УДК 004.9.056 **doi: 10.32620/reks.2022.1.10**

Г. І. ГАЙДУР, С. О. ГАХОВ, В. В. МАРЧЕНКО

Державний університет телекомунікацій, Київ, Україна

МЕТОД ПОБУДОВИ ДИНАМІЧНОЇ МОДЕЛІ ЛОГІЧНОГО ОБ'ЄКТА ІНФОРМАЦІЙНОЇ СИСТЕМИ ТА ВИЗНАЧЕННЯ ЗАКОНУ ЙОГО ФУНКЦІОНУВАННЯ

Предметом *дослідження в статті є методи виявлення вторгнень в інформаційні системи організацій для обґрунтування вимог до процесів функціонування агента моніторингу стану обраного логічного об'єкта.* ***Метою*** *є розроблення методу побудови динамічної моделі логічного об'єкта інформаційної системи та визначення закону його функціонування.* ***Завдання****: обґрунтувати необхідність створення агентів моніторингу станів безпеки логічних об'єктів інформаційних систем; визначити основні функції агентів моніторингу станів безпеки логічних об'єктів; запропонувати метод побудови динамічної моделі функціонування логічного об'єкта та визначення закону його функціонування. Використовуваними* ***методами*** *є: абстрагування, системний підхід, методи математичного моделювання з використанням положень теорії скінченних автоматів. Отримані такі* ***результати****. Запропоновано метод побудови динамічної моделі логічного об'єкта інформаційної системи. Динамічна модель функціонування обраного логічного об'єкта відображає допустимі процеси в просторі станів, які виникають при реалізації функцій відповідно до специфікацій, визначених протоколом. Дана динамічна модель подається системою алгебраїчних рівнянь в просторі станів, які утворюються в результаті формалізації процесів реалізації визначених функцій. Розв'язок системи алгебраїчних рівнянь в просторі станів як динамічної моделі логічного об'єкта представляє собою регулярний вираз для множини допустимих процесів. Даний регулярний вираз визначає множину можливих траєкторій в просторі станів, що становить закон функціонування даного логічного об'єкта.* ***Висновки****. Запропонований метод побудови динамічної моделі функціонування логічного об'єкта на відміну від існуючих базується на формалізації процесів реалізації часткових функцій протоколу, що дозволяє визначити закон функціонування обраного логічного об'єкта, забезпечити адекватність та точність відповідної моделі. Закон функціонування є основою для обґрунтування вихідних даних для постановки задач ідентифікації та діагностування стану безпеки логічного об'єкта інформаційної системи. Розв'язок даних задач потрібен для обґрунтування вимог до процесів функціонування агента моніторингу стану обраного логічного об'єкта та реагування на його зміни.*

Ключові слова: *вразливості інформаційних систем; логічний об'єкт інформаційної системи; стан безпеки інформаційної системи; динамічна модель логічного об'єкта; закон функціонування логічного об'єкта.*

Вступ

Вразливості інформаційних систем та їх експлуатація зловмисниками становлять серйозну проблему для сучасних організацій. Національна база даних вразливостей (National Vulnerability Database, NVD) Національного інституту стандартів і технологій США (National Institute of Standards and Technology, NIST) [1] є сховищем відомих суспільству вразливостей про які повідомляють фахівці з безпеки, дослідники та виробники програмного та апаратного забезпечення та які обліковані з присвоєнням CVE (Common Vulnerabilities and Exposures, CVEs).

Проведений аналіз показав, що у 2020 році було зареєстровано в NVD найбільшу кількість вразливостей програмного забезпечення, які стали відомі спільноті, за період з 2001 року. З 18352 вразливостей, облікованих в NVD за 2020 рік, отримали якісну оцінку серйозності вразливості програмного забезпечення (qualitative severity rankings) як критична – 4381, середня – 11206 та низька – 2765 вразливостей (рис. 1) [1].

Перший висновок, який можна зробити: спостерігається стійка тенденція зростання числа виявлених та облікованих спільнотою вразливостей програмного забезпечення. Основна причина: продовжує існувати гостра проблема розробки безпечного програмного забезпечення.

Другий висновок, який можна зробити: вразливості, незалежно від їх якісної оцінки серйозності, можуть експлуатуватися зловмисниками задля досягнення злочинних цілей. Тому, сьогодні створення та застосування

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

інформаційних систем організацій об'єктивно відбувається в умовах існування великої кількості відомих та невідомих (невиявлених на даний момент часу) вразливостей застосовуваного програмного забезпечення та високої ймовірності їх експлуатації зловмисниками.

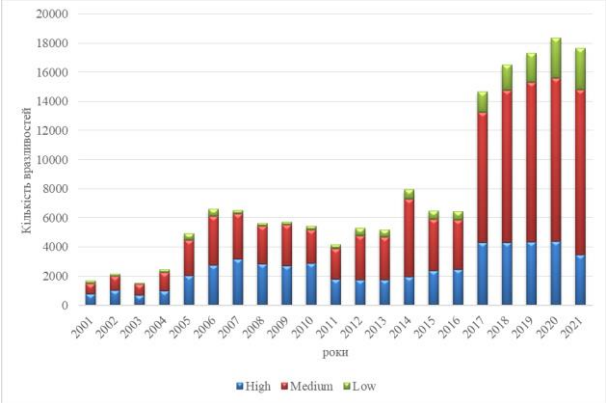

Рис. 1. Кількість облікованих вразливостей в National Vulnerability Database за роками [1]

На нашу думку, одним із шляхів вирішення проблеми наявності вразливостей інформаційних систем та їх експлуатації зловмисниками є моніторинг стану безпеки функціональних компонентів інформаційної системи (логічних об'єктів) та відповідне реагування у разі його порушення. Крім того, для ефективної протидії кібернетичним впливам на інформаційні системи організацій необхідні інструменти автоматичного моніторингу, ідентифікації, діагностування та реагування на події безпеки.

1. Аналіз літературних даних та постановка проблеми

В рекомендаціях NIST [2] зазначається, що виявлення вторгнень є процесом моніторингу подій, що відбуваються в комп'ютерній системі або мережі, їх аналізу на наявність ознак можливих інцидентів. Процес виявлення вторгнення логічно доповнюється процесом запобігання вторгненню як спроби зупинити виявлені можливі інциденти [2].

В системах кібербезпеки застосовуються різні методи виявлення вторгнень в інформаційні системи, а також їх комбінації. В [2–4] розглядаються три основних методи виявлення вторгнень:

– виявлення на основі сигнатур (Signature-Based Detection);

– виявлення на основі аномалій (Anomaly-Based Detection);

– виявлення на основі аналізу станів протоколу (Stateful Protocol Analysis).

