УДК 681.3.06

І.А. Терейковський

ОЦІНКА ДОКУМЕНТОВАНИХ МОЖЛИВОСТЕЙ FLASH MACROMEDIA ДЛЯ ЗДІЙСНЕННЯ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ІНФОРМАЦІЇ КЛІЄНТІВ ІНТЕРНЕТУ

Сформована схема потенційних загроз щодо несанкціонованого доступу до інформації клієнта Інтернету за допомогою інструментальних засобів Flash. Розглянуті найбільш імовірні випадки реалізації несанкціонованого доступу. Визначено, що деструктивні можливості інструментальних засобів Flash не обмежуються типовими засобами захисту локальної мережі.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Питання безпеки інформації — важлива частина процесу впровадження нових інформаційних технологій у всі сфери життя суспільства. Широкомасштабне використання обчислювальної техніки та телекомунікаційних систем у рамках територіально розподілених інформаційних систем, перехід на цій основі до безпаперової технології, збільшення обсягів оброблюваної інформації та розширення кола користувачів приводять до якісно нових можливостей несанкціонованого доступу (НСД) до ресурсів і даних інформаційних систем, до їх високої вразливості. Водночас рух інформаційних технологій у бік відкритих розподілених систем, широке використання мережі Інтернет як засобу міжкорпоративного спілкування надають проблемі захисту від НСД особливої актуальності. За оцінками зарубіжних правозахисних органів, річний збиток світової економіки від злочинів, пов'язаних з Інтернетом, становить декілька мільярдів доларів США. Багато цих злочинів спрямовані на одержання НСД до інформації, що зберігалась на комп'ютерах окремих громадян, та до інформаційних систем комерційних і урядових організації [4]. По матеріалах сайту rambler.ru, в 2003 році зафіксовані випадки несанкціонованого проникнення в комп'ютерні мережі університетів США та в особисті комп'ютери клієнтів деяких банків Італії. При цьому метою атаки було отримання НСД до конфіденційної інформації.

Таким чином, важливим аспектом дотримання достатнього рівня безпеки інформаційних комп'ютерних систем, пов'язаних з Інтернетом, є захист інформації від НСД. Реальний захист стає можливим тільки при використанні інтегральної технології безпеки, що практично реалізує методи, засоби і послуги забезпечення безпеки. З огляду на це у даній статті основний акцент зроблений на реалізаційних аспектах проблеми безпеки комп'ютерної інформації. В той же час використання інтегральної технології безпеки передбачає розгляд засобів не тільки захисту, але й нападу.

Цим визначається актуальність загальної проблеми даної статті — дослідження реалізаційних аспектів НСД до комп'ютерних ресурсів клієнтів мережі Інтернет, а також її зв'язок з глобальною науково-практичною задачею забезпечення інформаційної безпеки комп'ютерних мереж.

Аналіз досліджень і публікацій,

в яких започатковано розв'язання даної проблеми

Згідно діючих вітчизняних нормативних документів інформаційна система — це система, що організує пам'ять та маніпулювання інформацією в проблемній області. В ракурсі загальної проблематики статті під терміном інформаційна система будемо розуміти автоматизовану систему, призначену для організації, зберігання, доповнення, підтримки та надання користувачам інформації згідно їх прав та запитів.

Доступ до даних інформаційної системи передбачає надання даних системі обробки даних або одержання їх шляхом виконання операцій пошуку, читання та (або) запису. НСД — це навмисне звернення користувача до даних, доступ до яких йому заборонений, з метою їх прочитання, оновлення або знищення [2]. Захист інформації від НСД — це запобігання або суттєве ускладнення несанкціонованого доступу до програм і даних шляхом використання апаратних, програмних, криптографічних та організаційних методів і засобів захисту. Захист інформаційної системи від НСД, як правило, повинен передбачати виключення можливості вільного доступу з боку несанкціонованого користувача до ресурсів, програмного забезпечення інформаційної системи та інформації на персональних комп'ютерах. Загальнопоширеними є програмні та організаційні методи захисту. Програмні методи захисту — це сукупність алгоритмів та програм, що забезпечують розподіл доступу та виключення несанкціонованого використання інформації. Організаційні методи захисту — це строге регламентування процесу функціонування інформаційної системи.

