УДК 004.891

к.т.н., доц. **Чорненький В.І.** (ХмНУ)
д.т.н., с.н.с. **Сєлюков О.В.** (ТОВ «Укрспецконсалтинг»)
к.військ.н., доц. **Осипа В.О.** (ВІКНУ)
Глінський О.В. (ХмНУ)
Щерба В.І. (ХмНУ)

ВДОСКОНАЛЕННЯ МЕТОДУ ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМП'ЮТЕРНИХ МЕРЕЖ НА ОСНОВІ ФОРМУВАННЯ ПРАВИЛ ПОЛІТИКИ БЕЗПЕКИ

У статті розглянуто підхід, який об'єднує множину моделей і методику, для реалізації детального аналізу захищеності комп'ютерних мереж на етапах експлуатації і проектування, який базується на імітації дій порушника, побудові і аналізу графу загроз. Розроблені моделі комп'ютерних атак, порушника, аналізованої мережі. На відміну від існуючих моделей представлена модель комп'ютерних атак має наступні особливості: має вигляд ієрархічної структури, що дозволило для формування сценарного рівня використати експертні знання, а для рівня атакуючих дій – зовнішні бази даних вразливостей; забезпечує генерацію сценаріїв атак з урахуванням різноманітності цілей і рівня знань порушника. Представлена в роботі модель аналізованої мережі дозволяє не лише описати її конфігурацію, але і політику безпеки, що реалізовується в ній. Ця модель утримує також компоненти розпізнавання дій порушника і реакції мережі на них. Використання представлення послідовності виконання порушником атакуючих дій у вигляді графу і розробленого у рамках дисертаційного дослідження алгоритму його формування дозволило розробити модель оцінки рівня захищеності. Модель оцінки рівня захищеності комп'ютерних мереж охоплює множину різних показників захищеності і правил (формул), використовуваних для їх розрахунку. Особливість цієї моделі полягає в об'єднанні підходу Common Vulnerability Scoring System (для розрахунку рівня критичності атакуючої дії) і

модифікованої методики аналізу ризиків Facilitated Risk Analysis and Assessment Process, що забезпечило можливість розрахунку інтегрального показника «Рівень захищеності мережі». Розроблена методика аналізу захищеності комп'ютерних мереж на етапах проектування і експлуатації дозволяє істотно скоротити час на аналіз захищеності комп'ютерних мереж. При цьому використання запропонованої методики дозволить адміністраторові (чи проектувальникові) мережі проводити аналіз захищеності, визначати уразливості у використовуваному програмному і апаратному забезпеченні, виявляти «вузькі» місця в захищеності мережі, варіюючи різні параметри, що характеризують порушника. Ефективність застосування методики аналізу захищеності комп'ютерних мереж на етапах проектування і експлуатації визначається як властивість забезпечувати вироблення своєчасної і обґрунтованої інформації про захищеність комп'ютерної мережі. Критерієм ефективності є виконання вимог за показниками основних властивостей ефективності (своєчасності, обґрунтованості, ресурсоспоживання).

Ключові слова: комп'ютерns мережі, інформаційна безепека, правила політики безпеки.

Вступ. Захищеність комп'ютерної мережі визначається як ступінь адекватності реалізованих в ній механізмів захисту інформації існуючим в даному середовищі функціонування ризиків, пов'язаних із здійсненням загроз безпеки інформації, тобто здатність механізмів захисту забезпечити конфіденційність, цілісність і доступність інформації. Захищеність може надавати і часто надає вирішальний вплив на показники ефективності функціонування комп'ютерних мереж. Під загрозою розуміється сукупність умов і факторів, що визначають потенційну або реально існуючу небезпеку виникнення інциденту, який може привести до нанесення збитку функціонуванню комп'ютерної мережі [1].

Незалежно від конкретних видів загроз потрібно забезпечити такі основні властивості: цілісність, конфіденційність і доступність. Конфіденційність інформації – це стан інформації, при якому доступ до неї здійснюють тільки суб'єкти, що мають на нього право. Цілісність інформації – це стан інформації, при якому її зміна здійснюється тільки навмисно суб'єктами, що мають на нього право. Доступність інформації – це стан інформації, при якому суб'єкти, які мають право доступу, можуть реалізувати його безперешкодно [2]. На момент проведення дослідження завдання захисту переданої по vtht;s інформації від загроз цілісності і конфіденційності успішно вирішується застосуванням засобів криптографічного захисту інформації. В даному дослідженні під загрозами доступності інформації розуміються загрози інформаційної безпеки (ІБ), спрямовані на порушення доступності інформації.

Ситуація в даній області дослідження ускладнюється тим, що не дивлячись на велику кількість публікацій, в теперішньому часі не існує в достатній степені апробованих методик аналізу захищеності комп'ютерних мереж, виконання яких можливе на етапах проектування і експлуатації.

Завдання аналізу захищеності комп'ютерних мереж на різних етапах їх життєвого циклу, основними з яких є етапи проектування і експлуатації, все частіше стає об'єктом обговорення на спеціалізованих конференціях, присвячених забезпеченню інформаційної безпеки [3]. Така пильна увага до даної задачі пояснюється тим, що аналіз захищеності необхідний при контролі та моніторингу захищеності комп'ютерних мереж, при атестації автоматизованих систем (комп'ютерних мереж) та сертифікації засобів обчислювальної техніки за вимогами діючих нормативних документів і вимагає обробки великого обсягу даних в умовах дефіциту часу.

Постановка задачі. Система автоматизованого захисту (САЗ) повинна проводити аналіз захищеності комп'ютерних мереж на етапі проектування і експлуатації. Для задоволення цієї вимоги передбачається використати підхід, при якому аналізується модель комп'ютерної мережі. Ця модель будується на базі специфікацій, що описують конфігурацію мережі і політикою безпеки, що реалізовується в ній [4]. Специфікації описуються на спеціалізованих мовах, які базуються на XML [5]. На етапі проектування комп'ютерної мережі специфікації формуються проектувальником, на етапі експлуатації – в автоматичному режимі за допомогою програмних агентів, що функціонують на хостах.