Розглянемо більш детальніше метод виявлення на основі аналізу станів протоколу (Stateful Protocol Analysis). Сутність методу виявлення на основі аналізу станів протоколу полягає у порівнянні попередньо визначених профілів загальноприйнятого порядку правильної роботи протоколу для кожного його стану з подіями, які спостерігаються, для виявлення відхилень [2]. В [2] зазначається, що метод виявлення на основі аналізу станів протоколу базується на універсальному профілі розробленому постачальником. Зміст даного "універсального профілю", як він обґрунтовується та як створюється в [2] не висвітлюється.

Застосування методу виявлення на основі аналізу станів протоколу надає можливості визначати і відслідковувати стан мережевих, транспортних і прикладних протоколів, які мають поняття стану [2].

В [2] підкреслюється, що багато стандартів не є вичерпними для пояснення деталей протоколу, що викликає розбіжності між реалізаціями. Крім того, багато постачальників або порушують стандарти, або додають пропрієтарні функції, деякі з яких можуть замінювати функції, які визначені відповідними стандартами. Іноді повна інформація про пропрієтарні протоколи є недоступною, що ускладнює проведення всебічного і точного аналізу для реалізації у системах виявлення вторгнень.

В [2] відмічається, що моделі протоколів також зазвичай мають враховувати відмінності в реалізації кожного протоколу. Звичайно, у разі змін у стандартах протоколів та з виходом нових версій їх реалізацій, необхідно оновлювати моделі даних протоколів та налаштовувати системи виявлення відповідно до змін.

В [2] основними недоліками застосування методу виявлення на основі аналізу станів протоколу зазначається:

– часто дуже складно або неможливо розробити повністю точні моделі протоколів;

– застосування методу потребує використання багато обчислювальних ресурсів;

– застосування даного методу не дозволяє виявляти процеси, які не порушують характеристики загальноприйнятого порядку функціонування протоколу.

В роботі [5] звертається увага на те, що метод виявлення на основі аналізу протоколу з відстеженням стану ґрунтується на так званому "білому списку". На основі білого списку ідентифікуються будь-які аномальні пакети, які порушують визначену поведінку стану протоколу, зокрема IEC 60870-5-104 [5]. За поглядом авторів роботи [5] система виявлення вторгнень з відстеженням стану повинна бути здатною

ідентифікувати будь-який аномальний пакет, який порушує зумовлені переходи (діаграми) станів.

В роботі [5] було запропоновано використання автомата виявлення стану (Detection State Machine, DSM), функціонування якого описано в термінах скінченного автомата. Необхідним атрибутом автомата виявлення стану [5] є визначений набір "аварійних станів". На наш погляд визначення множини "аварійних станів" та її повноти буде викликати деякі труднощі.

За ідеєю авторів роботи [5, 14, 15] система виявлення вторгнень з відстеженням стану для моніторингу трафіку за протоколом IEC 60870-5-104 розгортається між клієнтом і сервером. На думку авторів роботи [5], система виявлення використовує DSM не тільки для опису важливої нормальної поведінки протоколу в формі переходів між станами, але також для виявлення неправильної поведінки протоколу та реагування у вигляді генерації сигналів тривоги.

На нашу думку, запропонований метод в [5], який базується на моніторингу трафіку та перехопленні пакетів не зовсім повно буде відображати стани функціональних компонентів клієнтів та сервера за протоколом IEC 60870-5-104.

Авторами роботи [6, 15] застосовується моделювання протоколу за допомогою скінченного автомата для «зменшення двозначності та неправильної інтерпретації специфікацій протоколу». На етапі проектування протоколів зв'язку завдання виявлення помилок та вразливостей його реалізації є дуже важливим. Причиною є те, що «протоколи зв'язку визначені частково, а підхід з кінцевим числом станів забезпечує гнучкий спосіб обробки невірних вхідних даних та неоднозначних специфікацій протоколу, які зазвичай не визначені або є розпливчастими» [6].

В [7] розкрито зміст формального аналізу протоколів безпеки, під час якого застосовується перевірка моделей. Пояснюються основні концепції, які задіяні в аналізі протоколів безпеки: абстракція повідомлень, протоколи як рольові автомати, модель зловмисника та специфікація властивостей безпеки.

Зазначається, що "формальний аналіз протоколів безпеки може допомогти прискорити стандартизацію, виявляючи проблеми на ранньому етапі та надаючи докази властивостей безпеки, якщо не виявлено жодних недоліків" [7]. У той же час, основною проблемою формального аналізу протоколів безпеки є те, що "сучасні методи та інструменти перевірки моделей дозволяють обробляти класичні протоколи автентифікації та обміну ключами реальної, але обмеженої складності" [7].

Існуючі проблеми щодо виявлення вторгнень в інформаційних системах організацій, недоліки існуючих методів виявлення на основі аналізу станів протоколів визначають актуальність подальшого дослідження даних питань.

2. Мета та задачі дослідження

Необхідно підкреслити, що забезпечення кібербезпеки інформаційної системи організації є складним процесом, який відбувається в умовах наявності вразливостей (в тому числі, як припущення) даної системи та можливої їх експлуатації зловмисниками. Точність моделей процесів функціонування компонентів інформаційної системи (тобто відповідно до вимог протоколу) є необхідною умовою їх подальшої реалізації, а також обґрунтування вимог та подальшої реалізації систем моніторингу їх стану.

Тому, ми визначаємо за мету даної роботи розроблення методу побудови динамічної моделі логічного об'єкта інформаційної системи та визначення закону його функціонування.

3. Зміст методу побудови динамічної моделі функціонування логічного об'єкта

Відповідно до [8], під протоколом розуміється набір правил і форматів (семантичних і синтаксичних), що визначають процедури зв'язку логічних об'єктів при виконанні ними функцій. Необхідно підкреслити, що, саме протоколи містять вимоги, які будуть виступати вихідними даними для побудови динамічних моделей функціонування відповідних логічних об'єктів інформаційних систем. У свою чергу, під логічним об'єктом розуміється активний елемент рівня взаємозв'язку відкритих систем, який виконує певну підмножину його функцій. притаманних для даного рівня. Коли розглядається взаємодія функціональних компонентів певного рівня Еталонної моделі взаємодії відкритих систем, то їх називають логічними об'єктами.

Для того, щоб ефективно протистояти кібернетичним впливам на процеси функціонування інформаційної системи необхідно щоб моніторинг, ідентифікація та діагностування стану безпеки обраного логічного об'єкта інформаційної системи відбувалися в режимі реального часу та, відповідно, мають бути автоматичними [9].

Проектування агентів моніторингу стану логічних об'єктів потребує розробки теорії даного питання та відповідної сукупності методів забезпечення її реалізації. Для вирішення проблеми виявлення шкідливих процесів на основі аналізу

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

станів обраного логічного об'єкта інформаційної системи необхідно розробити метод побудови динамічної моделі функціонування логічного об'єкта за відповідним протоколом, який забезпечить точність моделі функціонування обраного логічного об'єкта та можливість обґрунтувати вимоги до здійснення моніторингу його стану.