Аналіз літературних джерел показує, що особливо небезпечними та поширеними є такі методи НСД, як міжсайтовий скриптинг та поштові програми типу "троянський кінь". Як свідчить звіт міжнародної групи IP-спеціалістів Web Application Security Project (матеріали сайту www.fcenter.ru) вони впевнено входять до списку 10 сучасних найбільш критичних проблем вразливості веб-додатків.

У міжсайтовому скриптингу веб-додаток використовується як механізм перенесення атаки на браузер кінцевого користувача. Поштова програма типу "троянський кінь" представляє прикріплений до листа електронної пошти файл, що містить програму, яка дозволяє виконувати дії, що відрізняються від визначених у специфікації. Наприклад, користувач отримує файл з відеороликом, при перегляді якого запускається програма, що здійснює НСД.

Був проведений аналіз технологій створення веб-додатків, що потенційно володіють можливостями міжсайтового скриптингу та дають можливість створення поштових програм типу "троянський кінь". Результати аналізу показали, що загальнопоширеними технологіями, які потенційно дозволяють створити міжсайтовий скриптинг, є Java, ActiveX, VBA, JavaScript, VBScript, Flash Macromedia. Тому на безпеку технологій Java, ActiveX, VBA, JavaScript, VBScript звернена особлива увага. Еталоном безпеки може бути Java, яка передбачає три лінії оборони: надійність мови, контроль при отриманні програми та контроль при її виконанні [1, 4]. Крім того, існує ще один дуже важливий засіб забезпечення інформаційної безпеки — безпрецедентна відкритість Java-системи. Вихідні тексти Java-інтерпретатора доступні для

перевірки. Завдяки цьому існує велика ймовірність того, що помилки та недоліки першими будуть знаходити чесні спеціалісти, а не зловмисники. В той же час безпека технології Flash досліджена не достатньо. Відзначимо, що дана технологія є досить поширеною для створення та перегляду анімованих зображень (фільмів Flash). Показ фільму, реалізований спеціальним програвачем Flash, який може бути встановленим на комп'ютері при типовій інсталяції сучасних версій загальнопоширеного браузера Microsoft Intrnet Explorer. Особливістю Flash є висока якість показу при невеликому обсязі файлу з фільмом, що забезпечується використанням повноцінної об'єктно-орієнтованої скриптової мови програмування ActionScript [3]. Саме можливості ActionScript, на наш погляд, роблять сайт, на якому розміщений фільм Flash, потенційно небезпечним.

Аналіз досліджень, присвячених поштовим програмам типу "троянський кінь", показав, що написати таку програму дозволяють практично всі розповсюджені системи прикладного програмування, в тому числі і ActionScript. Внаслідок простоти та розповсюдженості найчастіше використовують мову VBA.

Існує досить багато програмних засобів захисту від цих програм. Наприклад, антивірус Касперського, який містить спеціальний модуль Office Guard, що контролює виконання макросів VBA. В той же час можливості типових засобів захисту проти НСД за допомогою ActionScript описані не достатньо. Організаційні заходи захисту полягають в знищені (без перегляду) поштовим клієнтом електронних листів з файлами, сигнатура яких свідчить про потенційну небезпеку. Загальноприйнято знищувати файли з розширеннями exe, vbs, com, bat. При цьому файл з розширенням swf (фільм Flash) вважається безпечним.

Невирішені раніше частини загальної проблеми, котрим присвячується стаття

– Шляхи НСД до інформації клієнта Інтернету за допомогою інструментальних засобів Flash визначені не в повному обсязі.

– Можливості типових засобів захисту локальної мережі від НСД вказаного типу досліджені не достатньо.

– Концепція захисту локальної мережі від НСД вказаного типу не сформована.

Постановка завдання

– Визначення шляхів НСД до інформації клієнта Інтернету за допомогою інструментальних засобів Flash.

– Визначення можливостей типових засобів захисту локальної мережі від НСД вказаного типу та формування концепції захисту.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів

Розглянемо документовані інструментальні засоби середовища Flash, що потенційно можуть бути використані для НСД до інформації. В зв'язку з певними обмеженнями середовища Flash доцільно розглянути тільки ті інструментальні засоби, які дозволяють читати, записувати, передавати інформацію, запускати зовнішні програми, керувати апаратним забезпеченням та визначати можливості програмного забезпечення комп'ютера клієнта.