Під час роботи САЗ повинна формувати сценарії комп'ютерних атак, враховувати модель порушника, проводити розрахунок множини показників, що характеризують захищеність комп'ютерної мережі в цілому і її окремих компонентів, враховувати топологію аналізованої мережі, склад програмного і апаратного забезпечення, політику безпеки, що реалізовується. Результатами роботи САЗ являються множина виявлених вразливостей, графи атак, «вузькі» місця в захищеності комп'ютерної мережі (найбільш критичні компоненти комп'ютерної мережі, вірогідність атаки яких найвища), множина показників захищеності, рекомендації по підвищенню рівня захищеності аналізованої мережі [6]. Отримані результати гарантують вироблення обґрунтованих рекомендацій по усуненню виявлених «вузьких» місць і посиленню захищеності комп'ютерної мережі в цілому.

На змістовному рівні наукове завдання даного дослідження можна сформулювати таким чином: розробити методику аналізу захищеності комп'ютерних мереж на етапах проектування і експлуатації, що базується на побудові графу загроз і розрахунку множини показників, що характеризують рівень захищеності комп'ютерної мережі в цілому і окремих її компонентів [7]. Реалізація цієї методики системами аналізу захищеності повинна дозволяти не лише оцінювати рівень захищеності мережі, але і досягати його необхідного значення шляхом зміни конфігурації аналізованої мережі і політики безпеки, що реалізовується в ній.

Для реалізації аналізу захищеності комп'ютерних мереж на етапах проектування і експлуатації необхідно розробити моделі комп'ютерних атак і порушника, аналізованої комп'ютерної мережі, побудови графу загноз і оцінки рівня захищеності.

Основна частина. Модель аналізованої комп'ютерної мережі дозволяє представити топологію мережі, використовуване програмне і апаратне забезпечення, реакцію мережі на виконувані порушником атакуючі дії.

Запропонована в статті роботі модель аналізованої комп'ютерної мережі базується на основних принципах, описаних в роботах [8, 9], присвячених створенню підходу для представлення конфігурації комп'ютерної мережі (топології, використовуваного ПЗ і АЗ). Проте, для завдання аналізу захищеності, окрім компонента, що описує конфігурацію мережі, модель комп'ютерної мережі повинна містити компонент, що дозволяє задавати реакцію мережі на атакуючі дії.

Отже, модель порушника можна представити таким чином:

$$M_{П} = \langle K_H, K_У, p_M \rangle,$$

де K_H – первинні знання про аналізовану комп'ютерну мережу; $K_У$ – знання і уміння порушника; $p_M \in K_H$ – первинне положення порушника в комп'ютерній мережі.

Первинні знання порушника про комп'ютерну мережу що атакується $K_H \subset D$ – описуються з використанням моделі аналізованої мережі. K_H містить як мінімум один хост, з якого порушник розпочинає реалізацію атакуючих дій. У загальному випадку цей параметр дозволяє імітувати дії більш обізнаних порушників(наприклад, внутрішніх, які володіють такою інформацією, як, наприклад, топологія мережі або використовувані на хостах сервіси і їх версії).

Знання і уміння порушника задаються у вигляді множини відомих йому операційних систем і сервісів: $K_У = \langle OS_{ПОР}, NS_{ПОР} \rangle$, де $OS_{ПОР} = \{os_i\}_{i=1}^{N_Y^{OS}}$, $os_i \in OS$, NS_Y^{OS} – число відомих порушникові ОС; $NS_{ПОР} = \{ns_i\}_{i=1}^{N_Y^{NS}}$, $ns_i \in NS$, NS_Y^{NS} – число відомих порушникові сервісів; OS – множина OC і NS – множина мережевих сервісів, сформульована по БД вразливостей.

Позначимо $T = \{t_i\}_{i=1}^{N}$ множина цілей реалізації, що атакують дії, формоване з використанням концептуальної моделі атак, де t_1 – «Розвідка», t_2 – «Впровадження»,… (етапи сценарію і підцілі реалізації цих етапів, наприклад, t_k – «Сканування портів» як підціль «Розвідки»).

$$M_{KA}^{РП} = \left\langle M_{П}, T^{РП}, O, P^{РП}, F^{РП} \right\rangle,$$

де $M_{П}$ – модель порушника; $T^{РП} = \{t_i^{РП}\}_{i=1}^{K_{РП}} \subset T$ – множина цілей реалізації атакуючих дій, $K_{РП} \le \|T\|$ – число цілей; $O = \{o_i\}_{i=1}^{K_o} \subset D$ – множина аналізованих (атакуючих) об'єктів, $K_O \le \|D\|$ – число аналізованих об'єктів; $P^{РП} = \{p_{PM}, p_{EK}\}$ – множина параметрів процесу аналізу захищеності, де p_{PM} – рівень моделювання ($p_{PM} \in P_{PM} = \{p_{PM}^1, p_{PM}^2\}$: p_{PM}^1 = «Високий» – моделювання робиться на рівні ідентифікаторів атакуючих дій, p_{PM}^2 = «Низький» – моделювання робиться на рівні представлення мережевих пакетів і команд ОС); $p_{EK} \in \{true, false\}$ – параметр, що встановлює режим використання експлойтів (при $p_{EK} = true$ замість імітації атакуючих дій використовуються експлойти – цей режим може бути використаний в дослідницьких цілях для підтвердження працездатності експлойта в реальних умовах експлуатації комп'ютерної мережі); $F^{РП}$ – множина функцій даного компонента.

Компонент розпізнавання дій порушника використовується для перетворення представлення атакуючих дій у вигляді послідовності мережевих пакетів або команд ОС в ідентифікатори атак(наприклад, «Delete_File»). В основу функціонування цього компонента покладений сигнатурний метод, що поступає на вхід моделі комп'ютерної мережі послідовність мережевих пакетів або команд ОС порівнюється із заздалегідь визначеними сигнатурами і у разі виявлення схожості визначається ідентифікатор атаки.

