обов'язками.

Ще один загальний принцип полягає в тому, щоб мінімізувати обсяг інформації про сервер, що можуть одержати користувачі. Багато серверів у випадку звернення по імені каталогу й відсутності файлу index.html (index.php або default.asp) у ньому, видають HTML-варіант змісту каталогу. У цьому змісті можуть зустрітися імена файлів з вихідними текстами CGI-процедур або з іншою конфіденційною інформацією. Такого роду “додаткові можливості” доцільно відключати, оскільки зайве знання зловмисника множить ризики власника сервера або WEB-додатка, що розташовано на цьому сервері.

1.6 Аутентифікація у відкритих мережах

Методи, що застосовуються у відкритих мережах для підтвердження й перевірки правомірності доступу суб'єктів до інформації, повинні бути стійкі до пасивного й активного прослуховування мережі за допомогою спеціальних програмних і апаратних засобів. Суть роботи системи аутентифікації зводиться до наступного:

– суб'єкт демонструє знання секретного ключа, при цьому ключ або взагалі не передається по мережі, або передається в зашифрованому вигляді.

– суб'єкт демонструє володіння програмним або апаратним засобом генерації одноразових паролів або засобом, що працює в режимі “відповідь – запит – відповідь”. При

такій системі передачі перехоплення й наступне відтворення одноразового пароля або відповіді на запит нічого не дає зловмисникові.

– суб'єкт демонструє дійсність свого місця розташування, при цьому використається система навігаційних супутників.

1.7 Віртуальні приватні мережі

Одним з найважливіших завдань є захист потоків корпоративних даних, що передаються по відкритих мережах. Відкриті канали можуть бути надійно захищені одним методом – криптографічним.

Відзначимо, що так називані виділені лінії не мають особливі переваги перед лініями загального користування в плані інформаційної безпеки. Виділені лінії хоча б частково будуть розташовуватися в неконтрольованій зоні, де їх можуть пошкодити або здійснити несанкціоноване підключення до них. Єдина реальна перевага – це гарантована пропускна здатність виділених ліній, а зовсім не підвищена захищеність. Втім, сучасні оптоволоконні канали здатні задовольнити різні потреби великої кількості абонентів, в тому числі й потреби у створенні безпечного каналу.

Цікаво згадати, що в мирний час 95% трафіку Міністерства оборони США передається через мережі загального користування (зокрема через Internet). У воєнний час ця частка повинна становити “лише” 70%. Американські військові покладаються на мережі загального користування тому, що розвивати власну інфраструктуру в умовах швидких технологічних змін – заняття дуже дороге й безперспективне, не виправдане навіть для критично важливих національних організацій тільки у виняткових випадках [13].

Представляється природним покласти на брандмауер завдання шифрування й дешифрування корпоративного трафіку на шляху в зовнішню мережу та навпаки. Щоб таке шифрування/дешифрування стало можливим, повинний відбутися початковий розподіл ключів. Сучасні криптографічні технології пропонують для цього цілий ряд методів.

Після того як брандмауери здійснили криптографічне закриття корпоративних потоків даних, територіальна віддаленість сегментів мережі проявляється лише в різній швидкості обміну з різними сегментами. В іншому вся мережу виглядає як єдине ціле, а від абонентів не потрібне залучення яких-небудь додаткових захисних засобів.

Віртуальні приватні мережі (Virtual Private Network або VPN) є розширенням приватної мережі, що здійснює Internet. VPN дає користувачам можливість послати дані між двома комп'ютерами по загальнодоступній або відкритій мережі в такій спосіб, що імітує властивості каналів зв'язку типу "крапка-крапка". Власне кажучи, це робить віддалений

комп'ютер фактично частиною приватної мережі шляхом створення зашифрованого тунелю в загальнодоступній мережі. Діяльність, пов'язана з конфігуруванням і створенням VPN, відома як робота у віртуальній приватній мережі.

Щоб емулювати зв'язок "точка-точка", дані інкапсулюються, або обертаються, у пакет, при цьому заголовок містить інформацію про маршрутизацію, дозволяючи даним перетинати загальнодоступну або відкриту міжнародну мережу транзитом для досягнення місця призначення. Для емуляції приватного зв'язку й підтримки конфіденційності посилають данні, що зашифровані. Пакети, перехоплені в загальнодоступній відкритій мережі, незрозумілі зловмиснику без ключів кодування. Частина підключення, у якому інкапсульовані дані називається тунель.

VPN-підключення дозволяють користувачам, що працюють удома або в дорозі, з'єднуватися безпечним способом з віддаленим сервером організації, використовуючи інфраструктуру маршрутизації, що забезпечується суспільною міжнародною мережею (типу Internet). З погляду користувача VPN-підключення є прямим підключенням між комп'ютером користувача й сервером організації. Природа проміжної мережі несуттєва для користувача, тому що йому здається, начебто дані послані по спеціалізованому приватному зв'язку [14].

VPN дозволяє корпорації з'єднуватися з філіями або з іншими компаніями по загальнодоступній мережі (типу Internet) при підтримці високої безпеки зв'язку.

В обох випадках безпечне підключення по міжнародній мережі виглядає для користувача як приватний мережний зв'язок, незважаючи на те що цей зв'язок проходить по суспільній міжнародній мережі (звідси виникла назва – віртуальна приватна мережа).

Технологія VPN розв’язує проблеми, що супроводжують тенденцію до збільшення обсягу дистанційної роботи й широкому поширенню глобальних операцій, де співробітники повинні мати можливість з'єднуватися із центральними ресурсами й взаємодіяти один з одним.

Щоб дати службовцем можливість з'єднуватися з обчислювальними ресурсами організації незалежно від їхнього місця розташування, корпорація повинна розгорнути масштабоване рішення віддаленого доступу. Як правило, корпорації вибирають або таке рішення, у якому внутрішньому відділу інформаційних систем поручається закупівля, установка й підтримка модемних пулів організації й інфраструктури приватної мережі; або вибирають VAN (value-added network) рішення, у якому вони оплачують субдоговір з іншими компаніями на купівлю, установку й обслуговування модемних пулів і інфраструктури телекомунікацій.

Жодне із цих рішень не дає необхідної масштабованості в термінах вартості, гнучкого адміністрування й вимог до підключень. Тому має сенс замінити модемні пули й

інфраструктуру приватних мереж менш дорогим рішенням, заснованим на технології Internet, щоб бізнес міг зосередитися на областях його основної компетенції. За допомогою Internet-рішення всього кілька інтернет-підключень через служби інтернет-провайдерів (Internet Service Provider або ISP) і комп'ютери VPN-серверів можуть обслуговувати потреби віддаленої роботи в мережі сотень або тисяч віддалених клієнтів і філій.

Технологія VPN дає віддалений доступ до ресурсів організації по суспільній мережі Internet при підтримці таємності інформації.

Замість того щоб дзвонити з використанням зв’язку між городами на сервер організації або на сервер посередника мережного доступу NAS (network access server), користувач набирає номер місцевого інтернет-провайдера. Використовуючи підключення до місцевого провайдера, VPN-клієнт створює VPN-підключення між комп'ютером віддаленого доступу й VPN-сервером організації по Internet.

Два традиційних методи з'єднання віддалених офісів з домашньою корпоративною мережею полягали в тому, щоб здійснювати модемне підключення, що працювало по суспільній телефонній мережі, що комутується, PSTN (public switched telephone network), або використати спеціалізовану орендовану WAN, використовуючи фрейм-ретранслятор або синхронну схему протоколу PPP (Point-to-Point Protocol). Ці методи вимагають значних витрат часу на адміністрування й доволі не дешеві в обслуговуванні. Типова синхронна схема T1, що управляє фреймом-ретранслятором, PPP або декількома PSTN лініями може коштувати тисячі доларів на місяць, становлячи істотні регулярні витрати компанії.

Використання міжсайтової VPN-технології дозволяє компанії скоротити щомісячні регулярні витрати на швидкодіючі схеми. Використання зв'язку через місцевого інтернет-провайдера на вилучених офісних сайтах і єдиної швидкодіючої схемі в загальному офісі дозволяє компанії зробити кілька швидкодіючих підключень, керування оверлеєм фрейму-ретранслятора, обслуговування архітектури маршрутизації WAN і пов'язані з ними істотні регулярні фінансові й адміністративні витрати.

Існує два методи використання VPN-технології для підключення локальних мереж на віддалених сайтах [15]:

1. Завжди включена VPN. Використання виділених ліній для підключення філій до локальної мережі організації (LAN). Замість того щоб використати дорогу спеціалізовану міжміську схему між філіями й корпоративним центром, маршрутизатори як філій, так і центра можуть використати місцеву спеціалізовану схему й місцевий інтернет-провайдер для підключення до Internet. Програмне забезпечення VPN використовує підключення до місцевого інтернет-провайдера й Internet для створення VPN між маршрутизатором філії й центральним маршрутизатором компанії.

2. Включення по вимозі VPN. Використання лінії модемного зв'язку для підключення філій до інтернету. Замість того щоб мати у філії маршрутизатор, що дозволяє робити дзвінки між містами до корпоративного або NAS-серверу, маршрутизатор філії може викликати місцевого інтернет-провайдера. Маршрутизатор філії використає підключення до місцевого інтернет-провайдера для створення VPN-підключення між маршрутизатором філії й центральним корпоративним маршрутизатором по Internet.

В обох випадках засоби, що відповідають за з'єднання філій і центрального офісу із Internet, є локальними. Будь-який із цих підходів дозволяє корпорації уникнути додаткових витрат на зв'язок між містами, пов'язаних з використанням PSTN-ліній, або витрат на орендований канал, тому що обидві сторони роблять місцеві телефонні звінки, або роблять ближні підключення орендованого каналу до свого інтернет-провайдеру. Інтернет-провайдер має справи із проблемами проміжного мережного зв'язку, із проблемами інтернет-маршрутизації й дозволом імен сайтів, тобто всі складності вилучені з роботи глобальної мережі шляхом використання VPN-підключення між сайтами.

При використанні конфігурації VPN-підключення центральний корпоративний маршрутизатор, що діє як VPN-сервер, повинен бути пов'язаний з місцевим інтернет-провайдером по виділеній лінії, що завжди включена й приймає вступників запити на підключення 24 години на добу та 7 днів на тиждень. Віддалені сайти не мають потреби в активних підключеннях для зв'язку. Є багато ситуацій, коли корпорація захоче мати підключення тільки при необхідності, так що підключення можуть бути сконфігуровані або як «завжди включені», або як «включені по вимозі», які активізуються тільки при необхідності.

В об'єднаних мережах деяких організацій частина відомчих даних настільки секретна, що місцева мережа відділу фізично роз'єднана з іншою частиною об'єднаної мережі організації. Таким прикладом можуть бути дані відділу кадрів компанії, що блокуються від загального доступу, або політика Microsoft, що складається в блокуванні даних, що стосується розробки серверів, від персоналу, що не входить у коло розроблювачів. По суті, найкращий спосіб гарантії того, що дані не будуть скомпрометовані, полягає в тому, щоб взагалі заборонити зв'язок, реалізуючи «повітряний зазор» між захищеними ресурсами й загальним мережним доступом. Хоча цей метод захищає конфіденційну інформацію відділу, він створює проблеми доступу до інформації для користувачів, не зв'язаних фізично з окремими локальними мережами.

Технологія VPN забезпечує рішення, що дозволяє локальній мережі відділу зв'язуватися з об'єднаною мережею організації, але при цьому залишатися технічно екранованої й захищеної за допомогою VPN-сервера.

У цій конфігурації мережа фізично підключає екрановану мережу відділу до іншої частини корпорації. Однак використовуючи VPN-сервер як шлюз до мережних ресурсів екранованого відділу, мережний адміністратор може гарантувати, що тільки ті користувачі об'єднаної мережі організації, які мають відповідні повноваження (credentials) (засновані на політиці необхідного рівня поінформованості в межах компанії), можуть встановлювати VPN-підключення з VPN-сервером і одержувати доступ до захищених ресурсів відділу. Крім того, весь зв'язок між віддаленою робочою станцією й VPN-сервером може бути зашифрована для збереження конфіденційності даних. Шляхом використання VPN-сервера як шлюзу, користувачі, що не мають належних повноважень, не можуть переглядати локальну мережу відділу, а користувачі, що мають належний дозвіл на доступ, можуть переглядати локальну мережу відділу з дотриманням повної таємності й захистом по внутрішній мережі компанії

Таким чином VPN дозволяє вирішити цілу низьку проблем пов’язану з забезпеченням комп’ютерної безпеки на сучасному етапі розвитку глобальних мереж.

1.8 Сучасні тенденції у розробці систем захисту

Основним засобом створення безпечного інформаційного середовища на сучасному етапі розвитку мережі Internet є такий клас додатків як брандмауер, про який вже згадувалося вище.

У самому загальному випадку брандмауер можна визначити як локальний або функціонально-розподілений програмний, апаратний або програмно-апаратний засіб, що реалізує контроль над інформацією, що надходить у комп'ютерну систему й виходить із неї.

Залежно від рівня моделі OSI, на якому відбувається контроль над інформацією, розрізняють брандмауери, які працюють на:

– мережному рівні, фільтрація відбувається на основі адрес відправника й одержувача пакетів, номерів портів транспортного рівня моделі OSI і статичних правил, заданих адміністратором;

– сеансовому рівні, при фільтрації не пропускаються пакети, які порушують специфікації стеку протоколів TCP/IP, що часто використовуються в зловмисних операціях (сканування ресурсів, проникнення через неправильні реалізації TCP/IP, завершення з'єднання, ін'єкція даних);

– рівні додатків, фільтрація відбувається на основі аналізу даних додатка, що передані усередині пакета.

Слід зазначити, що практично всі розроблювачі сучасних брандмауерів пропонують рішення, які працюють на всіх зазначених вище рівнях моделі OSI. Однак робота більшості "класичних" брандмауерів акцентується на мережному й сеансовому рівнях. Нерідко функціональні можливості роботи брандмауера на рівні додатків забезпечуються окремим модулем, робота якого, як правило, носить загальний характер і не враховує особливостей функціонування того або іншого додатку [16].

Брандмауери є необхідним елементом першої лінії оборони, але "класичні" брандмауери гарно справляються лише з атаками на мережному й сеансовому рівні. У випадку атаки "хробаків" або складних атак на рівні додатків з використанням постійно відкритих портів 80 (HTTP) і 443 (HTTPS) вони, як правило, безпомічні. Системи виявлення вторгнень (СВВ), що входять до складу брандмауерів, використовують в своїй роботі пасивні фільтри, через які пропускається мережний трафік з метою виявлення активності зловмисників. Для виявлення атак на рівні додатків використовується технологія сигнатур і виявлення аномальної поведінки, але в більшості випадків вони ці атаки не блокують, а тільки повідомляють про їхнє здійснення. До моменту реакції на атаку адміністратора системи запобігти масштабним ушкодженням системи часто буває занадто пізно.

Невисока ефективність СВВ і проблеми з їхнім керуванням стали настільки помітні, що у звіті "Gartner Information Security Hype Cycle", опублікованому в червні 2013 року, ці системи були названі провальними.

В 2016 році Gartner у черговому прес-релізі порадили використати системи запобігання вторгнень (СЗВ), які почали пропонувати традиційні виробники систем брандмауерів. На відміну від систем СВВ, які просто стежать за мережею й посилають повідомлення про тривогу, мережні СЗВ блокують атаки в момент їхнього виникнення й тільки потім здіймають тривогу.

1.9 Проблеми створення безпечного середовища для функціонування WEB-додатку

Слід зазначити, що не дивлячись на те, що у сучасному світі інформаційних технологій існує багато розробок, які покликані створити безпечне інформаційне середовище, створити повністю безпечне середовище для конкретного додатка вони ще не здатні. На сьогоднішній день створені надійні системи шифрування, безпечні канали доступу, високоефективні брандмауери, але кінцева точка мережі, яка являє собою у більшості випадків WEB-додаток, є слабо захищеною або незахищеною зовсім.

Проблему створення безпечного середовища функціонування WEB-додатків централізовано стали вивчати тільки з 2004 року. Для цього була сформована група "Консорціум із проблем безпеки WEB додатків" ("Web Application Security Consortium" group). До складу цієї групи ввійшли ряд провідних світових спеціалістів по безпеці й розробці мережних додатків, у тому числі й ведучий розробник популярного WEB-сервера Apache Раен Барнет (Ryan Barnett).

Вже в червні 2004 року в Internet були опубліковані перші результати роботи цієї групи – документ за назвою "Класифікація погроз" ("Threat Classification").

Видання цього документа переслідувало такі цілі: визначення всіх відомих атак на WEB-додатки, узгодження термінології, визначення структурованого підходу до класифікації атак.

У січні 2006 року цією же групою був опублікований документ під назвою "Критерії оцінки брандмауерів по захисту WEB-додатків" ("Web Application Firewall Evaluation Criteria") [17].

Цей документ не має юридичної сили й носить лише рекомендаційний характер. Він не містить ні алгоритмів, ні яких або обмежень, що накладають на розроблювальне програмне забезпечення. Документ являє собою набір характеристик, за допомогою яких стане можливо порівнювати різних брандмауерів для захисту WEB-додатків, які були й будуть розроблені. Також документ пропонує загальну термінологію, використання якої дозволить уникнути різночитань у середовищі розроблювачів і користувачів такого класу додатків.

Провівши детальний аналіз відомостей про методи здійснення атак на WEB-додатки, багато фахівців в області безпеки сходяться в думці, що можливо створити обмежену безліч відбитків (сигнатур) атак, які можуть бути використані для виявлення тієї чи іншої атаки з досить високою ймовірністю.

На сьогоднішній день найбільш успішним і популярним програмним брандмауером, що спеціалізує на захисті WEB-додатків, є проект ModSecurity. Цей брандмауер являє собою модуль для широко розповсюдженого WEB-сервера Apache. Модуль являє собою фільтр який перевіряє POST, GET і COOKIE параметри, які передаються між користувачем і віддаленим сервером у мережі Internet.

Варто зазначити, що ModSecurity вимагає кропіткого й точного настроювання за участю фахівця з безпеки WEB-серверу. Налаштування модуля "за замовчанням" не можуть використовуватися для захисту критичних до проникнення WEB-додатків (наприклад електронних банків або електронних магазинів).

Спробою створити найбільш повну конфігурацію для ModSecurity з урахуванням більшості можливих варіацій атак можна вважати рекомендації, опубліковані в книзі

видавництва O'Relly "Apache Cookbook". Це полегшило роботу з настроювання модуля, однак послуги фахівця для адаптації загальних рекомендацій з настроювання під конкретні завдання усе ще потрібні.

ModSecurity має істотний недолік – відсутність регулярного оновлення баз сигнатур атак. До недоліків цього модуля варто також віднести те, що він оперує лише жорстко заданими правилами й не має евристичних алгоритмів для детектування варіацій відомих атак і попередження нових типів атак. Крім того дії ModSecurity не враховують індивідуальних особливостей всіх WEB-додатків, які можуть обслуговуватися одним WEB-сервером.

Марсель Низамутдинов, один із провідних спеціалістів в області безпеки, указуючи на недоліки ModSecurity, у своїй книзі "Тактика защиты и нападения на WEB-приложения" опублікував ряд теоретичних прикладів успішних атак на захищений WEB-додаток.

Сучасна інфраструктура мережі Internet не дозволяє регулярно й систематично оновлювати бази сигнатур атак на WEB-додатки. Необхідно зазначити, що навіть якби була створена централізована оперативна система оновлення баз сигнатур, то це не стало б ідеальним рішенням проблеми хакерських атак на WEB-додатки в довгостроковій перспективі. У сучасному світі комп'ютерної злочинності хакери всі частіше стали автоматизувати свої проникнення, створюючи підмережі "комп'ютерів-зомбі", "троянських коней" і "хробаків", дії яких спрямовані проти WEB-додатків. Швидкість і масштаби атак з кожним днем все зростають. І іноді оновлення бази сигнатур може прийти занадто пізно, уже після того як атака відбулася.

У зв'язку з описаними вище недоліками існуючих рішень по захисту WEB-додатків в даній дипломній роботі автором запропоновано нову систему побудови захисту WEB-додатку і WEB-серверу взагалі. Запропонована система реалізує евристичні можливості за допомогою масиву нейронних мереж адаптивно-резонансної теорії, які оперують двійковими даними. Система працює на сьомому рівні моделі OSI і завдяки своїм унікальним властивостям, дозволяє не тільки ефективно боротися з існуючими типами атак, але й попереджати проведення нових типів атак. Основною перевагою системи є те, що вона не потребує оновлення бази сигнатур, бо будується на евристичному алгоритмі.

1.10 Висновки до розділу 1 та постановка задачі дослідження

В першому розділі магістерської роботи проведений огляд та аналіз інформаційної безпеки в мережі Internet, захист WEB-серверів, сучасні тенденції у розробці систем захисту

та проблеми створення безпечного середовища для функціонування WEB-додатку. За результатами проведеного огляду визначені задачі дослідження:

– здійснити вибір моделі мережі;
– визначити архітектуру мережі для проведення дослідження;
– розробити алгоритм навчання мережі;
– визначити переваги та недоліки моделі нейронної мережі;
– розробити засоби компенсації недоліків нейронної мережі.

З метою реалізації задачі дослідження розробити евристичну систему захисту WEB-додатків.

2 НЕЙРОННА МЕРЕЖА АРТ-1

2.1 Обґрунтування вибору моделі мережі

Як досліджувана модель нейронної мережі обрана мережа адаптивно-резонансної теорії (АРТ). Серед безлічі вже відомих моделей нейронних мереж є мережа, що схожа по своїй роботі з процесом мислення людини. Вона має здатність приймати рішення щодо подібності інформації, яка надійшла, з інформацією, що вже зберігається у пам'яті. Мережа АРТ-1 здатна приймати рішення на основі раніше отриманого досвіду (даних). Тому у якості моделі нейронної мережі для дипломної роботи взята саме нейронна мережа АРТ-1.

Мережа АРТ-1 є однією з різновидів мереж АРТ. Мережа АРТ-1 змодельована вперше Гроссбергом і Карпентером у середині 80 років минулого століття. АРТ-1 призначена для обробки образів, що містять двійкову інформацію.

АРТ-1 мережа змодельована як теорія, заснована на людському сприйнятті й обробці інформації. Поява нейронних АРТ мереж обумовлена спробою знайти відповідь на питання як біологічні організми здатні до пластичності при запам'ятовуванні нової інформації, при цьому не ставлячи під погрозу втрати стабільні данні, які було запам’ятовано раніше. Цю проблему Гроссберг назвав дилемою пластичності-стабільності [15]. Раніше вивчені й відомі моделі нейронних мереж при навчанні й подальшому розпізнаванні образів вимагали значних витрат часу на перенавчання при надходженні нового образу, тим самим вносячи зміни в зображення, що було запам’ятовано раніше. Такі мережі не могли дати стабільності при надходженні нової інформації. АРТ мережі, що буті більше схожими з біологічними мережами, були створені як ті, що не контролюються та самоадаптуються. Неконтрольовані з того погляду, що процес їхнього навчання може проходити без вчителя (тобто повністю в автономному режимі). Система сама проходить стадію навчання, виділяючи певні класи із пропонованих зображень. Система, заснована на неконтрольованому навчанні, завжди може регулюватися, на відміну від системи, призначеної для контрольованого навчання (навчання із вчителем), що ніколи не зможе навчатися без контролю.