Відповідно до RFC 4949 [8] під вторгненням (англ. intrusion) розуміється "подія безпеки або комбінація декількох подій безпеки, що є складовою частиною інциденту безпеки, при якому зловмисник отримує або намагається отримати доступ до системи або системного ресурсу, не маючи на те дозволу". Зробимо таке зауваження, що вторгнення в інформаційній системі буде мати відповідне відображення у вигляді процесу в системі, який виникає при цьому. Це не буде цільовим процесом системи, тому будемо називати такий процес шкідливим.

Необхідно зазначити, що носієм будь-якого процесу в інформаційній системі є окрема утворювана функціональна система, яку утворюють вибірково задіяні функціональні компоненти та зв'язки між ними, що виникають у ході даного процесу.

В загальному вигляді завдання забезпечення кібербезпеки інформаційної системи буде полягати в створенні таких умов функціонування інформаційної системи організації під дією кібернетичних впливів, щоб у ній виникали тільки ті процеси та утворювалися тільки ті функціональні системи, які відповідають цілям створення даної системи. Якщо у функціональному компоненті системи виникають тільки процеси, які відповідають цілям створення даної системи, то компонент буде перебувати у дозволеному стані – стані безпеки. Перебування функціонального компонента у дозволеному стані визначає його стан безпеки. У свою чергу, стан безпеки інформаційної системи визначається станом безпеки її функціональних компонентів.

В якому стані перебуває функціональний компонент системи не можливо оцінити в рамках самої системи. Дане завдання можна вирішити шляхом моніторингу стану безпеки функціональних компонентів системи. Для цього необхідно розробити та створити зовнішню систему – агент моніторингу стану безпеки функціонального компонента системи, який буде реалізовувати певну функцію ідентифікації та діагностування стану безпеки. Зовнішня система означає, що даний агент не входить до складу утворюваних цільових функціональних систем.

Необхідно підкреслити, що основу методу виявлення шкідливих процесів на основі аналізу станів логічного об'єкта має складати динамічна модель функціонування обраного логічного об'єкта (рис. 2). За допомогою даної моделі ми зможемо визначити закон функціонування обраного логічного об'єкта, провести його аналіз задля визначення вихідних даних для постановки задач ідентифікації та діагностування стану безпеки логічного об'єкта інформаційної системи.

Розглянемо зміст запропонованого методу побудови динамічної моделі функціонування логічного об'єкта та визначення закону його функціонування (рис. 2).

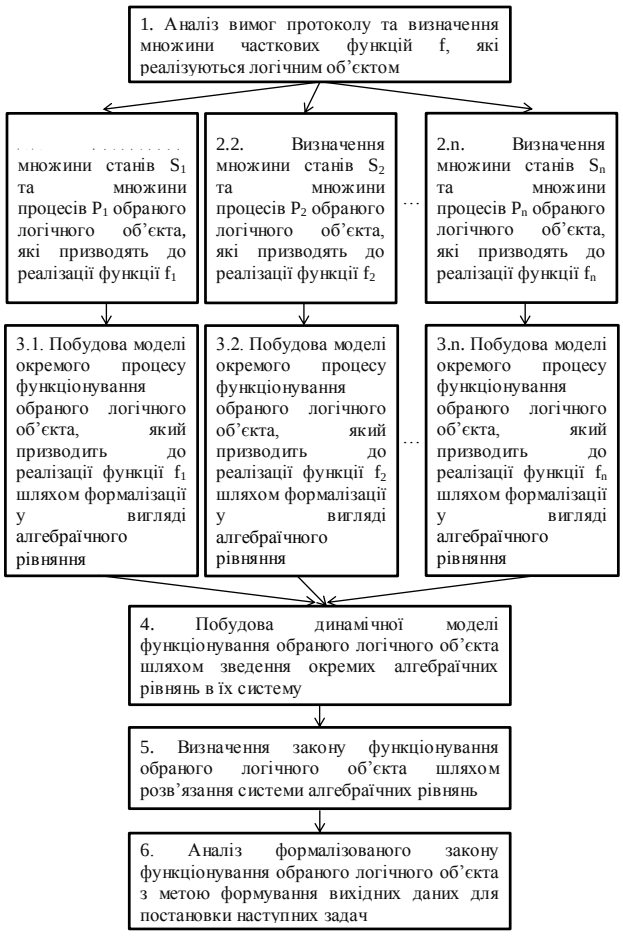

Рис. 2. Зміст методу побудови динамічної моделі логічного об'єкта

Передбачається, що динамічна модель функціонування логічного об'єкта буде представлена системою алгебраїчних рівнянь. Розв'язок системи рівнянь буде регулярним виразом, який визначає закон функціонування логічного об'єкта.

Застосування даного методу побудови динамічної моделі функціонування логічного об'єкта та визначення закону його функціонування дозволить робити правильну постановку та розв'язувати задачі визначення потрібних процесів (які передбачаються за відповідним протоколом) в

просторі станів обраного логічного об'єкта як скінченної автоматної системи. Правильне визначення структури простору станів логічного об'єкта в подальшому дозволить ставити різні прикладні задачі, зокрема задачу ідентифікації та діагностування стану безпеки, та визначати ефективні алгоритми їх розв'язку.

На першому кроці даного методу проводимо аналіз вимог обраного протоколу прикладного, транспортного, мережевого рівнів або послуг захисту з метою визначення множини часткових функцій f, які мають реалізовуватися логічним об'єктом. Виходячи з того, що кожна часткова функція f_n реалізується відповідним процесом, визначення та розгляд даних процесів є принциповою відмінністю нашого підходу.

Отже, для побудови динамічної моделі вихідними даними будуть застосовуватись вимоги згідно специфікацій відповідних протоколів, відповідно їх фактичної поведінки в системи та її компонентів.

Треба зазначити, що компоненти системи (логічні об'єкти), які функціонують за протоколами прикладного, транспортного, мережевого рівнів та послуг захисту реалізують визначену протоколом скінченну множину функцій та мають поняття стану. Кожна функція реалізується процесом, який має відображення в відповідні стани системи та переходи між ними. Тому, для дослідження питань функціонування логічних об'єктів інформаційної системи за відповідними протоколами будемо застосовувати абстрагування та моделювання з використанням положень теорії скінченних автоматів.

Постановка задачі аналізу скінченної автоматної системи полягає в знаходженні регулярного виразу для множини допустимих процесів. Вихідними даними задачі аналізу є відношення переходів та множина допустимих процесів [10].

Процеси, які реалізують множину функцій за відповідним протоколом, будуть складати множину допустимих процесів логічного об'єкта. Множина допустимих процесів дискретної системи представляє собою мову в алфавіті станів [10]. Тому, для опису даних процесів можна застосовувати методи визначень алгебри мов.

На другому кроці даного методу (див. рис. 2) визначаємо множину станів S_n та множину процесів P_n обраного логічного об'єкта, які призводять до реалізації функції f_n.