Визначимо основну функцію компонента, що описує рівень параметризації процесу А3 і обліку характеристик порушника моделі комп'ютерних атак: $genZ : O \to O \cdot T^{РП}$ – функція формує множину цілей даного рівня. Кожна така ціль представляє собою пару (об'єкт, мета атаки):

$$genZ(O) = Z = \{z_i\}_{i=1}^{K_{РП}} = \{(o, t_i)\}_{i=1}^{K_{РП}},$$

де $o \in O$, $t_i \in T^{РП}$.

Вхідними даними для алгоритму формування графу загроз є: (1) конфігурація аналізованої мережі, що описує топологію, склад ПЗ і АЗ; (2) множина атакуючих дій; (3) множина параметрів, що характеризують порушника. Результатом роботи алгоритму є дерево атак [10].

Для розробки алгоритму формування графу загроз уточнимо перший етап типового сценарію вторгнення, розділивши його на два: (1-1) визначення функціонуючих хостів; (1-2) реалізація сценаріїв (множина дій) розвідки для кожного хоста, виявленого на першому етапі. Другий і третій етапи уточнимо таким чином: (2) другий етап полягає в реалізації атакуючих дій, що використовують уразливості програмного і апаратного забезпечення і загальних дій користувача; (3) третій етап включає реалізацію дій з переміщення порушника на успішно атакований хост. На базі цих етапів будується алгоритм формування графу загроз (рис. 1).

Розвідувальними діями, на основі яких формується множина сценаріїв розвідки, є наступні дії: (1) nmap OS – виконання цієї дії дозволяє порушникові упізнати тип і (можливо) точну версію операційної системи; (2) nmap services – виконання цієї дії дозволяє порушникові отримати список відкритих на хості портів; (3) banners – виконання цієї дії дозволяє порушникові дістати назви і версії мережевих сервісів, що функціонують на хості, шляхом аналізу банерів. При виконанні сценаріїв атак порушник може реалізувати різну комбінацію перелічених вище розвідувальних дій.

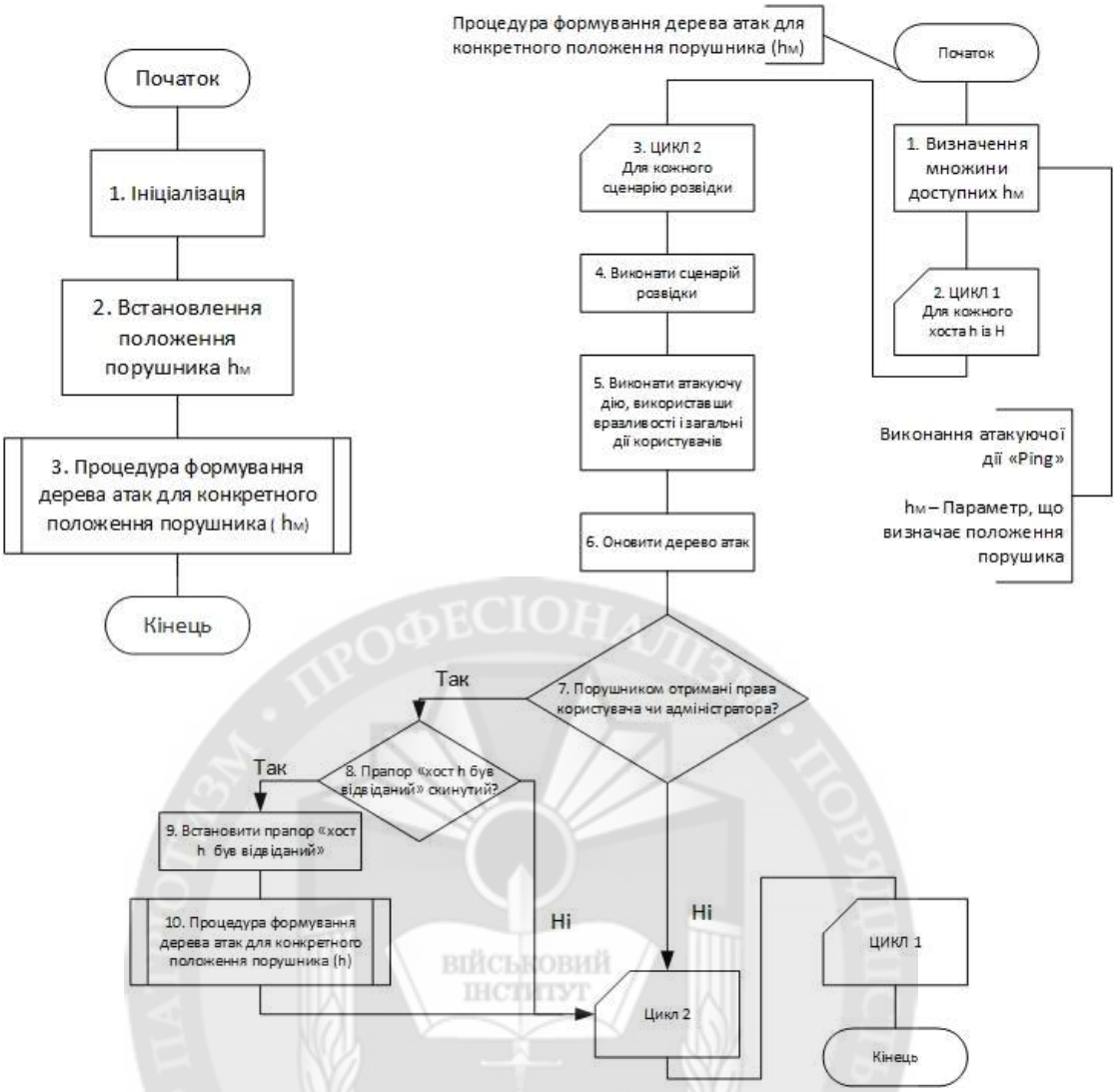

Рис. 1. Алгоритм формування графу загроз

Під виконанням атакуючої дії розуміється оновлення конфігурації аналізованої мережі згідно з метою, що досягається цією дією, і заданим об'єктом, що атакується. Наприклад, метою дії *pipeupadmin* є отримання порушником привілеїв адміністратора на хості, що атакується, за наявності привілеїв локального користувача. При виконанні цієї дії на хості *Host* станеться наступна зміна конфігурації мережі: привілеї порушника на хості *Host* змінюється з «локальний користувач» на «адміністратор».