Функції loadVariables() та loadVariablesNum() дозволяють завантажити дані із текстового

файлу в середовище Flash. Важливий момент, який треба мати на увазі при використанні цієї функції, полягає в тому, що дані повинні бути представлені у вигляді пар ім'я/величина. Функція може бути використана Flash не тільки для одержання інформації, але й для її передачі. Робота функції реалізована у фоновому режимі.

Функція getURL() може бути використана для передачі даних у сценарій, що виконується на стороні сервера. Крім того, за допомогою даної функції можна завантажити нову веб-сторінку або відкрити нове вікна браузера. Передачу даних можна здійснювати методами get та post. За допомогою цієї функції можна також викликати функцію, написану мовою програмування JavaScript. Використання функції JavaScript дозволяє більш гнучко передавати дані на сервер та здійснювати операції доступу до файлів. Ще однією важливою особливістю інтеграції даної функції з JavaScript є доступ до cookie-файлів. Причому можна як записувати cookie-файли, так і читати з них інформацію. Таким чином, можна дізнатися, які сайти переглядав користувач.

Функції loadVariables() та getURL() досить схожі між собою в аспекті передачі даних. Однією з основних відмінностей між ними є те, що при передачі даних за допомогою getURL() може з'явитися нове вікно браузера, яке буде сигналом для користувача про несанкціоновані дії фільму Flash.

Функція FSCommand() дозволяє передавати до двох рядків інформації в будь-яку прикладну програму, де виконується фільм Flash. У будь-якому веб-браузері реалізація даної функції може бути використана для виклику функцій, що існують у конкретному документі HTML і написані мовами JavaScript та VBScript. Організація такого виклику багато в чому аналогічна виклику з використанням функції getURL(). Особливістю функції FSCommand() при її реалізації в автономному програвачеві Flash є можливість запуску зовнішніх прикладних програм. Для цього необхідно використати опцію exec та вказати абсолютний або відносний шлях до запускаючого файлу прикладної програми.

Крім функцій для завантаження та відправки даних можна використовувати декілька об'єктів Flash, Sound, LoadVars, MovieClip, XML та XMLSocket.

Об'єкт Sound дозволяє завантажувати із сервера на комп'ютер клієнта звукові файли в форматі MP3. З точки зору НСД даний об'єкт не містить загроз для безпеки комп'ютера клієнта.

Об'єкти LoadVars та MovieClip дозволяють завантажувати у фільм Flash дані із зовнішніх файлів. Реалізація відповідних методів цих об'єктів принципово не відрізняється від функції loadVariables(). Крім того, об'єкт LoadVars аналогічно функції loadVariables() дозволяє відправляти дані на сервер по протоколу HTTP.

Об'єкт XML використовується для завантаження та відправки даних у форматі XML згідно протоколу HTTP. Для завантаження даних використовується метод load(), для передачі — метод send(). Крім того, метод sendAndLoad() передає на сервер документ XML та завантажує відповідь сервера в об'єкт XML.

Об'єкт XMLSocket використовується для завантаження та відправки даних в форматі XML з використанням прямого гніздового з'єднання зі спеціальною частиною програмного забезпечення серверу. Він служить для двостороннього обміну інформацією в реальному масштабі часу. Спочат-

ку методом connect() встановлюється з'єднання. Після цього передача/прийом даних здійснюються методами send() та onXML(). Завершення сеансу зв'язку здійснюється методом close().

Можливості фільму Flash по керуванню апаратним забезпеченням комп'ютера клієнта полягають в керуванні показу інформації на екрані, програванні звукових файлів, регулюванні гучності звуку, балансу лівого та правого звукових каналів і друкуванні зображення із фільму. Документовані можливості об'єктів для керування апаратним забезпеченням та визначення можливостей комп'ютерної системи, на наш погляд, не дають можливостей для НСД до інформації клієнта.

Описані можливості об'єктів та функцій Flash, що потенційно несуть загрозу НСД до інформації клієнта Інтернету, представлені на рис. 1.

