УДК 004.735

Унгул Володимир Валерійович
студент
Національний технічний університет України «Київський політехнічний інститут»
Унгул Владимир Валерьевич
студент
Национальный технический университет Украины «Киевский политехнический институт»
Unhul Volodymyr V.
Student

АНАЛІЗ ТА РОЗРОБКА МЕТОДІВ ДЕОБФУСКАЦІЇ СКРИПТІВ ДЛЯ ВИЯВЛЕННЯ ЗАГРОЗ ІНФОРМАЦІЙНОЇ СТІЙКОСТІ КОМП'ЮТЕРА

АНАЛИЗ И РАЗРАБОТКА МЕТОДОВ ДЕОБФУСКАЦИИ СКРИПТОВ ДЛЯ ВЫЯВЛЕНИЯ УГРОЗ ИНФОРМАЦИОННОЙ УСТОЙЧИВОСТИ КОМПЬЮТЕРА

ANALYSIS AND DEVELOPMENT OF METHODS DEOBFUSKATSIYI SCRIPTS TO IDENTIFY THREATS TO INFORMATION COMPUTER SUSTAINABILITY

Анотація. *В роботі досліджуються проблемні питання в захисті інформаційних систем та пропонуються методи усунення цих проблем. Метою є покращення систем захисту комп'ютерної інформації від скриптових вірусів, які потрапляють до комп'ютера з мережі інтернет, а саме при перегляді WEB-сторінок із вбудованим вірусним програмним забезпеченням. Описани принципи створення та побудовані алгоритми протидії обфусцированим скриптовим вірусам.*

Ключові слова: *Обфускація, Деобфускація, Розшифровування, WEB-сторінки, JavaScript, скриптовий вірус.*

Аннотация. *В работе исследуются проблемные вопросы в защите информационных систем и предлагаются методы устранения этих проблем. Целью является улучшение систем защиты компьютерной информации от скриптовых вирусов, которые попадают к компьютеру из сети интернет, а именно при просмотре WEB-страниц с встроенным вирусным программным обеспечением. Описаны принципы создания и построены алгоритмы противодействия обфусцированим скриптовым вирусам.*

Ключевые слова: *Обфускация, Деобфускация, Расшифровка, WEB-страницы, JavaScript, скриптовый вирус.*

Summary. *It analyzes the problems in protecting information systems and proposes methods eliminate these problems. To improve the systems of information protection of scripting viruses that enter your computer from the Internet, such as when watching WEB-page in-viral software. Describes the creation and counter the algorithm obfustsyrovanym scripting viruses.*

Key words: *Obfuskatsiya, Deobfuskatsiya, Decryption, WEB-page, JavaScript, script virus.*

Вступ

З кожним днем зростає кількість інформаційних комп'ютерних систем, які потребують захисту, надійності в обробці й використанні даних, разом із ними зростає кількість різновидів вірусів та вірусного коду, які можуть негативно вплинути або взагалі внести критичні зміни в роботу будь-якої інформаційної системи. В процесі виконання наукового дослідження винайдені та представлені принципово нові рішення по захисту інформаційної системи від зашифрованих скриптових комп'ютерних вірусів.

1. АНАЛІЗ ТА ОГЛЯД ПРОБЛЕМАТИКИ ПРЕДМЕТНОЇ ОБЛАСТІ ДОСЛІДЖЕННЯ

1.1. Гармонізація понятійної бази

В зв'язку з тим, що проблеми протидії зашифрованим скриптовим вірусам є досить новою, в науково-практичних джерелах є деяка розбіжність в термінології та поняттях. Тому на першому етапі досліджень проведена гармонізація понятійної бази.

Гармонізація базувалась на наступних принципах:

- Використані поняття та терміни повинні відповідати загальновизнаним та не протирічити між собою.
- Використані поняття та терміни повинні відповідати меті дослідження.

В даній статті особлива увага приділяється обфускації програмного коду та веб-додатків написаних на скриптовій мові javascript. Обфускація — це приведення виконуваного програмного коду до виду, який зберігає його функціональність, але ускладнює аналіз, розуміння алгоритму роботи і модифікації при декомпіляції [1]. Іншими словами це заплутування коду. «Заплутування» коду може здійснюватися на рівні алгоритму, сирцевого тексту або асемблерного тексту. Існують спеціальні програми, що виробляють обфускацію, їх називають обфускаторами. Є деяка кількість шляхів обфускації, яка може реорганізовувати програмний код в автоматичному режимі або в ручному.

Цілі обфускації:

– складнення декомпіляції та вивчення програм з метою виявлення функціональності;
– Ускладнення декомпіляції програм з метою запобігання обходу систем перевірки ліцензій;
– Порушення авторських прав програмістів і приховування авторства;
– Демонстрація неочевидних можливостей мови і кваліфікації програміста.