Для розв'язку задачі аналізу для логічного об'єкта за конкретним протоколом необхідно визначити множину процесів його функціонування в просторі станів деякої дискретної системи (другий крок методу побудови динамічної моделі функціонування логічного об'єкта). Правильне визначення структури простору станів, а саме множини станів та функції переходів, визначає подальшу ефективність алгоритму вирішення завдань моніторингу, ідентифікації та діагностування станів безпеки (небезпеки).

Необхідно підкреслити, що процеси функціонування логічного об'єкта змінюють його стан. Послідовності таких змін можна представити у вигляді орієнтованих графів (діаграм переходів). Вершинами такого графа є стани системи, а дуги зв'язують вершини за умов можливості переходу з одного стану в інший. Також динамічну модель логічного об'єкта можна описати системою алгебраїчних рівнянь в просторі станів.

На третьому кроці методу (див. рис. 2) будуємо моделі окремих процесів функціонування обраного логічного об'єкта, який призводить до реалізації кожної функції множини f шляхом формалізації у вигляді алгебраїчних рівнянь.

Необхідно відмітити, що множина допустимих процесів скінченної автоматної системи представляє собою мову в алфавіті станів і є регулярною. Відношення станів s та допустимих процесів F_s скінченної автоматної системи описуються канонічними системами лінійних рівнянь в алгебрі регулярних мов [10], наприклад,

$$F_s = \alpha(s) \vee V_{s' \to s} F_{s'} s,$$

де $\alpha(s) = (\text{якщо } s \in S_0 \text{, то s, інакше } \varnothing)$,

S_0 –множина початкових станів.

На четвертому кроці (див. рис. 2) будуємо динамічну модель функціонування обраного логічного об'єкта шляхом зведення окремих алгебраїчних рівнянь в їх систему.

На цьому кроці розв'язуємо задачу аналізу скінченної автоматної системи. Розв'язок системи алгебраїчних рівнянь в просторі станів як динамічної моделі логічного об'єкта представляє собою регулярний вираз для множини допустимих процесів. Даний регулярний вираз визначає множину його можливих траєкторій в просторі станів, що становить закон функціонування даного логічного об'єкта. За умови повної визначеності станів і допустимих процесів скінченної автоматної системи система лінійних рівнянь має єдиний розв'язок.

Необхідно підкреслити, що повна визначеність станів і допустимих процесів розкриває сутність даного логічного об'єкта та є необхідною умовою (критерієм) визначення його стану безпеки.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

На п'ятому кроці методу (див. рис. 2) визначаємо закон функціонування обраного логічного об'єкта шляхом розв'язання системи алгебраїчних рівнянь.

Саме закон функціонування обраного логічного об'єкта є джерелом вихідних даних для постановки та розв'язку задачі ідентифікації та діагностування його стану безпеки. В результаті аналізу формалізованого закону функціонування обраного логічного об'єкта ми отримаємо точні вихідні дані, а саме допустимі початкові стани, множину наступних допустимих станів, множину подій та послідовності переходів зі стану в стан.

На шостому кроці (див. рис. 2) проводимо аналіз формалізованого закону функціонування обраного логічного об'єкта з метою формування вихідних даних для постановки наступних задач.

4. Застосування методу побудови динамічної моделі логічного об'єкта інформаційної системи та визначення закону його функціонування на прикладі стеку протоколів IPsec

Проведемо дослідження взаємодії системи логічних об'єктів інформаційної системи на прикладі протоколу захищеного каналу IPsec [11–13] із застосуванням запропонованого вище методу.

Необхідно підкреслити, що вимоги стеку протоколів IPsec мають неформалізований характер, тому застосовуємо метод аналізу за ключовими словами (наприклад, слова, які застосовуються в [11–13]: "must", "must not", "required", "shall", "shall not", "should", "should not", "recommended", "may" та "optional").

Основу захищеного каналу IPsec складають база даних політик безпеки SPD (Security Policy Database), база даних безпечних асоціацій SAD (Security Association Database), база даних авторизації партнерів PAD (Peer Authorization Database), а також протокол автентикуючого заголовку AH (Authentication Header), протокол інкапсулюючого захисту блоку даних ESP (Encapsulating Security Payload) та протокол обміну ключами в Internet IKE (Internet Key Exchange).

Метою функціонування системи обробки трафіку за стеком протоколів IPsec є створення умовної межі між захищеними і незахищеними інтерфейсами для хоста або для мережі (рис. 3) [11]. Кожен пакет, базуючись на відповідних політиках SPD, визначених селекторами, або захищається (PROTECT), використовуючи сервіси безпеки IPsec, або відкидається (DISCARD), або йому дозволяється ігнорувати захист IPsec (BYPASS).

База даних політик безпеки SPD утворюється шляхом декартового добутку множин селекторів $sel_1 \times sel_2 \ldots \times sel_n$. Елементами бази є кортежі $(sel_1 \times sel_2 \ldots \times sel_n)$, де $sel_i \in Sel_i, 1 \le i \le n$ На множинах Sel_1, Sel_2, Sel_n задані функціональні відношення $F_{DISCARD}, F_{BYPASS}, F_{PROTECT}$ такі, що існує не більше одного елемента d із D (b із B, p із P відповідно), такого що

$$(sel_1, sel_2, \ldots, sel_n, d) \in F_{DISCARD},$$
$$(sel_1, sel_2, \ldots, sel_n, b) \in F_{BYPASS},$$
$$(sel_1, sel_2, \ldots, sel_n, p) \in F_{PROTECT}.$$

Елемент p із P є образом елемента $(sel_1, sel_2, \ldots, sel_n)$ при відображенні $F_{PROTECT}$ та при порівнянні кортежів селекторів бази даних та елемента трафіка та виступає визначальним для вибору елементів наступних баз даних SAD і PAD.

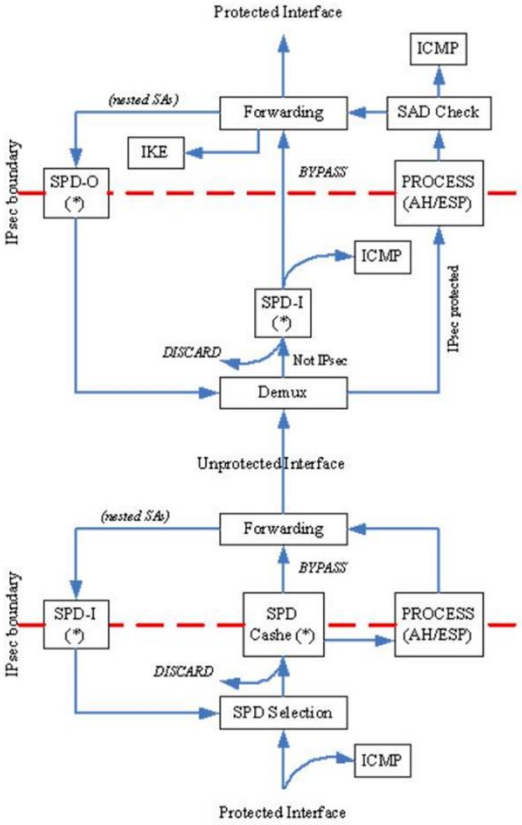

Рис. 3. Структурна модель системи обробки трафіку за стеком протоколів IPsec [11]

У базі даних SAD елемент p виступає образом елемента бази $(sa_1, sa_2, \ldots, sa_n)$, де $sa_i \in SA_i, 1 \le i \le n,$ який визначає набір параметрів безпечної асоціації для визначеного елементу

трафіка та визначає порядок застосування протоколів AH та ESP. Функціональне відношення можливо подати в такому вигляді $(p, sa_1, sa_2, \ldots, sa_n, spi) \in F_{SA}$.