Під самоадаптацією розуміється алгоритм пошуків образів у пам'яті. Нейронна мережа працює в умовах, що постійно змінюються, так що визначена схема пошуку, що відповідає деякій структурі інформації, може надалі виявитися неефективною при зміні цієї структури. У теорії адаптивного резонансу це досягається введенням спеціалізованої системи, що припиняє подальший пошук резонансу в пам'яті, і ухвалює рішення щодо новизні інформації.

Нейронна мережа адаптивної-резонансної теорії відносить вхідне зображення до одного зі сформованих класів у процесі навчання, якщо воно відповідає заданому критерію подібності й у достатньому ступені подібно із прототипом цього класу. Далі відбувається модифікація вхідного зображення для більшої відповідності із пропонованим зображенням – корегуються ваги зв’язків. Якщо вхідне зображення в недостатньому ступені подібно із пропонованим зображенням, у цьому випадку виділяється додатковий нейрон і формується новий клас зображень. Виділення додаткового нейрона під новий клас зображень відбувається завдяки наявності вільних, незадіяних нейронів у верстві, що розпізнає. Таким чином, запам'ятовуються нові зображення, запобігаючи модифікації зображень, що вже знаходяться у пам’яті.

Такі унікальні властивості нейронної мережі адаптивно-резонансної теорії зумовлені особливостями її структури та алгоритму функціонування, опис яких наведено у наступних підрозділах.

2.2 Архітектура нейронної мережі АРТ-1

В магістерській роботі розглядається модель нейронної мережі АРТ-1.

Базова архітектура мереж АРТ (рис. 2.1) включає три групи нейронів: поле F1 вхідних обробних нейронів, що складає із двох шарів елементів, шар Y-нейронів розпізнавальних нейронів і керуючий нейрон R.

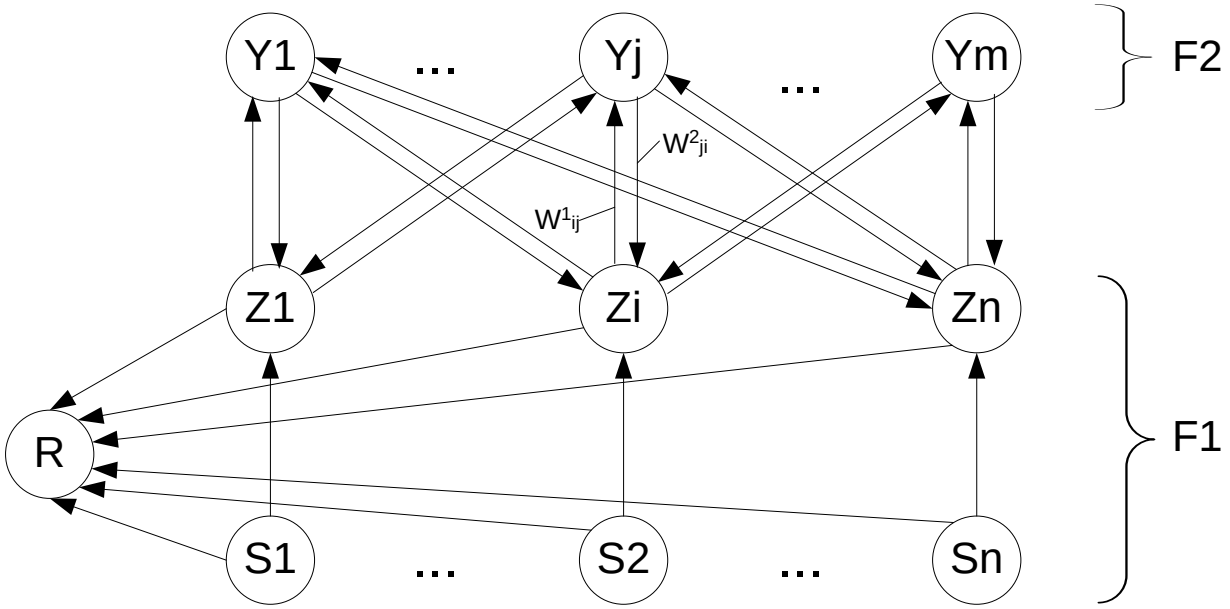


Рисунок 2.1 – Базова архітектура мережі АРТ

Архітектура мережі АРТ-1 крім наявності базової групи нейронів має додаткові зв'язки й елементи G1 і G2 (рис. 2.2).

Поле F1 вхідних обробних нейронів складається із двох шарів – вхідного шару S-елементів і інтерфейсного шару Z-елементів. Вхідний шар сприймає пропоноване зображення й передає отриману інформацію нейронам інтерфейсного Z-шару й керуючому нейрону R.

Кожний елемент Z_i (i = 1, ..., n) інтерфейсного шару пов'язаний з кожним елементом Y_j (j = 1, …, m) шару, що розпізнає, з Y двома видами зв'язків. Сигнали з інтерфейсного шару до шару Y передаються зв'язками, що йдуть знизу нагору з вагою W^1_{ij}, а із розпізнавального шару до інтерфейсного – зв'язками вагів W^2_{ji} , (j = 1, …, m, i = 1, …, n).

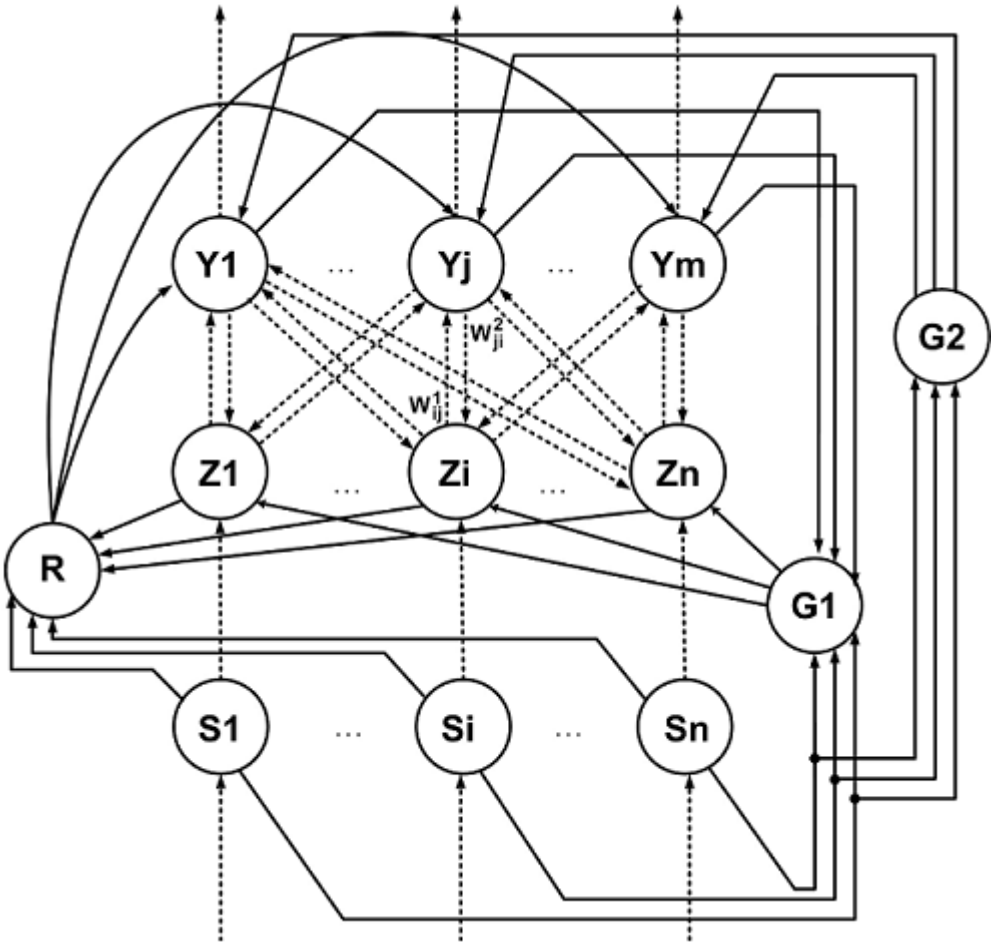


Рисунок 2.2 – Архітектура нейронної мережі АРТ-1

Шар Y є шаром конкуруючих нейронів, що змагаються. У будь-який час кожний елемент Y_j (j = 1, …, m) розпізнавального шару може перебувати в одному із трьох станів: 1 – активний, бере участь у змаганнях; 0 – неактивний, але нейрон може брати участь у

змаганнях; -1 – загальмований, не бере участь у змаганнях при пред'явленні поточного зображення.

Після пред'явлення вхідного зображення активним залишається тільки один нейрон, що розпізнає (нейрон-переможець), всі інші Y-елементи мають нульові або негативні вихідні сигнали. Виділений нейрон, що розпізнає, допускається до навчання вхідним зображенням тільки в тому випадку, коли його ваговий вектор зв'язків із шару Y до шару Z подібний до вхідного вектора. Це рішення приймається за допомогою R-нейрона й параметра подібності, а так само сигналів, що надходять із вхідного й інтерфейсного шарів елементів.

Якщо отриманий параметр подібності задовольняє заданому параметру подібності, то пропоноване зображення класифікується, щодо виділених класів при навчанні, відбувається коректування вагів зв'язків. Якщо ж параметр подібності не задовольняє заданому параметру, то поточний нейрон-переможець загальмовується й починається пошук іншого нейрона-переможця з нейронів, що залишилися, розпізнавального шару Y. При ситуації, коли всі нейрони шару, що розпізнає, загальмовані, виділяється новий клас зображення й коректуються ваги зв'язків.

Для подальшого розпізнавання вхідних образів була змодельована надбудова над верхнім розпізнавальним шаром нейронів. Вона являє з себе матрицю відповідностей, на горизонталі якої розташовані номери зображень, а по вертикалі - номера нейронів-переможців. У процесі розпізнавання, знаючи номер Y-нейрона, що спрацював, можна одержати увесь список подібних вхідному еталонних зображень. Ця програмна надбудова полегшує процес аналізу, надає людині, якщо це буде необхідно, пояснення того, чому було прийняте те чи інше рішення.

2.3 Алгоритм навчання мережі АРТ-1

При опису алгоритму використалися наступні позначення:

m – максимальне число елементів, що розпізнають;

n – число компонентів у вхідному векторі;

S^k – n-мірний бінарний вхідний вектор, k = 1, …, q;

q – число вхідних векторів;

$U_{вихS} = (U_{вихS1}, …, U_{вихSm})$ – вхідний шар;

$U_{вихZ} = (U_{вихZ1}, …, U_{вихZn})$ – інтерфейсний шар;

$U_{вихY} = (U_{вихY1}, …, U_{вихYm})$ – шар, що розпізнає;

||X|| - норма вектора X;

||Z|| – норма вектора Z;

P – заданий параметр подібності, 0<p<1;

P_{sh} – отриманий параметр подібності;

W^1_{ij} – вага зв'язку від елемента Z_i (i = 1, …, n) до елемента Y_j (j = 1, …, m);

W^2_{ji} – вага зв'язку від елемента Y_j до елемента Z_i (j = 1, …, m; i = 1, …, n)

L – константа, що перевершує одиницю.

Представимо алгоритм навчання мережі АРТ-1 крок за кроком.

Крок 1. Ініціалізація параметрів, завдання початкових значень: n, m, L, p, вагів зв'язків W_{ij}^1 та W_{ji}^2, шарів вхідного, інтерфейсного та розпізнавального ($U_{вихSi} = S_i^k$, $U_{вихZi} = 0$, де i = l, ..., n).

$$W_{ij}^1 = 1/(1+ n); \qquad (2.1)$$
$$W_{ji}^2 = 1.$$

Крок 2. Поки не виконуються умови завершення, виконуються кроки 3 – 14 алгоритму навчання нейронної мережі.

Крок 3. Для кожного вхідного зображення S^k (k = 1, .., q) виконуються кроки 4 – 14.

Крок 4. Задаються нульові вхідні сигнали всіх елементів, що розпізнаються, у шарі Y.

$$U_{вихYj} = 0, j=1, \ldots, m. \qquad (2.2)$$

Крок 5. Обчислюється норма вектора вихідних сигналів нейронів вхідного шару:

$$\| U_{вихS} \| = \|S^k\| = \sum_{i=1}^{n} S_i^k . \qquad (2.3)$$

Крок 6. Формуються вхідні й вихідні сигнали елементів інтерфейсного шару:

$$U_{вхZi} = U_{вихSi}, i =1, \ldots, n; \qquad (2.4)$$
$$U_{вихZi} = U_{вхZi} , i =1, \ldots, n.$$

Крок 7. Для кожного не загальмованого Y-нейрона ($U_{вихYj} \neq -1$) розраховується його вихідний сигнал:

$$U_{вихYj} = \sum_{i=1}^{n} W_{ij}^1 \cdot U_{вихZi}, j = 1, \ldots, m. \qquad (2.5)$$

Крок 8. Поки не знайдено Y-нейрон, ваговий вектор якого відповідно до заданого значення параметра подібності P відповідає вхідному вектору S^k, виконуються кроки 9 - 12.

Крок 9. У шарі Y-нейронів визначається нейрон Y_J, що задовольняє умові:

$$U_{вихYJ} \geq U_{вихYj}, \quad j = 1, .., \ m. \tag{2.6}$$

Якщо таких елементів декілька, те вибирається елемент із найменшим індексом. Якщо всі елементи розпізнавального шару $U_{вихYJ} = - 1$ загальмовані, вважається, що вхідне зображення не може бути класифіковане.

Крок 10. Розраховуються вихідні сигнали Z-елементів:

$$U_{вихZi} = U_{вихSi} \, W_{Ji}^2, \quad i = 1, \ldots, n. \tag{2.7}$$

Крок 11. Обчислюється норма вектора вихідних сигналів інтерфейсного шару:

$$\| U_{вихZ} \| = \sum_{i=1}^{n} U_{вихZi}. \tag{2.8}$$

Крок 12. Обчислюється параметр подібності P_{sh}:

$$P_{sh} = \|U_{вихZ}\| / \|S^k\|. \tag{2.9}$$

Якщо $P_{sh} < P$, тобто умова не виконується, елемент Y_J загальмовується ($U_{вихYJ} = - 1$), здійснюється перехід до кроку 8 алгоритму навчання нейронної мережі.

Якщо $P_{sh} \geq P$ та умова можливості навчання нейрона Y_J виконується, тоді здійснюється перехід до наступного кроку алгоритму.

Крок 13. Адаптуються ваги зв'язків елемента Y_J.

$$W_{ij}^1 = (LU_{вихZi})/(L-1+\|U_{вихZ}\|), \quad i=1,\ldots,n, \tag{2.10}$$

$$W_{Ji}^2 = U_{вихZ}, \ i=1, \ldots, n.$$

Крок 14. Перевіряються умови завершення. Умовами завершення роботи можуть бути: відсутність змін ваг W_{ij}^1 W_{ji}^2, якщо протягом епохи або досягнення заданого числа епох.

Крок 15. Завершення роботи.

2.4 Недоліки моделі нейронної мережі АРТ-1

Використовуючи класичну структуру нейронної мережі АРТ-1, при тестуванні роботи мережі, і були зроблені деякі зауваження, що наведено нижче.

1. Порушення динамічності системи. Неможливість динамічного розширення мережі при надходженні нових еталонних образів, коли всі нейрони вже були розподілені. При значенні параметра подібності близького до одиниці треба, щоб під кожне нове еталонне зображення, що надійшло, виділявся новий Y нейрон шару розпізнавання. При статичному розподілі нейронів на етапі навчання можлива ситуація, коли мережа не зможе запам'ятати новий вектор, через невідповідність подоби. У цій ситуації всі нейрони для вектора, що надійшов на вхід, будуть загальмовані, і подальше навчання мережі буде неможливим.

2. Можливе невірне розпізнавання образів. Логічне порушення при розпізнаванні вхідного двійкового вектора. При даній структурі мережі й значенні параметра подібності близьким до одиниці, з урахуванням розмірності вектора, що навчається, можна сказати, що при зміні трьох параметрів при формуванні розпізнаваного вектора (тобто, різниця між вхідним і еталонним вектором повинна становити не більше шістнадцяти одиничних значень) маємо значний ризик отримання невірних даних. Тобто при незначній зміні параметрів відбувається значні зміні у вхідному векторі. Тобто цілком легітимні дії користувача можуть бути розпізнані як нелегітимні і всі його подальші спроби встановити контакт з системою будуть заблоковані.

3. Неможливість простежування відповідності між номером навчального вектора й номером нейрона, що спрацював, для подальшого розпізнавання вхідних векторів.

4. Неможливість чіткого ухвалення рішення в процесі розпізнавання зображень для різних категорій користувачів при статичному завданні параметра подібності. При навчанні нейронної мережі часто трапляється така ситуація, при якій один нейрон запам'ятовує образ декількох зображень. Чим менше заданий параметр подібності мережі, тим більше еталонних векторів буде лягати на один нейрон. При цьому різні еталонні вектора можуть нести в собі різну інформацію й, відповідно, приймати різне рішення з того приводу, чи легітимні дії користувача чи ні. Така ситуація при заниженому параметрі подібності може призвести до того, що зловмисник проникне у система, а при завищеному – до того, що будуть заблоковані дії легітимних користувачів.

2.5 Засоби компенсації недоліків нейронної мережі АРТ-1

Для усунення недоліків роботи нейронної мережі в роботі зроблене наступне:

1. Для розв’язання проблеми порушення динамічності системи було ухвалене рішення – побудувати модель нейронної мережі з комбінуванням динамічних і статичних масивів. Динамічні масиви дозволять розширювати мережу на скільки це буде необхідним. Границю розширенню нейронній мережі ставить лише обсяг оперативної пам’яті комп’ютера;

2. Для розв’язання проблеми можливого невірного розпізнавання образів, коли при незначній зміні параметрів двійковий вектор отримує дуже значні зміни, які відбиваються на результаті розпізнавання, було прийнято особливі правила кодування вхідних параметрів. При обраних правилах кодування близькі по своїй суті значення вхідних параметрів мають близькі по двійковій структурі коди.

3. Для того, щоб спостерігати за процесом прийняття рішення нейронною мережею, до класичної структури мережі було додано спеціальні масиви, що динамічно розширюються. У цих масивах зберігається вся історія векторів, що були пов’язані з кожний нейроном мережі. Аналіз цієї інформації дозволяє зробити висновок чому саме мережа прийняла те чи інше рішення. Також ця інформація дозволяє зробити швидке перенавчання окремо взятого нейрона з виключенням помилково розпізнаного вектору (такі дії називаються "відкатом системи").

4. Для поліпшення якості розпізнавання образів було розроблену спеціальну систему нейронних мереж. Для кожної сторінки WEB-додатку, що захищається, відводиться одна нейронна мережа, яка несе в собі інформацію про всі легітимні дії з цією сторінкою. Нейронна мережа, що захищає окремо взяту сторінку, має не тільки здатність запам'ятовувати легітимні дії користувача, але й відрізняти легітимні дії від нелегітимних. Окрім набору нейронних мереж, що захищають окремі сторінки WEB-додатку, існує це одна додаткова нейронна мережа, що відповідає за класифікацію користувачів. Класифікація користувачів потрібна для того, щоб встановлювати для нейронних мереж, що захищають сторінки WEB-додатку, параметра подібності відповідно до кожного класу користувача. Це потрібно для того, щоб нейронна мережа ставилася до дій "подозрілих" користувачів з більшою "увагою".

Таким чином, стандартна структура нейронної мережі в процесі дослідження її недоліків, щодо розв’язання конкретної задачі, набила деяких нових рис. До нейронної мережі було додано спеціальні блоки для зберігання історії по кожному нейрону, а також було введено спеціальний механізм управління зміною параметра подібності для кожної

мережі, що захищає окремо взяті сторінки WEB-додатку. Змінена структура нейронної мережі зображена на рис. 2.3.

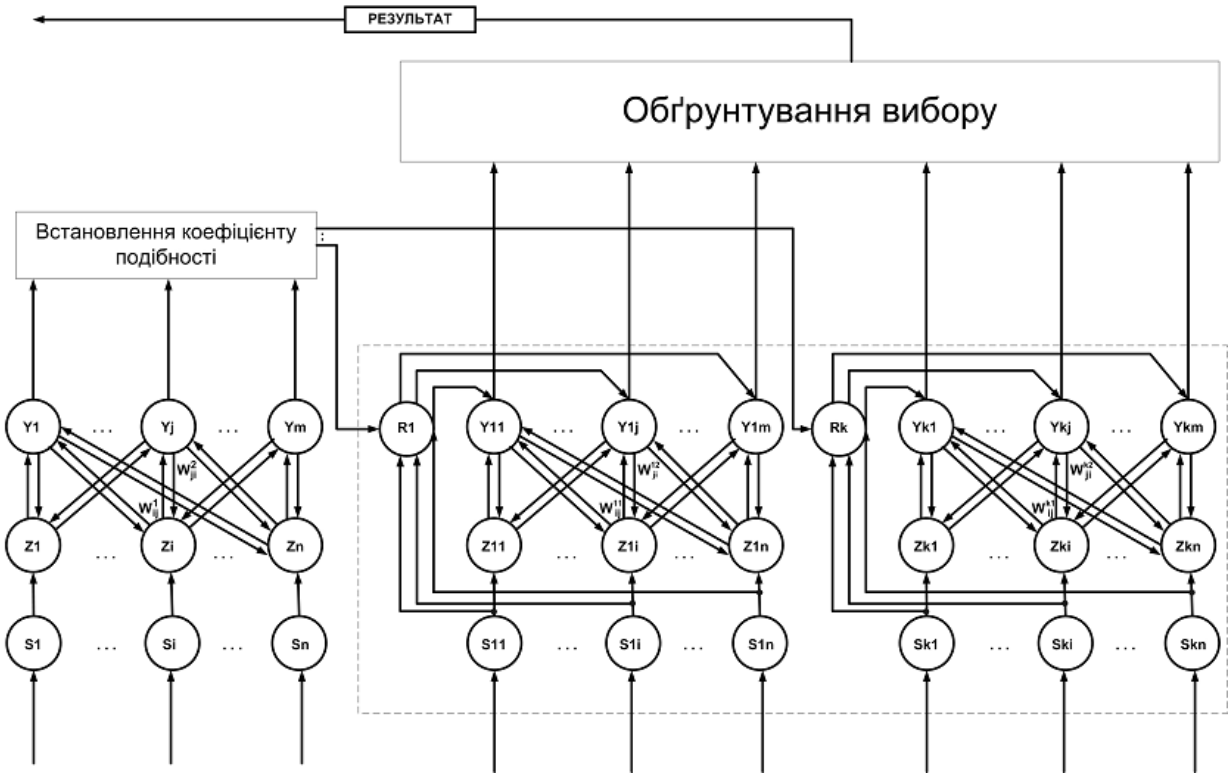


Рисунок 2.3 – Модифікована структура мережі АРТ-1

Після одержання результатів класифікації користувача (нейронна мережа зліва на рис. 3.3) та встановлення коефіцієнту подібності відповідно заданих правил, модифікуються коефіцієнти подібності для кожної з k нейронних мереж, що захищають сторінки WEB-додатку.