Після реалізації кожного сценарію з множини сценаріїв розвідки робиться перевірка умов виконання атакуючих дій, що використовують уразливості програмного і апаратного забезпечення і загальних дій користувача. Якщо поточна конфігурація аналізованої мережі задовольняє цим умовам, то атакуючі дії виконуються. Якщо поточна дія в сценарії атаки належить до класів дій, що призводять до отримання порушником прав локального користувача або адміністратора на хості, що атакується, порушник може «перейти» (змінити своє положення в мережі) на цей хост. Якщо перехід на інший хост здійснюється, вищеописана послідовність дій повторюється для нового положення порушника.

Пропонована методика аналізу захищеності ґрунтується на обліку програмно-технічної складової аналізу захищеності і не використовує активні засоби тестування (передбачається використання імітації дій порушника, спрямованих на модель аналізованої мережі).

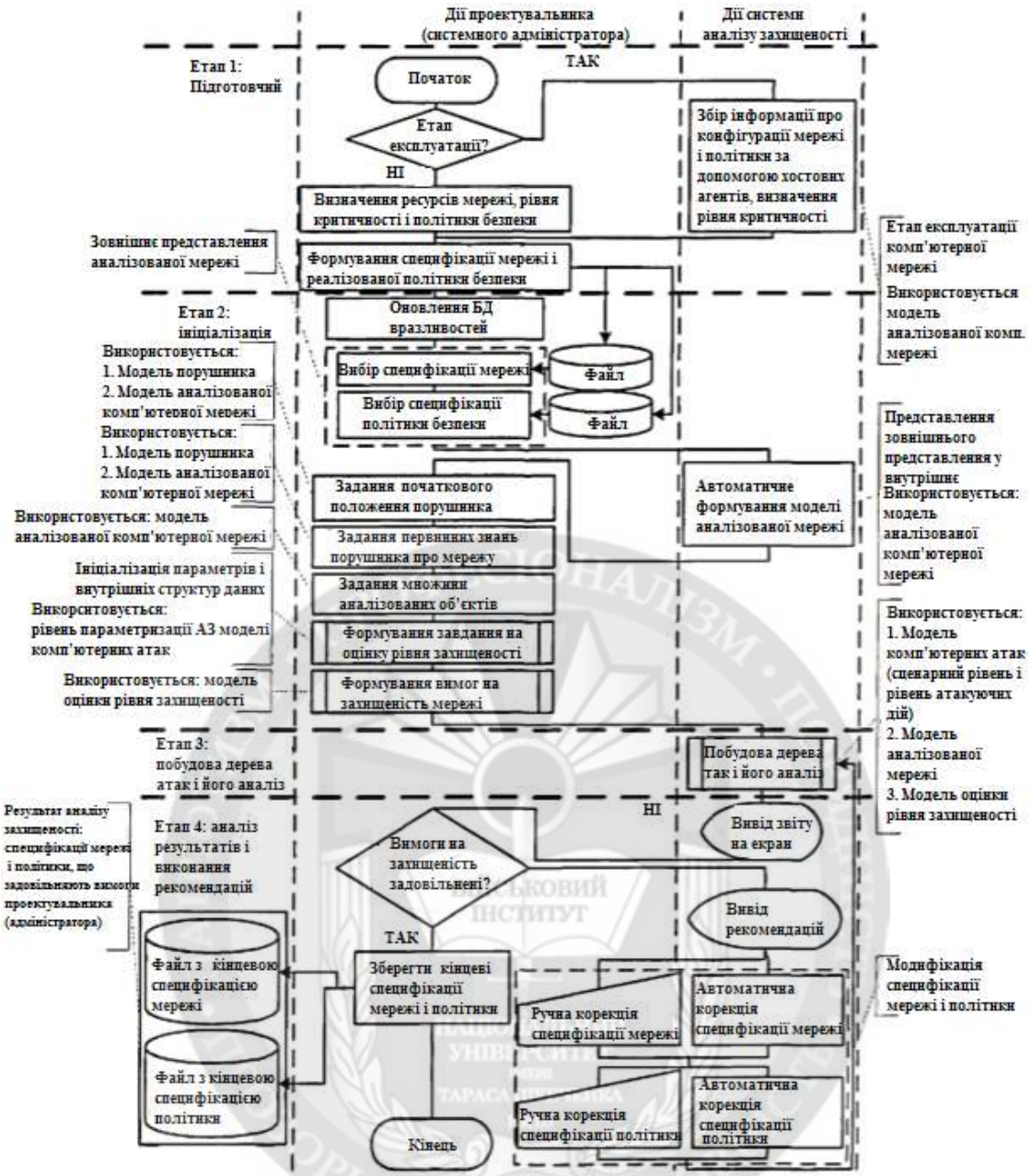

Рис. 2. Методика аналізу захищеності комп’ютерних мереж на етапах проектування і експлуатації

Множина процедур, що виконуються системою аналізу захищеності, складається з наступних елементів: (1) автоматичне формування моделі аналізованої комп'ютерної мережі (формування на базі заданих специфікацій конфігурації мережі і політики безпеки внутрішньої моделі мережі); (2) побудова графу загроз і його аналіз; (3) виведення звіту аналізу захищеності на екран; (4) автоматична модифікація (коригування) специфікацій мережі і політики безпеки на основі сформованих рекомендацій у разі отримання незадовільного результату.

Пропонована методика аналізу захищеності комп'ютерних мереж на етапах проектування і експлуатації дозволяє:

1. виявити уразливості використовуваного програмного і апаратного забезпечення, порушення політики безпеки, «вузькі місця» в захищеності комп'ютерної мережі;

2. надати допомогу в плануванні і здійсненні інформаційного захисту на етапах проектування і експлуатації комп'ютерних мереж;

3. обґрунтувати вибирання використовуваних (чи планованих до використання) засобів захисту інформації;

4. оцінити ефективність різних засобів захисту інформації, порівняти різні варіанти їх використання.