Таким чином, документовані можливості інструментальних засобів Flash дозволяють несанкціоновано читати дані з комп'ютера, передавати їх в мережу та записувати дані. Крім того, фільм Flash може запускати зовнішні програми та має доступ до функцій, написаних мовами JavaScript та VBScript.

Для оцінки рівня небезпеки потенційних загроз було проведено комп'ютерне моделювання за допомогою спеціально розроблених фільмів Flash та серверного програмного забезпечення. Універсальність результатів моделювання забезпечувалась використанням як серверу Apache, так і IIS 5.0. Сервери функціонували на платформі Windows 2000 Server. Програмне забезпечення сервера Apache для прийому даних розроблено мовою PHP, для сервера IIS 5.0 — за технологією ASP з використанням мови Visual Basic. Відправним пунктом моделювання стало припущення про те, що на клієнтський комп'ютер фільм Flash може потрапити або при перегляді вебсайту, або у вигляді файлу, прикріпленого до листа електронної пошти. Відзначимо, що прикріплені до електронного листа файли фільмів Flash (*.swf) вважаються безпечними і, як правило, відкриваються користувачами.

В першому випадку програвач фільму Flash виконується в середовищі браузера. При цьому до фільму застосовується політика безпеки браузера до відповідної зони Інтернету. В другому випадку фільм Flash завантажується на комп'ютер клієнта, а програвач Flash виконується як самостійний програмний додаток.

Перегляд фільму Flash, розміщеного на веб-сайті за допомогою браузера Microsoft Internet Explorer, при застосуванні типової для зони Інтернету політики безпеки показав, що жоден із документованих інструментальних засобів не зміг ні прочитати, ні записати дані на локальний комп'ютер. Також у цьому випадку фільм Flash не зміг запустити зовнішні програми.