Якщо перша мережа, що відповідає за класифікацію користувачів не знайшла відповідного відбитку вектору, то вважаться, що користувач раніше не робив ніяких дій, які могли викликати "підозру" у системи захисту. В такому випадку для нейронних мереж, що захищають сторінки WEB-додатку встановлюється деяке значення параметра подібності за замовчанням.

Коли мережа, що відповідає за класифікацію користувачів, знаходить у своїй пам’яті відбиток вектору подібний до вектора, що надійшов, то для нейронних мереж, що захищають сторінки WEB-додатку, встановлюється більш низький коефіцієнт подібності, тобто система буде ставитися до такого користувача більш ретельно, бо його дії раніше викликали підозру.

Нейронні мережі, що захищають сторінки WEB-додатку працюють за таким же принципом, як і нейронна мережа, що класифікує користувачів, але результати роботи першої інтерпретуються з точністю до навпаки. Коли нейронна мережа знайшла у своїй пам’яті відбиток вектору, що надійшов на входи, то поведінка користувача вважається нормальною, бо на початковому етапі нейронну мережу навчили поняттю "нормальної поведінки".

Якщо нейронна мережа, що захищає окремо взяту сторінку WEB-додатку, не знаходить відповідності вхідного вектору до векторів, що раніше були збережені в пам’яті, то система починає стежити за таким користувачем. Якщо кількість дій, що визивають "занепокоєння" у системи перевищує деяке заздалегідь задане число, то система добавляє відбиток користувача до нейронної мережі класифікації користувачів з поміткою "підозрілий користувач". Останнє означає, що коефіцієнт подібності для такого користувача зменшується і якщо він у подальшому буде проводити "підозрілі" дії, то система класифікує його як зловмисника і блокує його доступу до WEB-додатку з видачею повідомлення адміністратору системи.

Адміністратор, проглянувши висновок системи і підтвердивши, що користувача було вірно класифіковано як зловмисника, тим самим навчає систему. Таким чином, чим більше часу працює система, тим "обізнаніше" вона стає.

Треба особливо зазначити, що система може цілком працювати без втручання адміністратора при відповідних налаштуваннях параметрів "лояльності" системи.

2.6 Висновки до розділу 2

В другому розділі обґрунтовано вибір моделі мережі. Як досліджувана модель нейронної мережі обрана мережа адаптивно-резонансної теорії (АРТ), яка має здатність приймати рішення щодо подібності інформації, що надійшла з інформацією та вже зберігається у пам'яті. Визначена архітектура та алгоритм навчання нейронної мережі, що передбачає покрокове виконання дій. Використовуючи класичну структуру нейронної мережі при тестуванні роботи мережі були зроблені зауваження. Для усунення недоліків роботи нейронної мережі в роботі розроблені засоби компенсації .

3 РОЗРОБЛЕННЯ ЕВРИСТРИЧНОЇ СИСТЕМИ ЗАХИСТУ WEB-ДОДАТКІВ

3.1 Виділення перспективного напрямку вдосконалення систем захисту інформації

Системи виявлення вторгнень, як вже було відзначено вище, не в змозі створити безпечне середовище функціонування WEB-додатку. Системи запобігання вторгнень (СЗВ) мають великий потенціал, однак точність і ефективність їх роботи на сучасному етапі розвитку технологій інформаційної безпеки викликає безліч дорікань, а значить ці додатки вимагають подальшої вдосконалення й потребують внесення корінних змін.

Доробка СЗВ може бути здійснена у двох основних напрямках:

– у напрямку вдосконалення сигнатурного аналізатора;
– у напрямку вдосконалення аналізатора аномалій (евристичний аналіз).

Метод сигнатурного аналізу добре випробуваний на антивірусному програмному забезпеченні й зараз активно впроваджується у СЗВ, де показує відмінні результати по відбиттю відомих атак.

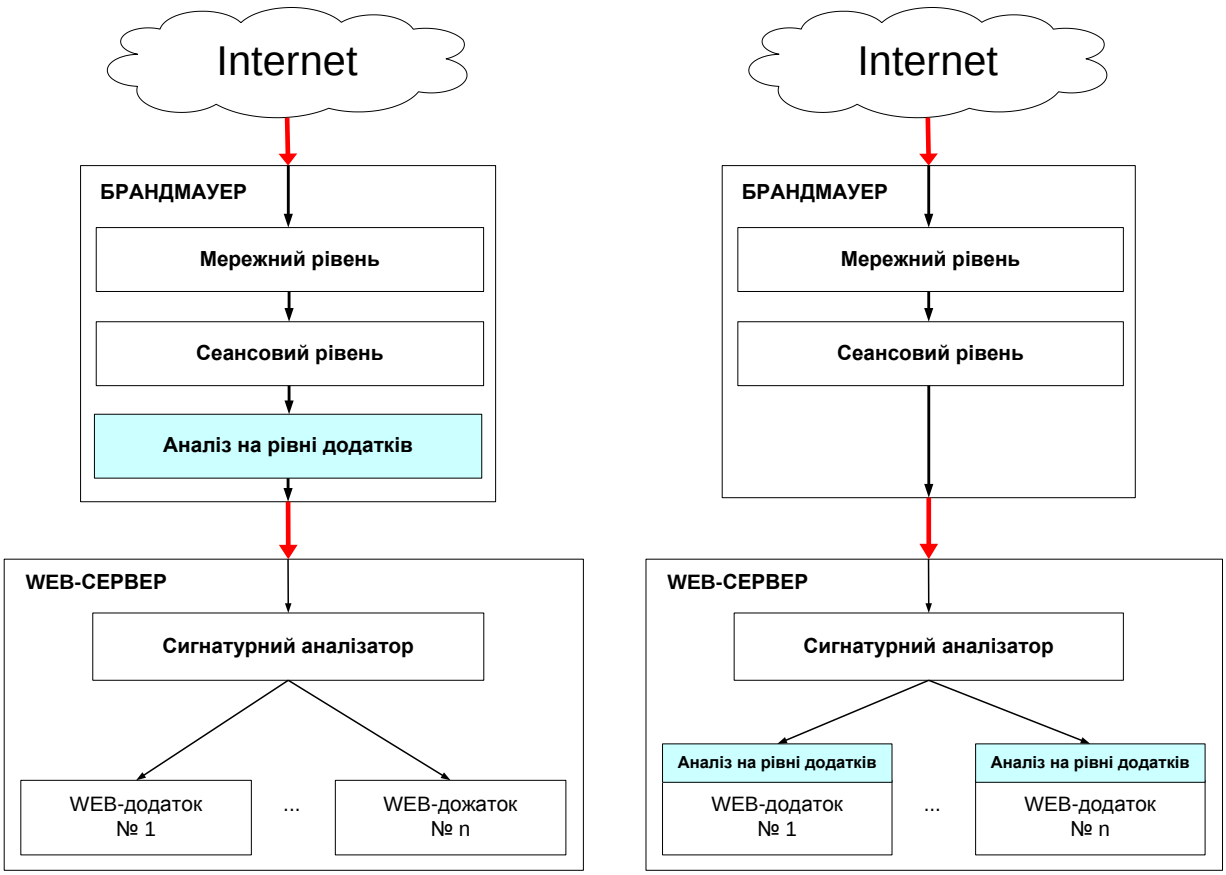
Метод аналізу аномалій поведінки користувача WEB-додатка заслуговує більше пильного вивчення.

3.2 Схема побудови захисту WEB-додатку

Більшу частину атак на WEB-додатки можна розпізнати тільки на рівні додатків (сьомий рівень моделі OSI). На рис. 3.1а зображена класична схема побудови захисту WEB-додатку, що реалізує аналіз даних на рівні додатків у рамках брандмауера. Однак брандмауер не враховує й не може враховувати всіх особливостей функціонування WEB-додатка, який він захищає, і, як наслідок, дуже часто не може відрізнити дії зловмисного користувача від дій легітимного користувача [16, 17].

З такої ситуації можливі два виходи: "навчити" брандмауер всім особливостям поведінки користувачів кожного WEB-додатку, що знаходиться на захищеному WEB-сервері, або ж винести контроль на рівні додатків з рамок брандмауера в рамки самого WEB-додатку (рис. 3.1б). Другий варіант представляється найбільш логічним і зручним.

Коли аналіз на рівні додатків переноситься в рамки самого WEB-додатку, він набуває інших якісних ознак, відкривається ряд додаткових можливостей для аналізу й збору інформації про потенційного атакуючого.



а) б)

Рисунок 3.1– Схеми побудови системи захисту WEB-додатку
а) класична схема; б) схема, що пропонується

У запропонованій схемі (див. рис. 3.1б) аналіз на рівні додатків здійснюється системою, що складається з набору так званих "давачів" і евристичного аналізатору. Система "давачів" збирає інформацію в декількох розрізах: POST-параметри, GET-параметри, COOKIE-параметри, операції з базою даних, операції з файловою системою, помилки й попередження в процесі роботи користувача та ін. Інформація від "давачів" й деяка інша додаткова інформація про користувача (така як IP адреса, час початку сесії та ін.) є вхідною для евристичного аналізатора.

3.3 Створення безпечного середовища для функціонування WEB-додатку

Ядром евристичного аналізатора є нейронна мережа адаптивної-резонансної теорії (АРТ). Для розв'язуваного класу завдань, як вже було зазначено вище, найбільше всього підходить мережа АРТ-1. Головне завдання, що покладене на нейронну мережу, є завдання виявлення атак, які не були виявлені на етапі сигнатурного аналізу.

Потрібно особливо відзначити, що немає необхідності навчати нейронну мережу всім відомим на сьогоднішній день видам атак. "Знати" існуючі атаки повинен сигнатурний аналізатор (перша ланка оборони), а евристичний аналізатор повинен "вміти відрізняти" поведінку легітимного користувача від поведінки зловмисного користувача (друга ланка оборони). Іншими словами, сигнатурний аналізатор повинен "вміти бачити" аномалії поведінки, щоб завчасно послати сигнал реагування.

Однак дуже важливо, щоб евристичний аналізатор не був занадто "жорстким" у визначенні відхилення поведінки користувача від нормального шаблону й у той же час він не повинен бути занадто "м'яким". Цю проблему можна вирішити двома способами:

– підбором оптимального коефіцієнта подоби;
– використання різних коефіцієнтів подоби для різних категорій користувачів.

Перший варіант недостатньо гнучкий для нашого завдання. У деяких системах підібрати єдиний коефіцієнт подоби може бути просто неможливо, тому звернемося до другого варіанта.

Виділимо чотири базові категорії користувачів WEB-додатка з погляду безпеки.

До першої категорії віднесемо так званих перевірених користувачів. Це користувачі яких адміністратор власноруч прописав у списки довірі. Цим користувачам дозволені будь-які дії без перевірки евристичним аналізатором. До цієї категорії рекомендовано включати суворо обмежене коло осіб. Частіше всього статус перевіреного користувача має адміністратор та один або декілька операторів системи.

До другої категорії віднесемо користувачів, дії яких не викликають підозри (яких, звісно, більшість). Таких користувачів евристичний аналізатор перевіряє у звичайному режимі, коли коефіцієнт подоби встановлено на середньому рівні.

До третьої категорії віднесемо "підозрілих" користувачів. Це такі користувачі, за якими була помічена деяка підозріла активність у попередні періоди часу (не обов’язково в межах поточної сесії), однак зібраних даних недостатньо, щоб визначити користувача як зловмисника. К цієї категорії користувач може попасти як в категорію користувачів, дії яких не викликають підозри, так і в категорію зловмисників.

До четвертої категорії віднесемо користувачів, яких було класифіковано як зловмисників. Для таких користувачів доступ до системи блокується повністю. Вилучити ідентифікатор користувача з цієї категорій (тим самим розблокувавши доступ до системи) може тільки адміністратор через панель адміністрування.

Для реалізації поставлених перед ним завдань евристичний аналізатор повинен складатися з декількох нейронних мереж АРТ-1. Кількість нейронних мереж повинна дорівнювати кількості сторінок WEB-додатку (у середньому до 25) і ще однієї нейронної

мережі, що відповідає за віднесення користувача до тієї або іншої категорії (і відповідно визначає коефіцієнт подоби для мереж, які захищають сторінки WEB-додатку).

Перед тим як WEB-додаток буде відкрито для доступу з Internet, адміністратор проводить навчання нейронних мереж, що захищають сторінки (кожна мережа свою сторінку). Адміністратор активізує режим навчання й починає роботу з додатком, намагаючись ініціювати "крайні ситуації", тобто такі ситуації, коли значення параметра (наприклад, розмір переданого файлу, кількість GET параметрів в одному запиті та ін.) досягають спочатку дозволеного мінімуму, а потім дозволеного максимуму. Такий режим роботи з додатком навчає нейронну мережу поняттю "нормальної поведінки" користувача. Поняття "нормальної поведінки" для різних сторінок сайту може сильно відрізнятися, тому для кожної сторінки сайту, що захищається, передбачена своя окрема нейронна мережа.

Нейронна мережа, що пройшла навчання, може виявляти аномалії поведінки користувачів і відносити останніх до однієї із трьох категорій: "звичайні" користувачі (відповідності серед збережених раніше векторів не знайдено), "підозрілі" користувачі (знайдено відповідність вектору в рамках коефіцієнту подоби) або зловмисники (знайдено точну відповідність до вектора, що було раніше запам’ятовано). Після закінчення навчання адміністратор переводить мережу в робочий режим і відкриває доступ до WEB-додатку з Internet.

Система "давачів" збирає й віддає у вигляді двійкового вектора на вхід нейронної мережі деяку інформацію:

– кількість і сумарний обсяг GET-параметрів, що передаються у вигляді URL;

– кількість і сумарний обсяг POST-параметрів, що передаються у тілі HTTP пакету;

– кількість і сумарний обсяг COOKIE-параметрів, що збережені під час сеансу в сесії;

– MIME типи переданих файлів, якщо такі було передано;

– номер відповіді із заголовка HTTP, яка показує чи вірно був сформований запит до сторінки сайту;

– імена таблиць у базі даних, що було використано при генерації сторінки;

– дії проведені з таблицями в базі даних (вибірка, вставлення, оновлення, видалення, об’єднання та ін.);

– номери помилок, які виникли при роботі скриптів, або нуль, якщо таких не виникло.

Нейронна мережа порівнює наданий на вхід вектор з векторами, що були відкладені в пам'яті нейронної мережі в процесі навчання, і робить висновок чи нормальна поведінка користувача, що призвела до створення такого вектора, чи ні. Якщо мережа не може точно визначити, що відбувається атака, однак ступінь відхилення від моделі нормальної поведінки досить велика, то дані про потенційного зловмисника запам'ятовуються окремою мережею,

яка відповідає за віднесення користувачів до тієї або іншої категорії. Наступного разу, коли користувач повернеться на сайт і буде проводити деякі дії, що викликають підозру, нейронна мережа класифікує його як "підозрілого" користувача й посилить "жорсткість" евристичного аналізу шляхом корекції коефіцієнта подоби. Якщо підозри підтвердяться, то користувач буде переведений у категорію зловмисників, і тоді всі його наступні дії будуть заблоковані.

Незважаючи на те, що нейронна мережа, що відповідає за віднесення користувача до тієї або іншої категорії, і нейронна мережа, що відповідає за захист конкретної сторінки сайту, мають різні функціональні призначення, робота їх заснована на одному й тому ж принципі. Відмінність цих мереж складається лише в тих даних, які вони запам'ятовують. Перша мережа запам'ятовує дані про підозрілого користувача (IP адреса, країна, найменування й версія браузера, найменування й версія операційної системи, мова системи, є чи підтримка Flash, є чи підтримка Java, кількість точок на екрані, глибина кольорів, стартова сторінка браузера та ін.), а друга – дані про нормальну поведінку користувачів системи. Аналізуючи вихід першої нейронної мережі, ми робимо висновок про необхідність підвищення коефіцієнта подоби при перевірці за допомогою другої нейронної мережі. Аналізуючи вихід другої нейронної мережі, ми робимо висновок про те нормальна поведінка користувача, або ж вона відхиляється від шаблона нормальної поведінки.

3.4 Приклад функціонування системи захисту

Як вже було сказано вище, нейроні мережі, що захищають сторінки WEB-додатку, і нейронна мережа, що відповідає за класифікацію користувачів, працюють на одному й тому ж самому принципі, тому в даному підрозділі буде наведений приклад функціонування лише нейронної мережі, що відповідає за класифікацію користувачів. Буде показано, що ця нейронна мережа здатна розпізнати зловмисника, який раніше проявляв активність, навіть якщо він вжив заходів, що ускладнюють його ідентифікацію евристичною системою.

У реальній нейронній мережі вхідний вектор, що відповідає за ідентифікацію користувача, досить великий, ми ж заради простоти обмежимося вектором довжиною в п'ять бітів.

Перші два біти нашого вектора визначають найменування клієнту користувача (00 – Internet Explorer, 01 – FireFox, 10 – Opera, 11 – інший), третій біт визначає чи встановлений на комп'ютері Flash програвач (0 – не встановлений, 1 – встановлений), четвертий біт визначає мова системи(0 – російська, 1 – інша) і нарешті останній біт визначає тип операційної системи (0 – UNIX подібна, 1 – операційна система з сімейству Windows).

Припустимо, що в нас є дані про трьох користувачів, до яких необхідно застосувати більше "жорсткий" евристичний аналіз: $X_1 = (00001)^T$, $X_2 = (00110)^T$, $X_3 = (01111)^T$. Також у нас є дані про користувача X_3, що з метою маскування змінив свій браузер з FireFox на якийсь інший браузер і намагається провести деякі несанкціоновані дії. Вхідний вектор для цього користувача буде мати вигляд $X_4 = (11111)^T$.

На рис. 3.2 зображена спрощена схема мережі АРТ-1.

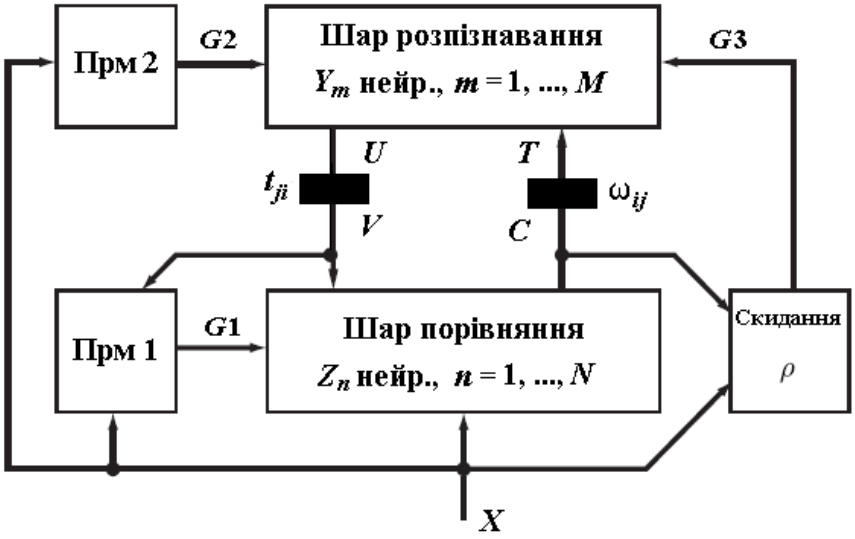


Рисунок 3.2 – Спрощена схема нейронної мережі АРТ-1

Вхідний вектор мережі $X = (X_1, ..., X_n, ..., X_N)$ має N компонент. У шарі розпізнавання запам'ятовується M класів образів, по одному класу на кожний нейрон m = 1, ..., M. Основну роботу із класифікації робить шар порівняння й шар розпізнавання. Схеми приймачів (Прм 1, Прм 2) і схема скидання управляють режимом роботи мережі й генерують керуючі сигнали G1, G2 і сигнал скидання G3 відповідно. Матриця безперервних ваг і матриця двійкових ваг на рис. 3.2 позначені ω_{ij} й t_{ji} відповідно.

Вхідний двійковий вектор X, при проходженні через мережу, проходить такі перетворення: $X \to C \to T \to U \to V$. Тут C – вихідний вектор шару порівняння, T – вхідний вектор шару розпізнавання, U – вихідний сигнал шару розпізнавання, V – вхідний вектор для шару розпізнавання й сигнал заборони для Прм 1.

Параметр подоби візьмемо $\rho = 0{,}6$. Матриці ω_{ij} й t_{ji} ініціалізуються початковими значеннями згідно:

$$0 < \omega_{ij} < \frac{\lambda}{\lambda - 1 + N}; \qquad \frac{\beta - 1}{d} < t_{ji} \le 1,$$

де $\lambda \in (1, 2]$; β - константа; $d > 0$.

Розмірність вектора N = 5, параметр λ приймемо як λ=1,5. Одержимо матриці ваг:

$$\omega_{ij} = 0{,}2;\ t_{ji} = 1,\quad i = \overline{1, 5};\ j = \overline{1, 4}.$$

Навчимо мережу першим трьом векторам.

При надходженні на шар порівняння вектора X_1 на виході шару порівняння одержуємо вектор $C_1 = X_1$. На всіх входах шару розпізнавання маємо сигнал:

$$T_m = \sum_{i=1}^{5} \omega_{1i} C_i = 0{,}2 \cdot 0 + 0{,}2 \cdot 0 + 0{,}2 \cdot 0 + 0{,}2 \cdot 0 + 0{,}2 \cdot 1 = 0{,}2,\ m = \overline{1, M}.$$

Нейроном-переможцем стає нейрон з найменшим індексом, тобто нейрон Y1. Ваги зв'язків t1n ($n = \overline{1, N}$) приймають значення: (0, 0, 0, 0, 1).

Обчислимо параметр подоби для вектора X_1:

$$S = \frac{1 \cdot 0 + 1 \cdot 0 + 1 \cdot 0 + 1 \cdot 0 + 1 \cdot 1}{0 + 0 + 0 + 0 + 1} = 1.$$

Так як S > ρ , то значить поданий на вхід вектор X_1 створить перший збережений у пам'яті образ. Відповідно буде відкоректована матриця ω_{ij}:

$$\omega_{1i} = \frac{1{,}5 \cdot 0}{0{,}5 + 0 + 0 + 0 + 0 + 1} = 0, \qquad i = \overline{1, 4}; \quad \omega_{15} = \frac{1{,}5 \cdot 1}{0{,}5 + 0 + 0 + 0 + 0 + 1} = 1.$$

Далі на вхід будуть подані вектора X_2 і X_3, які також будуть "запам’ятовані" мережею. В результаті навчання матриці ω_{ij} й t_{ji} будуть мати вигляд:

$$\omega_{ij} = \begin{vmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0{,}6 & 0{,}6 & 0 \\ 0 & 0{,}33 & 0{,}33 & 0{,}33 & 0{,}33 \\ 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 \end{vmatrix}; \qquad t_{ji} = \begin{vmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{vmatrix}.$$

Атакуючий $X_4 = (11111)^T$, змінивши свій браузер, намагається залишитися непоміченим мережею. У цьому випадку $T_1 = 1$, $T_2 = 1{,}2$, $T_3 = 1{,}32$. Вибираємо нейрон Y_3 с максимальним значенням T. Розрахуємо для нього S = 0,8 > ρ . У такий спосіб вектор X_4 був правильно віднесений до третього класу, тобто зробивший спробу залишитися непоміченим атакуючий все ж таки був правильно класифікований.