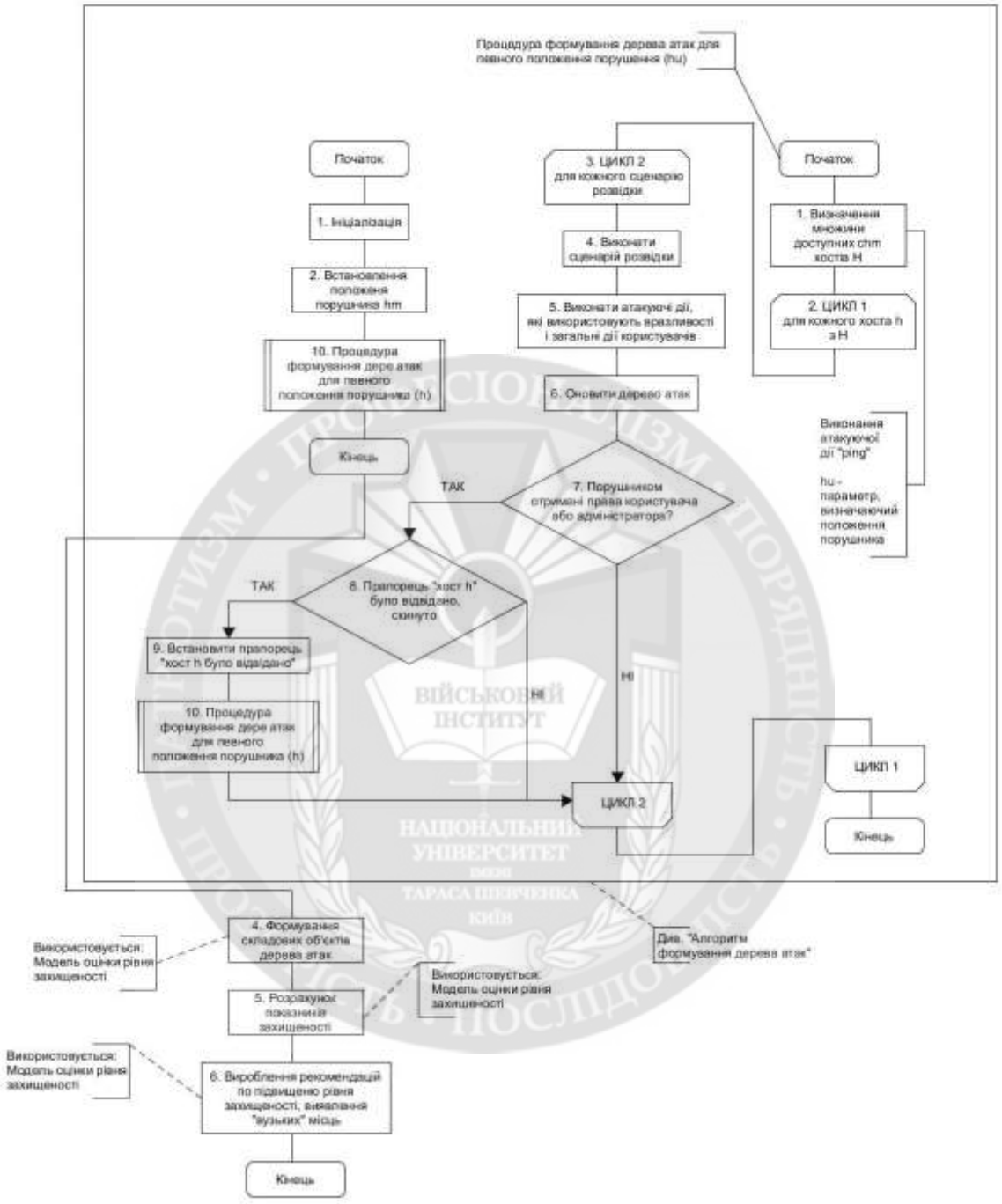

Рис. 3. Формування графу загроз

На етапах проектування і експлуатації комп'ютерної мережі САЗ взаємодіє з моделлю аналізованої комп'ютерної мережі. Ця модель створюється на базі специфікацій конфігурації мережі і використовуваної в ній політики безпеки. Ці специфікації на етапі проектування формуються проектувальником, а на етапі експлуатації для їх формування використовується підсистема збору інформації про аналізовану комп'ютерну мережу, що складається з наступних основних елементів: (1) джерел даних (хостових програмних агентів) і (2) збирача інформації. Хостові програмні агенти здійснюють збір необхідних для створення моделі

аналізованої комп'ютерної мережі даних. Так, наприклад, ці агенти можуть реалізовувати аналіз конфігураційних файлів операційної системи і різних програмних засобів. Збирач інформації служить для збору даних, що поступає від хостових агентів, їх представлення на спеціалізованих мовах SDL і SPL і передачі компонентам САЗ для аналізу.

Загальна архітектура системи аналізу захищеності представлена на рис. 4.