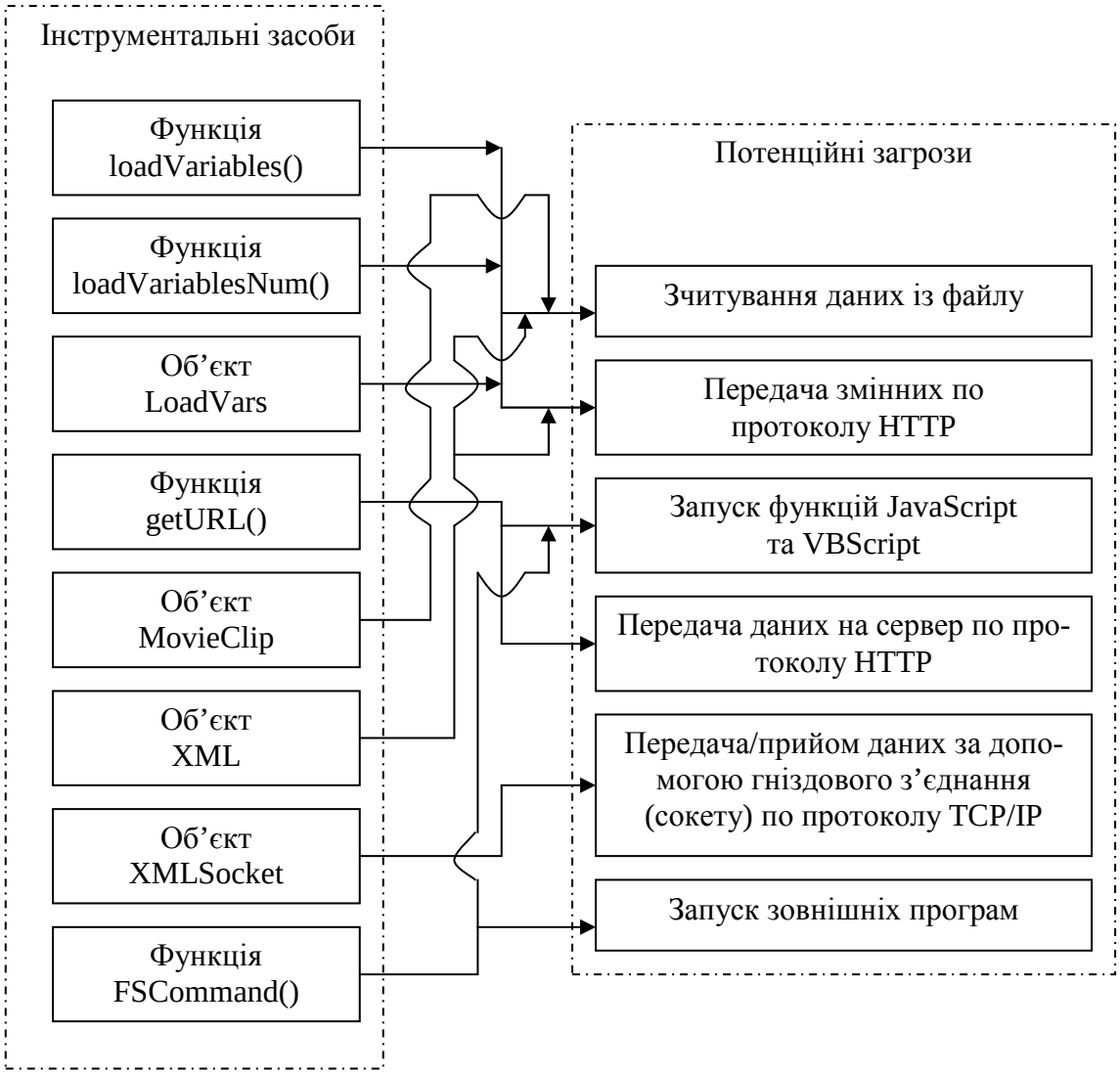

Рис. 1. Схема потенційних загроз об'єктів та функцій

У той же час були реалізовані можливості Flash по виконанню функцій JavaScript, передачі даних на сервер по протоколу HTTP та за допомогою сокетів. Внаслідок застосування типової політики безпеки деструктивні можливості функцій JavaScript мінімальні. Отже, єдиним напрямом НСД може бути аналіз cookie-файлів. Результати аналізу можуть бути передані віддаленому зловмиснику. При цьому інформативність такого аналізу досить низька. Таким чином, перегляд за допомогою браузера Microsoft Internet Explorer з типовою політикою безпеки, розміщеного на веб-сайті фільму Flash, практично не містить загрози НСД. Відзначимо, що зменшення рівня безпеки може призвести до серйозних наслідків. При цьому функції JavaScript дозволяють запускати небезпечні компоненти ActiveX, які дають змогу зловмиснику одержати НСД до інформації клієнта. Зменшення рівня безпеки можливе при збереженні та наступному перегляді вебсайту з фільмом Flash. У цьому випадку браузер застосовує до сайту менш жорстку політику безпеки, яка додатково дозволяє читати та записувати інформацію на локальний комп'ютер. Перегляд фільму Flash, надісланого електронною поштою, показав, що всі документовані можливості інструментальних засобів по зчитуван-

ню, передачі інформації та запуску зовнішніх програм були реалізовані в повному обсязі. Розглянуто вплив на вказані можливості інструментальних засобів деяких засобів захисту локальної мережі. Засоби захисту включали в себе загальнопоширені антивірусні програми та мережні екрани.

Загальнопоширена антивірусна програма AVP (антивірус Касперського) на потенційно загрозливі можливості фільму Flash не вплинула. Використання мережевого екрану не дозволило фільму Flash встановити гніздове з'єднання з сервером. Проте зчитані з локального комп'ютера дані були передані на сервер по протоколу HTTP. При цьому використання функції getURL() призвело до відкриття вікна браузера. Ця обставина може бути діагностичним сигналом про спробу НСД. У той же час використання функцій loadVariables(), loadVariablesNum() та об'єкта LoadVars відбувалось непомітно для користувача і дозволило зчитувати інформацію з файлів локального комп'ютера та передавати її на сервер. Відзначимо, що використання зловмисником функції loadVariables() найбільш ймовірно з причини її підтримки практично всіма поширеними версіями програвача Flash.

Суттєвою проблемою цілеспрямованого не санкціонованого зчитування та зміни інформації є необхідність визначення зловмисником хоча б приблизної назви файлу. Ця обставина змушує зловмисника розробити програму пошуку інформації. При загальнопоширених обмеженнях на обсяг електронного листа це може досить відчутно вплинути на ефективність атаки. Тому зловмисник може частково перенести аналіз одержаної інформації на сервер.