Нейронні мережі, які захищають окремі WEB сторінки сайту, працюють по тому ж принципу, але результат їхньої роботи інтерпретується з точністю до навпаки: якщо була знайдена відповідність вхідного вектора вектору в пам'яті мережі, то це нормальна ситуація, а якщо відповідності не було знайдено, то, можливо, ми маємо справу з атакою й необхідно більш пильно стежити за поточним користувачем.

3.5 Вибір мови програмування для реалізації системи

Для створення програми, що реалізує захист WEB-додатку з можливостями евристичного аналізу обрано мову PHP.

Мова PHP має такі переваги серед інших мов програмування:

– простота синтаксису;

– швидкість інтерпретатору;

– в PHP вбудовані бібліотеки для роботи з MySQL, PostgreSQL, mSQL, Oracle, dbm, Hyperware, Informix, InterBase, Sybase;

– через стандарт відкритого інтерфейсу зв'язку з базами даних (Open Database Connectivity Standart — ODBC) можна підключатися до всіх баз даних, до яких існує драйвер;

– безкоштовність;

– наявність вихідного коду.

З точки зору типізації, PHP є вільно типізованою мовою програмування. Немає необхідності явного визначення типу змінних, хоча така можливість існує. В разі звернення до змінної, ядро PHP трактує її тип відповідно до контексту. За необхідності можливе приведення змінної до певного типу за допомогою відповідних конструкцій мови. Також можливе визначення типу відповідної змінної на певному етапі виконання сценарію. Імена змінних не чутливі до регістру символів.

PHP надає широкий спектр функцій для пошуку та заміни тексту. Для цього використовують як традиційний підхід, так і спеціальний підхід, що базується на використанні регулярних виразів. При цьому в мові реалізована підтримка двох видів регулярних виразів — Perl-сумісні та POSIX-сумісні, що розрізняються за синтаксисом та особливостями роботи.

До змішаних типів належать масиви, хеши та об'єкти. Масиви в сенсі мови є наборами змінних, що згруповані в єдину змінну. Вимога однотипності наповнення масивів не ставиться. Технічно, масиви являють собою впорядковані карти, що відображають ключові значення на позиції змінних даних. Вмістом значення, на яке вказує ключ може бути будь-

чим, що можна подати у вигляді змінної. Не існує жодних обмежень, крім об'єму пам'яті, що накладаються на кількість ключів масиву.

Оператори в сенсі мови дозволяють виконувати відповідну дію над одним чи кількома операндами. Оператори бувають трьох типів — унарні, бінарні та тернарні. Оператори, як і в інших мовах характеризуються не лише дією, а й асоціативністю та приоритетністю. Особливістю булевих операцій порівняння – розрізнення двох класів (з врахуванням типу і без врахування типу), при якому відбувається приведення до відповідного типу. Округлення відбуваються завжди в меншу сторону. В мові реалізовані особливі класи операторів — виконання, управління помилками та перевірки приналежності до класу.

Функції в сенсі мови є контейнерами коду. На цьому і базується можливість умовного визначення функції. В цьому випадку висувається вимога попередньої декларації викликаної функції, що не обов'язково в інших випадках. Можливості перевизначення чи деактивації функції не існує. Результат, який повертає функція може мати будь-який тип.

В мові реалізована функціональність посилань. Можливо створити скільки завгодно синонімів, що посилаються на єдиний сегмент даних. При вивільненні будь-якого з псевдонімів, сегмент даних залишається в пам'яті до моменту завершення сценарію або вивільнення усіх посилань.

Протокол HTTP, засобами якого, як правило, обмінюються інформацією клієнт та Web-сервер не надає змогу зберегти стан сеансу взаємодії. Це випливає із тим, що між клієнтом та сервером не встановлюється постійне з'єднання і клієнт не надає жодних відомостей, що можуть виділити його з поміж інших активних на протязі деякого часу. Альтернативою COOKIES є концепція сесій, яка знайшла свою реалізацію в PHP. В сесії можна зберігати різні дані, включаючи об'єкти.

Тісна інтеграція PHP з WWW технологією (насамперед з протоколом HTTP) зробило цю мову ідеальною мовою для створення WEB-додатків. Розроблювана система захисту є нічим іншим як WEB-додатком.

Слід зазначити, що у PHP є один великий конкурент – це технологія Active Server Pages.

Active Server Pages (ASP, укр. активні серверні сторінки) – це технологія від компанії Microsoft, що дозволяє динамічно формувати автоматично оновлюванні WEB-сторінки з боку WEB-сервера. Технологія подається у формі додатку до WEB-серверу Internet Information Services (IIS).

Більшість сторінок, що створені за допомогою даної технології, написані мовою C#, але WEB-майстер вільний використовувати будь-яку мову, за умови, що для неї існує та проінстальований відповідний Active Scripting механізм.

Через те, що ASP сьогодні використовують для створення майже 20% WEB-додатків у мережі Internet, для подальшої комерційної реалізації розробленої системи захисту буде необхідна розробка версії ще й на ASP.

Версія для ASP та серверу IIS буде алгоритмічно повністю аналогічна версії для PHP та серверу Apache, але буде виконана у базисі іншої мови програмування. Таким чином показники ефективності функціонування системи залишаться незмінними.

3.6 Організація вхідних та вихідних даних

Нейронна мережа ART-1 має можливість оперувати лише двійковими даними, тому встає необхідність кодування вхідних даних для подальшого перетворення у двійкове уявлення. У табл. 3.1 наведено повний перелік вхідних даних для нейронної мережі класифікації користувачів з зазначенням правил їх кодування.

Таблиця 3.1 – Вхідні параметри мережі класифікації користувачів

Назва параметру	Довжина	Кодування
IP адреса	4 по 1 байту	Відповідно до ASCII
Країна	1 байт	Цифрове кодування відповідно до ISO 3166
Назва браузера	1 байт	0 – Internet Explorer 1 – Opera 2 – Mozilla FireFox 3 – інший
Версія браузера	4 по 1 байту	Відповідно до ASCII
Операційна система	1 байт	0 – Windows 1 – UNIX подібна 2 – інша
Версія операційної системи	4 по 1 байту	Відповідно до ASCII
Чи є підтримка Java	1 байт	255 – є 0 – немає
Чи є підтримка JavaScript	1 байт	255 – є 0 – немає
Чи є підтримка Flash	1 байт	255 – є 0 – немає

Режим екрану	1 байт	0 – 640x480 1 – 800x600 2 – 1024x768 3 – 1280x1024 4 – інший
Кількість кольорів	1 байт	0 – 8 біт 1 – 16 біт 2 – 24 біта 3 – 32 біта 4 – інше

В табл. 3.2 наведено повний перелік вхідних даних для нейронної мережі, що захищає сторінку додатку.

Таблиця 3.2 – Вхідні параметри мережі, що захищає сторінку додатку

Назва параметру	Довжина	Кодування
Кількість GET параметрів	1 байт	Переводиться у двійкову форму як є
Об’єм GET параметрів	6 по 1 байту	Відповідно до ASCII
Кількість POST параметрів	1 байт	Переводиться у двійкову форму як є
Об’єм POST параметрів	6 по 1 байту	Відповідно до ASCII
Кількість COOKIE параметрів	1 байт	Переводиться у двійкову форму як є
Об’єм COOKIE параметрів	6 по 1 байту	Відповідно до ASCII
MIME тип файлу, що завантажується	1 байт	Кодування відповідно до RFC 2822
Код відповіді HTTP	1 байт	0 – для коду 200 (документ є на сервері) 1 – для коду 301 (документ перенесено) 2 – для коду 302 (документ тимчасово перенесено) 3 – для коду 401 (потрібна

		авторизація) 4 – для коду 403 (доступ заборонено) 5 – для коду 404 (документ не знайдено) 6 – для коду 500 (внутрішня помилка серверу) 7 – інший код
Таблиці в базі даних, що було використано	8 по 1 байту	Відповідно до ASCII
Дія з таблицею	1 байт	0 – update 1 – delete 2 – insert 3 – select 4 – інше
Номер помилки, що виникла	1 байт	Відповідно ASCII, або 0

Вихідними даними для мережі, що класифікує користувачів, є число, що показує чи було знайдено відповідність вхідного образу до образу, раніше збереженого в пам’яті. Відповідно цього результату програмна надбудова над нейронною мережею з врахуванням коефіцієнту подоби відносить користувача до однієї з трьох категорій користувачів і встановлює відповідні коефіцієнти подоби для нейронних мереж, що захищають сторінки WEB-додатку.

Вихідними даними для мережі, що захищає сторінки WEB-додатку, є число, що показує чи було знайдено відповідність вхідного образу до образу, що раніше було збережено в пам’яті. Якщо відповідність було знайдено, то система робить висновок про нормальну поведінку користувача, у іншому випадку (з врахуванням коефіцієнту подоби) робиться висновок про те, що дії користувача викликають підозру і за ним треба більш пильно стежити.

Нейронні мережі можуть працювати у двох режимах: у режимі навчання і у звичайному робочому режимі. У режимі навчання нейронна мережа запам’ятовує подані на вхід вектори, а у робочому режимі нейронна мережа класифікує вектори.

3.7 Ефективність евристичної системи

Евристична система виявлення та відбиття атак на WEB-додатки відповідно до концепції ешелонованої оборони [18, 19] утворює третю ланку захисту. Данні потрапляють на вхід нейронних мереж евристичного аналізатора вже після того як вони пройшли фільтрацію брандмауером та сигнатурним аналізатором (який може входити як в брандмауер так і у склад WEB-серверу).

Таким чином евристична система виявлення і відбиття атак компенсує недоліки [20] притаманні сигнатурним методам аналізу: неможливість виявлення модифікованих, неможливість виявлення нових типів атак, неможливість врахувати особливості побудови WEB-додатку, що захищається.

Для того, щоб підтвердити ефективність розробленої системи було проведено тести на реальному WEB-сервері у мережі Internet.

Як тестовий майданчик було обрано сайт, що міститься за адресою http://www.altsolution.net на базі хостіг-провайдеру HVOSTING (http://www.hvosting.net). WEB-сервер на якому розміщено цей сайт встановлено на апаратному сервері з конфігурацією: dual Xeon WoodCrest 1.8Ghz, дискова система – 6x SATAII Seagate 7200.10 160G, що з'єднані у RAID5, пам'ять 4Gb FB-DIMM Reg ECC. Сервер захищено вбудованим в операційну систему FreeBSD брандмауером та сигнатурним аналізатором ModSecurity з стандартними налаштуваннями.

Для початкової тестової перевірки можливостей евристичної системи було створено WEB-додаток з однієї сторінки. У WEB-додатку біло залишено уразливість типу SQL injection [21, 22], що пов'язана з несанкціонованим додаванням SQL коду до запитів.

При перевірці на SQL injection було використано HTTP-запит такого виду: http://www.altsolution.net/index.php?id=123))+UNION+select+name, password+from+users+where+1. Такий запит при відсутності системи захисту привів би до виводу даних про всіх користувачів системи (у тому числі і їх паролів), а не тільки даних про гостей сайту.

Запит було пропущено брандмауером, бо для нього така послідовність символів цілком легітимна і не порушує специфікацію протоколу HTTP. ModSecurity, який має правила для виявлення атак типу SQL injection, теж пропустив ці данні, бо в його правилах було зазначено, що всі атаки типу SQL injection повинні містити в собі лапки. Тестовий запит навмисно було побудовано без лапок з використанням тої особливості версій MySQL 4.X, що запит може об'єднуватися зі ще одним запитом (UNION) без лапок.

Евристичний аналізатор отримав данні про запит и знайшов в ньому таку конструкцію мови SQL як UNION. При навчанні нейронної мережі на вхід подавалися вектори, які містили тільки конструкцію SELECT, тому нейрона мережа відразу виявила відхилення від шаблону нормальної поведінки.

Тепер проведемо комплексний тест на вразливості WEB-додатку для цього використаємо автоматизовану систему online перевірки XSpider від провідного розробника систем аудиту Positive Technologies.

На тестову систему встановимо WEB-додаток PHPBB, що являє собою форум з деякими додатковими можливостями.

Тестування будемо проводити в чотири етапи. Перший етап буде проходити з виключеним ModSecurity та виключеним евристичним аналізатором. Другий етап буде проходити з включеним ModSecurity та виключеним евристичним аналізатором. Третій етап буде проходити з виключеним ModSecurity та включеним евристичним аналізатором. Та четвертий етап буде проходити з включеним ModSecurity та включеним евристичним аналізатором.

На рис. 3.3 наведено сумарні результати тестування на першому етапі, коли захист був майже відсутній.

Рисунок 3.3 – Результати перевірки XSpider WEB-додатку при виключених ModSecurity та евристичному аналізаторі

Сумарна кількість знайдених уразливостей становить 128 штук (без урахувань підозр на уразливості).

На рис. 3.4 наведено сумарні результати тестування на другому етапі. На цьому етапі було використано лише стандартний засіб захисту ModSecurity, що було встановлено і налаштовано провайдером. Зазначимо, що налаштування ModSecurity не були оптимізовані під WEB-додаток, що тестувався.

Рисунок 3.4 – Результати перевірки XSpider WEB-додатку при включеному ModSecurity та виключеному евристичному аналізаторі

Сумарна кількість уразливостей скоротилася до 41 одиниці (без урахувань підозр на уразливості).

На рис. 3.5 наведено сумарні результати тестування на третьому етапі, на якому ModSecurity було відключено, а евристичний аналізатор включено.

Рисунок 3.5 – Результати перевірки XSpider WEB-додатку при відключеному ModSecurity та включеному евристичному аналізаторі

Сумарна кількість уразливостей становить 28 одиниць, що вже на цьому етапі менше ніж на другому етапі.

На рис. 3.6 наведено сумарні результати тестування на четвертому етапі, на якому ModSecurity та евристичний аналізатор було включено. Слід зазначити, що данні проходили спочатку через ModSecurity а потім потрапляли на евристичний аналізатор.

Рисунок 3.6 – Результати перевірки XSpider WEB-додатку при включеному ModSecurity та включеному евристичному аналізаторі

Сумарна кількість уразливостей, виявлених на четвертому етапі тестування, становить 16 одиниць.

Можна зробити підсумок, що використання евристичного аналізатору, як додаткової ланки захисту, зменшило кількість виявлених уразливостей на 39%, а відповідно і зменшило можливості зловмисників для проведення атаки на WEB-додаток.

3.8 Розробка інтерфейсу користувача

Інтерфейсна частина програми "Система евристичного виявлення та відбиття атак на WEB-додатки" являє собою набір XHTML сторінок, які генеруються серверними скриптами, що написані на мові PHP.

Головне меню програми, що наведено на рис. 3.7, містить такі пункти:

– теоретичні аспекти;
– нейронна мережа класифікації користувачів;
– нейронна мережа захисту сторінок;
– налаштування програми.

Кожний з цих пунктів посилається на окрему сторінку.

Всі данні, що система отримує від користувача зберігаються у базі даних, що знаходиться на сервері в Internet.

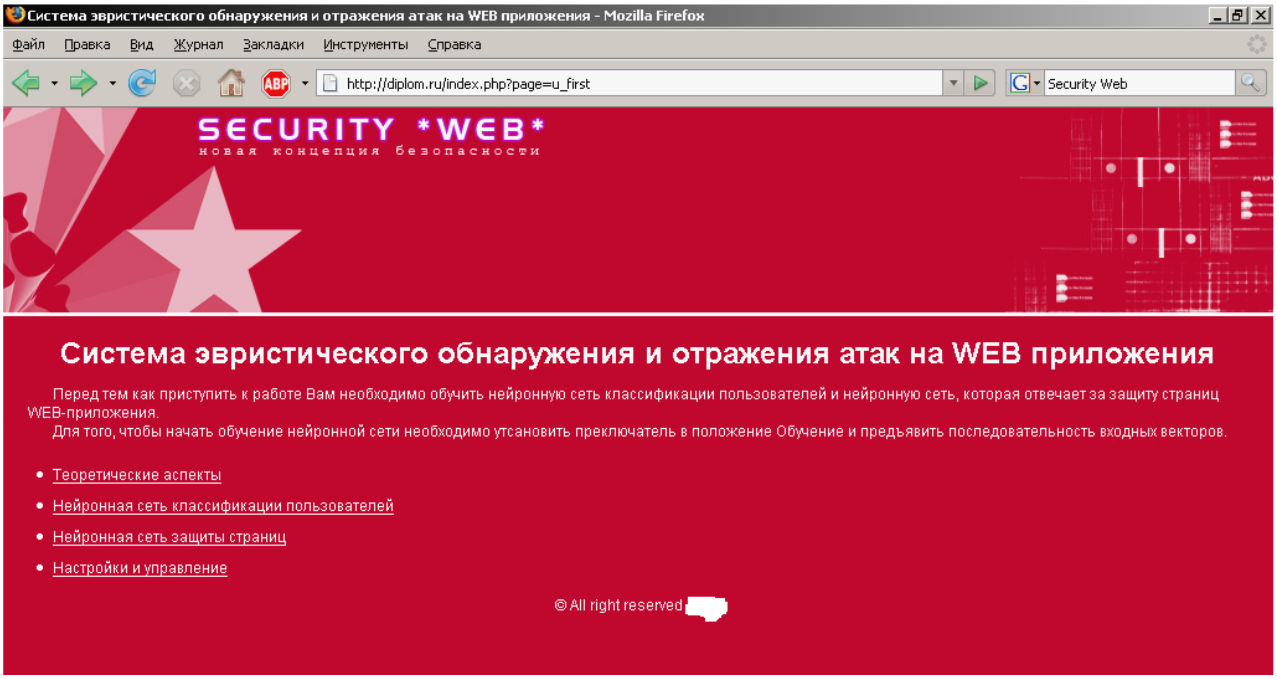


Рисунок 3.7 – Головне меню програми

3.9 Нейронна мережа класифікації користувачів

При виборі пункту головного меню "Нейронна мережа класифікації користувачів" користувач отримує доступ до форми, яка дозволяє оперувати параметрами, які подаються на вхід мережі, що класифікує користувачів.

Доступні такі параметри: IP адреса, країна, найменування браузеру, версія браузеру, найменування операційної систем, версія операційної системи, чи є підтримка Java, чи є підтримка JavaScipt, чи є підтримка Flash, дозвіл екрану, глибина кольорів.

Нейронна мережа може перебувати у режимі навчання та у робочому режимі. Подання вектору на вхід нейронної мережі у режимі навчання призводить до зміні матриць вагових коефіцієнтів. В режимі навчання користувачу видаються повідомлення про те, який нейрон запам’ятав вхідний вектор (рис. 3.8).

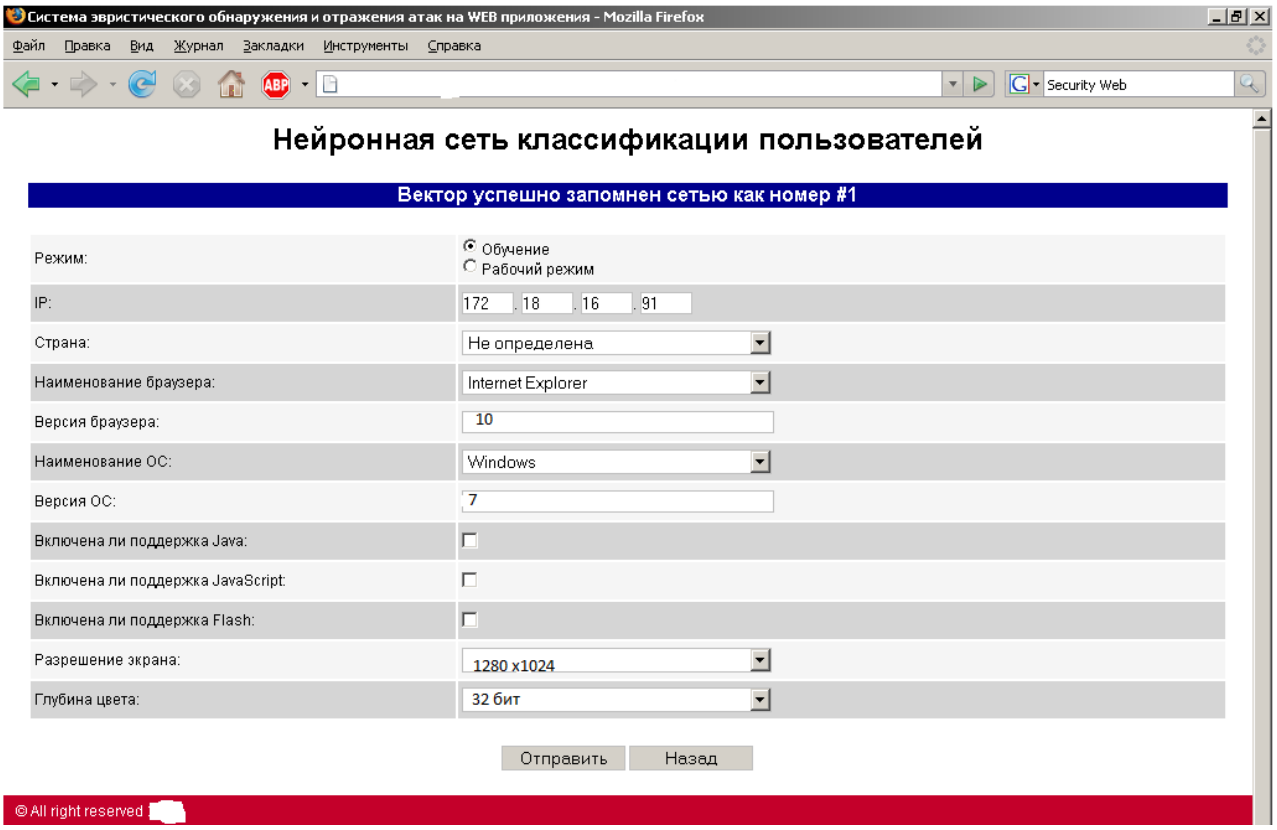


Рисунок 3.8 – Навчання мережі, що відповідає за класифікацію користувачів

В робочому режимі програма не змінює значення матриць вагових коефіцієнтів. Якщо система розпізнала поданий на вхід вектор – то користувачу видається повідомлення, що знайдено сигнатуру атакуючого (рис. 3.9).

