УДК 004.056.52 **DOI:10.30837/rt.2022.2.209.11**

В.О. ПОДДУБНИЙ, Р.Ю. ГВОЗДЬОВ, О.В. СЄВЄРІНОВ, канд. техн. наук,
В.М. ФЕДОРЧЕНКО, канд. техн. наук

ОБ'ЄКТНО-ОРІЄНТОВАНА МОДЕЛЬ ФОРМАЛЬНОГО ОПИСУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ

Вступ

Під час проєктування (побудови) систем захисту інформації в інформаційно-комунікаційних системах розробники стикаються з великою кількістю проблем. Одна з таких проблем – це створення опису інформаційно-комунікаційної системи та механізмів захисту, який би повністю відображав систему, інформацію та зв'язки між об'єктами системи. Такий опис повинен бути формалізованим, тобто мати таке представлення, яке базується на чітко визначених математичних концепціях. В свою чергу, математичні концепції визначають синтаксис і семантику подання, що дозволяє унеможливити неоднозначність розуміння моделі.

Метою статті є розгляд алгоритму формального опису на основі взаємозв'язків об'єктів.

Процес побудови опису інформаційно-комунікаційної системи

Основним етапом при проєктуванні та побудові систем захисту інформації в інформаційно-комунікаційних системах (далі – ІКС) є документований опис роботи інформаційної системи. Існують багато підходів та методів для такого опису, але в основному детально розглядаються та аналізуються наступні компоненти інформаційно-комунікаційної системи:

– фізичне середовище;
– середовище обчислювальної системи;
– середовище користувачів;
– інформаційне середовище.

При розгляді фізичного середовища здійснюється аналіз апаратних засобів обробки інформації, комунікаційного обладнання, а також режим функціонування цих об'єктів.

При розгляді обчислювальної системи інформаційно-комунікаційної системи описується загальний склад технічних і програмних засобів, їхні зв'язки, особливості конфігурації, архітектури й топології.

При аналізі середовища користувачів фіксується функціональний та кількісний склад користувачів, їх функціональні обов'язки та рівень кваліфікації, повноваження щодо допуску до відомостей, які обробляються в ІКС, доступу до ІТС та її окремих компонентів, рівень можливостей різних категорій користувачів в системі.

При розгляді інформаційного середовища аналізу підлягає вся інформація, що обробляється, а також зберігається в ІКС. Також виділяється критична інформація в системі та властивості захищеності інформації, що повинні бути їм притаманні (конфіденційність, цілісність, доступність).

Типовий зміст документу (інструкції) опису системи містить неформальний опис наведених вище середовищ функціонування системи, може містити загальну структурну схему, схему інформаційних потоків та безліч інших таблиць і схем (правила розмежування доступу, перелік та представлення в системі інформаційних об'єктів тощо) [1, 2].

Як приклад, на рис. 1 наведена загальна структурна схема типової інформаційно-комунікаційної системи, яка представляє собою веб-сайт, що функціонує під керуванням веб-серверів, які, в свою чергу функціонують у віртуальному середовищі. Фізичний (апаратний) сервер у складі окремого сегменту мережі має доступ до мережі Інтернет через комунікаційне обладнання та міжмережевий екран. Адміністрування серверу здійснюється через робочу станцію адміністратора серверу, яка підключення до комутатора.