У базі даних PAD елемент p може виступати образом елемента бази $(id_1, id_2, \ldots, id_n)$, де $id_i \in ID_i, 1 \le i \le n$, який визначає набір ідентифікаторів, які зіставляються з типами блоків даних протоколу IKE з метою утворення активної безпечної асоціації.

Можливо задати добуток відображень $F_{SA}(F_{PROTECT}(sel_1, sel_2, \ldots, sel_n)) = spi$ (під час вибору протоколу ESP), що являє собою операцію суперпозиції функцій.

Процес функціонування захищеного каналу має можливість розповсюджуватися віртуальним (логічним) симплексним каналом, характеристики якого не розглядаються. Також, в якості обмеження припускаємо, що дані бази PAD враховані в інших базах (SPD та SAD), часткове врахування ICMP-трафіка. Дані обмеження не змінюють загальної природи процесу функціонування системи.

Необхідно зазначити, що трафік, який перетинає межу IPsec, є об'єктом управління доступом. Необхідною умовою під час обробки всього трафіка є звертання до SPD (рис. 4) [11]. У початковий момент часу процес перебуває у вихідних станах a_0^1 сторони, що передає, та a_0^2 сторони, що приймає. Функції переходів f_1 та f_2 задаються базами даних (таблицями переходів) SPD1, SPD2, SAD1 та SAD2 відповідно. Параметри p^1 та p^2 визначають кореляцію SPD1 та SAD1, SPD2, та SAD2 відповідно.

Під час надходження пакету до захищеного каналу процес P_1 (див. рис. 4) зі стану a_0^1 у відповідності до функції переходів, що задається SPD1, може перейти в один із трьох станів: a_1^1 (подія d – відкидання пакету), a_2^1 (подія b – передача пакету без змін) або a_3^1 (подія p – обробка засобами IPsec).

У першому випадку процес P_1 у відповідності до SPD1 відкидає пакет, при цьому посилає повідомлення m_1^1 протоколу ICMP та повертається в початковий стан.

У другому випадку процес P_1 у відповідності до SPD1 передає пакет для функції вихідного пересилання та після завершення цього процесу повертається в початковий стан.

У третьому випадку процес P_1 у відповідності до SPD1 встановлює відповідну політику безпеки для обробки пакету (внутрішня подія p^1, яка показує звернення процесу до SAD1, та перехід у стан a_4^1). При неможливості вибрати відповідну політику безпеки (параметри безпечної асоціації) процес відкидає пакет, при цьому посилає повідомлення m_2^1 протоколу ICMP та повертається в початковий стан.

У стані a_4^1 здійснюється вибір параметрів безпечної асоціації (SA, Security Association) та обробка пакету криптографічними засобами протоколу. Під час встановлення відповідного контексту захищений пакет обробляється, передається функції вихідного пересилання та після завершення цього процесу повертається в початковий стан. Якщо неможливо вибрати відповідний контекст у SAD1 процес відкидає пакет, при цьому посилає повідомлення m_3^1 протоколу ICMP та повертається в початковий стан.

Під час надходження пакету приймаючий процес P^2 (див. рис. 4) зі стану a_0^2 у відповідності до функції переходів, що задається SPD2, може перейти в один із трьох станів: a_1^2 (подія d – відкидання пакету), a_2^2 (подія b – передача пакету без змін) або a_3^2 (подія spi – обробка засобами IPsec).

Реакція процесу P_2 для перших двох випадків буде аналогічною реакції процесу P_1. У третьому випадку реакція процесу відрізняється тим, що процес звертається спочатку до SAD2, а потім вже до SPD2.

У результаті аналізу діаграм переходів процесу функціонування системи (табл. 1) та, покладаючи в основу отримання потрібного кінцевого результату (за цієї умови забезпечується доступність інформації), стає можливим побудувати регулярний вираз, який визначає закон функціонування системи, що розглядалася, при дотриманні якого забезпечується захищеність процесів функціонування системи під час розподіленої взаємодії.

Розв'яжемо задачу аналізу скінченної автоматної системи.

Початковим станом процесу функціонування системи є a_0^1 Допустимими (потрібними) заключними станами системи є