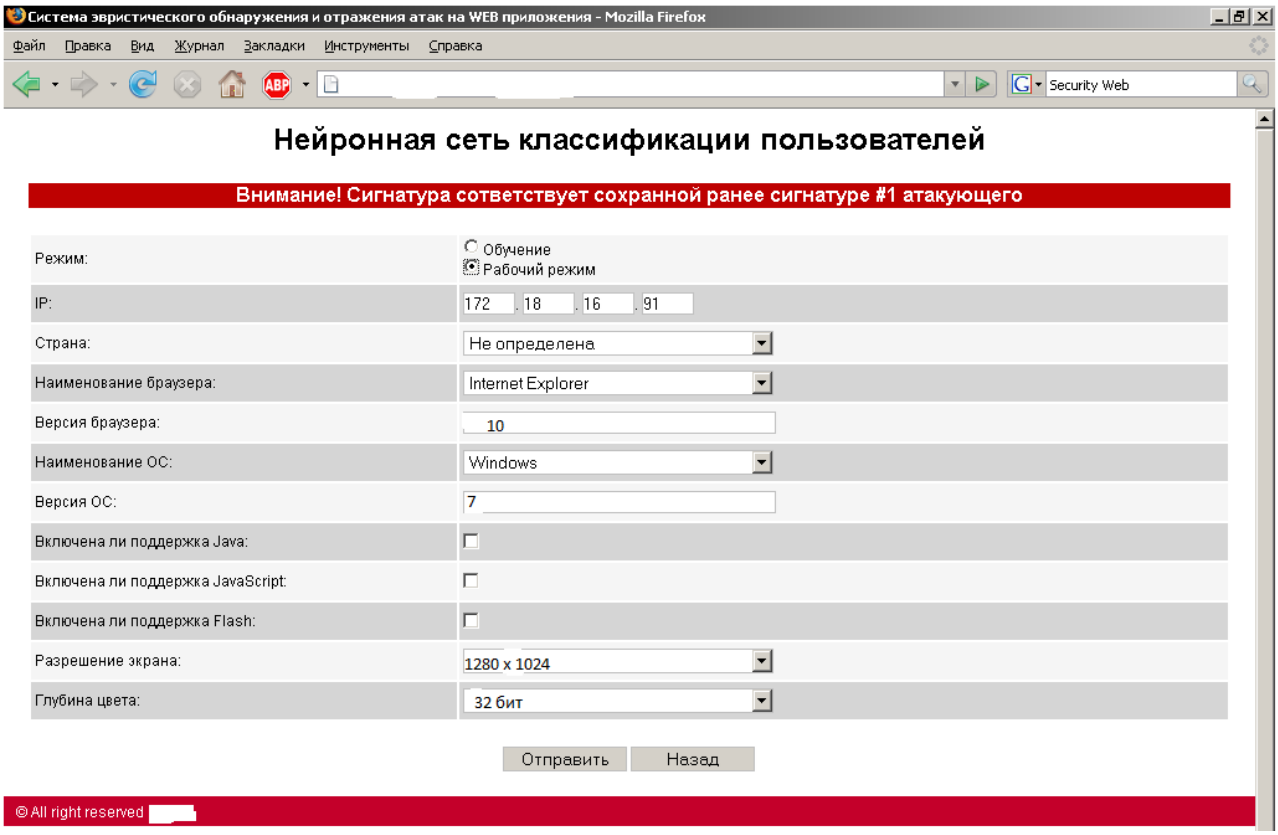


Рисунок 3.9 – Повідомлення програми, коли було знайдено відповідність до раніше збереженого вектору

Якщо система не розпізнала поданий на вхід вектор – то виводиться повідомлення про те, що користувач не викликає підозри (рис. 3.10).

Перед початком роботи системи, що захищає конкретний WEB-додаток не потрібно навчати мережу класифікації користувачів. Ця мережа походить навчання в процесі роботи.

Мережа класифікації користувачів зберігає інформацію про "підозрілих" користувачів. Результат класифікації мережі подається на програмний блок обґрунтування вибору, котрий розшифровує результат класифікації мережі.

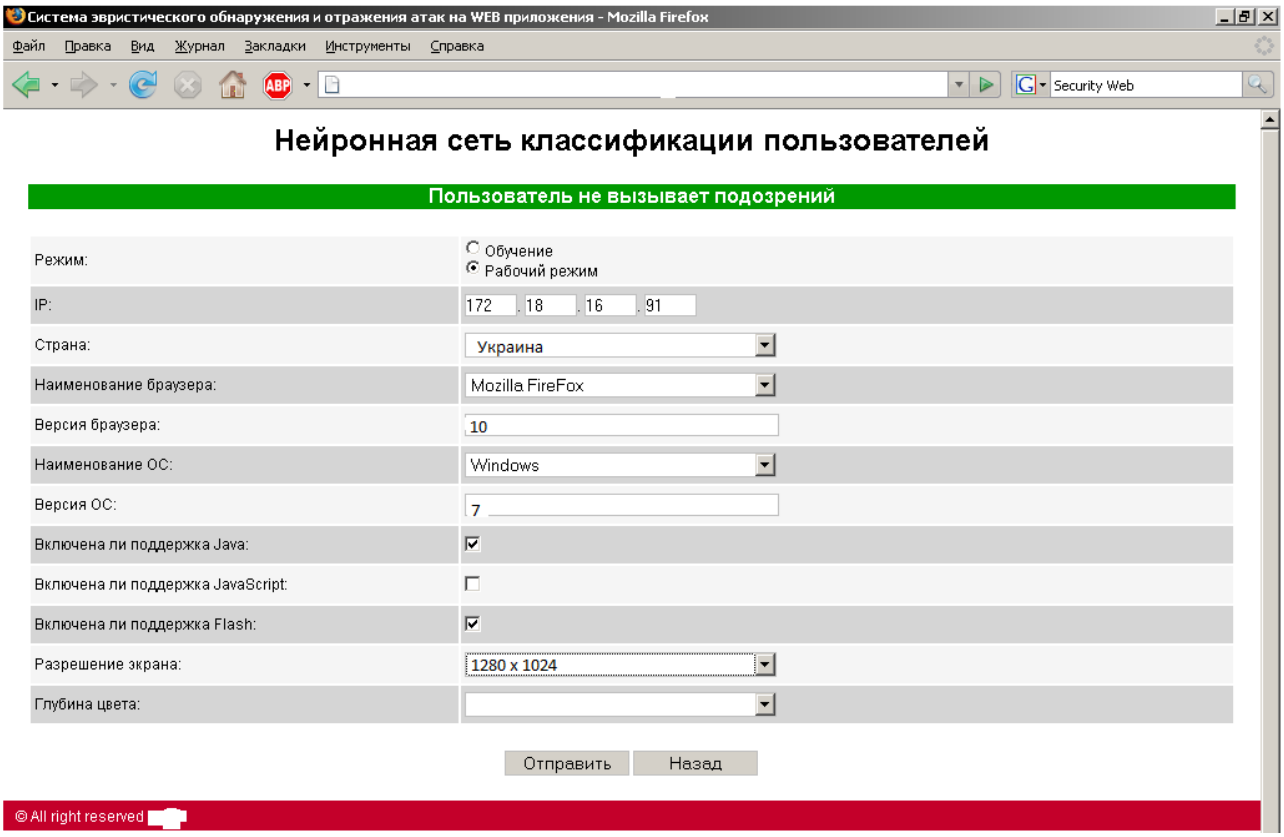


Рисунок 3.10 – Повідомлення програми, коли відповідність до раніше збережених векторів не було знайдено

Якщо мережею було запам’ятовано користувача як зловмисника і для нього було заблоковано доступ, то відмінити заборону може лише адміністратор системи через спеціальній інтерфейс.

3.10 Нейронні мережі, що захищають сторінки

При виборі пункту головного меню "Нейронна мережа захисту сторінок" користувач отримує доступ до форми, яка дозволяє оперувати параметрами, які подаються на вхід мережі, що захищає сторінки WEB-додатку.

Доступні такі параметри: кількість переданих GET параметрів, об’єм переданих GET параметрів, кількість переданих POST параметрів, об’єм переданих POST параметрів,. кількість переданих COOKIE параметрів, об’єм переданих COOKIE параметрів, тип файлу, що передається, код відповіді HTTP, ім’я таблиці в базі даних, дія з таблицею в базі даних, номер помилки, що виникла при виконанні скрипта.

Нейронна мережа може перебувати у режимі навчання та у робочому режимі. В режимі навчання користувачу видаються повідомлення про те, який нейрон запам’ятав вхідний вектор (рис. 3.11).

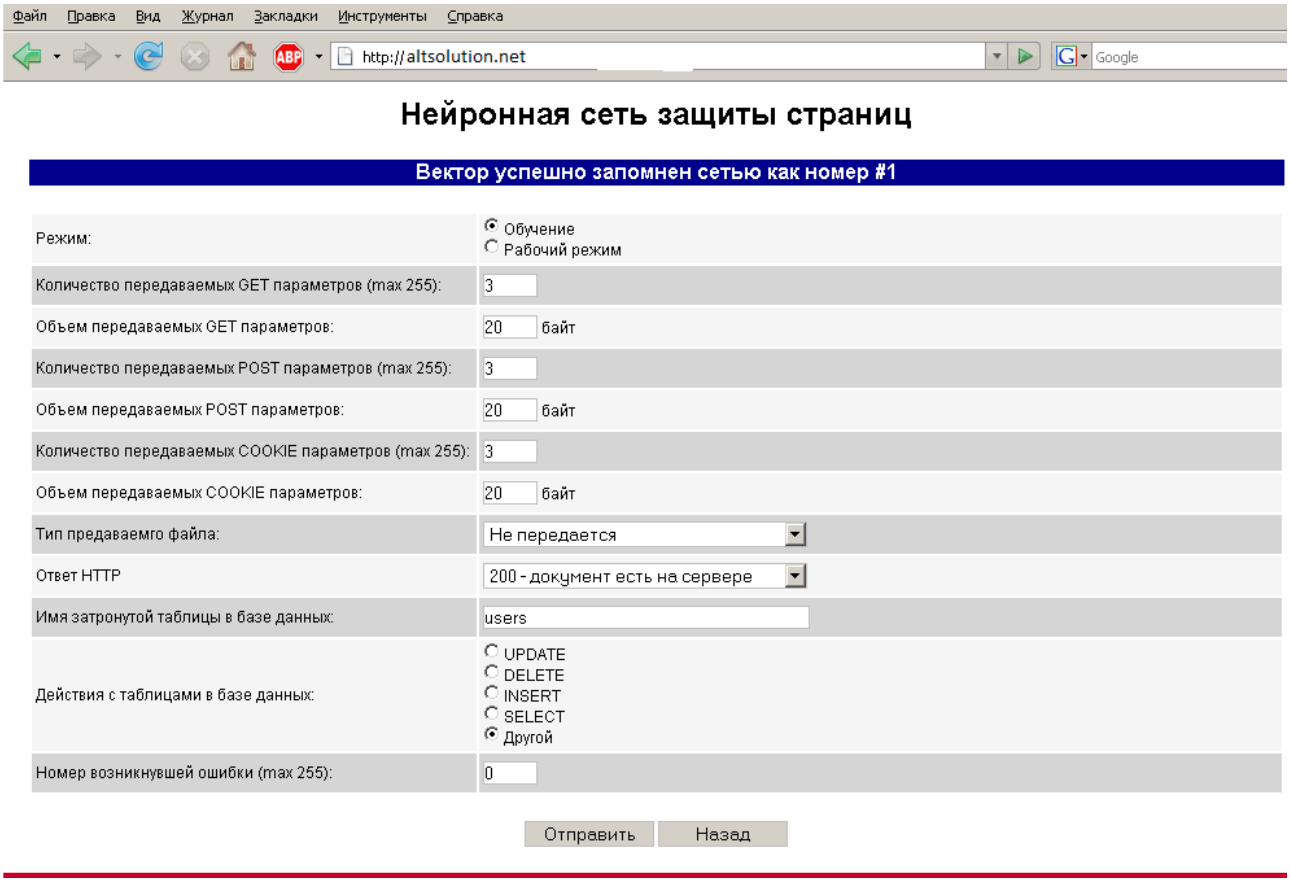


Рисунок 3.11 – Навчання мережі, що відповідає за захист сторінок WEB-додатку

В робочому режимі програма не змінює значення матриць вагових коефіцієнтів нейронної мережі, що захищає сторінки WEB-додатку. Якщо система розпізнала поданий на вхід вектор – то користувачу видається повідомлення, що поведінка користувача відповідає шаблону нормальної поведінки (рис. 3.12).

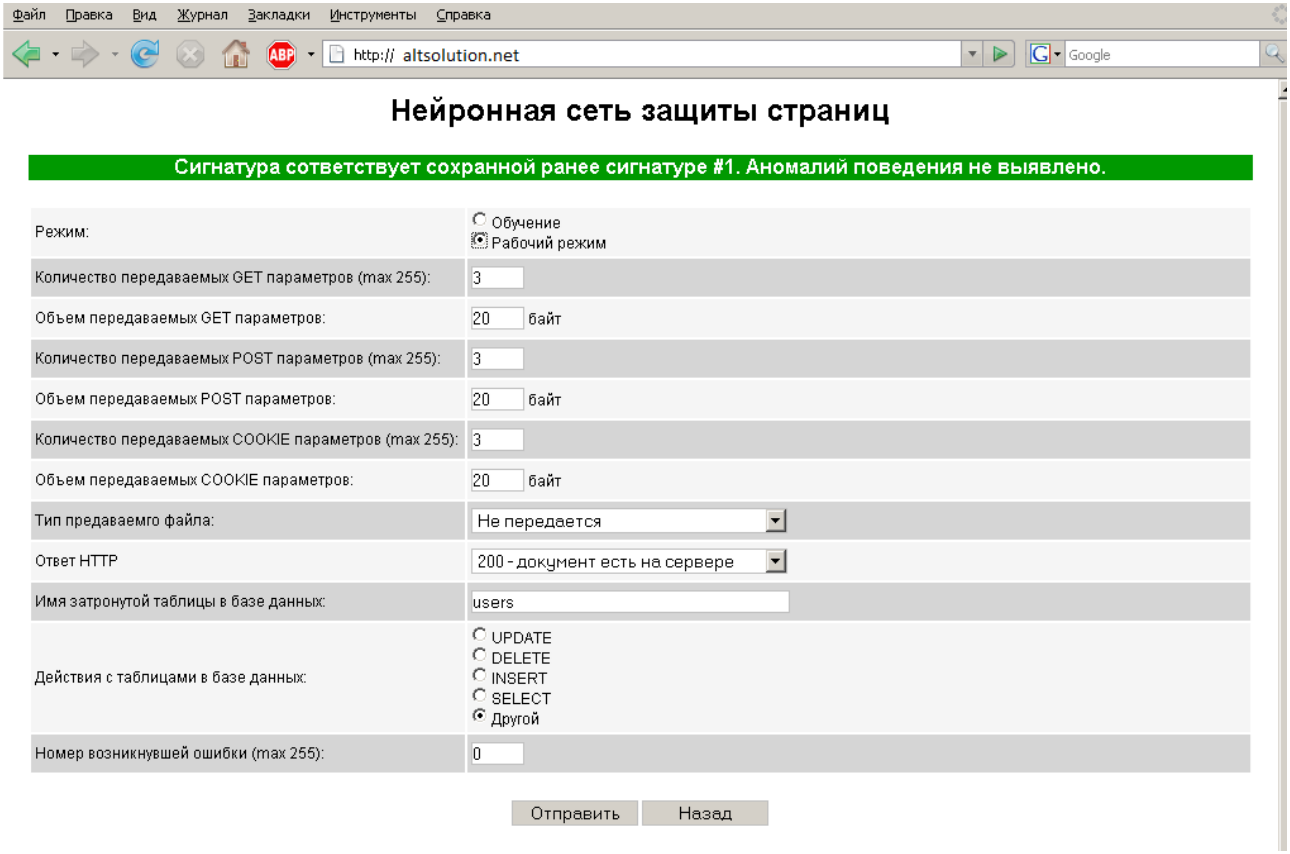


Рисунок 3.12 – Повідомлення програми, коли було знайдено відповідність до раніше збереженого вектору

Якщо ж нейронна мережа, що відповідає за захист сторінки WEB-додатку, не знайшла відповідності раніше збереженому вектору, то подається сигнал тривоги (рис. 3.13).

Коли система генерує сигнал тривоги, то відбувається донавчання нейронної мережі, що відповідає за класифікацію користувачів. В такому випадку нейронна мережа захисту сторінок WEB-додатку вже буде знати про те, що такий користувач раніше проводив “підозрілі” дії і буде “придивлятися” до нього пильніше (тобто знизить коефіцієнт подоби).

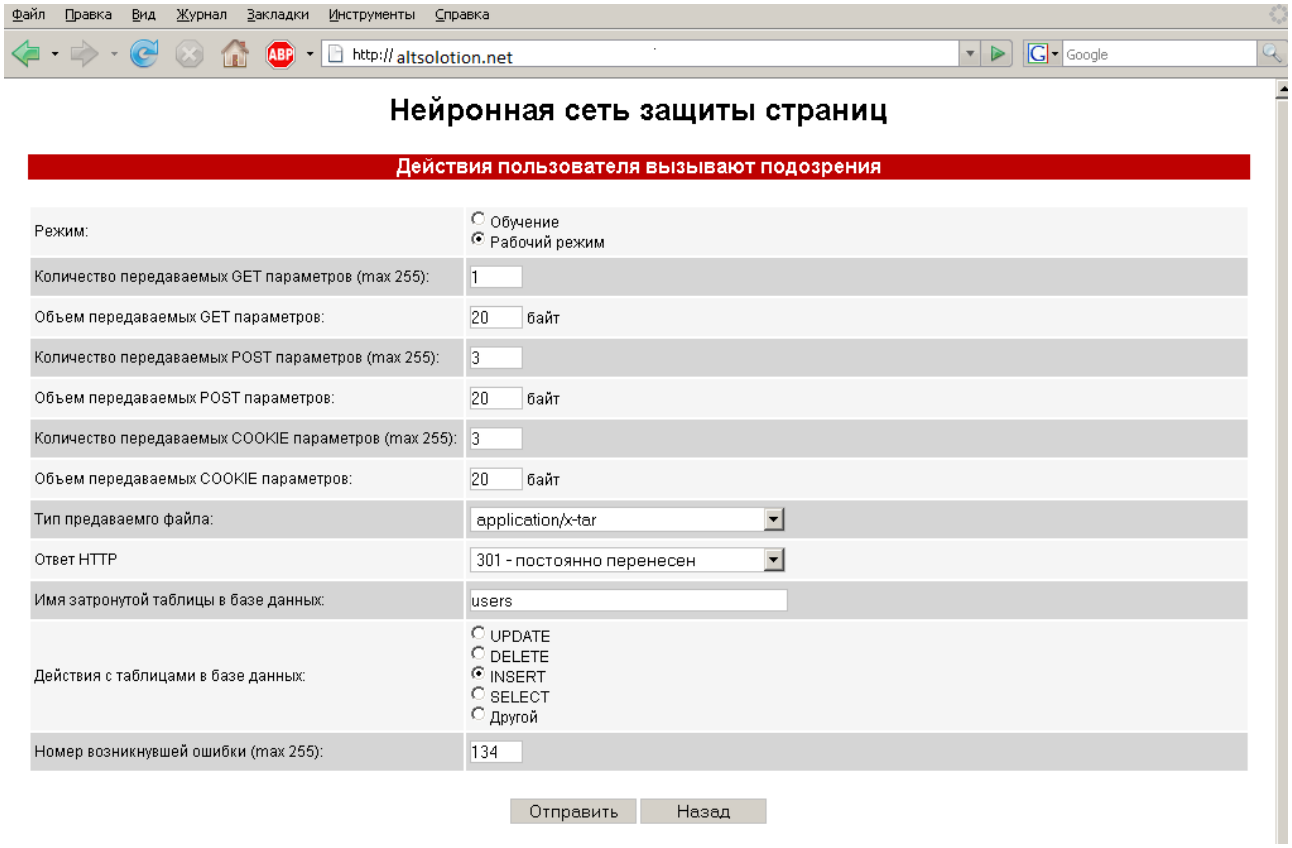


Рисунок 3.13 – Повідомлення програми, коли відповідність до раніше збережених векторів не було знайдено

Особливо слід зазначити, чим більше працює система тим “розумнішою” вона стає. Система, яка пройшла достатньо довгий період навчання, завжди має переваги перед системою, яка пройшла менший період навчання. Крім навчання на начальному етапі система має можливість проводити до навчання в процесі роботи.

3.11 Режим налаштування

Для нормальної роботи нейронної мережі потрібні деякі налаштування. Розроблений програмний продукт надає інтерфейс налаштування (рис. 3.14.) через панель адміністрування, що захищено паролем.

Адміністратору доступні для налаштування такі параметри:

– максимальна кількість елементів, що може бути розпізнано мережею;
– розмірність вхідних векторів;
– початкове значення коефіцієнту подоби;
– параметр адаптації зв’язків нейронної мережі.

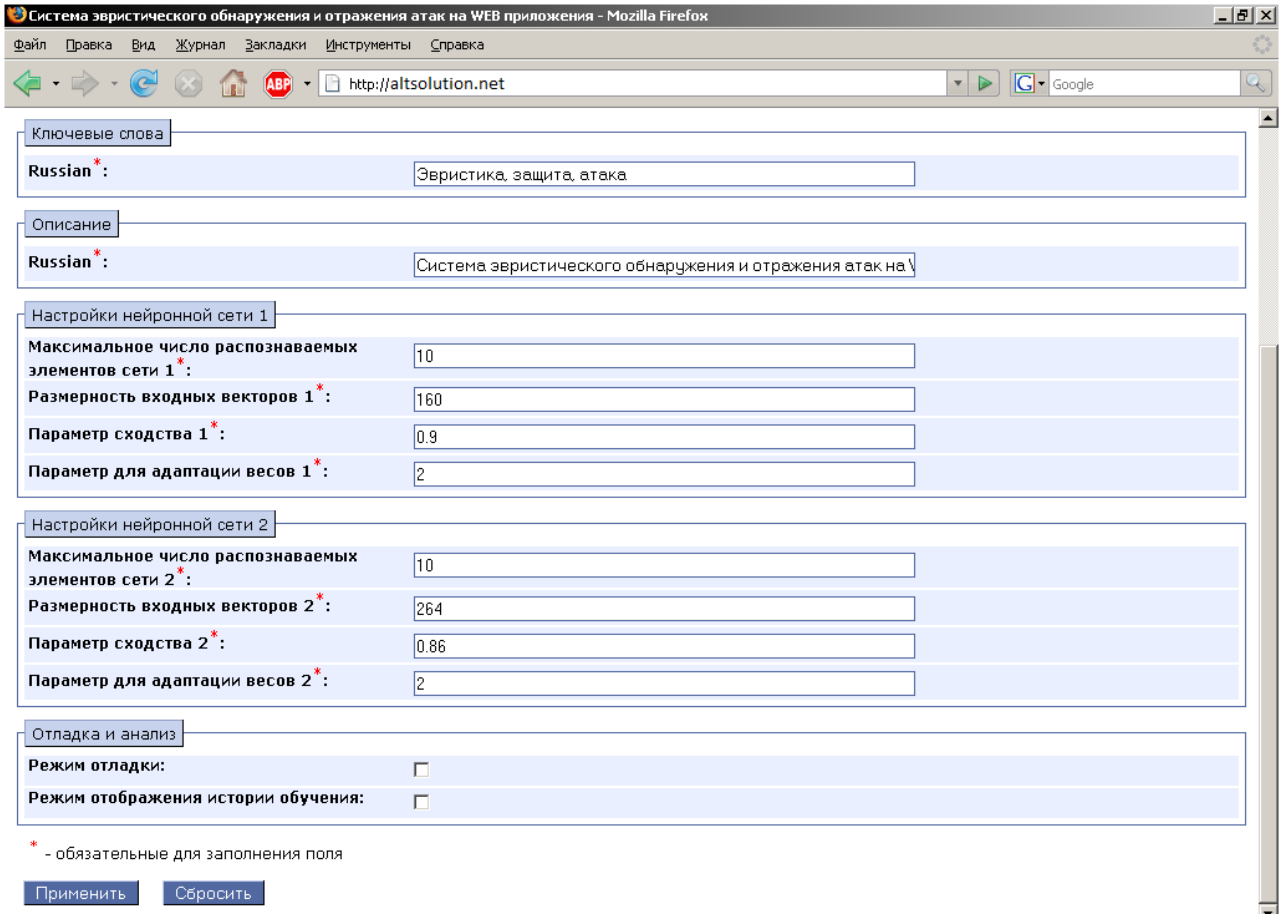


Рисунок 3.14 – Сторінка налаштувань параметрів нейронних мереж

Налаштування треба робити після встановлення програми на сервер. В процесі роботи міняти налаштування не потрібно.