Останнім часом, в інтернет середовищі значно поширилась тенденція написання шкідливого коду і прихованість його за допомогою методів обфускації. Такі вірусні програми та скрипти легко обходять існуючі антивірусні засоби, тому що виявити шкідливий функціонал досить складно. Щоб дослідити такий код треба проводити деобфускацію. В деяких випадках її треба робити в декілька кроків, тому що код може бути обфусцированим декілька разів. Тобто вже обфусцирований код піддається новій обфускації і так далі.

Деобфускація — це процес, приведення обфусцированого коду до виду, який дозволить вивчати та анлізувати його функціонал. В даний момент часу, не має систем, які б змогли проаналізувати будь-який обфусцирований код, але існують деобфускатори (програми, які надають змогу проаналізувати функціонал або привести код до зрозумілого виду), які «заточені» тільки під певний різновид обфускації. Метою дослідження є можливість аналізувати будь-який обфусцирований код, незважаючи, якими засобами та методами він був обфусцирован.

1.2. Методи шифрування (обфускації) скриптової мови JavaScript

Існує дуже велика кількість методів обфускації, яких із кожним днем стає дедалі більше. Ми спробували їх розділити на три категорії.

1.2.1. Обфускація мінімізаторами

Існують готові програмні засоби, які надають змогу в автоматичному режим зробити «зтискання» коду. Таким видом обфускації користуються в більшій мірі виробники програмного забезпечення. Код, який отримаємо на виході, можна зашифрувати ще одним методом, які будуть розглянуті пізніше в нашій роботі.

Серед загальновідомих мінімізаторів [2] можна виділити JS Packer, JSmin, YUI Compressor, Closure compiler та це далеко не повний їх список.

Написаний код на скриптовій мові JavaScipt виду:

```
function MyClass(){
    this.foo = function(argument1, argument2){
        var addedArgs = parseInt(argument1)+parseInt(arg
        ument2);
        return addedArgs;
    }
    var anonymousInnerFunction = function(){
        // do stuff here!
        }
    }
```

За допомогою мінімізаторів приймає такий вигляд:

```
function MyClass(){this.foo=function(c, b){var d=
parseInt(c)+parseInt(b); return d}; var a=function()
{}};
```

або такий:

```
var _0xd799=["\x66\x6F\x6F"]; function MyClass()
{this[_0xd799[0]]=function (_0xefcax2,_0xefcax3)
{var _0xefcax4=parseInt(_0xefcax2)+parseInt(_0x-
efcax3); return _0xefcax4;}; var _0xefcax5=function
(){};};
```

або такий:

```
eval(function(p, a, c, k, e, d){e=function(c){return
c}; if(!''.replace(/^/, String)){while(c—){d[c]=k[c]||c}
k=[function(e){return d[e]}]; e=function(){return'\\
w+'}; c=1}; while(c—){if(k[c]){p=p.replace(new
RegExp('\\b'+e(c)+'\\b','g'), k[c])}}return p}
('4 0="3 5!";9 2(1){6(1+"\\7"+0)}2("8");',10,10,'a|ms-
g|MsgBox|Hello|var|World|alert|n|OK|function'.
split('|'),0,{})).
```

З першого погляду отриманий код важко проаналізувати та все ж таки не існує нічого неможливого. Подібну обфускацію можна провести і в ручному режимі, що, можливо, навіть ускладнить його деобфускацію.

1.2.2. Методи Braifuck

Такий підхід перетворює код до невпізнання [3]. Навіть незрозуміло, що перед нами виконуваний JavaScript скрипт.

Мізерний скрипт alert(0) можна перетворити в такий вид:

```
([][(![]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])
[+[]]+(![]+[]+[][[]])[+!+[]+[+[]]]+(![]+[])
[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])
[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])
```

[+!+[]+[+[]]]+(!![]+[])[+!+[]]+(!![]+[])
[+[]]][([][(![]+[])[+[]]+(![]+[]+[][[]])
[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])
[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])
[+!+[]]+[])[!+[]+!+[]+!+[]]+(![]+[])
[+!+[]]+(![]+[])[!+[]+!+[]]+(!![]+[])
()[(![]+[])[+!+[]]+(![]+[])[!+[]+!+[]]+(!![]+[])
[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]+(!![]+[])[+[]]])(+[]);

або в такий:

ﾟωﾟﾉ= /｀m´）ﾉ ~┻━┻ //*´∇｀*/ ['_']; o=(ﾟｰﾟ) =_=3; c=(ﾟΘﾟ) =(ﾟｰﾟ)-(ﾟｰﾟ); (ﾟДﾟ) =(ﾟΘﾟ)= (o^_^o)/ (o^_^o);(ﾟДﾟ)={ﾟΘﾟ: '_' ,ﾟωﾟﾉ : ((ﾟωﾟﾉ==3) +'_') [ﾟΘﾟ] ,ﾟｰﾟﾉ :(ﾟωﾟﾉ+ '_')[o^_^o -(ﾟΘﾟ)] ,ﾟДﾟﾉ:((ﾟｰﾟ==3) +'_') [ﾟｰﾟ] }; (ﾟДﾟ) [ﾟΘﾟ] =((ﾟωﾟﾉ==3) +'_') [c^_^o];(ﾟДﾟ) ['c'] = ((ﾟДﾟ)+'_') [(ﾟｰﾟ)+(ﾟｰﾟ)-(ﾟΘﾟ)];(ﾟДﾟ) ['o'] = ((ﾟДﾟ)+'_') [ﾟΘﾟ];(ﾟoﾟ)=(ﾟДﾟ) ['c']+(ﾟДﾟ) ['o']+(ﾟωﾟﾉ +'_')[ﾟΘﾟ]+ ((ﾟωﾟﾉ==3) +'_') [ﾟｰﾟ] + ((ﾟДﾟ) +'_') [(ﾟｰﾟ)+(ﾟｰﾟ)]+ ((ﾟｰﾟ==3) +'_') [ﾟΘﾟ]+((ﾟｰﾟ==3) +'_') [(ﾟｰﾟ) - (ﾟΘﾟ)]+(ﾟДﾟ) ['c']+((ﾟДﾟ)+'_') [(ﾟｰﾟ)+(ﾟｰﾟ)]+ (ﾟДﾟ) ['o']+((ﾟｰﾟ==3) +'_') [ﾟΘﾟ];(ﾟДﾟ) ['_'] =(o^_^o) [ﾟoﾟ] [ﾟoﾟ];(ﾟεﾟ)=((ﾟｰﾟ==3) +'_') [ﾟΘﾟ]+ (ﾟДﾟ) .ﾟДﾟﾉ+((ﾟДﾟ)+'_') [(ﾟｰﾟ) + (ﾟｰﾟ)]+((ﾟｰﾟ==3) +'_') [o^_^o -ﾟΘﾟ]+((ﾟｰﾟ==3) +'_') [ﾟΘﾟ]+ (ﾟωﾟﾉ +'_') [ﾟΘﾟ]; (ﾟｰﾟ)+=(ﾟΘﾟ); (ﾟДﾟ)[ﾟεﾟ]='\\'; (ﾟДﾟ).ﾟΘﾟﾉ=(ﾟДﾟ+ ﾟｰﾟ)[o^_^o -(ﾟΘﾟ)];(oﾟｰﾟo)=(ﾟωﾟﾉ +'_')[c^_^o];(ﾟДﾟ) [ﾟoﾟ]='\"';(ﾟДﾟ) ['_'] ((ﾟДﾟ) ['_'] (ﾟεﾟ+(ﾟДﾟ)[ﾟoﾟ]+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (ﾟΘﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((o^_^o) +(o^_^o))+ ((o^_^o) - (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((o^_^o) +(o^_^o))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+((ﾟｰﾟ) + (ﾟΘﾟ))+ (c^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+((o^_^o) +(o^_^o))+ (c^_^o)+ (ﾟДﾟ) [ﾟεﾟ]+((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟΘﾟ)+ (ﾟДﾟ)[ﾟoﾟ]) (ﾟΘﾟ)) ('_');

де взагалі використовуються символи, яких немає навіть на розкладці клавіатури. Хоча з першого погляду все виглядає досить страшно та здебільшого до такого виду можна привести в автоматичному режимі. Існує деяка кількість Braifuck-подібних конверторів для JavaScript.

До даного виду обфускації також можна віднести написання коду на езотеричних мовах програмування таких як Whitespace, JAPH та інших.

1.2.3. Метод запечатування

В першому способі на виході ми отримували код схожий на JavaScirpt, у другому зовсім не схожий, а метод запечатування його робить взагалі прихованим.

Обфусцированый код буде складатися з двох частин: видима частина (може використовуватися будь-який спосіб із вищеперерахованих для її обфускації) і прихована частина.

Реалізовується це таким чином: «Шкідливий код», який ми хочемо сховати, перетворюється на строку, яка складається зі знаків табуляції (біт 1) та пробілів (бит 0). Як результат, ми отримуємо в багато разів більше коду, ніж у нас було. Видима частина буде декодувати приховану частину та її виконувати: декодуватиме біти в числа, а числа перетворить в символ String.fromCharCode(), а далі виконає функцію eval. Приклад:

```
decodeAndEval(document.getElementById
(«evilCode»).innerHTML);
<div id=»evilCode»>
</div>
```

До цього методу обфускації коду можна також віднести пакування скрипта JavaScript в CSS [4]. На сторінці користувача буде відображатися картинка, яка може бути навіть фоновою, але при виконанні коду нашкодить вашому комп'ютеру. Такий спосіб шифровки реалізовується таким чином: відбувається зтискання коду та з'являється можливість реалізації інтелектуальних систем відновлення зображень винятково на растровій мові. Вказуючи просторове положення такого зображення-коду, ми можемо формувати дуже інтересні структуровані по принципу нарізання (tilling) бібліотеки практично безграничного розміру, високо-оптимізовані по трафіку та часу доступу до конкретної ділянки коду (рис. 1.1).