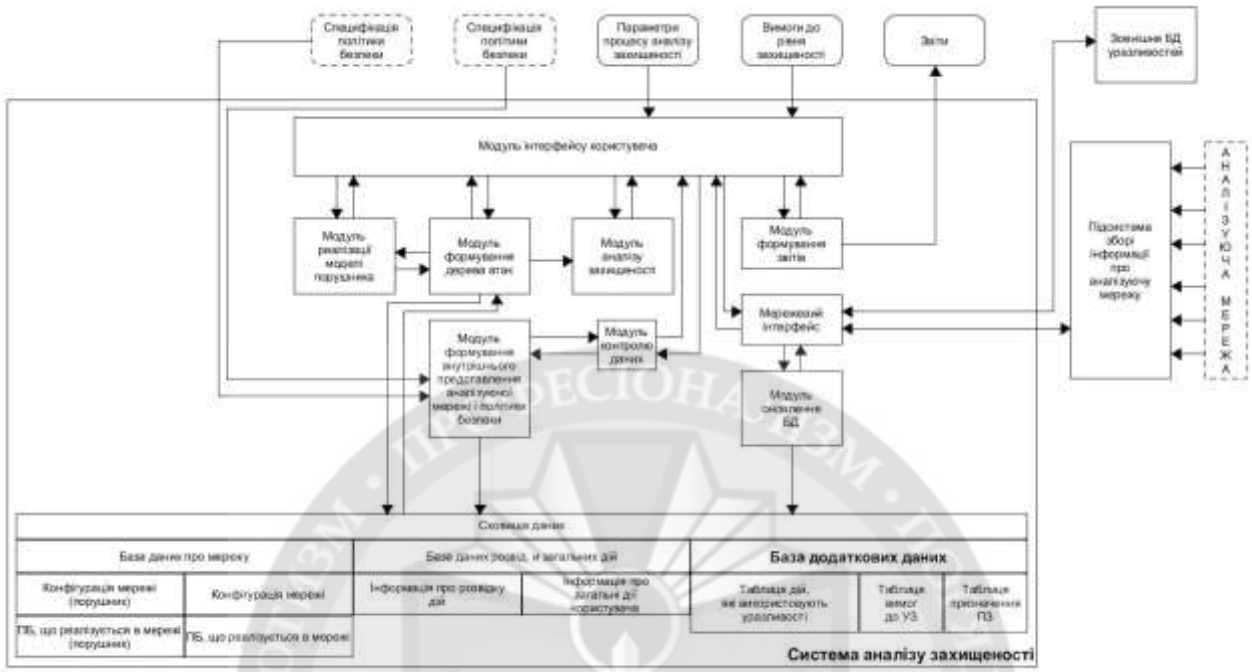

Рис. 4. Загальна архітектура САЗ

Мережевий інтерфейс забезпечує взаємодію САЗ із зовнішнім середовищем: звернення до зовнішніх баз даних вразливостей за оновленнями; зв'язок з підсистемою збору інформації про аналізовану мережу.

Системи, що вводяться в САЗ специфікації, і політики безпеки повинні описувати компоненти системи (мережі), що захищається, з необхідною мірою деталізації. Якщо потрібних для аналізу рівня захищеності даних не вистачає (наприклад, користувач не визначив версію використовуваного мережевого сервісу), система повинна запропонувати користувачеві ввести необхідну інформацію на основі бази даних програмного забезпечення. Для виявлення некоректних або невизначених даних, які потрібні для аналізу захищеності, служить модуль *контролю даних*.

Сховище даних складається з наступних елементів: компонент, що містить інформацію про мережу і політику безпеки (у вигляді тих, що відповідають програмних об’єктів, що реалізовується в ній; бази цих дій, вимог до рівня захищеності і назв програмного забезпечення; компонент, що містить інформацію про розвідувальні дії і загальні дії користувача.

База дій, що використовують уразливості, вимог і назв ПЗ складається з наступних таблиць: таблиця дій, що використовують уразливості; таблиця вимог до рівня захищеності; таблиця назв програмного забезпечення.

Таблиця дій, що використовують уразливості (на відміну від інших таблиця бази даних) будується на основі зовнішньої бази даних вразливостей (наприклад, NVD). Атакуючі дії в цій таблиці діляться на наступні групи: дії, спрямовані на отримання прав локального користувача; дії, спрямовані на отримання прав адміністратора; дії, спрямовані на порушення конфіденційності цілісності і доступності.

Таблиця вимог до рівня захищеності містить зумовлені експертним способом набори значень показників захищеності.

Таблиця назв ПЗ використовується модулем контролю даних для виявлення помилок у використовуваній специфікації комп'ютерної мережі і формування рекомендованих для використання програмних засобів, у разі відсутності в специфікації необхідних для аналізу захищеності даних.

Компонент, що описує розвідувальні дії, служить для представлення дій, спрямованих на видалене отримання інформації про хосту або мережу. Опис розвідувальних дій не міститься в зовнішніх базах даних вразливостей. Інформацію про методи і засоби реалізації порушником розвідувальних дій можна отримати лише експертним шляхом.

Компонент, що описує загальні дії користувача, містить інформацію про можливі дії користувача, що виконуються відповідно до наявних у нього повноважень.

Модуль оновлення БД служить для завантаження відомостей з відкритих баз даних вразливостей (наприклад, з OSVDB – open source vulnerability database) і трансляції їх в таблицю атакуючих дій, що використовують уразливості ПЗ і АО.

Модуль формування графу загроз робить побудову графу загроз, імітуючи дії порушника в аналізованій комп'ютерній мережі і використовуючи інформацію про доступні дії різних типів (що атакують, розвідувальних, загальних), про конфігурацію мережі і політику безпеки, що реалізовується в ній.

Модуль аналізу графу загроз робить обхід побудованого графу загроз і розрахунок показників захищеності.

Модуль реалізації моделі порушника забезпечує облік при побудові графу загроз первинного положення порушника, рівня знань і умінь, первинних знань про аналізовану комп'ютерну мережу. Рівень знань і умінь порушника визначає використовуваний ним набір атакуючих дій.

Модуль аналізу захищеності на базі графу загроз формує множину трас і загроз, робить розрахунок показників захищеності для них, оцінює загальний рівень захищеності комп'ютерної мережі, порівнює отримані результати з вимогами, визначеними користувачем, виявляє слабкі місця у безпеці і формує рекомендації по підвищенню рівня захищеності аналізованої комп'ютерної мережі.

Модуль формування звітів служить для агрегації отриманих в процесі аналізу захищеності даних (інформації про виявлених вразливостей, «вузьких» місцях, рекомендацій по підвищенню рівня захищеності) і формування на їх основі єдиного звіту.

Висновки. Розроблена методика аналізу захищеності комп'ютерних мереж на етапах проектування і експлуатації дозволяє істотно скоротити час на аналіз захищеності комп'ютерних мереж. При цьому використання запропонованої методики дозволить адміністраторові (чи проектувальникові) мережі проводити аналіз захищеності, визначати уразливості у використовуваному програмному і апаратному забезпеченні, виявляти «вузькі» місця в захищеності мережі, варіюючи різні параметри, що характеризують порушника.