Класична архітектура нейронної мережі не дає відповідь на запитання про те, чому саме було прийняте те чи інше рішення.

Для розробленого програмного продукту можна включити спеціальний режим налаштування (рис. 3.15), який дозволяє крок за кроком прослідити за тим, як нейронна мережа приймає рішення. Крім того в цьому режимі для користувача доступні всі данні історій, тобто список векторів які було запам’ятовано кожним нейроном в процесі навчання.

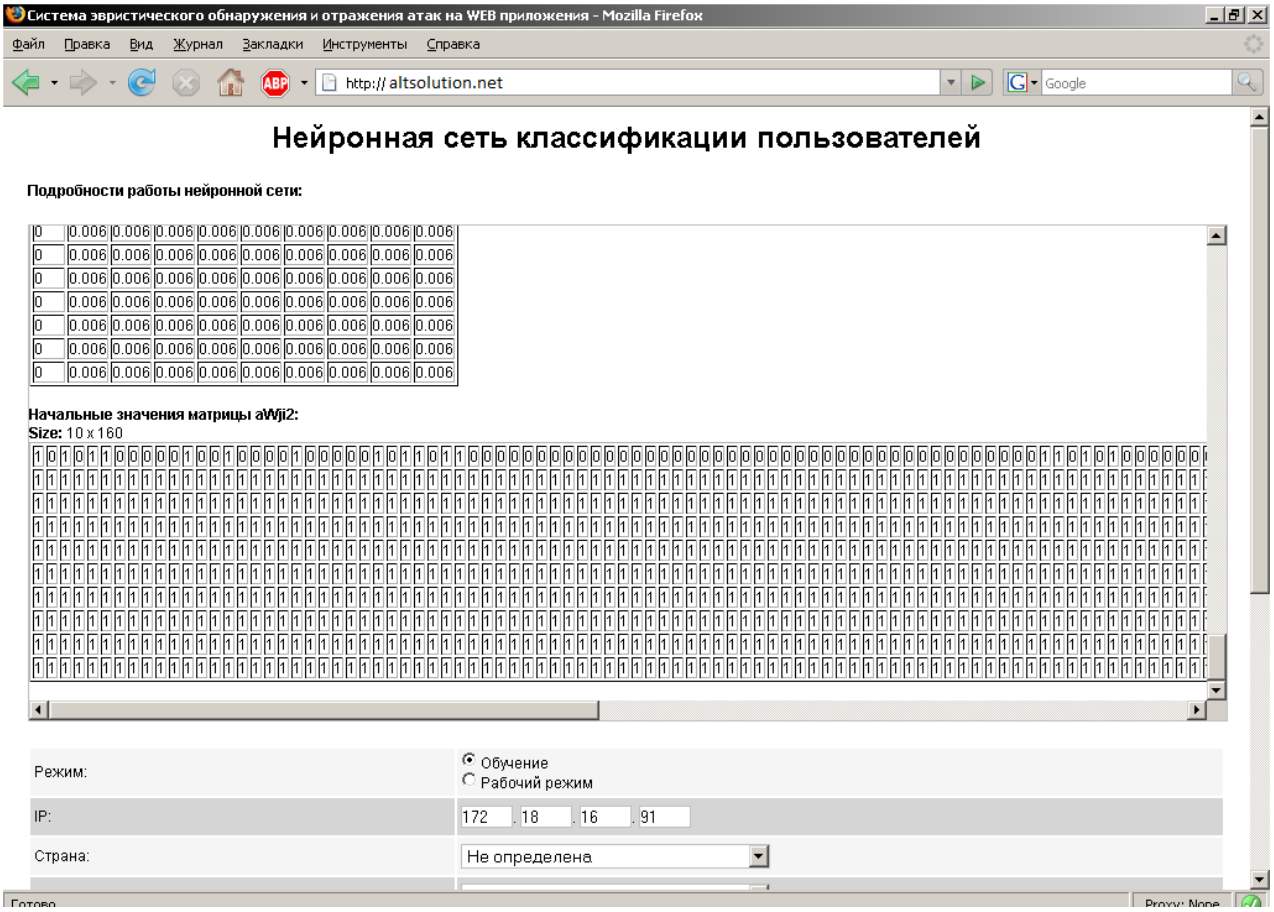


Рисунок 3.15 – Вікно програми у режимі налаштування

Використання режиму від лагодження найбільш виправдовує себе на етапі тестування системи адміністратором. При нормальній роботі нейронної мережі цей режим частіше всього виключають, бо він виводить багато надлишкової інформації.

Включити або виключити режим від лагодження можна через інтерфейс налаштування.

3.12 Переваги та недоліки запропонованої схеми

Запропонована схема має як переваги перед аналогами, так і недоліки.

Переваги запропонованої схеми в наступному:

– основною перевагою системи є її здатність до виявлення нових типів атак, коли сигнатурний аналіз безсилий у силу своєї статичної природи;

– не вимагає відновлення сигнатур, тому що засновано на аномаліях поведінки, тобто не потребує розробки і підтримки доволі не дешевої інфраструктури у мережі Internet, яка б дозволяла регулярно отримувати оновлення сигнатурних баз;

– дає можливість відслідковувати дії користувача, що неодноразово робить спроби проникнення, тобто "слідкує" за користувачем впродовж усіх циклів роботи з WEB-додатком;

– повністю адаптується під особливості WEB-додатку що захищає.

Недоліки запропонованої схеми:

– залежність від мови програмування, на якому написаний WEB-додаток;

– необхідність витрат часу для початкового навчання нейронної мережі;

– можливість помилкових спрацьовувань при недостатньому періоді навчання, що може викликати блокування легітимних дій користувачів системи.

Як можна побачити, переваги запропонованої системи значно вагоміші за недоліки. При достатньому періоді навчання евристичної системи кількість невірних спрацювань можна звести майже до нуля. Таким чином перспективність використання запропонованого евристичного аналізатора в рамках вже розроблених систем попередження вторгнень очевидна.

3.13 Висновки до розділу 3

У третьому розділі визначені перспективні напрямки вдосконалення систем захисту інформації. Зазначено, що більшу частину атак на WEB-додатки можна розпізнати тільки на рівні додатків (сьомий рівень моделі OSI). Розроблена схема побудови захисту WEB-додатку. У запропонованій схемі аналіз на рівні додатків здійснюється системою, що складається з набору так званих "давачів" і евристичного аналізатору. Зазначено, що для розв'язуваного класу завдань найбільше всього підходить мережа АРТ-1. Головне завдання, що покладене на нейронну мережу, є завдання виявлення атак, які не були виявлені на етапі сигнатурного аналізу. Наведено приклад функціонування системи захисту. Для створення програми, що реалізує захист WEB-додатку з можливостями евристичного аналізу обрано мову PHP , наведено її переваги та результати дослідження з застосуванням розробленої програми.

РОЗДІЛ 4
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1. Загальні питання з охорони праці

Умови праці на робочому місці, безпека технологічних процесів, машин, механізмів, устаткування та інших засобів виробництва, стан засобів колективного та індивідуального захисту, що використовуються працівником, а також санітарно-побутові умови повинні відповідати вимогам нормативних актів про охорону праці. В [23] визначається, що охорона праці - це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження життя, здоров'я і працездатності людини у процесі трудової діяльності.

Завданням даної магістерської роботи було дослідити та розробити програмні засоби для забезпечення безпеки WEB-додатків користувачів комп’ютерних систем від несанкціонованого втручання в їх роботу. Дана робота з точки зору питань з охорони праці проводилась в офісному приміщенні при нормальних кліматичних умовах з використанням сучасного персонального комп’ютера та офісної техніки (принтера та сканера).

При роботі з обчислювальною технікою змінюються фізичні і хімічні фактори навколишнього середовища: виникає статична електрика, електромагнітне випромінювання, змінюється температура і вологість, рівень вміст кисню і озону в повітрі. Повітря забруднюється шкідливими хімічними речовинами антропогенного походження за рахунок деструкції полімерних матеріалів, які використовуються для обробки приміщень та обладнання. Неправильна організація робочого місця сприяє загальному і локальній напрузі м'язів шиї, тулуба, верхніх кінцівок, викривлення хребта і розвитку остеохондрозу. На всіх підприємствах, в установах, організаціях повинні створюватися безпечні і нешкідливі умови праці. Забезпечення цих умов покладається на власника або уповноважений ним орган (далі роботодавець). Умови праці на робочому місці, безпека технологічних процесів, машин, механізмів, устаткування та інших засобів виробництва, стан засобів колективного та індивідуального захисту, що використовуються працівником, а також санітарно-побутові умови повинні відповідати вимогам нормативних актів про охорону праці. Роботодавець повинен впроваджувати сучасні засоби техніки безпеки, які запобігають виробничому травматизмові, і забезпечувати санітарно-гігієнічні умови, що запобігають виникненню професійних захворювань працівників. Він не має права вимагати від працівника виконання роботи, поєднаної з явною небезпекою для життя, а також в умовах, що не відповідають законодавству про охорону праці. Працівник має право відмовитися від дорученої роботи,

якщо створилася виробнича ситуація, небезпечна для його життя чи здоров'я або людей, які його оточують, і навколишнього середовища.

4.1.1 Правові та організаційні основи охорони праці

Основним організаційним напрямом у здійсненні управління в сфері охорони праці є усвідомлення пріоритету безпеки праці і підвищення соціальної відповідальності держави, і особистої відповідальності працівників.

Державна політика в галузі охорони праці визначається відповідно до Конституції України Верховною Радою України і спрямована на створення належних, безпечних і здорових умов праці, запобігання нещасним випадкам та професійним захворюванням. Відповідно до статті 3 [23] законодавство про охорону праці складається з [24, 25] та прийнятих відповідно до них нормативно-правових актів, норм міжнародного договору (ратифіковані Конвенції і Рекомендації МОТ, директиви Європейської Ради).

На законодавчому рівні визначено такі пріоритетні напрямки з безпеки праці:

– кожен працівник несе безпосередню відповідальність за порушення зазначених Законом, нормами і правилами вимог;

– напрямки реалізації конституційного права громадян на їх життя і здоров’я в процесі трудової діяльності:

– пріоритет життя і здоров’я працівників по відношенню до результатів виробничої діяльності підприємства;

– повна відповідальність роботодавця за створення належних – безпечних і здорових умов праці;

– соціальний захист працівників, повне відшкодування збитків особам, які потерпіли від нещасних випадків на виробництві та професійних захворювань;

– комплексне розв’язання завдань охорони праці;

– підвищення рівня промислової безпеки шляхом забезпечення суцільного технічного контролю за станом виробництв, технологій та продукції, а також сприяння підприємствам у створенні безпечних та нешкідливих умов праці;

– соціальний захист працівників, повне відшкодування збитків особам, які потерпіли від нещасних випадків на виробництві та професійних захворювань;

– використання економічних методів управління охороною праці, участь держави у фінансуванні заходів щодо охорони праці;

– використання світового досвіду організації роботи щодо поліпшення умов і підвищення безпеки праці на основі міжнародної співпраці.

Користувачі персональних комп'ютерів, для яких ця робота є головною, підлягають медичним оглядам: попереднім — під час влаштування на роботу і періодичним — протягом професійної діяльності раз на два роки. Жінок з часу встановлення вагітності та в період годування дитини грудьми до роботи з ПК не допускають.

Обов'язки працівників щодо додержання вимог нормативно-правових актів з охорони праці (ст. 14), відповідальність робітників всіх категорій за порушення вимог щодо охорони праці (ст. 44) та структура організації/виробництв системи управління охорони праці визначені безпосередньо «Інструкцією на робоче місце № 1», та іншими затвердженими власними нормативними актами з питань охорони праці (правилами, нормами, регламентами, положеннями, стандартами, інструкціями та іншими документами, обов'язковими до виконання), тобто тих, що діють на підприємстві/організації, і визначені в [26].

Наявні трудові відносини між працівниками і роботодавцями в Україні за темою роботи регулюються [24], відповідно до якого права працюючої людини на охорону праці охороняються всебічно та норми охорони праці неухильно інтегровані до правил внутрішнього розпорядку організації/підприємства.

4.1.2 Організаційно-технічні заходи з безпеки праці

В організації/підприємстві проводиться навчання і перевірка знань з питань охорони праці відповідно до вимог [27], затвердженого наказом Держнаглядохоронпраці України від 26.01.2005 N 15, зареєстрованого в Міністерстві юстиції України 15.02.2005 за N 231/10511.

Також впроваджені організаційні заходи з пожежної безпеки - навчання і перевірку знань відповідно до вимог [28], затвердженого наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 29.09.2003 N 368, зареєстрованого в Міністерстві юстиції України 11.12.2003 за N 1148/8469.

Обов'язковими вимогами враховане наступне:

– не слід допускати до роботи осіб, що в установленому порядку не пройшли навчання, інструктаж та перевірку знань з охорони праці, пожежної безпеки та цих Правил.

– на підприємстві/організації, де експлуатуються ПК з ВДТ і ПП, розробляється інструкція з охорони праці відповідно до [29], затвердженого наказом Держнаглядохоронпраці від 29.01.98 N 9, зареєстрованого в Міністерстві юстиції України 07.04.98 за N 226/2666.

–ознайомлення з правилами безпеки праці, одержання відповідних інструктажів засвідчується у журналі інструктажів.

–перед допуском до самостійної роботи кожен працівник має право на навчання з питань охорони праці і роботодавець зобов'язаний, і проводить таке навчання у вигляді двох інструктажів з питань охорони праці:

1. Вступного, який проводять працівники служби охорони праці об'єкта господарювання з усіма працівниками, яких приймають на роботу незалежно від їхньої освіти та стажу роботи за програмою, в якій подають загальні питання охорони праці із врахуванням її особливостей на об'єкті господарювання;

2. Первинного, який проводять керівники структурних підрозділів на місці праці з кожним працівником до початку їхньої роботи на цьому робочому місці.

Проходження працівником цих інструктажів з питань охорони праці підтверджується записами у відповідних журналах обліку інструктажів і скріплюється підписами осіб, які проводили інструктажі та осіб, які отримали інструктажі.

3. Повторний (не рідше одного разу в 6 місяців);

4. Позаплановий (при зміні правил охорони праці);

5. Поточний (проводять з працівниками перед виконанням робіт, на яких оформляється наряд-допуск)

– обов'язкові організаційні заходи перед початком, під час і після завершення роботи повинні включати перевірку (візуально) наявності і справності електрообладнання та його заземлення, а під час виконання роботи вимогу «не залишати без нагляду обладнання, яке працює». Після закінчення роботи - вимагається прибирання робочого місця, відключення всіх електроприладів від електромережі.

Не допускається:

– виконувати обслуговування, ремонт та налагодження ПК з ВДТ і ПП безпосередньо на робочому місці оператора;

– зберігати біля ПК з ВДТ і ПП папір, дискети, інші носії інформації, запасні блоки, деталі тощо, якщо вони не використовуються для поточної роботи;

– відключати захисні пристрої, самочинно проводити зміни у конструкції та складі ПК з ВДТ і ПП або їх технічне налагодження;

–працювати з ВДТ, у яких під час роботи з'являються нехарактерні сигнали, нестабільне зображення на екрані тощо;

–працювати з матричним принтером за відсутності вібраційного килимка та зі знятою (піднятою) верхньою кришкою.

4.2 Аналіз стану умов праці

4.2.1 Вимоги до приміщень

Робота над створенням такої системи проходитиме в приміщенні відповідної установи (компанії, підприємстві тощо). Для даної роботи достатньо однієї людини, для якої надано робоче місце зі стаціонарним комп'ютером. ГПКетричні розміри приміщення зазначені в таблиці 4.1.

Таблиця 4.1 – Розміри приміщення

Найменування	**Значення**
Довжина, м	5
Ширина, м	5
Висота, м	3
Площа, $м^2$	25
Об'єм, $м^3$	75

Згідно з [30] розмір площі для одного робочого місця оператора персонального комп'ютера має бути не менше 6 кв. м, а об'єм — не менше 20 куб. м. Отже, дане приміщення цілком відповідає зазначеним нормам. Для зручності спільної роботи з іншими працівниками (обговорення ідей, з'ясування проблем і т.д.) в кімнаті є дивани і журнальний стіл, обставлені живими квітами. Також робочий процес пов'язаний з багатьма документами, теками, журналами для чого приміщення облаштоване принтером і шафою для зручності. Задля дотримання визначеного рівня мікроклімату в будівлі встановлено систему опалення та кондиціонування. Для забезпечення потрібного рівного освітленості кімната має вікно та систему загального рівномірного освітлення, що встановлена на стелі. Для дотримання вимог пожежної безпеки встановлено порошковий вогнегасник та систему автоматичної пожежної сигналізації.

4.2.2 Вимоги до організації місця праці

При порівнянні відповідності характеристик робочого місця нормативним основні вимоги до організації робочого місця [31] і відповідними фактичними значеннями для робочого місця, констатуємо повну відповідність в таблиці 4.2.

Таблиця 4.2 - Характеристики робочого місця

Найменування параметра	**Фактичне значення**	**Нормативне значення**
Висота робочої поверхні, мм	750	680 ÷800
Висота простору для ніг, мм	730	не менше 600
Ширина простору для ніг, мм	660	не менше 500
Глибина простору для ніг, мм	700	не менше 650
Висота поверхні сидіння, мм	470	400 ÷500
Ширина сидіння, мм	400	не менше 400
Глибина сидіння, мм	400	не менше 400
Висота поверхні спинки, мм	600	не менше 300
Ширина опорної поверхні спинки, мм	500	не менше 380
Радіус кривини спинки в горизонтальній площині, мм	400	400
Відстань від очей до екрану дисплея, мм	800	700 ÷800

Робочий стіл на досліджуваному місці також містить достатньо простору для ніг. Крісло, що використовується в якості робочого сидіння, є підйомно-поворотним, має підлокітники і можливість регулювання за висотою і кутом нахилу спинки, також воно м'яке і виконане з екологічної шкіри, що дає можливість працювати у комфорті. Екран монітору знаходиться на відстані 0.8 м, клавіатура має можливість регулювання кута нахилу 5-15°. Отже, за всіма параметрами робоче місце відповідає нормативним вимогам.

Приміщення кабінету знаходиться на другому поверсі трьох поверхової будівлі і має об’єм 78 м^3, площу — 18 м^2. У цьому кабінеті обладнано три місця праці, з яких два укомплектовані ПК.

Температура в приміщенні протягом року коливається у межах 18–24°С, відносна вологість — близько 50%. Швидкість руху повітря не перевищує 0,2 м/с. Шум на робочому місці знаходиться на рівні 50 дБА. Система вентилювання приміщення — природна неорганізована, а опалення — централізоване.

Розміщення вікон забезпечує природне освітлення з коефіцієнтом природного освітлення не менше 1,5%, а загальне штучне освітлення, яке здійснюється за допомогою восьми люмінесцентних ламп, забезпечує рівень освітленості не менше 200 Лк.

У кабінеті є електрична мережа з напругою 220 В, яка створює небезпеку ураження електричним струмом. ПК та периферійні пристрої можуть бути джерелами електромагнітних випромінювань, аерозолів та шкідливих речовин (часток тонеру, оксидів нітрогену та озону).

За ступенем пожежної безпеки приміщення належить до категорії В. Кабінет має бути оснащений переносним вуглекислотним вогнегасником ВВК-5.

Наявна аптечка для надання долікарської допомоги, а також у кабінеті роблять вологе прибирання та щоденно провітрюють приміщення.

4.2.3 Навантаження та напруженість процесу праці

Як приклад наведено опис процесу праці оформлення роботи під час виконання магістерської роботи за фізичним навантаженням робота відноситься до категорії легкі роботи (Іа), її виконують сидячи з періодичним ходінням. Щодо характеру організації роботи, то розділи роботи необхідно виконати у встановлені конкретні терміни. За ступенем нервово-психічної напруги виконання роботи можна віднести до II – III ступеня і кваліфікувати як помірно напружений – напружений за умови успішного виконання поставлених завдань.

Під час виконання робіт використовують ПК та периферійні пристрої, що призводить до навантаження на окремі системи організму. Такі перекоси у напруженні різних систем організму, що трапляються під час роботи з ПК, зокрема, значна напруженість зорового аналізатора і довготривале малорухоме положення перед екраном, не тільки не зменшують загального напруження, а навпаки, призводять до його посилення і появи стресових реакцій.

Найбільшому ризику виникнення різноманітних порушень піддаються: органи зору, м’язово скелетна система, нервово-психічна діяльність, репродуктивна функція у жінок.

Тобто наявне психофізіологічні небезпечні та шкідливі фактори:

а) фізичного перевантаження:

- статичного;
- динамічного;

б) нервово-психічного перевантаження:

- розумового перенапруження;
- монотонності праці;
- перенапруження аналізаторів;
- емоційних перевантажень.

Роботу за дипломним проектом визнано, таку, що займає 50% часу робочого дня та за восьмигодинної робочої зміни рекомендовано встановити додаткові регламентовані перерви:

- для розробників програм тривалістю 15 хв. через кожну годину роботи.

4.3 Виробнича санітарія

На підставі аналізу небезпечних та шкідливих факторів при виробництві (експлуатації), пожежної безпеки можуть бути надалі вирішені питання необхідності забезпечення працюючих достатньою кількістю освітлення, вентиляції повітря, організації заземлення, тощо.

4.3.1 Аналіз небезпечних та шкідливих факторів при роботі на ПК

Роботу, пов'язану з персональним комп’ютером (далі - ПК) з відео дисплейними терміналами (далі - ВДТ), у тому числі на тих, які мають робочі місця, обладнані ПК з ВДТ і периферійними пристроями (далі - ПП), виконують із забезпеченням виконання [32], які встановлюють вимоги безпеки до обладнання робочих місць, до роботи із застосуванням ПК з ВДТ і ПП. Переважно роботи за проектами виконують у кабінетах чи інших приміщеннях, де використовують різноманітне електрообладнання, зокрема персональні комп’ютери (ПК) та периферійні пристрої.