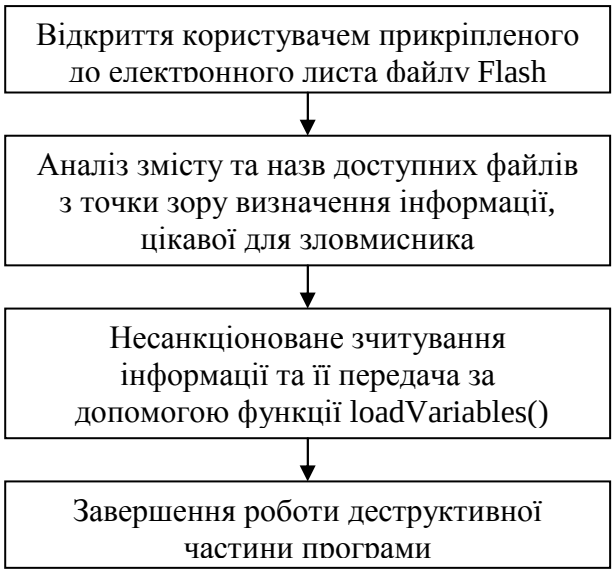

Рис. 2. Функціональна схема поштової програми Flash типу "троянський кінь"

У цьому випадку обсяг листа зменшиться, але збільшиться трафік по протоколу HTTP між фільмом Flash та сервером, на який зловмисник буде передавати інформацію. Це може бути діагностичним сигналом про спробу НСД. Таким чином, найбільш небезпечним та ймовірним засобом НСД до інформації клієнта Інтернету за допомогою Flash є поштова програма типу "троянський кінь", функціональна схема якої показана на рис. 2.

Проведена оцінка можливостей НСД з використанням технології Flash дозволяє сформувати відповідну концепцію захисту, схема якої показана на рис. 3.

Концепцією передбачено ряд програмних та організаційних заходів по діагностиці та забороні НСД. Реалізація організаційних заходів практично знищує небезпеку НСД, хоча значно ускладнює роботу користувачів; реалізація програмних заходів зручніша для користувача, але потребує використання мережевих екранів та розробки нового програмного забезпечення.