Ефективність застосування методики аналізу захищеності комп'ютерних мереж на етапах проектування і експлуатації визначається як властивість забезпечувати вироблення своєчасної і обґрунтованої інформації про захищеність комп'ютерної мережі. Критерієм ефективності є виконання вимог за показниками основних властивостей ефективності (своєчасності, обґрунтованості, ресурсоспоживання).

ЛІТЕРАТУРА:

1. Таненбаум Э.С., Компьютерная сеть / Э.С. Таненбаум // Прентис-Холл, индийской Международной Эд.; 5-е издание. 2010. – 960 с.

2. Абрамов Г.В. Моделирование передачи данных по каналу конкурирующего доступа в системах реального времени / Г.В. Абрамов., А.Е. Емельянов // Вестник Воронежского государственного университета. Серия: Системный анализатор и информационные технологии, №4, 2014. – С. 26-31.

3. Литвинов К.А. Оценка информационной эффективности телекоммуникационной сети со случайной топологией и разным числом узлов / К.А. Литвинов, И.И. Пасечников // Вестник Тамбовского университета. Серия: Естественные и технические науки, Т.19, №2, 2014. – 399-407 с.

4. Северенц Ч.Р. Введение в сети: как Интернет работает / Ч.Р. Северенц // CreateSpace независимые издательские платформы, 2015. –122 с.

5. Литвинов К.А. Алгоритм оптимизации маршрутизации в информационной сети на основе приминение параметра кибернетической мощности / К.А. Литвинов, И.И. Пасечников // Радиолокация, навигация, связь: сб. материалов XXI международной научн. техн. конф. Т.3.-Воронеж: Воронежский государственный университет (ВГУ), 2015. – С. 1032-1044.

6. Настасе Р. Компьютерная сеть: Руководство для начинающих по освоению компьютерных сетей и модели OSI. / Р. Настасе // независимо опубликовано. 2017. – 138 с.

7. Муляр І.В., Предметно-орієнтований погляд на розробку програмного забезпечення / І.В. Муляр, В.О.Браун, В.К. Шваб, Я.М. Проценко, Р.М. Глушко // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2017. – Вип. № 57. – С. 123- 133.

8. Курносов М. Г. Назначение ветвей параллельной программы на процессорные ядра распределенной вычислительной системы. *Многопроцессорные вычислительные и управляющие системы:* матер. междун. науч.-техн. конференции. Таганрог, 2007. – С. 227-231.

9. Левин В. К. Современные суперкомпьютеры семейства МВС. Лаборатория Параллельных Информационных Технологий, НИВЦ МГУ. URL: http://www.computer-museum.ru/histussr/super_phase_0.htm (дата звернення: 02.06.2018).

10.Литвинов О.А., Хандецький В.С. Розподілена обробка інформації: монографія. Д.: ТОВ «Баланс-Клуб», 2013. 314 с.

11.Палагин А.В., Опанасенко В.Н. Реконфигурируемые вычислительные системы: Основы и приложения: монографія. Киев: Просвіта, 2006. 280 с.

12.Палагин А. В., Яковлев С. Ю. Системная интеграция средств компьютерной техники. Вінниця: Універсум-Вінниця, 2005. 680 с.

REFERENCES:

1. Tanenbaum, A. (2010), Computer network, Prentice Hall, Indian International Ed.; 5th edition, New York.

2. Abramov, H.V. and Emelianov, A.E. (2014), “Modelirovanie peredachi danyih po kanalu konkurirueschego dostupa v sistemah realnogo vremeni”, [Simulation of data transmission over a competing access channel in real-time systems], Bulletin of Voronezh state University. Series: System analysis and information technologies, No. 4, pp. 26-31.

3. Lytvynov, K.A. and Pasechnykov, Y.Y. (2014), “Otsenka ynformatsyonnoi effektyvnosty telekommunykatsyonnoi sety so sluchainoi topolohyei y raznym chyslom uzlov”, [Evaluation of information efficiency of telecommunication network with random topology and different number of nodes], Bulletin of Tambov University. Series: Natural and technical Sciences, Vol. 19 No. 2, pp. 399-407.

4. Severance, C. (2015), Introduction to Networking: How the Internet Works, CreateSpace Independent Publishing Platform; 1 edition, Detroit , Michigan.

5. Lytvynov, K.A. and Pasechnykov, Y.Y. (2015), “Alhorytm optymyzatsyy marshrutyzatsyy v ynformatsyonnoi sety na osnove prymynenye parametra kybernetycheskoi moshchnosty”, [The algorithm of routing optimization in the information network based on the application of the parameter of cybernetic power], Radar, navigation, communication: collection of materials of the XXI international scientific and technical conference, Vol. 3. Voronezh: Voronezhskyi hosudarstvennyi unyversytet (VHU), pp. 1032-1044.

6. Nastase, R. (2017), Computer Networking: Beginner’s guide for Mastering Computer Networking and the OSI Model, Independently published, Romania, Bucharest.

7. Muliar I.V., Braun V.O., Shvab V.K., Procenko Ya.M. and Glushko R.M. (2017), ”Predmetno-oriyentovanij poglyad na rozrobku programnogo zabezpechennya ” [Analysis of approaches to the structural build of web-applications], Zbirnyk naukovyh prac' Vijs'kovogo instytutu Kyi'vs'kogo nacional'nogo universytetu imeni Tarasa Shevchenka, No. 57, pp. 123-133.

8. Kurnosov M. H. (2007), “Naznachenye vetvei parallelnoi prohrammy na protsessornye yadra raspredelennoi vychyslytelnoi systemy” [Assigning branches of a parallel program to the processing cores of a distributed computing system], Mnohoprotsessornye vychyslytelnye y upravliaiushchye systemy: mater. mezhdun. nauch.-tekhn. Konferentsyy, Tahanroh, pp. 227-231.