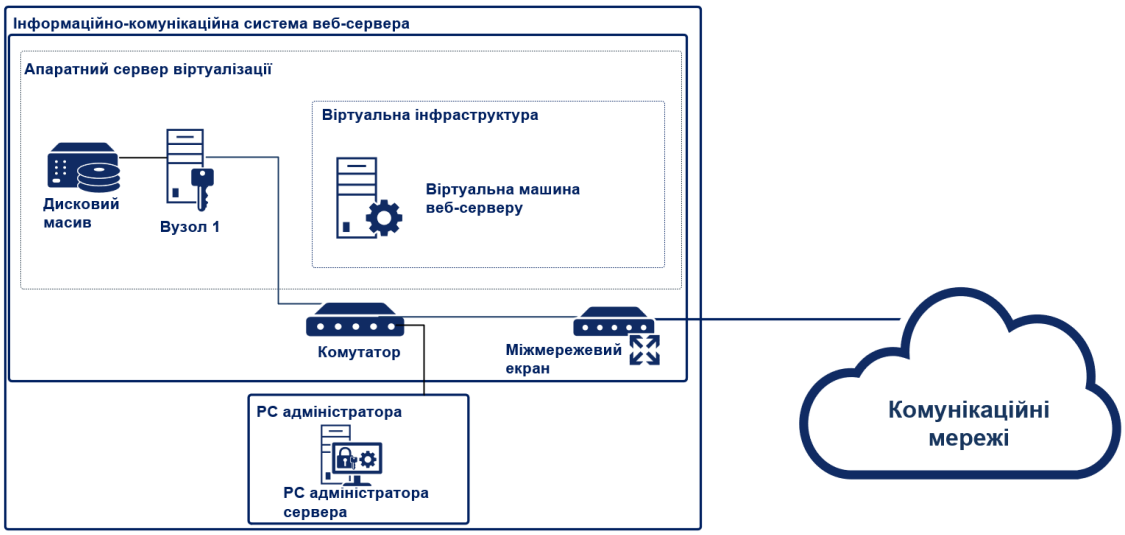

Рис. 1. Загальна структурна схема типової ІКС

Наведена на рис. 1 структурна схема є прикладом простої у розумінні системи. Зазвичай інформаційно-комунікаційні системи мають набагато більше технічних засобів, функцій, користувачів, в деяких випадках навіть мати у своєму складі спеціалізовані апаратні засоби захисту інформації.

Виникає необхідність у механізмі єдиного опису системи, що буде включати в себе всі середовища. Такий опис буде однозначно формалізований з чітко визначеними математичними поняттями. Механізм єдиного формального опису або методика формального опису ІКС буде однозначна в розумінні та слугуватиме керуючим описом при розробці політики безпеки інформації в ІКС.

Основні проблеми при побудові алгоритму формального опису ІКС є розробка уніфікованої системи опису, що дозволить врахувати усі варіанти зміни стану системи та складність розуміння такого опису.

Проблему складності розуміння опису можна вирішити шляхом залучення висококваліфікаційного персоналу та навчання нових користувачів, що відповідальні за дані задачі.

Проблема розробки єдиного формального опису може критично вплинути на менеджмент процесів управління системою, бо може виникнути ситуація, коли методика формального опису не має інструментів (математики) опису нових механізмів або функцій. Цю проблему можна вирішити шляхом тестового впровадження методики опису до різних ІКС та постійний аналіз і покращення алгоритму опису та математичної бази [3].

Формальні методики опису ІКС

Проблема створення методик формального опису не є новою, найбільш часто розглядалися такі мови формального опису, як UML, розширення UMLsec, Ponder 2.

В роботі [4] пропонується використання мови UML або розширення UMLsec для побудови моделі мережі. Проте, така модель складніша за рахунок переліку стереотипів та властивості даних, оскільки UML – це універсальна мова, яка створювалася для опису в області розробки ПЗ, системного програмування, бізнес процесів. Розширення UMLsec додає додаткові стереотипи та типи даних, ускладнюючи існуючу модель. Це не означає, що за допомогою UML неможливо здійснювати опис системи, даний процес буде більш складним і потре-

буватиме більше часу. Нотація мови UML не має змогу відобразити головні елементи ІКС та архітектуру механізмів захисту системи.

Загальна структура запропонованої методики

Пропонується створення нової моделі формального опису системи. В даній системі пропонується зосередитися на типах об'єктів та взаємодії об'єктів один з іншим. В такій схемі відбувається зосередження уваги на таких поняттях як:

1. Об'єкт;
2. Характеристики об'єкту;
3. Тип взаємодії з об'єктом.

Об'єкт – фізичний, операційна система, віртуальний пристрій, програма, інформація. Абстрактна модель, що має чітке відображення, має характеристики, цінність для ІКС, може взаємодіяти з іншими об'єктами.

Характеристики об'єкту являються його змінними, до даних характеристик відносяться як його явні характеристик та характеристики що надаються політикою безпеки ІКС (вимоги до КЦД, користувачі що можуть використовувати об'єкт)

Тип взаємодії (характеристика) – вплив одного об'єкта на інший, внаслідок якого відбувається взаємодія двох об'єктів,.

Об'єкт, що відображає інформацію, не містить деяких полів, що буде показано далі.

Дана модель схожа до UML, проте пропонується зменшення та переробка стереотипів. Дані стереотипи реалізовані в вигляді окремих полів. Перелік полів наведений в таблиці 1. Деякі поля можуть мати рівні (тобто являтися заголовками для інших).

Структурна форма об'єкту наведена нижче, кожний об'єкт починається з заголовку першого рівня (Element) та містить окремі характеристики. Внесення та обробку таких елементів планується виконати за допомогою програмного забезпечення. Знаком «#»зображені коментарі.