$$a_1^1, a_2^1, a_3^1, a_4^1, a_5^1, a_1^2, a_2^2, a_3^2, a_4^2, a_5^2.$$

Шукана подія

$$S_\Sigma = S_{DISCARD} \vee S_{BYPASS} \vee S_{PROTECT}.$$

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

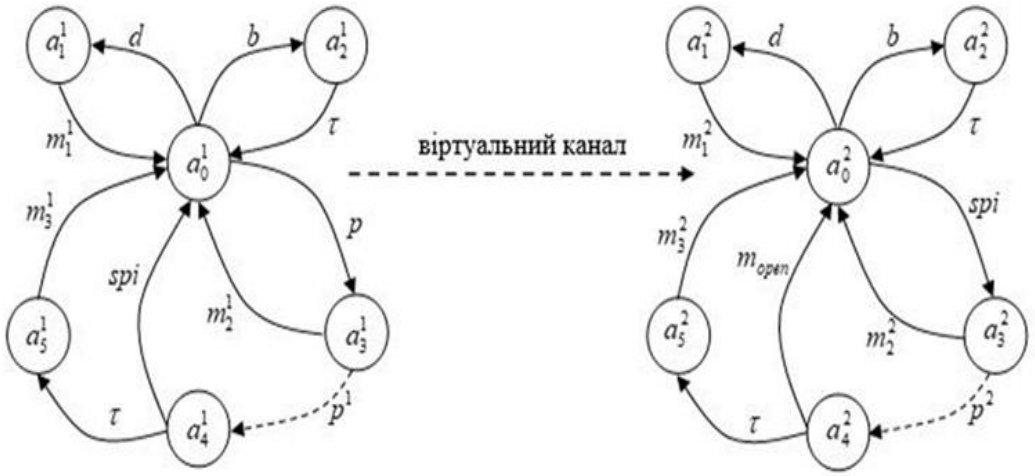

Рис. 4. Динамічна модель функціонування захищеного каналу за протоколом IPsec

Таблиця 1

Таблиця переходів захищеного каналу за протоколом IPsec

Процес	P_1	P_2	P_1	P_2	P_1	P_2	P_1	P_2	P_1	P_2	P_1	P_2
A S	a_0^1	a_0^2	a_1^1	a_1^2	a_2^1	a_2^2	a_3^1	a_3^2	a_4^1	a_4^2	a_5^1	a_5^2
d	a_1^1	a_1^2	-	-	-	-	-	-	-	-	-	-
b	a_2^1	a_2^2	-	-	-	-	-	-	-	-	-	-
p	a_3^1	-	-	-	-	-	-	-	-	-	-	-
spi	-	a_3^2	-	-	-	-	-	-	a_0^1	-	-	-
m_{open}	-	-	-	-	-	-	-	-	-	a_0^2	-	-
p^1	-	-	-	-	-	-	a_4^1	-	-	-	-	-
p^2	-	-	-	-	-	-	-	a_4^2	-	-	-	-
m_1^1	-	-	a_0^1	-	-	-	-	-	-	-	-	-
m_2^1	-	-	-	-	-	-	a_0^1	-	-	-	-	-
m_3^1	-	-	-	-	-	-	-	-	-	-	a_0^1	-
m_1^2	-	-	-	a_0^2	-	-	-	-	-	-	-	-
m_2^2	-	-	-	-	-	-	-	a_0^2	-	-	-	-
m_3^2	-	-	-	-	-	-	-	-	-	-	-	a_0^2
τ	-	-	-	-	a_0^1	a_0^2	-	-	a_5^1	a_5^2	-	-

Подія $S_{DISCARD}$, під час якої відбувається відкидання пакету, має вираз:

$$S_{DISCARD} = d \vee bd \vee p \vee pp^1\tau \vee pp^1spi\ d \vee$$
$$\vee pp^1spi\ spi \vee pp^1spi\ spi\ p^2\tau.$$

Подія S_{BYPASS} під час якої відбувається передача пакету без змін, має вираз: $S_{BYPASS} = b \vee bb$. Подія $S_{PROTECT}$, під час якої здійснюється обробка засобами IPsec, має вираз:

$$S_{PROTECT} = pp^1spi\ spi\ p^2.$$

Таким чином, стає можливим визначити формалізований закон функціонування системи S_Σ:

$$S_\Sigma = d \vee b(e \vee b \vee d) \vee p(e \vee p^1(\tau \vee spi(d \vee \vee spi(e \vee p^2(e \vee \tau))))),$$

де e – пусте слово.

Необхідно підкреслити, що саме високорівневий опис процесів функціонування системи обробки трафіку за стеком протоколів IPsec дозволяє описати та формалізувати процеси функціонування логічних об'єктів. Кожен процес функціонування логічних об'єктів має реалізувати одну із часткових функцій.

5. Оцінка адекватності динамічної моделі функціонування логічного об'єкта

Необхідно відмітити, що під час оцінювання адекватності моделей при реалізації дискретних систем застосовується поняття *гомоморфізму* [10]. Розкриємо сутність даного поняття.

Нехай S та S' – дискретні системи з множиною допустимих процесів F та F' відповідно. Розглянемо відображення $\gamma: S \to S'$. Дане відображення природним чином можна продовжити до відображення $\gamma: P(S) \to P(S')$, якщо вважати, що $\gamma(s_1 \ldots s_n) = \gamma(s_1) \ldots \gamma(s_n)$. Відображення γ називають *гомоморфізмом* системи S у S', якщо образ допустимого процесу системи S при цьому відображенні є допустим процесом системи S'. При цьому S' називається гомоморфною моделлю, а S – гомоморфною реалізацією системи S'. Така термінологія пояснюється практичними задачами [10].

При дослідженні властивостей системи S в результаті абстрагування ми створюємо модель S', яка є гомоморфною моделлю. Якщо ми побудували модель S', то система S, яка буде створено за цією моделлю, буде гомоморфною реалізацією S'. При цьому, при спостереженні допустимого процесу p функціонування системи S, яка реалізує систему S' за допомогою гомоморфізму γ, ми однозначно відновлюємо процес функціонування $q = \gamma(p)$ системи S'.

Гомоморфна реалізація *S* системи *S'* називається повною, якщо кожний допустимий процес системи *S'* має реалізацію, тобто $\gamma(F) = F'$.

Зробимо деякі суттєві зауваження.

По-перше, специфікація протоколів прикладного, транспортного, мережевого рівнів та послуг захисту визначає сутність відповідних логічних об'єктів та зміст їх динамічних моделей.

По-друге, рівень деталізації динамічної моделі відповідних логічних об'єктів інформаційних систем, яка описується в термінах станів та процесів, є достатнім для її дослідження та постановки задач ідентифікації та діагностування його стану безпеки.

6. Обговорення результатів дослідження

Інформаційні системи організацій функціонують в умовах існування вразливостей застосовуваного програмного забезпечення та високої ймовірності їх експлуатації зловмисниками. Тому, для ефективної протидії кібернетичним впливам на інформаційні системи організацій необхідні інструменти автоматичного моніторингу, ідентифікації діагностування та реагування на події безпеки.

Серед недоліків методу виявлення вторгнень на основі аналізу станів протоколу в [2] зазначалось те, що часто дуже складно або неможливо розробити повністю точні моделі протоколів. На наш погляд, саме виділення цілей функціонування логічного об'єкта та побудова його динамічної моделі повністю усуває даний недолік, а також забезпечує її адекватність. Адекватність динамічних моделей логічних об'єктів за запропонованим в даній роботі методом має забезпечуватися їх гомоморфною реалізацією.

Те, що застосування методу виявлення на основі аналізу станів протоколу "не може виявляти атаки, які не порушують характеристики загальноприйнятої поведінки протоколу" [2, 4] не є його недоліком, бо потрібні саме ознаки існування атаки (шкідливого процесу) через даний логічний об'єкт. Даний момент визначає необхідність існування окремої функції захисту.

Висновки

Запропонований у роботі метод побудови динамічної моделі функціонування логічного об'єкта за відповідним протоколом на відміну від існуючих базується на побудові динамічних моделей реалізації часткових функцій протоколу, що дозволяє визначити закон функціонування обраного логічного об'єкта (як множина допустимих траєкторій в просторі станів), забезпечити адекватність та точність відповідної моделі.

Динамічна модель функціонування логічного об'єкта за відповідним протоколом є джерелом вихідних даних для постановки та розв'язання задачі ідентифікації та діагностування станів безпеки відповідного логічного об'єкта.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Внесок авторів: концепція, рецензування, методологія, моделювання – **Г. І. Гайдур**, **С. О. Гахов**; оцінка адекватності, редагування – **В. В. Марченко**. Ця стаття написана в рамках виконання ініціативної держбюджетної науково-дослідної роботи за темою: *«Методологія виявлення шкідливих процесів в інформаційних системах»* (реєстраційний номер НДР 0121Г113613). Усі автори прочитали та погодилися з опублікованою версією рукопису.

Література

1. CVSS Severity Distribution Over Time. National Vulnerability Database. Information Technology Laboratory, NIST [Електронний ресурс]. – Режим доступу: https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time#. – 19.11.2021.