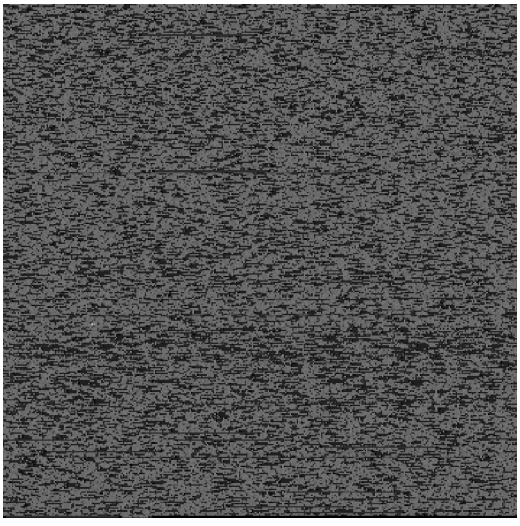

Рисунок 1.1. Приклад запечатаного скрипта в зображення

1.2.4. Узагальнена структурна схема шляхів обфускації

Із вище продемонстрованих та описаних категорій обфускації скриптів можна побудувати узагальнену структурну схему шляхів обфускації, яка зображена на рис. 1.2.

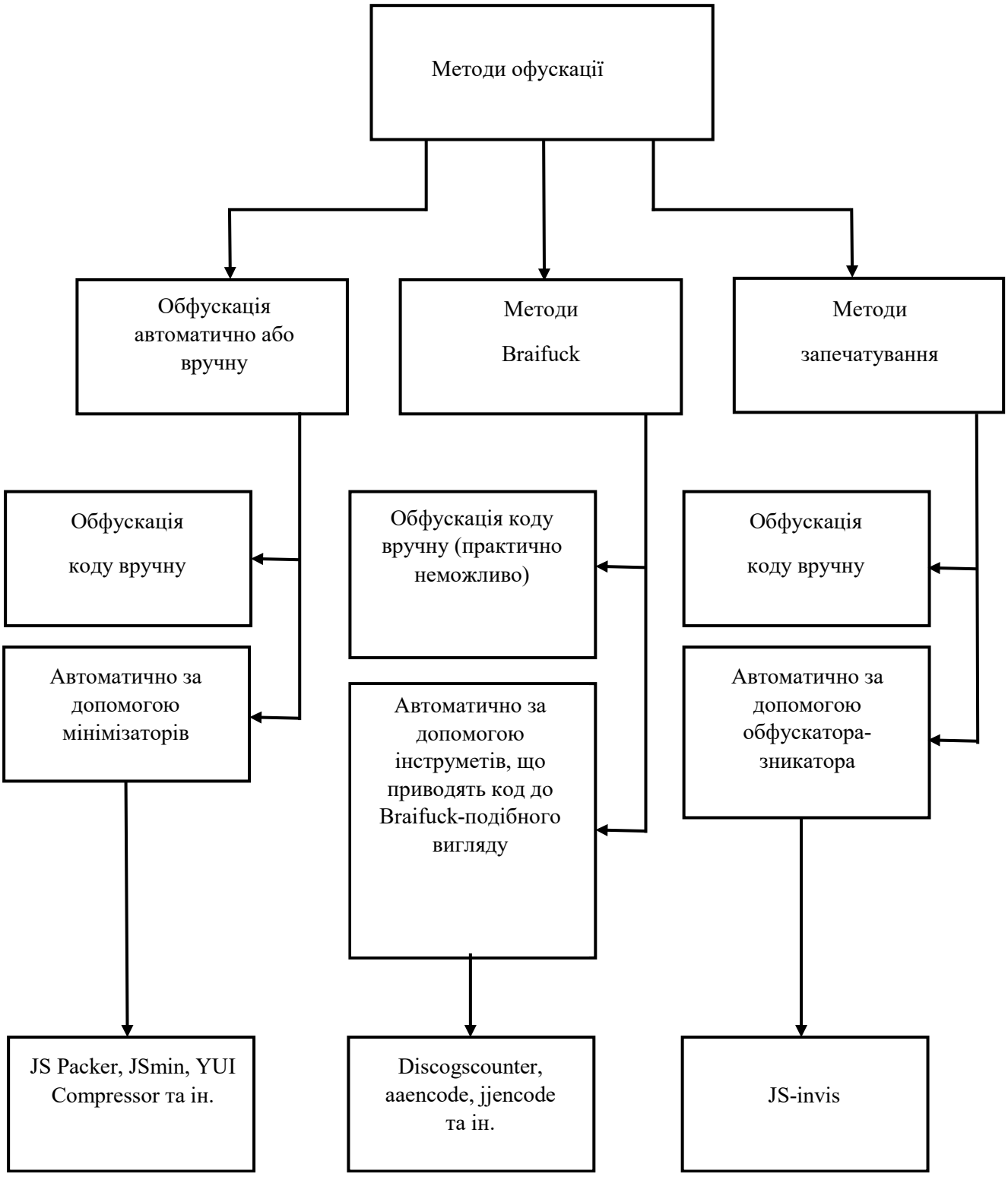

Рисунок 1.2. Узагальнена структурна схема шляхів обфускаціїї

2. РОЗРОБКА МЕТОДІВ ДЕОБФУСКАЦІЇ JAVASCRIPT

Аналіз літературних джерел не виявив завершеного алгоритму деобфускації зашифрованого коду JavaScript. Знайдено тільки характерні приклади деобфускації. Тому на основі ідеї розшифровування скриптів та деяких запропонованих шляхів аналізу обфусцированого коду запропонуємо деякі методи дуобфускації JavaScript.