Element:
ID: # ID елемента для посилань
Type: Physical/OS/VM/ Program/Information/ #Тип елемента
Name: #назва елемента
CIA: x/y/z # К/Ц/Д в якісній шкалі
UserRead: #Перелік користувачів, що можуть читати об'єкт
UserWrite: #Перелік користувачів, що можуть змінювати об'єкт
UserCreate: #Перелік користувачів, що можуть створювати об'єкт
UserDel: #Перелік користувачів, що можуть видаляти об'єкт
Domen: #Елементи, що виконують даний елемент
  ElementD1: ID
  ElementD2: ID
    …….
Connected in: #Вхідні з'єднання
  Connection 1:
    Element: ID #Елемент, з яким відбувається з'єднання
    Transition element: ID #Елемент, що передається (посилання)
    Type connected: admin control/local use/ send data #Тип з'єднання
  Connection 2:
  …….
Connected out:
  Connection 1:
    Element: ID
    Transition element: ID
    Type connected: admin control/local use/ send data
  Connection 2:
  ……

Таблиця 1

Назва	Пояснення	Значення, що може набувати	Пояснення
Element	Заголовок окремого об'єкту	-	Рівень 1
ID	ID об'єкту слугує для технічних потреб при програмній реалізації моделі. Також може слугувати для відображення групи елементів	Беззнакове ціле число	
Type	Тип елементу	Physical	Фізичний пристрій
		OS	Операційна система
		VM	Гіпервізор
		Program	Програмний засіб
		Information	Дані/інформація
Name	Назва елементу (пояснення)	Рядок	
CIA	Вимоги до об'єкту відносно його цілісності/ конфіденційності/доступності	Беззнакове ціле число для цілісності/ конфіденційності/ доступності	Максимальне значення встановлюється згідно політики безпеки
UserRead	Перелік користувачів, що можуть читати об'єкт	Рядок	Згідно політики безпеки
UserWrit	Перелік користувачів, що можуть змінювати об'єкт	Рядок	Згідно політики безпеки
UserCreate	Перелік користувачів, що можуть створювати об'єкт	Рядок	Згідно політики безпеки
Domen	Заголовок доменів. Перелік об'єктів, для яких об'єкт являється доменом (обробляються) об'єктом	-	Рівень 2
ElementDx	Посилання на елемент за допомогою ID	Беззнакове ціле число (з ID, що були створені)	Кількість елементів необмежена
Connected in	Заголовок об'єктів, що взаємодіють на даний об'єкт		Рівень 2
Element: ID	Елемент, з яким відбувається з'єднання	Беззнакове ціле число (з ID, що були створені)	
Transition element	Елемент, що передається	Беззнакове ціле число (з ID, що були створені)	
Type connected	Тип взаємодії	admin control	адміністративний контроль
		local use	використання ресурсів
		send data	відправка даних
Connected out	Заголовок об'єктів, з якими взаємодіє даний об'єкт		Рівень 2
Element: ID	Елемент, з яким відбувається з'єднання	Беззнакове ціле число (з ID, що були створені)	
Transition element	Елемент, що передається	Беззнакове ціле число (з ID, що були створені)	
Type connected	Тип взаємодії	admin control	адміністративний контроль
		local use	використання ресурсів
		send data	відправка даних

Процес побудови формального опису з використанням запропонованої методики

Процес створення опису системи здійснюється по наступних етапах:

1. Визначається перелік інформації що функціонує в системі;
2. Створюються об'єкти інформації;
3. Визначаються об'єкти, що здійснюють обробку інформації;
4. Поетапно створюються об'єкти Physical (фізичний), OS (операційна система), VM (віртуальний), Program (програмний), Information (інформаційний), що здійснюють обробку інформації;

5. Формується логічний зв'язок об’єктів, що були створені;

6. Політикою безпеки визначається цінність кожного об’єкту та визначаються ролі користувачів;

7. Внесення політики безпеки до створеної структури;

8. Перегляд та взаємне доповнення політики та створеної структури.

Як приклад розглянемо взаємодію веб-браузера та веб-сервера. Створення моделі відбуватиметься поетапно.

1. На етапі №1 відбувається визначення об’єктів інформації (в даному прикладі це веб-сторінка та веб-запит).

2. На етапі №2 відбувається залучення даної моделі для створення об’єктів інформації:

Element: # Елемент веб-сторінки:
ID: 100
Type: Information
Name: Web-page
CIA:
UserRead:
UserWrite:
UserCreate:
UserDel:
Domen: -
Connected in: -
Connected out: -

Element: #Веб-запит :
ID: 101
Type: Information
Name: request
CIA:
UserRead:
UserWrite:
UserCreate:
UserDel: -
Domen: -
Connected in: -
Connected out: -

На даному етапі об’єкти не містять полів пов’язаних з політикою безпеки. Об’єкт інформації не містить полів Domen, Connected in, Connected out, за визначенням властивості інформації.