2. Scarfone, K. Guide to Intrusion Detection and Prevention Systems (IDPS). Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-94 [Text] / K. Scarfone, P. Mell. – NIST, Gaithersburg, MD, 2007. – 127 p. DOI: 10.6028/NIST.SP.800-94.

3. Mudzingwa, D. A Study of methodologies used in intrusion detection and prevention systems (IDPS) [Text] / D. Mudzingwa, R. Agrawal // 2012 Proceedings of IEEE Southeastcon. – 2012. – P. 1–6. DOI: 10.1109/secon.2012.6197080.

4. Intrusion Detection Strategies in Smart Grid [Text] / P. Ponmurugan, C. Venkatesh, M. Divya Priyadharshini, S. Balamurugan // In book: Design and Analysis of Security Protocol for Communication. John Wiley & Sons. – February 2020. – P. 223–245. DOI: 10.1002/9781119555759.ch10.

5. Stateful Intrusion Detection for IEC 60870-5-104 SCADA Security [Text] / Y. Yang, K. McLaughlin, S. Sezer, Y. B. Yuan, W. Huang // IEEE PES General Meeting. Conference & Exposition. – 2014. – P. 1–5. DOI: 10.1109/PESGM.2014.6939218.

6. Aljeaid, D. Analysis of Security Protocols using Finite-State Machines [Text] / D. Aljeaid, X. Ma, C. Langensiepen // International Journal of Advanced Research in Artificial Intelligence. – 2015. – Vol. 4, No. 4. – P. 46–53. DOI: 10.14569/IJARAI. 2015.040407.

7. Basin, D. Model Checking Security Protocols [Text] / D. Basin, C. Cremers, C. Meadows // In: Clarke E., Henzinger T., Veith H., Bloem R. (eds) Handbook of Model Checking. Springer, Cham., 2018. – P. 727–762. DOI: 10.1007/978-3-319-10575-8_22.

8. Shirey, R. RFC 4949. Internet Security Glossary, Version 2 [Text] / R. Shirey. – Network Working Group, August 2007. – 365 p.

9. Гайдур, Г. І. Теоретичний підхід до вирішення проблеми виявлення шкідливих процесів на основі аналізу станів логічного об'єкта інформаційної системи [Текст] / Г. І. Гайдур, С. О. Гахов // Телекомунікаційні та інформаційні технології. – 2021. – № 1 (70). – С. 79–87. DOI: 10.31673/2412-4338.2021.017987.

10. Капитонова, Ю. В. Математическая теория проектирования вычислительных систем [Текст] / Ю. В. Капитонова, А. А. Летичевский – М. : Наука, 1988. – 295 с.

11. Kent, S. Security Architecture for the Internet Protocol. Request for Comments: 4301 [Текст] / S. Kent, K. Seo. – Network Working Group, December 2005. – 102 p.

12. Kent, S. IP Authentication Header. Request for Comments: 4302 [Text] / S. Kent. – Network Working Group, December 2005. – 35 p.

13. Kent, S. IP Encapsulating Security Payload (ESP). Request for Comments: 4303 [Text] / S. Kent. – Network Working Group, December 2005. – 45 p.

14. Нечітка ієрархічна оцінка якості комплексних систем захисту інформації [Текст] / І. В. Шелехов, Н. Л. Барченко, В. В. Кальченко В К. Ободяк // Радіоелектронні і комп'ютерні системи. – 2020. – № 4(96). – С. 106-115. DOI: 10.32620/reks.2020.4.10.

15. Резильєнтність комп'ютерних систем в умовах кіберзагроз: таксономія та онтологія [Текст] / С. М. Лисенко, В. С. Харченко, К. Ю. Бобровнікова, Р. В. Щука // Радіоелектронні і комп'ютерні системи. – 2020. – № 1(93). – С. 17-28. DOI: 10.32620/reks.2020.1.02.

References

1. *CVSS Severity Distribution Over Time. National Vulnerability Database. Information Technology Laboratory, NIST*. Available at: https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time# (accessed 19.11.2021).

2. Scarfone, K., Mell, P. *Guide to Intrusion Detection and Prevention Systems (IDPS). Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-94*. NIST, 2007. 127 p. DOI: 10.6028/NIST.SP.800-94.

3. Mudzingwa, D., Agrawal, R. A study of methodologies used in intrusion detection and prevention systems (IDPS). *2012 Proceedings of IEEE Southeastcon*, 2012, pp. 1–6. DOI: 10.1109/SECon.2012.6197080.

4. Ponmurugan, P., Venkatesh, C., Priyadharshini, M. Divya., Balamurugan, S. Intrusion Detection Strategies in Smart Grid. *In book: Design and Analysis of Security Protocol for Communication. John Wiley & Sons*, February 2020, pp. 223–245. DOI: 10.1002/9781119555759.ch10.

5. Yang, Y., McLaughlin, K., Sezer, S., Yuan, Y. B., Huang W. Stateful Intrusion Detection for IEC 60870-5-104 SCADA Security. *IEEE PES General Meeting. Conference & Exposition*, 2014, pp. 1–5. DOI: 10.1109/PESGM.2014.6939218.

6. Aljeaid, D., Ma, X., Langensiepen, C. Analysis of Security Protocols using Finite-State Machines.

International Journal of Advanced Research in Artificial Intelligence, 2015, vol. 4, no. 4. pp. 46–53. DOI: 10.14569/IJARAI.2015.040407.

7. Basin, D., Cremers, C., Meadows, C. Model Checking Security Protocols. In: Clarke E., Henzinger T., Veith H., Bloem R. (eds) *Handbook of Model Checking. Springer, Cham*, 2018, pp. 727–762. DOI: 10.1007/978-3-319-10575-8_22.

8. Shirey, R. *RFC 4949. Internet Security Glossary, Version 2*. Network Working Group, 2007. 365 p.

9. Gajdur, G. I., Gaxov, S. O. Teorety`chny`j pidxid do vy`rishennya problemy` vy`yavlennya shkidly`vy`x procesiv na osnovi analizu staniv logichnogo ob'yekta informacijnoyi sy`stemy` [Theoretical approach to solving the problem of detecting malicious processes based on the analysis of the states of the entity of the information system]. *Telekomunikacijni ta informacijni texnologiyi – Telecommunication and Informative Technologies*, 2021, no. 1(70), pp. 79-87. DOI: 10.31673/2412-4338.2021.017987.

10. Kapitonova, Yu. V., Letichevskii, A. A., *Matematicheskaya teoriya proektirovaniya vychislitel'nykh sistem* [Mathematical theory of computing systems design]. Moscow, Nauka Publ., 1988. 295 p.

11. Kent, S., Seo, K. *Security Architecture for the Internet Protocol. Request for Comments: 4301*. Network Working Group, December 2005. 102 p.