2.1. Розшифровування JavaScript, який було обфуцировано за допомогою мінімізатора

1) Визначаємо обфусцированый код JavaScript. Якщо ми хочемо дізнатися чи є на певній WEB-сторінці шкідливий код, нам треба її просканувати за допомогою інструментів.net fraimwork та виявити наявність JavaScript скриптів. При обфускації код може прийняти зовсім незрозумілий вигляд і втратити характерні ознаки та це не стане завадою для його коректного виконання на Вашому комп'ютері і як результат захований вірус може нанести чималу шкоду вашому електронному пристрою. Для визначення зашифрованого скрипта будемо використовувати типові приклади та результати роботи обфускаторів мінімізаторів. Маємо певний набір ключових слів та функцій, які вказують на те, що деякий фрагмент або фрагменти сторінки — це обфусцированый JavaScript.

2) Починаємо розбір зашифрованого коду. Завантажуємо підозрілий код у строкову змінну. Спочатку ініціалізуємо перший знайдений зашифрований фрагмент коду WEB-сторінки.

3) Аналізуємо підозрілий скрипт. Оскільки ми визначили, що шифрування відбувалося методом мінімізаторів, то для таких випадків характерним є упорядковування коду. Додаємо символ нового рядка після кожної крапки з комою.

4) Отримуємо імена функцій JavaScript. Для цього окремо скануємо кожний отриманий рядок. Об'явлені змінні в обфуцированому коді передаємо до функції alert(), для того щоб отримати реальні імена функцій JavaScript.

5) Аналізуємо отриманий функціонал на безпечність використання. Результатом попередніх дій стало виявлення функцій, які при певному наборі шляхом аналізу можуть дати відповідь на питання чи зашкодить виконуючий скрипт роботі нашої комп'ютерної системи.

6) Якщо на сторінці виявлено декілька зашифрованих скриптів, то результати першого просканованого коду зберігаємо у вихідний файл та переходимо знову до пункту 2, де розпочинаємо аналізування наступного підозрілого фрагменту.

7) Формування висновку про безпечність посилання. Тільки після того, як будуть розшифровані всі підозрілі скрипти ми зможемо зробити висновок, наскільки є надійним певне посилання.

Для даного методу деобфускації розроблено наступний алгоритм, який зображено на рис. 2.1.

2.2. Розшифровування JavaScript, який було обфуцировано за допомогою BraiFuck-подібного методу

1) Визначаємо обфуцированый код JavaScript. Для того щоб визначити прихований JavaScript код BraiFuck-подібного вигляду треба використовувати xml-файл, який матиме в собі підбірку типових Braifuck-подібних скриптів та окремих символів.

2) Розпочинаємо розбір зашифрованого коду. Завантажуємо підозрілий фрагмент у строкову змінну.

3) Розшифровуємо код. Запускаємо цикл FOR по всій довжині вмісту змінної.

4) За одну ітерацію оброблятимемо один символ.

5) Дістаємо значення зашифрованого тексту-коду. Як усім відомо, повернути значення певного Braifuck-подібного зашифрованого скрипта просто, слід лише використати правильний деобфускатор, але для цього треба виконати дуже глибокий аналіз. Тому пропонуємо вміст скрипту отримати універсальним способом. Визначаємо ASCII-код символа:

- Якщо код має значення між 36 і 61 (не включно), то додаємо до нього 25, а символ, відповідаючий результуючому коду, зберігаємо в нову змінну.
- Якщо код має значення між 61 і 86 (не включно), то віднімаємо від нього 25, а символ, відповідаючий результучому коду, зберігаємо у ту ж таки нову змінну.

6) Декодуємо. Після того, як ми перейшли від Braifuck-подібного вигляду до більш зрозумілого нашій системі розпізнавання вірусів виду, отримане треба декодувати. Для цього нам треба реалізувати виклик функції eval() для запуску результату декодування.

7) Аналізуємо функціонал на безпечність використання. Можемо мати один із двох результатів:

- Якщо результатом деобфускації є код, в якому ми можемо проаналізувати функціонал, тобто ключеві слова, які визивають деякі функції, то переходимо до оцінки безпечності такого коду.
- Якщо результатом деобфускації є код, в якому проаналізувати функціонал не вдається, то треба перейти до попереднього методу деобфускації JavaScript, який було розглянуто в 2.1. Такий підхід демонструє, що обфускація була проведена у декілька кроків, де спочатку скористалися методом мінімізації, а потім методом приведення коду до Braifuck-подібного вигляду.