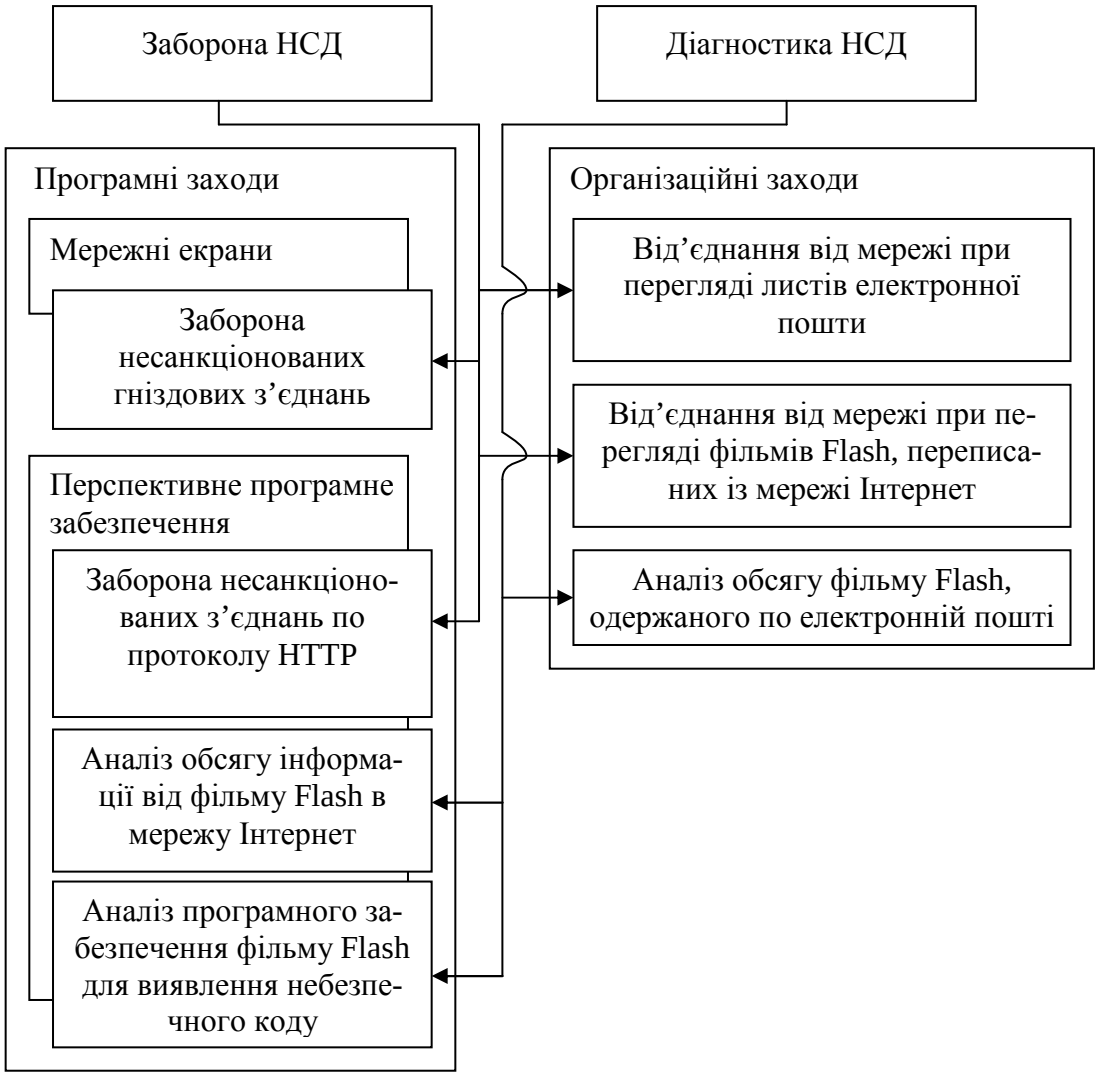

Рис. 3. Схема концепції захисту від НСД

Визначена схема (див. рис. 1) потенційних загроз щодо НСД до інформації клієнта Інтернету за допомогою інструментальних засобів Flash.

Доведено, що використання в клієнтській частині веб-додатку фільму Flash не містить загрози НСД при типовій для зони Інтернету політиці безпеки.

Доведено, що найбільш ймовірним та небезпечним засобом НСД є прикріплений до електронного листа файл з програмою типу "троянський кінь". Побудована функціональна схема такої програми (див. рис. 2). Визначено, що деструктивні можливості цієї програми не обмежуються типовими засобами захисту локальної мережі.

Висновок

Сформована концепція захисту від атак даного типу.

Перспективи подальших розвідок у даному напрямі полягають у дослідженні шляхів НСД до інформації клієнтів Інтернету за допомогою інструментальних засобів інших загальнопоширених технологій. До таких технологій слід віднести Java, ActiveX, JavaScript, VBScript. Результатом досліджень може стати універсальна система захисту клієнтів мережі Інтернету від спроб НСД. Крім того, цікавим напря-

мом є дослідження недокументованих можливостей Flash.

1. *Гарнаев А., Гарнаев С.* Web-программирование на Java и JavaScript. — СПб: БХВ-Петербург, 2002. — 1040 с.
2. *ДСТУ 3396.2-97.* Захист інформації. Технічний захист інформації. Терміни і визначення. — К.: Держстандарт України. — 1998. — 12 с.
3. *Китинг Д.* Flash MX. Искусство создания web-сайтов. — К.:ТИД ДС, 2002. — 848 с.
4. *Рейнольдс М.* Электронная коммерция. — М.: Лори, 2002. — 538 с.
5. *Таненбаум Э.* Компьютерные сети. — СПб.: Питер, 2002. — 848 с.

Отримано ***09.06.04***

Терейковський Ігор Анатолійович
канд. техн. наук

Місце роботи автора:
Київський національний торгівельно-економічний університет, кафедра інформаційних технологій та систем

Київ, вул. Кіото 19, к 526.

Тел.: (8-067) 909 5867, 531 4869.
E-mail: terejkowski@rambler.ru