12. Kent, S. *IP Authentication Header. Request for Comments: 4302.* Network Working Group, December 2005. 35 p.

13. Kent, S. *IP Encapsulating Security Payload (ESP). Request for Comments: 4303*. Network Working Group, December, 2005. 45 p.

14. Shelexov, I. V., Barchenko, N. L. et al. Nechitka iyerarxichna ocinka yakosti kompleksny`x sy`stem zaxy`stu informaciyi [A hierarchical fuzzy quality assessment of complex security information systems]. *Radioelektronni i komp'uterni sistemi – Radioelectronic and computer systems*, 2020, no. 4(96), pp. 106-115. DOI: 10.32620/reks.2020.4.10.

15. Lysenko, S. M., Kharchenko, V. S. et al. Rezy`l`yentnist` komp'yuterny`x sy`stem v umovax kiberzagroz: taksonomiya ta ontologiya [Computer systems resilience in the presence of cyber threats: taxonomy and ontology]. *Radioelektronni i komp'yuterni sy`stemy`*, 2020, vol.93, no. 1(93), pp. 17-28. DOI: 10.32620/reks.2020.1.02.

Надійшла до редакції 24.11.2021, розглянута на редколегії 16.02.2022

МЕТОД ПОСТРОЕНИЯ ДИНАМИЧЕСКОЙ МОДЕЛИ ЛОГИЧЕСКОГО ОБЪЕКТА ИНФОРМАЦИОННОЙ СИСТЕМЫ И ОПРЕДЕЛЕНИЯ ЗАКОНА ЕГО ФУНКЦИОНИРОВАНИЯ

Г. И. Гайдур, С. А. Гахов, В. В. Марченко

Предметом исследования в статье есть методы выявления вторжений в информационные системы организаций для обоснования требований к процессам функционирования агента мониторинга состояния выбранного логического объекта. **Целью** является разработка метода построения динамической модели логического объекта информационной системы и определение закона его функционирования. **Задачи**: обосновать необходимость создания агентов мониторинга состояний безопасности логических объектов информационных систем; определить основные функции агентов мониторинга состояний безопасности логических объектов; предложить способ построения динамической модели функционирования логического объекта и определения закона его функционирования. **Используемые методы**: абстрагирование, системный подход, методы математического моделирования с использованием положений теории конечных автоматов. Получены следующие **результаты**. Предложен метод построения динамической модели логического объекта информационной системы. Динамическая модель функционирования выбранного логического объекта отражает допустимые процессы в пространстве состояний, возникающих при реализации функций в соответствии со спецификациями, определенными протоколом. Данная динамическая модель представляется системой алгебраических уравнений в пространстве состояний, образующихся в результате формализации процессов реализации определенных функций. Решение системы алгебраических уравнений в пространстве состояний как динамической модели логического объекта представляет собой регулярное выражение для множества допустимых процессов. Данное регулярное выражение определяет множество возможных траекторий в пространстве состояний, что составляет закон функционирования данного логического объекта. **Выводы.** Предложенный метод построения динамической модели функционирования логического объекта, в отличие от существующих, базируется на формализации процессов реализации частичных функций протокола, что позволяет определить закон функционирования выбранного логического объекта, обеспечить адекватность и точность соответствующей модели. Закон функционирования является основой для обоснования исходных данных для постановки задач идентификации и диагностирования состояния безопасности логического объекта информационной системы. Решение данных задач необходимо для обоснования требований к процессам функционирования агента мониторинга состояния выбранного логического объекта и реагирования на его изменения.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Ключевые слова: уязвимости информационных систем; логический объект информационной системы; состояние безопасности информационной системы; динамическая модель логического объекта; закон функционирования логического объекта.

METHOD FOR CONSTRUCTING A DYNAMIC MODEL OF A LOGICAL OBJECT OF THE INFORMATION SYSTEM AND DETERMINING THE LAW OF ITS FUNCTIONING

Halyna Haidur, Sergii Gakhov, Vitalii Marchenko

The **subject** of the research in this article is the methods for detecting intrusions into the information systems of organizations to justify the requirements for the functioning of the monitoring agent of the selected logical object. The **aim** is to develop a method for building a dynamic model of the logical object of the information system and determine the law of its operation. **Tasks:** to substantiate the need to create security monitoring agents for logical objects of information systems; identify the main functions of security monitoring agents for logical objects; to propose a method for building a dynamic model of the functioning of a logical object and determining the law of its functioning. The **methods** used are abstraction, system approach, and methods of mathematical modeling using the provisions of the theory of finite automata. The following **results** were obtained. A method for constructing a dynamic model of a logical object of an information system is proposed. The dynamic model of the operation of the selected logical object reflects the allowable processes in the space of states that occur during the implementation of functions following the specifications defined by the protocol. This dynamic model is represented by a system of algebraic equations in the space of states, which are formed because of the formalization of the processes of realization of certain functions. The solution of a system of algebraic equations in the space of states as a dynamic model of a logical object is a regular expression for a set of admissible processes. This regular expression defines the set of possible trajectories in the space of states, which is the law of operation of this logical object. **Conclusions**. The proposed method for building a dynamic model of the logical object in contrast to the existing one is based on the formalization of the processes of implementing of partial functions of the protocol, which allows determining the law of the selected logical object, to ensure the adequacy and accuracy of the model. The law of functioning is the basis for the substantiation of initial data for a statement of problems of identification and diagnosing of a condition of the safety of logical objects of an information system. The solution to these problems is needed to substantiate the requirements for the functioning of the agent to monitor the state of the selected logical object and respond to its changes.

Keywords: vulnerabilities of information systems; the logical object of the information system; information system security status; dynamic model of a logical object; the law of functioning of a logical object.

Гайдур Галина Іванівна – д-р техн. наук, проф., зав. каф. інформаційної та кібернетичної безпеки, Державний університет телекомунікацій, Київ, Україна.

Гахов Сергій Олександрович – канд. військ. наук, доц., доц. каф. інформаційної та кібернетичної безпеки, Державний університет телекомунікацій, Київ, Україна.

Марченко Віталій Вікторович – асп. каф. інформаційної та кібернетичної безпеки, Державний університет телекомунікацій, м. Київ, Україна.

Halyna Haidur – Doctor of Technical Science, Professor, Head of Department of Information and Cyber Security, State University of Telecommunications, Kyiv, Ukraine,
e-mail: gaydurg@gmail.com, ORCID: 0000-0003-0591-3290, ResearchGate: Galyna-Gaidur.

Sergii Gakhov – Candidate of Military Science, Associate professor, Associate professor of department of Information and Cyber Security, State University of Telecommunications, Kyiv, Ukraine,
e-mail: gakhov@ukr.net, ORCID: 0000-0001-9011-8210, ResearchGate: Sergii-Gakhov.

Vitalii Marchenko – PhD student, Department of Information and Cyber Security, State University of Telecommunications, Kyiv, Ukraine,
e-mail: vetaldominus@gmail.com, ORCID: 0000-0003-4271-3132, ResearchGate: Vitalii-Marchenko-2.