Для даного методу деобфускації розроблено наступний алгоритм, який зображено на рис. 2.2.

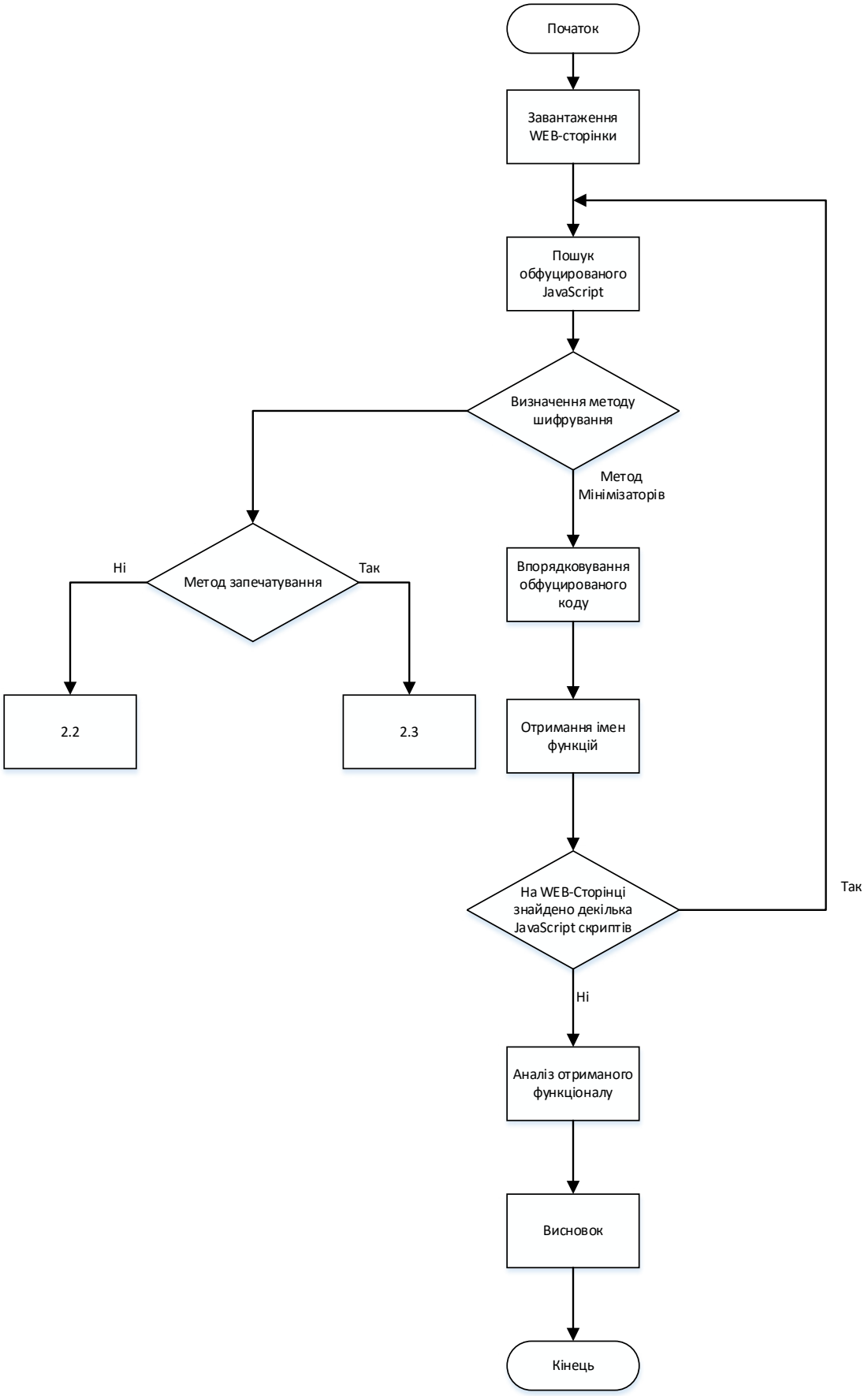

Рисунок 2.1. Алгоритм деобфускаціїї