Робочі місця мають відповідати вимогам [31, 32].

Це передбачає, що визначена виробнича діяльність пов’язана з наявністю певної кількості небезпечних та/або шкідливих виробничих факторів. Тому у першій частині цього підрозділу за результатами аналізу повинні бути визначені такі фактори.

Робота ПК та периферійних пристроїв супроводжує виділення багатьох хімічних речовин, зокрема озону, оксидів нітрогену та аерозолів (високодисперсних частинок тонера). Для прикладу, за умов роботи з ПК виникають наступні небезпечні та шкідливі чинники: несприятливі мікрокліматичні умови, освітлення, електромагнітні випромінювання, забруднення повітря шкідливими речовинами (джерелом яких може бути принтер, сканер та ін.), шум, вібрація, електричний струм, електростатичне поле, напруженість трудового процесу та інше.

Аналіз небезпечних та шкідливих виробничих факторів виконується у табличній формі (табл. 4.3).

Таблиця 4.3 - Аналіз небезпечних і шкідливих виробничих факторів

Небезпечні і шкідливі виробничі фактори	Джерела факторів (види робіт)	Кількісна оцінка	Нормативні документи
1	2	3	4
фізичні			
- підвищена температура поверхонь обладнання	Експлуатація ПК	2	ДСН 3.3.6.042-99
- підвищений рівень шуму на робочому місці	Система охолодження ПК	2	ДСН 3.3.6.037-99
- підвищений рівень вібрації	Система охолодження ПК, привід	2	ДСН 3.3.6.039-99 ДСТУ ГОСТ 12.1.012-90
- недостатність природного світла	Порушення умов праці (вимог до приміщень)	2	ДБН В.2.5-28:2015
- недостатнє освітлення робочої зони	Порушення гігієнічних параметрів виробничого середовища	3	ДБН В.2.5-28:2015
- підвищена яскравість світла	Порушення умов праці (організації місця праці-налагодження моніторів)	1	ДСанПіН 3.3.2.007-98
психофізіологічні:			
- нервово-психічна перевантаження (розумове, перенапруження аналізаторів-зорових)	- пошук інформації для постановки теми; - пошук та аналіз аналогів і літератури; - пошук наявних технологій, моделювання та аналіз алгоритмів; - виконання роботи за темою диплома, тестування; - оформлення роботи	4	НПАОП 0.00-1.28-10 ДСанПіН 3.3.2.007-98
- фізичні (статичне –	порушення умов праці	2	НПАОП 0.00-1.28-10

сидіння)	(організації місця праці-сидіння користувача,) та організації робочого часу - безпервна робота)		ДСанПіН 3.3.2.007-98

4.3.2 Пожежна безпека

Небезпека розвитку пожежі на обчислювальному центрі обумовлюється застосуванням розгалужених систем електроживлення ПК, вентиляції і кондиціювання. Небезпека загоряння пов'язана з особливістю комп'ютерів - із значною кількістю щільно розташованих на монтажній платі і блоках електронних вузлів і схем, електричних і комутаційних кабелів, резисторів, конденсаторів, напівпровідникових діодів і транзисторів. Надійна робота окремих елементів і мікросхем в цілому забезпечується тільки в певних інтервалах температури, вологості і при заданих електричних параметрах. При відхиленні реальних умов експлуатації від розрахункових можуть виникнути пожежонебезпечні ситуації.

Висока щільність елементів в електронних схемах призводить до значного підвищення температури окремих вузлів (80…100 ℃). При проходженні електричного струму по провідниках і деталей виділяється тепло, що в умовах їх високої щільності може привести до перегріву, і може служити причиною запалювання ізоляційних матеріалів. Слабкий опір ізоляційних матеріалів дії температури може викликати порушення ізоляції і привести до короткого замикання між струмоведучими частинами обладнання (шини, електроди). Також ймовірна небезпека внаслідок перевантаження напруги, розрядки зарядів статичної електрики, пошкодження обладнання та електропроводки. Електростатичний розряд виникає під час тертя двох ізольованих матеріалів.

Пожежна безпека при застосуванні ПК забезпечується:

– системою запобігання пожежі,

– системою протипожежного захисту,

– організаційно-технічними заходами.

Згідно [33] таке приміщення, площею 25 м^2, відноситься до категорії "В" (пожежонебезпечної) та для протипожежного захисту в ньому проектом передбачено устаткування автоматичною пожежною сигналізацією із застосуванням датчиків-сповіщувачів РІД-1 (сповіщувач димовий ізоляційний) в кількості 1 шт., і застосуванням первинних засобів пожежогасіння. Відповідно до норм первинних засобів пожежогасінні пропонується використовувати:

–ручний вуглекислий вогнегасник ОУ-5 в кількості 1 шт. або хімічний пінний ОХП-10 – 1 шт;

–повсть 1 1 м2, кошму 2×1,5 м2 або азбестове полотно 2×2 м2 в кількості 1 шт.

Виникнення пожежі можливе, якщо на об'єкті є горючі речовини, окислювач і джерела запалювання. Вірогідність пожежної небезпеки приймається значною, якщо ймовірна взаємодія цих трьох чинників. Горючими компонентами є: будівельні матеріали для акустичної і естетичної обробки приміщень, перегородки, підлоги, двері, ізоляція силових, сигнальних кабелів і т.д.

Горючими матеріалами в приміщенні, де розташовані ПК, є:

–поліамід – матеріал корпусу мікросхем, горюча речовина, температура самозаймання 420 ˚С,

–полівінілхлорид – ізоляційний матеріал, горюча речовина, температура запалювання 335˚С, температура самозаймання 530 ˚С,

–склотекстоліт ДЦ – матеріал друкарських плат, важкогорючий матеріал, показник горючості 1.74, не схильний до температурного самозаймання,

–пластикат кабельний №.489 – матеріал ізоляції кабелів, горючий матеріал, показник горючості більше 2.1,

–деревина – будівельний і обробний матеріал, з якого виготовлені меблі, горючий матеріал, показник горючості більше 2.1, температура запалювання 255 ℃, температура самозаймання 399 ˚С.

Для відводу теплоти від ПК діє система кондиціонування. Тому кисень, як окиснювач процесів горіння, є в будь-якій точці приміщень ВЦ.

Простори усередині приміщень в межах, яких можуть утворюватися або знаходиться пожежонебезпечні речовини і матеріали відповідно [33] відносяться до пожежонебезпечної зони класу П-IIа. Це обумовлено тим, що в приміщенні знаходяться тверді горючі та важкозаймисті речовини та матеріали. Приміщенню, у якому розташоване робоче місце, присвоюється II ступень вогнестійкості.

Потенційними джерелами запалювання можуть бути:

–іскри і дуги короткого замикання;

–електрична іскра при замиканні і розмиканні ланцюгів;

–перегріви від тривалого перевантаження,

–відкритий вогонь і продукти горіння,

–наявність речовин, нагрітих вище за температуру самозаймання,

–розрядна статична електрика.

Причинами можливого загоряння і пожежі можуть бути:

– несправність електроустановки;

– конструктивні недоліки устаткування;

– коротке замикання в електричних мережах;

– запалювання горючих матеріалів, що знаходяться в безпосередній близькості від електроустановки.

Продуктами згорання, що виділяються на пожежі, є: окис вуглецю; сірчистий газ; окис азоту; синильна кислота; акромін; фосген; хлор і ін. При горінні пластмас, окрім звичних продуктів згорання, виділяються різні продукти термічного розкладання: хлорангідридні кислоти, формальдегіди, хлористий водень, фосген, синильна кислота, аміак, фенол, ацетон, стирол [34].

Для захисту персоналу від дії небезпечних і шкідливих чинників пожежі проектом передбачається застосування промислового протигаза, що фільтрує, з коробкою марки «В» із сірою відміткою забарвлення – захист від неорганічних газів (хлор, фтор, бром, сірководень, сірковуглець, хлорциан, галогени), а цей фільтр не захистить від СО (тобто від чадного газу).

Можливе також відповідне застосування фільтрувальної коробки з маркуванням «СО» із фіолетовим забарвленням на фільтрі означає, що він захищає від Чадного газу. Або фільтру для протигазу з літерним маркуванням «SX» із фіолетовим забарвленням захистить від спец речовин таких як (зарин, зоман та фосген).

4.3.3 Електробезпека

На робочому місці виконуються наступні вимоги електробезпеки: ПК, периферійні пристрої та устаткування для обслуговування, електропроводи і кабелі за виконанням та ступенем захисту відповідають класу зони за ПУЕ (правила улаштування електроустановок), мають апаратуру захисту від струму короткого замикання та інших аварійних режимів. Лінія електромережі для живлення ПК, периферійних пристроїв і устаткування для обслуговування, виконана як окрема групова три-провідна мережа, шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів. Штепсельні з'єднання та електророзетки крім контактів фазового та нульового робочого провідників мають спеціальні контакти для підключення нульового захисного провідника. Електромережа штепсельних розеток для живлення персональних ПК, укладено по підлозі поруч зі стінами відповідно до затвердженого плану розміщення обладнання та технічних характеристик обладнання. Металеві труби та гнучкі металеві рукави заземлені. Захисне

заземлення включає в себе заземлюючих пристроїв і провідник, який з'єднує заземлюючий пристрій з обладнанням, яке заземлюється - заземлюючий провідник.

4.4 Гігієнічні вимоги до параметрів виробничого середовища

4.4.1 Мікроклімат

Мікроклімат робочих приміщень – це клімат внутрішнього середовища цих приміщень, що визначається діючої на організм людини з'єднанням температури, вологості, швидкості переміщення повітря. В даному приміщенні проводяться роботи, що виконуються сидячи і не потребують динамічного фізичного напруження, то для нього відповідає категорія робіт Іа. Отже оптимальні значення для температури, відносної вологості й рухливості повітря для зазначеного робочого місця відповідають [35] і наведені в таблиці 4.4:

Таблиця 4.4 – Норми мікроклімату робочої зони об’єкту

Період року	Категорія робіт	Температура C^0	Відносна вологість %	Швидкість руху повітря, м/с
Холодна	легка-1 а	22 - 24	40 – 60	0,1
Тепла	легка-1 а	23 - 25	40 – 60	0,1

Дане приміщення обладнане системами опалення, кондиціонування повітря або припливно-витяжною вентиляцією. У приміщенні на робочому місці забезпечуються оптимальні значення параметрів мікроклімату: температури, відносної вологості й рухливості повітря у відповідності [35]. Рівні позитивних і негативних іонів у повітрі мають відповідати [35]. Для забезпечення оптимальних параметрів мікроклімату в приміщенні проводяться перерви в роботі користувача, з метою його провітрювання. Існують спеціальні системи кондиціонування, які забезпечують підтримання в приміщенні балансу оптимальних параметрів мікроклімату. Контроль параметрів мікроклімату в холодний і теплий період року здійснюється не менше 3-х разів на зміну (на початку, середині, в кінці).

4.4.2 Освітлення

Світло є природною умовою існування людини. Воно впливає на стан вищих психічних функцій і фізіологічні процеси в організмі. Хороше освітлення діє тонізуюче, створює гарний настрій, покращує протікання основних процесів вищої нервової діяльності.

Збільшення освітленості сприяє поліпшенню працездатності навіть в тих випадках, коли процес праці практично не залежить від зорового сприйняття. При поганому освітленні людина швидко втомлюється, працює менш продуктивно, виникає потенційна небезпека помилкових дій і нещасних випадків.

Освітленість приміщення має велике значення при роботі на ППК. Вона багато в чому визначається колірною і мережевий обстановкою. Для зменшеного поглинання світла стеля і стіни вище панелей (1,5-1,7м.). Якщо вони не облицьовані звукопоглинальним матеріалом, фарбуються білою водоемульсійною фарбою (коефіцієнт відбиття повинен бути не менше 0,7). Для забарвлення стіни панелей рекомендується віддавати перевагу світлим фарбам.

Основний потік природного світла при цій повинен бути зліва. Не допускається спрямування основного світлового потоку природного світла праворуч, ззаду і спереду працівника на ППК.

Робота на ППК може здійснюватися за таких видах освітлення:

–загальному штучному освітленні, коли відео монітори розташовуються по периметру приміщення або при центральному розташуванні робочих місць у два ряди по довжині кімнати з екранами, звернені в протилежні сторони;

–суміщене освітлення (природне + штучне) тільки при одному і трьох рядном розташуванні робочих місць, коли екран і поверхню робочого столу знаходяться перпендикулярно світла несучій стіні. При цьому штучне освітлення буде виконане стельовими або підвісними люмінесцентними світильниками, рівномірно розміщеними по стелі рядами паралельно світловим прорізам так, щоб екран відео монітора знаходився в зоні захисного кута світильника, і його проекції не доводилися на екран. Працюючі на ППК не повинні бачити відображення світильників на екрані. Застосовувати місцеве освітлення при роботі на ППК не рекомендується.

Природне освітлення, коли робочі місця з ППК розташовуються в один ряд по довжині приміщення на відстані 0,8 - 1,0 м від стіни з віконними прорізами, і екрани знаходяться перпендикулярно цієї стіни. Основний потік природного світла при цій повинен бути зліва. Не допускається спрямування основного світлового потоку природного світла праворуч, ззаду і спереду працює на ППК. Оптимальна відстань очей до екрана відео монітора повинна

становити 60-70 см, допустиме не менше 50 см. Розглядати інформацію ближче 50 см не рекомендується.

У проекті, що розробляється, передбачається використовувати суміщене освітлення. У світлий час доби використовуватиметься природне освітлення приміщення через віконні отвори, в решту часу використовуватиметься штучне освітлення. Штучне освітлення створюється газорозрядними лампами.

Штучне освітлення в робочому приміщенні передбачається здійснювати з використанням люмінесцентних джерел світла в світильниках загального освітлення, оскільки люмінесцентні лампи мають високу потужність (80 Вт), тривалий термін служби (до 10000 годин), спектральний складом випромінюваного світла, близький до сонячного. При експлуатації ПК виконується зорова робота IV в розряду точності (середня точність). При цьому нормована освітленість на робочому місці (Ен) рівна 200 лк. Джерелом природного освітлення є сонячне світло.

У приміщенні, де розташовані ПК передбачається природне бічне освітлення, рівень якого відповідає [36]. Джерелом природного освітлення є сонячне світло. Регулярно повинен проводитися контроль освітленості, який підтверджує, що рівень освітленості задовольняє [36] і для даного приміщення в світлий час доби достатньо природного освітлення.

Розрахунок освітлення.

Для будівель виробництв світловий коефіцієнт приймається в межах 1/6 - 1/10:

$$\sqrt{a^2+b^2}\cdot S_b = (1/8 \div 1/10)\cdot S_n \qquad (4.1)$$

де S_b – площа віконних прорізів, м^2;

S_n – площа підлоги, м^2.

$S_n = a \cdot b = 5 \cdot 5 = 25$ м^2

$S_{вік} = 1/8 \cdot 25 = 3{,}125$ м^2

Приймаємо 2 вікна площею $S = 1{,}6$ м^2 кожне.

Світильники загального освітлення розташовуються над робочими поверхнями в рівномірно-прямокутному порядку. Для організації освітлення в темний час доби передбачається обладнати приміщення, довжина якого складає 5 м, ширина 5 м, світильниками ЛПО2П, оснащеними лампами типа ЛБ (дві по 80 Вт) з світловим потоком 5400 лм кожна.

Розрахунок штучного освітлення виробляється по коефіцієнтах використання світлового потоку, яким визначається потік, необхідний для створення заданої освітленості при загальному рівномірному освітленні. Розрахунок кількості світильників *N* здыйснюэться по формулі:

$$n = \frac{E \cdot S \cdot Z \cdot K}{F \cdot U \cdot M} \tag{4.2}$$

де *E* – нормована освітленість робочої поверхні, визначається нормами – 300 лк;

S – освітлювана площа, м2; S = 25 м2;

Z – поправочний коефіцієнт світильника (для стандартних світильників Z = 1.1 - 1.3) приймаємо рівним 1,1;

K – коефіцієнт запасу, що враховує зниження освітленості в процесі експлуатації – 1,5;

U – коефіцієнт використання, залежний від типу світильника, показника індексу приміщення і т.п. – 0,575

M – число люмінесцентних ламп в світильнику – 2;

F – світловий потік лампи – 5400лм.

Підставивши числові значення у формулу (4.2), отримуємо:

$$n = \frac{300 \cdot 25 \cdot 1{,}1 \cdot 1{,}5}{5400 \cdot 0{,}575 \cdot 2} \approx 2{,}64$$

Приймаємо освітлювальну установку, яка складається з 3-х світильників, які складаються з двох люмінесцентних ламп загальною потужністю 160 Вт, напругою – 220 В.

Потужність електроосвітлювальної установки з урахуванням місцевого освітлення визначається за формулою:

$$N = \frac{n \cdot W + (0{,}1 \div 0{,}2) \cdot n \cdot W}{1000}, \text{кВт} \tag{4.3}$$

де n– розрахункова кількість ламп для освітлення даного приміщення;

W – потужність однієї лампи, Вт;

(0,1÷0,2) – додаткова потужність для ламп місцевого освітлення, Вт.

$$N = \frac{3 \cdot 160 + 0,2 \cdot 3 \cdot 160}{1000} = 0,576\ кВт$$

4.4.3 Шум та вібрація, електромагнітне випромінювання

Рівень шуму, що супроводжує роботу користувачів персональних комп'ютерів, а також зовнішніми чинниками, коливається у межах 50–65 дБА [33]. Шум такої інтенсивності на тлі високого ступеня напруженості праці негативно впливає на функціональний стан користувачів. Тому на практиці рекомендують знижувати фактичний рівень шуму у приміщеннях, де створюють комп'ютерні програми, виконують теоретичні та творчі роботи, проводять навчання до 40 дБА, а в приміщеннях, де виконують роботу, що потребує зосередженості, — до 55 дБА. У залах опрацювання інформації та комп'ютерного набору рівні шуму не повинні перевищувати 65 дБА.

Шум часто є причиною зниження рівня працездатності, підвищення рівня загальної та професійної захворюваності, частоти виробничих травм. Шум є загальнобіологічним подразником, який негативно впливає на всі органи і системи організму. У разі тривалого систематичного впливу шуму може виникнути патологія з переважним ураженням слуху, центральної нервової і серцево-судинної систем.

Для зниження шуму на шляху його поширення передбачається розміщення в приміщенні штучних поглиначів. Для зниження рівня шуму стелю або стіни вище 1.5 - 1.7 метра від підлоги повинні облицьовуватися звукопоглинальним матеріалом з максимальним коефіцієнтом звукопоглинання в області частот 63-8000 Гц. Додатковим звукопоглинанням в КВТ можуть бути фіранки, підвішені в складку на відстані 15-20 см. Від огорожі, виконані з щільної, важкої тканини. У приміщенні з ПК коректований рівень звукової потужності не перевищує 45 дБА. Оскільки рівень шуму не перевищує гранично допустимих величин, які встановлені санітарними нормами, заходи для зниження шуму не проводяться.

Віброізоляція можливо здійснювати за допомогою спеціальної прокладки під системний блок, який послаблює передачу вібрацій робочого столу. Вібрація на робочому місці в приміщенні, що розглядається, відповідає нормам [33]. Допустимий рівень вібрацій на робочому місці: - для 1 ступеня шкідливості до 3 дБ; - для 2-3 - 1-6 дБ; - для 3 - більше 6 дБ.

Для захисту від електромагнітного випромінювання передбачаються наступні заходи:

– застосування нових плазмових моніторів,

– віддалення робочого місця не менше, ніж на 0,4 – 0,5 м, оскільки напруженість електричного поля зменшується при віддаленні від джерела поля,

– встановлення раціональних режимів роботи персоналу (обмеження часу перебування),

– раціональне розміщення в робочому приміщенні устаткування, що випромінює електромагнітну енергію.

4.4.4 Вентилювання

У приміщенні, де знаходяться ПК, повітрообмін реалізується за допомогою природної організованої вентиляції (вентиляційні шахти). Цей метод має забезпечити приток потрібної кількості свіжого повітря, що визначається [36] (30 $м^3$ на годину на одного працюючого).

Також має здійснюватися провітрювання приміщення, в залежності від погодних умов, тривалість повинна бути не менше 10 хв. Найкращий обмін повітря здійснюється при наскрізному провітрюванні.

4.5 Заходи з організації виробничого середовища та попередження виникнення надзвичайних ситуацій

Відповідно до санітарно-гігієнічних нормативів та правил експлуатації обладнання наводимо приклади деяких заходів безпеки.

Заходи безпеки під час експлуатації персонального комп’ютера та периферійних пристроїв передбачають:

– правильне організування місця праці та дотримання оптимальних режимів праці та відпочинку під час роботи з ПК;

– експлуатацію сертифікованого обладнання;

– дотримання заходів електробезпеки;

– забезпечення оптимальних параметрів мікроклімату;

– забезпечення раціонального освітлення місця праці (освітленість робочого місця не перевищувала 2/3 нормальної освітленості приміщення).

Зниження рівня шуму та вібрації:

– у джерелі виникнення, шляхом застосування раціональних конструкцій, нових матеріалів і технологічних процесів;

– звукоізолювання устаткування за допомогою глушників, резонаторів, кожухів, захисних конструкцій, оздоблення стін, стелі, підлоги тощо;

– використання засобів індивідуального захисту).

Заходи безпеки під час експлуатації інших електричних приладів передбачають дотримання таких правил:

– постійно стежити за справним станом електромережі, розподільних щитків, вимикачів, штепсельних розеток, лампових патронів, а також мережевих кабелів живлення, за допомогою яких електроприлади під'єднують до електромережі;

– постійно стежити за справністю ізоляції електромережі та мережевих кабелів, не допускаючи їхньої експлуатації з пошкодженою ізоляцією;

– не тягнути за мережевий кабель, щоб витягти вилку з розетки;

– не закривати меблями, різноманітним інвентарем вимикачі, штепсельні розетки;

– не підключати одночасно декілька потужних електропристроїв до однієї розетки, що може викликати надмірне нагрівання провідників, руйнування їхньої ізоляції, розплавлення і загоряння полімерних матеріалів;

– не залишати включені електроприлади без нагляду;

– не допускати потрапляння всередину електроприладів крізь вентиляційні отвори рідин або металевих предметів, а також не закривати їх та підтримувати в належній чистоті, щоб уникнути перегрівання та займання приладу;

– не ставити на електроприлади матеріали, які можуть під дією теплоти, що виділяється, загорітися (канцелярські товари, сувенірну продукцію тощо).

4.6 Охорона навколишнього природного середовища

4.6.1 Загальні дані з охорони навколишнього природного середовища

Діяльність за темою магістерської роботи в процесі її виконання впливає на навколишнє природне середовище і регламентується нормами діючого законодавства [39-43].

Основним екологічним аспектом в процесі діяльності за даними спеціальностями є процеси впливу на атмосферне повітря та процеси поводження з відходами, які утворюються, збираються, розміщуються, передаються на видалення (знешкодження), утилізацію, тощо в ІТ галузі.