3. На етапі №3 відбувається визначення об’єктів, що здійснюють обробку інформації. В прикладі якості веб-сервера використовується Apache2, в якості веб-браузера Google Chrome. В даному прикладі ми не будемо опускатися до низьких рівнів опису об’єктів (Операційна система та фізичний пристрій) для спрощення прикладу. Глибину опису розробник вибирає сам на свій розсуд та згідно з висунутих вимог.

4. Далі, на етапі №4 здійснюється створення об’єктів обробки інформації:

Element: #Apache
ID: 103
Type: Program
Name: Apache2
CIA:
UserRead:
UserWrite: -
UserCreate:
UserDel:
Domen:
Connected in:
Connected out:

Element: # Google Chrome
ID: 104
Type: Program
Name: Chrome
CIA:
UserRead:
UserWrite: -
UserCreate:
UserDel:
Domen:
Connected in:
Connected out:

5. На етапі №5 формується зв’язок елементів, заповнюються поля взаємозв’язку (Connected in, Connected out) та вносяться елементи, для яких об’єкт являється доменом виконання (Domen):

Element: #Apache
ID: 103
Type: Program
Name: Apache2
CIA:

Element: # Google Chrome
ID: 104
Type: Program
Name: Chrome
CIA:

UserRead:
UserWrite: -
UserCreate:
UserDel:
Domen:
Element: 100 #домен для веб-сторінки
Connected in:
Connection 1:
Element: 104 #вхідне #з'єднання з веб-браузером
Transition element: 102 #веб-браузер
Type connected: send data #передача даних
Connected out:
Connection 1:
Element: 104 #вхідне #з'єднання з веб-браузером
Transition element: 100# передача сторінки до веб-браузеру
Type connected: send data

UserRead:
UserWrite:
UserCreate:
UserDel:
Domen:
Element: 102 #Домен відповіді
Connected in:
Connection 1:
Element: 103 #Apache
Transition element: 100 #передача сторінки до веб-браузеру
Type connected: send data
Connected out:
Connection 1:
Element: 103
Transition element: 102 #передача запиту веб-браузером
Type connected: send data

6. На етапі №6 відбувається призначення об'єктам цінності та визначення користувачів, в якості прикладу – це адміністратор веб-серверу «Admin» та користувач «User». Тег «ALL» значить, що вибрані всі користувачі. Кінцевий опис виглядає так:

Element: # Елемент веб-сторінки:
ID: 100
Type: Information
Name: Web-page
CIA: 0/2/5
UserRead: ALL
UserWrite: Admin
UserCreate: Admin
UserDel: Admin
Domen: -
Connected in: -
Connected out: -

Element: #Веб-запит :
ID: 101
Type: Information
Name: request
CIA: 0/2/2
UserRead: User
UserWrite: User
UserCreate: User
UserDel: -
Domen: -
Connected in: -
Connected out: -

Element: #Apache
ID: 103
Type: Program
Name: Apache2
CIA: 0/2/5
UserRead: Admin
UserWrite: -
UserCreate: Admin
UserDel: Admin
Domen:
Element: 100 #домен для веб-сторінки
Connected in:
Connection 1:

Element: # Google Chrome
ID: 104
Type: Program
Name: Chrome
CIA: 0/0/0
UserRead: ALL
UserWrite: -
UserCreate: ALL
UserDel: ALL
Domen:
Element: 102
Connected in:
Connection 1:

Element: 104 #Google Chrome
Transition element: 102 #передача відповіді
Type connected: send data #передача даних
Connected out:
Connection 1:
Element: 104//вхідне з'єднання з веб-браузером
Transition element: 100 #передача сторінки
Type connected: send data

Element: 103 #Apache
Transition element: 100 #передача сторінки до веб-браузеру
Type connected: send data
Connected out:
Connection 1:
Element: 103
Transition element: 102 #передача запиту веб-браузером
Type connected: send data

На рис. 2 показано графічне представлення розглянутого прикладу у вигляді блок-схеми. Кожен блок містить посилання на об'єкт що був створений раніше.