зашифрованих скриптів мінімізаторами

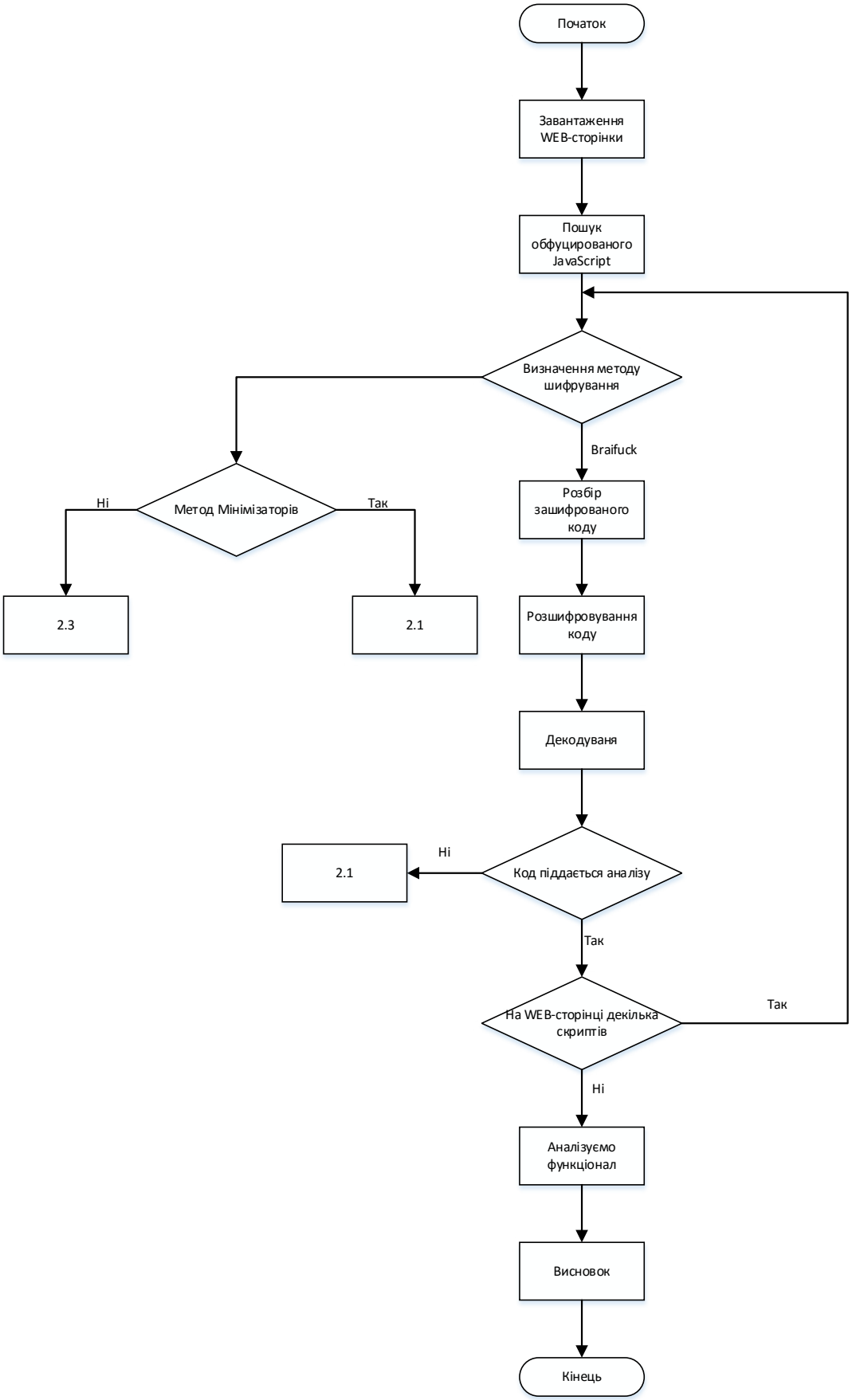

Рисунок 2.2. Алгоритм деобфускаціїї зашифрованих скриптів Braifuck-подібного виду