Немає впливу на атмосферне повітря при нормальних умовах праці, бо в приміщенні не використовуються сканери, принтери та інші джерела викиду забруднюючих речовин в повітря робочої зони.

В процесі діяльності користувача виникають процеси поводження з відходами ІТ галузі. Види відходів, утворення, яких можливо:

– відпрацьовані люмінесцентні лампи - І клас небезпеки;

– батарейки та акумулятори (малі) -ІІІ клас небезпеки;

– змінні носії інформації - IV клас небезпеки;

– відпрацьований ізолюючий матеріал, дроти та кабелі - IV клас небезпеки;

– макулатура - IV клас небезпеки;

– побутові відходи - IV клас небезпеки.

4.6.2 Вимоги до збору, пакування та розміщення відходів ІТ галузі

Вимоги зберігання виявлених за своєю роботою відходів визначаються відповідно [40].

Відходи в міру їх накопичення збирають у тару, відповідну класу небезпеки, з дотриманням правил безпеки, після чого доставляють до місця тимчасового зберігання відходів відповідно до затвердженої схеми їх розміщення, зазначені для зберігання відходів місця чи об'єкти повинні використовуватися лише для заявлених відходів.

Не допускається зберігання відходів у невстановлених схемою місцях, а також перевищення норм тимчасового зберігання відходів.

Способи тимчасового зберігання відходів визначаються видом, агрегатним станом і класом небезпеки відходів:

– відходи I класу небезпеки зберігаються в герметичній тарі (сталеві бочки, контейнери). У міру наповнення тару з відходами закривають герметично сталевий кришкою;

– відходи II класу небезпеки в залежності від агрегатного стану зберігаються в поліетиленових мішках, бочках, сховищах та інших видах тари, яка запобігає поширенню шкідливих речовин;

– відходи III класу небезпеки зберігаються в тарі, яка забезпечує локалізацію зберігання, дозволяє виконувати вантажно-розвантажувальні і транспортні роботи і виключає поширення в ОС шкідливих речовин;

– відходи IV класу небезпеки можуть зберігатися відкрито на промисловому майданчику у вигляді конусоподібної купи, звідки їх автонавантажувачем перевантажують у самоскид і доставляють на місце утилізації або захоронення;

– в разі тимчасового зберігання відходів у стаціонарних складах або промислових приміщеннях повинні бути забезпечені санітарно-гігієнічними етичні вимоги до повітря робочої зони згідно [35].

Не допускається змішування відходів різних видів і класів небезпеки з будівельними і побутовими відходами, відходами дерев'яної, металевої, синтетичної тари, відходами текстильних матеріалів (старий спецодяг, ганчірки) та інше.

Проведення заготовки, здачі, переробки та реалізації металобрухту встановлені в [44].

Особливий контроль наділяється збору і зберіганню відпрацьованих ртутьвмісних ламп (енергоощадних) як відходам I класу небезпеки, що збираються і обов’язково передаються на утилізацію підприємствам, що мають ліцензію на поводження з такими небезпечними відходами.

Всі відходи, що утворюються в процесі діяльності/роботи, підлягають обліку.

4.6.3 Визначення впливу та заходів щодо поводження з відходами ІТ галузі

З метою визначення та прогнозування впливу відходів на навколишнє середовище, своєчасного виявлення негативних наслідків, їх запобігання відповідно [45] повинен здійснюватися моніторинг місць утворення, зберігання, і видалення відходів. Відомості про місце утворення та місце розташування відходів зазначаються на «План схемі місці розміщення відходів організації / виробництва» та наводяться у таблиці 4.5, а відомості про склад і властивості відходів, що утворюються, а також ступінь їх небезпечності для навколишнього природного середовища та здоров'я людини у таблиці 4.6.

Таблиця 4.5 Відомості про місце утворення та місце розташування відходів

Код та найменування відходів за ДК -005-96	Технологічний процес або виробництво, де утворюються відходи / клас небезпеки	Місце розташування відходу, тара та її кількість, місткість, розміри у разі наявності майданчиків розташування відходів необхідно зазначити тип покриття та наявність даху)	№ на схемі (додається масштабна схема місць розміщення відходів)
7710.3.1.26 Лампи люмінесцентні, та відходи, які містять ртуть, інші зіпсовані або відпрацьовані (Відпрацьовані ртутьвмісні люмінесцентні лампи)	1	буд.4, в приміщені кладової S=100м^2, в кількість 20 од.	8401-ТХ

7720.3.1.01 Відходи комунальні (міські) змішані, у т.ч. сміття з урн (Побутові відходи)	4	зовнішній майданчик зберігання побутових відходів біля буд .4 S=5м² V= 2,08м³- 2од.	8401-ТХ
7710.3.1.01 Макулатура паперова та картонна (Макулатура)		буд .4 4 поверх в кім. 412 S =5,0 м.^{2}	8401-ТХ
7730.3.1.02 Матеріали пакувальні пластмасові зіпсовані, відпрацьовані чи забруднені (Матеріали пакувальні забруднені	4	буд .4 контейнер V=0,9м^3 (3 од.)	8401-ТХ
Змінні носії інформації	4	контейнер V=0,04м^3 (2 од.) буд .4	8401-ТХ
Батарейки та акумулятори (малі)	3	контейнер V=0,09м^3 (4 од.) буд .4	8401-ТХ

Таблиця 4.6 - Відомості про склад і властивості відходів, що утворюються, а також ступінь їх небезпечності для навколишнього природного середовища та здоров'я людини.

Назва відходів	Клас небезпечності	Хімічний (у долях відсотків складників або інших одиницях виміру) та морфологічний склад	Фізико-хімічні властивості
Відпрацьовані люмінесцентні лампи	I	**Ртуть** - 0,013 **Hg** **Скло** - 98,787**$(Na, K)_2 O\ 2SiO_2$** **Алюміній** - 1,2 **Al**	**Ртуть** – $T_{кип.}$ = 356,58°C $T_{плав.}$ = **-38,87°C** **Скло** -$T_{плав.}$=800°C **Алюміній** - $T_{кип.}$ = 2348°C $T_{плав.}$ = 660,1°C
Макулатура	IV	**Цинк** - 0,000053 – 0,000056 **Zn** **Свинець** - 0,000049 – 0,000051 **Pb** **Хром** - 0,000051 – 0,000054 **Cr** **Мідь** - 0,000033 – 0,000035 **Cu** **Целюлоза** - 97,299814 – 96,999804 **$(C_6H_{10}O_5)_n$** **Вода** - 2,7 – 3,0	Уривки та обрізки з паперових мішків **Цинк** $T_{кип.}$= 913°C $T_{плав.}$= 4,19°C **Свинець** $T_{кип.}$= 1751°C $T_{плав.}$= 327,3°C **Хром** $T_{кип.}$= 1890°C $T_{плав.}$= 2480°C **Мідь** $T_{кип.}$= 2580°C $T_{плав.}$= 1083°C **Целюлоза** $T_{возг. с обуглив.} \geq 100$°C

Побутові відходи	IV	Побутові відходи - 100 – 100, в т. ч.: Папір -30 - 17; [$(C_6H_{10}O_5)_n$ - целюлоза] Поліетилен -20 – 24; $(-CH_2 - CH_2 -)_n$ Деревина -5 – 3; [$(C_6H_{10}O_5)$ – целюлоза, лігнін] Матеріали текстильні -4 – 3; [$(C_6H_{10}O_5)_n$ - целюлоза Мінеральні домішки (пісок, глина) -4 – 9 Харчові відходи -37 –44;	Поліетилен - $T_{размяг.} \geq 150°C$ Твердий матеріал рослинного походження, не розчиняється у воді. Целюлоза, лігнін $T_{возг. с обуглив.} \geq 120°C$ Харчові відходи $T_{биоразл.} \geq 4^{o}$ C

Негативний вплив на ОС і людини визначається його хімічним складом.

Ртуть. У природних водах міститься в концентрації 0,00003 ... 0,0028 мг / л. Являючись потужним кумулятивним отрутою, з можливою канцерогенною і мутагенною дією. Процеси самоочищення водойм порушують концентрація ртуті понад 0,018 мг / л, порогова концентрація ртуті за впливом на санітарний режим водойм-0,01 мг / л. Наприкінці концентрація понад 0,03 є токсичною практично для всіх видів водних організмів. Надзвичайно токсична при попаданні з питною водою для теплокровних організмів, надходження ртуті з питною водою в кількості 75,0 ... 300,0 мг / доб. є смертельним. Відрізняється високою токсичністю для будь-яких форм життя. При отруєнні парами спостерігається слабкість, головний біль, біль в шлунку, роздратування по-чек, навіть нефрит; катаральні явища. Розвивається тремтіння рук, ніг, всього тіла. Виникає стан підвищеної психічної збудливості/ Пари ртуті проявляють нейротоксичність, особливо страждають вищі відділи нервової системи [46].

Скло. Нетоксичні, безпечно в навколишньому середовищу, не шкідлива в нирках і водоймах. Вдихання скляного пилу (волокон) призводить до силікоз в зв'язку з високим

вмістом сполук кремнію. Шкідливої дії не робить, але є небезпека механічних пошкоджень (порізи, травми).

Алюміній. Токсичний для водної біоти, теплокровних тварин і людей, в концентрації> 1 мг / л чинить негативний впливав на зростання с /г культур. У концентрації> 1 мг / л гальмує зростання мікрофлори водойм і стримує процеси самоочищення водойм. Рівень токсичності визначається формою, в якій знаходиться елемент. Впливає на обмін речовин і функції нервової системи . При попаданні на ґрунт, в воду і атмосферними повітря надає негативного впливу на НС і здоров'я людини.

Цинк. Малотоксичний для теплокровних тварин при надходженні з їжею і питної водою-концентрація в питній воді 11,2 ... 26,6 мг / л переноситься без будь-яких ознак інтоксикації. Дуже корисний для флори, будучи одним з найважливіших мікроелементів харчування, однак лише в концентрації до

0,2 мг / л, крім того, елемент силяється до кумуляції в грантах. Дуже токсичний для водних організмів, порушуючи процеси самоочищення водойм і стаючи токсичним для іхтіофауни в концентрації 0,15 ... 5,0 мг / л. Мутагенна і онкогенна небезпеку.

Свинець. У природних водах міститься в концентрації 0,001 - 0,023 мг / л. У концентрації 2,0 мг / л надає воді металевий присмак. Можливо має мутагенну і канцерогенну дію, значно збільшує токсичну дію інших металів. В конценрації 1,90 мг / л згубно діє на дафній, концентрація 0,1 мг / л погіршує процеси самоочищення водойм. Свинець токсичний для рослин в концентрації понад 5,0 мг / кг ґрунту.

Помірно токсичний. Викликає хронічне отруєння. Має здатність вражати центральну і периферичну нервову систему, кістковий мозок і кров, судини, синтез білка, генетичний апарат клітини.

Хром. Міститься в природних водах в концентрації 0,001 ... 0,112 мг / л. LK50 Cr (VI) для риб-30,0 ... 50,0 мг / л, LK50 Cr (III) для риб - 117,0 мг / л. Низькі концентрації хрому позитивно впливають на ріст рослин. Володіє канцерогенними властивістю.

Мідь. У природних водах міститься в концентраціях 0,001 ... 0,98 мг / л. У концентрації 0,5 мг / л забарвлює воду, в концентрації> 1,0 мг / л-помітно збільшує мутність води. Дуже токсична як для водних організмів, так і для рослин. У концентрації 0,001 мг / л гальмує розвиток синьо зелених водоростей, LK50 практично для всіх видів риб становить 0,18 ... 1,35 мг / л (короп, карась, окунь, щука, сом). Накопичується ґрунтом і рослинами. У концентрації 0,1 ... 0,2 мг / л надає токсичну дію на ріст рослин. Високотоксичний метал. Викликає гостре отруєння, має широкий спектр токсичної дії).

Целюлоза. Нетоксична. Досить легко піддається біодеструкції лігнін - і целюлозоруйнуючими бактеріями і деякими класами нищих грибів. У зв'язку з

нетоксичністю LD50 для тваринах не установлена. Токсичність визначається за вмістом важких металів, здатних мігрувати з неї в навколишнє середовище. При попаданні на ґрунт, в воду і атмосферне повітря чинить негативний вплив на ОС і здоров'я людини.

Поліетилен. Нетоксичний для всіх видів флори і фауни в зв'язку з дуже високою біологічною інертністю. Нерозчинний у водних середовищах і не впливає на санітарний режим водойм. Використання його не вимагає запобіжних заходів. Отруєння можливі при виробництві та переробці плівки, в результаті виділення окису вуглецю, альдегідів, органічних кислот [47]

Деревина. Нетоксична. Досить легко піддається біодеструкції лігнін- і целюлозоруйнуючими бактеріями і деякими класами нижчих грибів. У зв'язку з нетоксичністю LD50 для тварин не встановлена. Деревина нетоксична при використання. Але дія деревного пилу при рубці і переробці деревини викликає захворювання дихальних шляхів і шкіри.

Текстильне волокно. Нетоксична в зв'язку з біогенним походженням, проте для біодеструкції необхідна наявність вологи. Нетоксична при використанні. Токсична дія виникає (як результат механічні дії - наслідок пилу) при виробництві тканів і при переробці вторинних матеріалів; слабкий алерген.

4.7 Висновки до розділу 4

У четвертому розділі магістерської роботи проведений аналіз умов праці, шкідливих та небезпечних чинників, з якими стикається робітник. Визначено параметри і певні характеристики приміщення для роботи над запропонованим проектом написаному в дипломній роботі, описано, які заходи потрібно зробити для того, щоб дане приміщення відповідало необхідним нормам і було комфортним і безпечним для робітника. Приведені рекомендації щодо організації робочого місця, а також важливу інформацію щодо пожежної та електробезпеки.

Наведена схема, розміри приміщення та визначені значення температури, вологості й рухливості повітря, необхідна кількість і потужність ламп та інші параметри, значення яких впливає на умови праці робітника, а також – наведені інструкції з охорони праці, техніки безпеки при роботі на комп’ютері, визначені основні екологічні аспекти впливу на навколишнє природнє середовище та зазначені заходи щодо поводження з ними.

ВИСНОВКИ

В магістерській роботі запропоновано метод побудови евристичної системи захисту WEB-додатків, що має суттєві переваги порівняно з існуючими на сьогоднішній день методами детектування і відбиття атак.

До переваг систем захисту на базі запропонованого методу можна віднести:

– здатність до виявлення нових типів атак, коли сигнатурний аналіз безсилий у силу своєї статичної природи;

– система не вимагає відновлення сигнатур, тому що засновано на аномаліях поведінки, тобто не потребує розробки і підтримки доволі не дешевої інфраструктури у мережі Internet, яка б дозволяла регулярно отримувати оновлення сигнатурних баз;

– дає можливість відслідковувати дії користувача, що неодноразово робить спроби проникнення, тобто "слідкує" за користувачем впродовж усіх циклів роботи з WEB-додатком;

– повністю адаптується під особливості WEB-додатку що захищає.

Як показали проведені експерименти, система здатна виявляти атаки, які не було виявлено на попередніх етапах сканування ні брандмауером, ні фільтром ModSecurity. При достатньому періоді навчання евристична система здатна виявляти до 40% таких атак.

Розроблений метод може застосовуватися як в якості додаткової ланки захисту у вже існуючих системах запобігання вторгнень, так і в якості самостійної системи виявлення та відбиття атак.

В першому розділі магістерської роботи проведений огляд та аналіз інформаційної безпеки в мережі Internet, захист WEB-серверів, сучасні тенденції у розробці систем захисту та проблеми створення безпечного середовища для функціонування WEB-додатку. За результатами проведеного огляду визначені задачі дослідження:

З метою реалізації задачі дослідження розроблено евристичну систему захисту WEB-додатків.

В другому розділі обґрунтовано вибір моделі мережі. Як досліджувана модель нейронної мережі обрана мережа адаптивно-резонансної теорії (АРТ), яка має здатність приймати рішення щодо подібності інформації, що надійшла з інформацією та вже зберігається у пам'яті. Визначена архітектура та алгоритм навчання нейронної мережі, що передбачає покрокове виконання дій. Використовуючи класичну структуру нейронної мережі при тестуванні роботи мережі були зроблені зауваження. Для усунення недоліків роботи нейронної мережі в роботі розроблені засоби компенсації .

У третьому розділі визначені перспективні напрямки вдосконалення систем захисту інформації. Зазначено, що більшу частину атак на WEB-додатки можна розпізнати тільки на рівні додатків (сьомий рівень моделі OSI). Розроблена схема побудови захисту WEB-додатку. У запропонованій схемі аналіз на рівні додатків здійснюється системою, що складається з набору так званих "давачів" і евристичного аналізатору. Зазначено, що для розв'язуваного класу завдань найбільше всього підходить мережа АРТ-1. Головне завдання, що покладене на нейронну мережу, є завдання виявлення атак, які не були виявлені на етапі сигнатурного аналізу. Наведено приклад функціонування системи захисту. Для створення програми, що реалізує захист WEB-додатку з можливостями евристичного аналізу обрано мову PHP , наведено її переваги та результати дослідження з застосуванням розробленої програми.

У четвертому розділі роботи проведено аналіз умов праці, шкідливих та небезпечних чинників, з якими стикається робітник. Визначено параметри і певні характеристики приміщення для роботи над запропонованим проектом написаному в дипломній роботі, описано, які заходи потрібно зробити для того, щоб дане приміщення відповідало необхідним нормам і було комфортним і безпечним для робітника. Приведені рекомендації щодо організації робочого місця, а також важливу інформацію щодо пожежної та електробезпеки. Була наведена схема, розміри приміщення та наведено значення температури, вологості й рухливості повітря, необхідна кількість і потужність ламп та інші параметри, значення яких впливає на умови праці робітника, а також – наведені інструкції з охорони праці, техніки безпеки при роботі на комп’ютері. Також визначені основні екологічні аспекти впливу на навколишнє природнє середовище та зазначені заходи щодо поводження з ними

ПЕРЕЛІК ПОСИЛАНЬ

1. McGraw G. Building Security In. – New-York: Addison-Wesley,2006. – 448 p.
2. Гайкович В., Першин А. Безопасность электронных банковских систем. – М.: Единая Европа, 1994. – 264 с.
3. Гилстер П. Взгляд из Internet: Пер с англ. – К.: Диалектика, 1996. – 495 с.
4. Игер Б. Работа в сети / Под ред. А. Тихонова; Пер. с англ. – М.: БИНОМ, 1996. – 313 с.
5. Кент П. ПК и общество / Пер. с англ. В.Л. Григорьева. – М.: Компьютер, 1996. – 267 с.
6. Колесников О. Э. Политика безопасности в распределенных системах. – М.: Издат. фирма “Яуза”, 1996. – 281 с.
7. Крол Эд. Все об Internet: Руководство и каталог / Пер. с англ. С.М. Тимачева. – К.: BNV, 1995. – 591 с.
8. Левин В.К. Защита информации в информационно-вычислительных системах и сетях – К.: BNV, 1995. – 543 с.
9. Cheswick W.R., Bellovin S.M. Firewalls and Internet Security: Repelling the Wily Hacker. – New-York: Addison-Wesley, 1994. – 275 с.
10. Симонович С. В. Справочник программиста. – М.: АСТ-Пресс – 2001. – 654 с.
11. Симонович С. В. и др. Информатика и безопасность. – СПб.: Питер – 2002. – 560 с.
12. Shah S. Web hacking. – New-York: Addison-Wesley, 2004. – 376 p.
13. Низамутдинов М. Ф. Тактика защиты и нападения на WEB-приложения. – СПб.: БХВ-Петербург, 2005. – 432 с.
14. Заинцев И. В. Нейронные сети. Основные модели. – СПб.: БХВ-Петербург, 1999. – 458 с.
15. Руденко О. Г., Бодянський Є. В. Штучні нейронні мережі. – Х.: ТОВ "Компанія СМІТ", 2006. – 404 с.
16. Heiser J., Firstbrook P., Scholtz T. Gartner Information Security Hype Cycle: http://www.gartner.com/5_about/ press_releases/pr11june2003c.jsp, 2003
17. Paul E., Amrit T. Make Your IPS Work for You With Improved Tuning: http://www.gartner.com/5_about/press_releases/august2006.jsp, 2006
18. Auger R., Barnett R. Threat Classification: http://www.webappsec.org/projects/threat/v1/WASC-TC-v1_0.txt, 2004.
19. Robert A., Ryan B. Web Application Firewall Evaluation Criteria: http://www.webappsec.org/ projects/wafec/v1/wasc-wafec-v1.0.txt, 2006.

20. Bragg R., Strassberg K. Network Security. – Osborne: Mcgraw-Hill, 2006. – 896 p.

21. Coar C., Bowen R. Apache Cookbook. – Sebastopol: O'Relly, 2003. – 254 p.

22. Ristic I. Apache Security. – Sebastopol: O'Relly, 2005. – 420 p.

23. Закон України «Про охорону праці».

24. Кодексу законів України про працю.

25. Закон України "Про загальнообов'язкове державне соціальне страхування від нещасного випадку на виробництві та професійного захворювання, які спричинили втрату працездатності".

26. НПАОП 0.00-6.03-93 «Порядок опрацювання та затвердження власником нормативних актів про охорону праці, що діють на підприємстві».

27. НПАОП 0.00-4.12-05 «Типове положення про порядок проведення навчання і перевірки знань з питань охорони праці».

28. НАПБ Б.02.005-2003 «Типове положення про інструктажі, спеціальне навчання та перевірку знань з питань пожежної безпеки на підприємствах, в установах та організаціях України».

29. НПАОП 0.00-4.15-98 «Положення про розробку інструкцій з охорони праці».

30. ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень».

31. ДСанПіН 3.3.2.007-98 «Правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин».

32. НПАОП 0.00.-1.28-10 «Правил охорони праці під час експлуатації електронно-обчислювальних машин».

33. .НАПБ Б.03.002-2007. «Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою».

34. ГОСТ 12.1.044-89 ССБТ. «Пожаровзрывоопасность веществ и материалов. Номенклатура показателей и методы их определения».

35. ДСН 3.3.6.042-99. «Санітарні норми мікроклімату виробничих».

36. .ДБН-В.2.5-28-2006. «Природне і штучне освітлення».

37. ДСН 3.3.6.037-99. «Санітарні норми виробничого шуму, ультразвуку та інфразвуку».

38. ДБН В.2.5-67:2013 Опалення, вентиляція та кондиціонування.

39. Закон України «Про охорону навколишнього природного середовища».

40. Закон України «Про забезпечення санітарного та епідемічного благополуччя населення».

41. Закон України «Про відходи».

42. Закон України «Про охорону атмосферного повітря».

43. Закон України Закон України «Про захист населення і територій від надзвичайних ситуацій техногенного та природного характеру».

44. ДСанПіН 2.2.7.029. «Гігієнічні вимоги щодо поводження з промисловими відходами та визначення їх класу небезпеки для здоров'я населення».

45. Закон України «Про металобрухт».

46. ДСТУ 3911-99. Охорона природи. Поводження з відходами. Виявлення відходів і подання інформаційних даних про відходи. Загальні вимоги.

47. ДК 005-96. Державний класифікатор України. Класифікатор відходів.