9. Levyn V. K. (2018), “Sovremennye superkompiutery semeistva MVS” [Modern supercomputers of the MVS family], Laboratoryia Parallelnykh Ynformatsyonnykh Tekhnolohyi, NYVTs MHU. URL: www.computer-museum.ru/histussr/super_phase_0.htm (data zvernennia: 02.06.2018).

10. Lytvynov O.A. and Khandetskyi V.S. (2013), “Rozpodilena obrobka informatsii: monohrafiia” [Distributed processing of information], TOV «Balans-Klub», Dnepr, 314 pp.

11. Palahyn A.V. and Opanasenko V.N. (2006), “Rekonfyhuryruemye vychyslytelnye systemy: Osnovy y prylozhenyia: monohrafiia” [Reconfigurable computing systems: Fundamentals and applications], Prosvita, Kyev, 280 p.

12. Palahyn A. V. and Yakovlev S.Yu. (2005), “Systemnaia yntehratsyia sredstv kompiuternoi tekhnyky” [System integration of computer equipment], Universum-Vinnytsia, Vinnytsia, 680 p.

к.т.н., доц. Чорненький В.И., д.т.н., с.н.с. Селюков А.В.,
к.воен.н., доц. Осипа В.А., Глинский О.В., Щерба В.И.

СОВЕРШЕНСТВОВАНИЕ МЕТОДОВ ПОВЫШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ НА ОСНОВЕ ФОРМИРОВАНИЯ ПРАВИЛ ПОЛИТИКИ БЕЗОПАСНОСТИ

В статье рассмотрен подход, который объединяет множество моделей и методику, для реализации детального анализа защищенности компьютерных сетей на этапах эксплуатации и проектирования, основанный на имитации действий нарушителя, построении и анализа графу угроз. Разработанные модели компьютерных атак, нарушителя, рассматриваемой сети. В отличие от существующих моделей представлена модель компьютерных атак имеет следующие особенности: имеет вид иерархической структуры, что позволило для формирования сценарного уровня использовать экспертные знания, а для уровня атакующих действий - внешние базы данных уязвимостей; обеспечивает генерацию сценариев атак с учетом разнообразия целей и уровня знаний нарушителя. Представленная в работе модель рассматриваемой сети позволяет не только описать ее конфигурацию, но и политику безопасности, реализуемой в ней. Эта модель содержит также компоненты распознавания действий нарушителя и реакции сети на них. Использование представления последовательности выполнения нарушителем атакующих действий в виде графа и разработанного в рамках диссертационного исследования алгоритма его формирования позволило разработать модель оценки уровня защищенности. Модель оценки уровня защищенности компьютерных сетей охватывает множество различных показателей защищенности и правил (формул), используемых для их расчета. Особенность этой модели заключается в объединении подхода Common Vulnerability Scoring System (для расчета уровня критичности атакующего действия) и модифицированной методики анализа рисков Facilitated Risk Analysis and Assessment Process, что обеспечило возможность расчета интегрального показателя «Уровень защищенности сети». Разработана методика анализа защищенности компьютерных сетей на этапах проектирования и эксплуатации позволяет существенно сократить время на анализ защищенности компьютерных сетей. При этом использование предложенной методики позволит администратору (или проектировщику) сети проводить анализ защищенности, определять уязвимости в используемом программном и аппаратном обеспечении, выявлять «узкие» места в защищенности сети, варьируя различные параметры, характеризующие нарушителя. Эффективность применения методики анализа защищенности компьютерных сетей на этапах проектирования и эксплуатации определяется как свойство обеспечивать выработку своевременной и обоснованной информации о защищенности компьютерной сети. Критерием эффективности является выполнение требований по показателям основных свойств эффективности (своевременности, обоснованности, ресурсопотребления).

Ключевые слова: компьютерns сети, информационная безепека, правила политики безопасности

Ph.D. Chornenkyi V.I., prof. Selyukov A.V., Ph.D. Osipa V.A., Hlinskyi O.V., Shcherba V.I.

IMPROVEMENT OF THE METHOD OF INCREASING INFORMATION SECURITY OF COMPUTER NETWORKS ON THE BASIS OF FORMATION OF SAFETY POLICY RULES

The article shows an approach that combines a variety of models and techniques to implement a detailed analysis of the computer networks security at the exploitation and design stages, which is based on simulating the offender's actions, constructing and analyzing a graph of threats. Models of infringer computer attacks of the analyzed network are developed. Unlike existing models, the model introduced computer attacks has the following features: it has the form of a hierarchical structure, which allowed to use an expert knowledge to create a certain script level, and external vulnerability databases for level of attacking actions; It provides the generation of attack scenarios, taking into account the diversity of goals and level of knowledge of the offender. The model of the analyzed network presented in the work that allows not only to describe its configuration, but also the security policy that is implemented in it. This model also holds the components of the acknowledgment of an offender's actions and the network's response to them. Usage of the sequence representation of violations attacking actions in the form of a graph and developed in the framework dissertation of research algorithm of its formation allowed to develop a model for assessing the level of security. The model for assessing the level of computer networks security covers a variety of different indicators and rules of defence (formulas) used to calculate them. The peculiarity of this model is to combine the Common Vulnerability Scoring System approach (to calculate the criticality of the attacking action) and the Facilitated Risk Analysis and Evaluation Process Risk Analysis method, which provided an opportunity to calculate the integral value of the "Network Security Level". We developed a method to analyse the security of computer networks at the stages of design and exploitation which allows significantly reduce the time to analyze the security of computer networks. In this cace a usage of the proposed methodology will allow an administrator (or designer) to conduct a security analysis, identify vulnerabilities in the software and hardware that was used, and identify "bottlenecks" in the security of the network, varying the different parameters that characterize the offender. The efficiency to apply a method of analyzing the security for computer networks at the design and operation stages is defined as an ability to provide timely and reasonable information about the security of a computer network. The criterion of efficiency is the fulfillment of requirements according to the indicators of the main properties of efficiency (timeliness, validity, resource consumption).

Keywords: computer networks, information security, security policy rules.