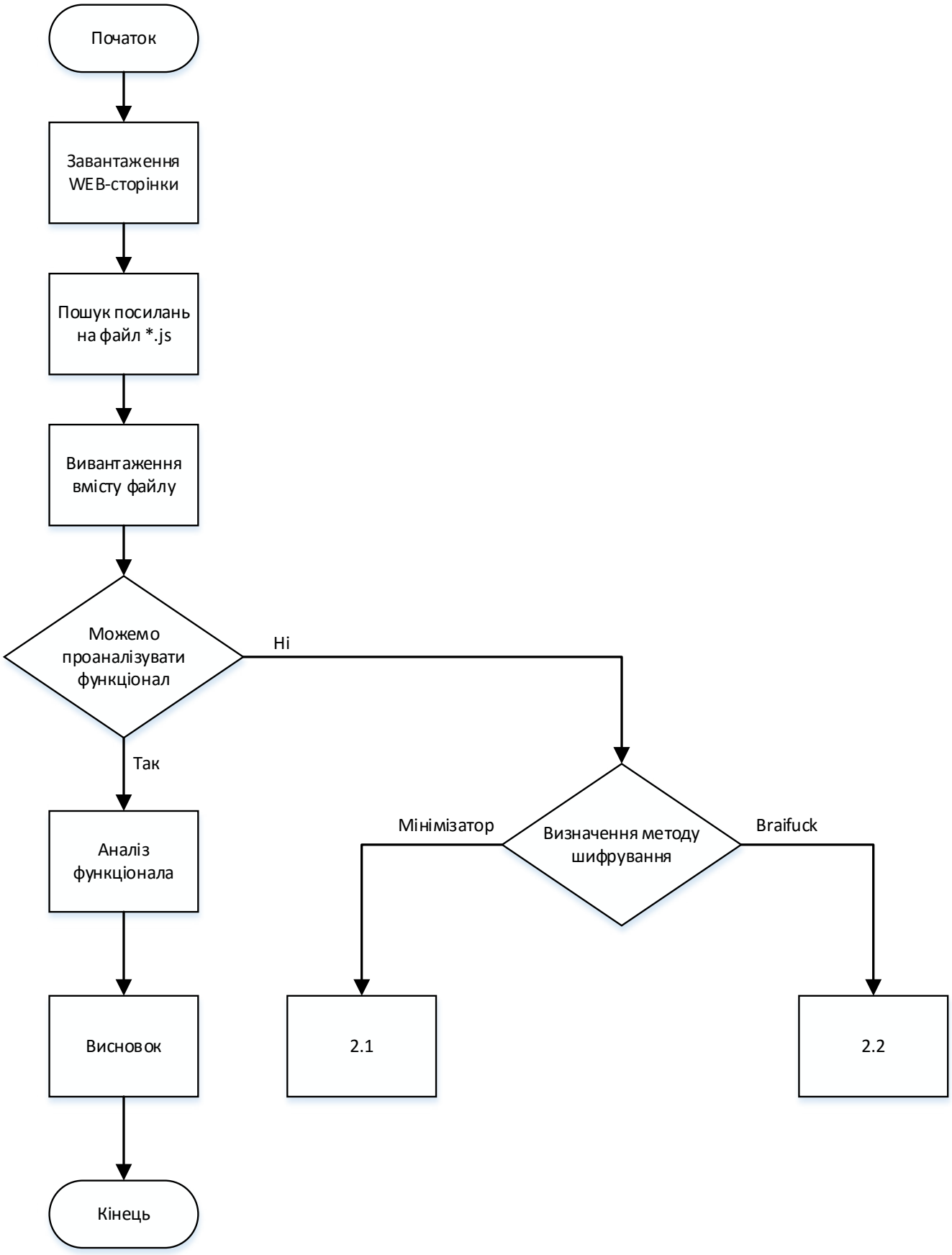

Рисунок 2.3. Алгоритм деобфускаціїї зашифрованих скриптів методом запечатування

2.3. Розшифровування JavaScript, який було обфусцировано за допомогою методу запечатування

1) Визначаємо посилання на файл JavaScript. Для цього скануємо сторінку і шукаємо посилання на файли із розширенням *.js.

2) Розпочинаємо розшифрування коду. Копіюємо вміст файлу в змінну. Після чого розпочинається процес сканування отриманого коду.

3) Визначаємо чи можемо ми проаналізувати функціонал, який зберігається у файлі чи потрібно провести процес деобфускації.

4) Визначаємо метод обфускації або напряму проводимо аналіз функціоналу. Якщо неможливо провести оцінку надійності коду — значить він прихований, а тому можливо й небезпечний. Для цього треба використати методи розпізнавання обфусцированих скриптів із попередніх пунктів. У файлі може зберігатися обфусцированый код методом мінімізації або методом, який приводить до Braifuck-подібного вигляду. Тому визначемо який саме метод використовується та перейдемо до розшифровування використовуючи методику запропоновану у пунктах 2.1 та 2.2.

5) Якщо на WEB-сторінці більше одного посилання на файл, то вони вистроюються в чергу і починаючи з пункту 2 проходять процес деобфускації.

Для даного методу деобфускації розроблено наступний алгоритм, який зображено на рис. 2.3.

Висновки

Представлені алгоритми та методи деобфускації скриптів рекомендовано використовувати в програмному забезпеченні інтегрованому із браузерами, для того щоб виявляти вірусну активність на WEB-ресурсах в режимі онлайн. Звісно дані алгоритми потребують деякої модифікації для більш результативної роботи при їх впровадженні, але представлена ідея класифікації обфусцированого коду по категоріях є досить новою і надає можливість розробити універсальні підходи до аналізування та розшифровування скриптів.

Література

1. Терейковський І. Нейронні мережі в засобах захисту комп'ютерної інформації / І. Терейковський. — К.: ПоліграфКонсалтинг. — 2007. — 198 с.

2. «Badass JavaScript»: інтернет блог, стаття: «Badass js is back white some badass obfuscation» — посилання: http://badassjs.com/post/2929065287/obfuscation/

3. «Adamcecc»: інтернет блог — посилання: http://adamcecc.blogspot.com/

4. «Ajaxian»: інтернет сайт, стаття «Want to pack JS and CSS really well? Convert it to a PNG and unpack it via Canvas», посилання: http://ajaxian.com/

5. Безруков Н. Н. Компьютерная вирусология / Н. Н. Безруков. — К. Инкомбук, 1990. — 450 с.

6. Біленчук П. Д. Комп'ютерна злочинність / П. Д. Біленчук, Б. В. Романюк. — К.: Атака, 2002. — 240 с.

7. Вилков А. С. Информационная безопасность персональных ЭВМ и мониторинг компьютерных сетей / А. С. Вилков. — М.: МИНИТ ФСБ России, 2005. — 210 с.