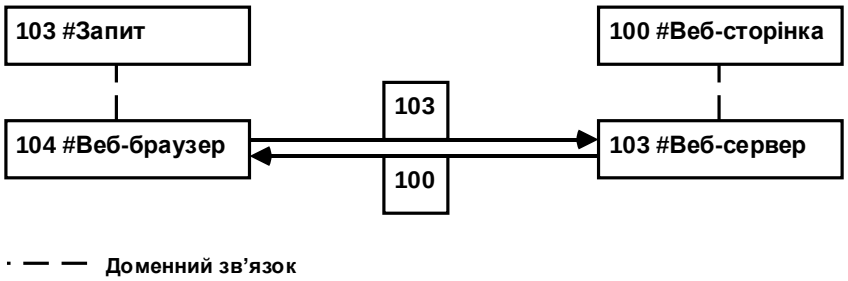

Рис. 2. Графічне представлення створеного прикладу

Можливості використання запропонованої моделі із залученням теорії графів

Пропонується подальший розгляд створених блок схем (графів) для дослідження можливостей використання даної моделі для симуляції кібератак. Оскільки кожний елемент містить поля, що зв'язують його з іншими елементами, а кожна атака має «точку входу» за допомогою теорії графів, можливо здійснювати обхід графу для визначення можливих шляхів горизонтального розповсюдження кібератаки.

Також в перспективі можливе додавання додаткових полів, що визначатимуть зрілість об'єкту (можливість об'єкту протистояти кібератакам). Після такого додавання стане можливим використання алгоритмів знаходження короткого шляху для визначення слабких місць мережі. До таких алгоритмів можна віднести алгоритм Дійкстри, Белмана – Форда, або знайти загальну зв'язність мережі за допомогою таких алгоритмів Клеймана, Прийм – Дійкстри та Крускаля. Такі алгоритми можуть бути залучені до процесу менеджменту вразливостями [5, 6].

Розробка програмних засобів для реалізації запропонованої моделі можлива будь-якою об'єктно-орієнтованою мовою програмування.

Висновки

Була запропонована модель формального опису інформаційно-комунікаційної системи з використанням об'єктного запису даних та графічного відображення. Основними перевагами такого опису є його цілеспрямованість під конкретні вимоги: опис ІКС, взаємозв'язок між об'єктами ІКС, взаємозв'язок опису ІКС та політики безпеки.

Наступними шляхами реалізації запропонованої моделі є:

– програмна реалізація засобу внесення та обробки даних;
– програмна реалізація представлення створюваних елементів у вигляді графів:

– дослідження можливості використання моделей графів для моделювання сценаріїв розповсюдження кібератаки;

– дослідження можливості додавання додаткових полів та можливості використання моделей графів для знаходження слабких місць мережі та визначення загальної зрілості мережі.

Така модель може пришвидшити розробку систем захисту інформації за рахунок автоматизації та стандартизації процесів, та покращити їх якість за рахунок формалізації та детального опису об'єктів, інтеграції з політикою безпеки. При наявності можливості використання теорії графів дана модель може здійснювати аналіз ІКС та будувати можливі шляхи розвитку атаки (з будь-якої точки мережі).

Список літератури:

1. НД ТЗІ 2.5-004.99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

2. Закон України «Про захист інформації в інформаційно-комунікаційних системах».

3. НД ТЗІ 2.7-010-09. Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.

4. Гвоздьов Р.Ю., Олійников Р.В. Метод та методика формального проєктування комплексної системи захисту інформації в інформаційно-телекомунікаційних системах // Радіотехніка. 2020. Вип. 203. С. 91-96.

5. Поддубний В.О., Сєвєрінов О., Пустомельник О. Менеджмент вразливостей як складова частина політики безпеки ІТС. Системи управління, навігації та зв'язку. Збірник наукових праць. Полтава : ПНТУ, 2020. Т. 4 (62). С. 55-58.

6. Poddubnyi V., Severinov O. Vulnerability management using a formalized description // Радіотехніка. 2020. Вип. 203. С. 121–125.

Надійшла до редколегії 07.06.2022

Відомості про авторів:

Поддубний Вадим Олександрович – аспірант кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Харківський національний університет радіоелектроніки, Україна; e-mail: vadym.poddubnyi@nure.ua, ORCID: https://orcid.org/0000-0002-4380-491X

Гвоздьов Роман Юрійович – аспірант кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Харківський національний університет радіоелектроніки, Україна; e-mail: roman.hvozdov@nure.ua, ORCID: https://orcid.org/0000-0002-5408-943X

Сєвєрінов Олександр Васильович – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Україна; e-mail: oleksandr.sievierinov@nure.ua, ORCID: https://orcid.org/0000-0002-6327-6405

Федорченко Володимир Миколайович – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри електронних обчислювальних машин, факультет комп'ютерної інженерії та управління, Україна; e-mail: volodymyr.fedorchenko@nure.ua, ORCID: https://orcid.org/0000-0001-7359-1460