FAST DISTINGUISHING ATTACK ON NTRUCipher + ENCRYPTION SCHEME

The NTRUCipher encryption system was proposed in 2017 as a symmetric version of the encryption scheme NTRUEncrypt, which is currently one of the fastest post-quantum cryptographic algorithms based on lattices in Euclidean space. The purpose of building NTRUCipher is to create a symmetric encryption scheme for practical applications, the security of which, similarly asymmetric, is based on the difficulty of solving only one computational problem. Preliminary exploring of this encryption scheme have been conducted, however the question of NTRUCipher's security against distinguishing attacks aimed at constructing statistical criteria for distinguishing sequences of encrypted messages and purely random sequences.This article shows that the NTRUCipher and even its natural improvement NTRUCipher+ proposed by analogy with the well-known provable secure version of asymmetric NTRU encryption scheme, are vulnerable to distinguishing attacks. Fast distinguishing attack on the NTRUCipher+ and (for a special case) even faster modification of this attack are proposed. Analytical estimates of both attacks' complexity are obtained, from which follows that they have polynomial time complexity and can be implemented in real-time. The obtained results show that other general constructions should be used to build symmetric NRTU-like encryption schemes.

Key words: post-quantum cryptography, lattice-based cryptography, distinguishing attack, discrete Fourier transform, NTRUEncrypt, NTRUCipher.

Олексійчук Антон Миколайович, доктор технічних наук, доцент, професор кафедри Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського».
E-mail: alex-dtn@ukr.net.
Orcid ID: 0000-0003-4385-4631.

Алексейчук Антон Николаевич, доктор технических наук, доцент, профессор кафедры Института специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт имени Игоря Сикорского".

Alekseychuk Anton Nikolaevich, Doctor of Technical Sciences, Assistant professor, Professor of The Institute of Special Communication and Information Protection of National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute".

Матійко Александра Андріївна, викладач кафедри Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».
E-mail: alexm1710@ukr.net.
Orcid ID: 0000-0002-6947-5958.

Матийко Александра Андреевна, преподаватель кафедры Института специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт имени Игоря Сикорского".

Matiyko Aleksandra Andriivna, teacher of Institute of Special Communication and Information Protection National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute".

DOI: 10.18372/2410-7840.22.14982
УДК 004[056.53+413.4]:303.732.46

МЕТОД СИНТЕЗУВАННЯ ПОВЕДІНКИ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Василь Цуркан

Визначено поведінку систем управління інформаційною безпекою через діяльність зі збереження конфіденційності, цілісності та доступності інформації в організаціях. Охарактеризовано її з боку структурних елементів послідовністю дій стосовно поводження з ризиками. Встановлено передумови такої діяльності. Серед них виокремлено визначення зовнішніх і внутрішніх обставин діяльності організацій, потреб і очікувань зацікавлених сторін, сфери та меж застосування систем управління інформаційною безпекою, встановлення критеріїв прийнятності та обирання методу оцінювання ризиків. Зважаючи на це запропоновано синтезування поведінки систем управління інформаційною безпекою за трьома аспектами. Для цього використано діаграми діяльності, послідовності та кінцевого автомату в графічній нотації SysML. Кожною зі зазначених діаграм синтезовано її особливості як окремих структурних елементів, так і систем управління інформаційною безпекою загалом. Діаграмою діяльності специфіковано поведінку через контрольовану послідовність дій. Характерною особливістю такого специфікування є орієнтованість на встановлення умов їх-

нього виконання. Водночас представлення об'єктів як вхідних і вихідних даних кожної дії. Часові особливості передавання і приймання об'єктів між структурними елементами систем управління інформаційною безпекою відображено діаграмою послідовності через їхнє взаємодіяння. Основою такої взаємодії є встановлення послідовності обміну повідомленнями. Він можливий або між системами управління інформаційною безпекою і їхнім середовищем, або між структурними елементами на будь-якому рівні ієрархії. У цьому випадку як структурні елементи, так і системи управління інформаційною безпекою тлумачаться окремими сутностями – лініями життя. Взаємодіяння між ними представляється обміном повідомленнями. Змінення станів при настанні визначених умов відображено діаграмою кінцевого автомату. Її використання орієнтоване на описання поведінки за схемою "стан – перехід". Тож поведінку представлено послідовним проходженням вершин графу кінцевого автомату направленими дугами. Завдяки цьому встановлено особливості діяльності систем управління інформаційною безпекою в організаціях методом синтезування їхньої поведінки.

***Ключові слова**: система управління інформаційною безпекою, поведінка, синтезування поведінки, діяльність, взаємодія, кінцевий автомат, SysML.*

ВСТУП

Поведінка систем управління інформаційною безпекою визначається діяльністю зі збереження конфіденційності, цілісності та доступності інформації в організаціях. Дана діяльність характеризується послідовністю дій з боку їхніх структурних елементів стосовно поводження з ризиками. Серед них виокремлюються, зокрема, оцінювання і оброблення [1]. Передумовами цьому є визначення зовнішніх і внутрішніх обставин діяльності організацій, потреб і очікувань зацікавлених сторін, сфери застосування систем управління інформаційною безпекою, встановлення критеріїв прийнятності та обирання методу оцінювання ризиків. Цим аспектом враховуються особливості поведінки як діяльності з огляду на послідовність дій, умов їхнього виконання, потоку об'єктів, наприклад: ідентифікованих ризиків, оцінок ризику, прийнятних, неприйнятних або залишкових ризиків. Заразом виконання дій структурними елементами систем управління інформаційною безпекою може розглядатися через взаємодію. Нею встановлюються часові особливості передавання і приймання об'єктів. Об'єкти передаються (приймаються) між окремими структурними елементами. Тому взаємодією як аспектом поведінки реалізується варіант використання систем управління інформаційною безпекою, наприклад, оцінювання ризиків. Через таку взаємодію змінюється поведінка як структурних елементів, так і систем загалом. Це обумовлюється створенням і знищенням об'єктів, зміненням значень їхніх атрибутів. Водночас до цього спонукає задоволення умов переходу структурного елементу з одного стану в інший. До того ж реалізування варіантів використання, наприклад, оброблення ризику за умови перевищення його оцінки встановленого прийнятного рівня. Такі особливості розглядаються у межах окремого аспекту поведінки систем управління інформаційною безпекою. Насамперед змінення станів структурних елементів або виконання ними дій при настанні визначених умов [1 – 5].

Отже, синтезування поведінки систем управління інформаційною безпекою в організаціях є актуальним завданням.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Системи управління інформаційною безпекою розробляються в організаціях за вимогами та настановами, імплементованих в Україні, міжнародних стандартів [1, 6]. Результати моделювання процесів і компонентів даних систем викладено в [7]. Вирішення цього завдання зведено до оцінювання ризику на основі лінійних діафантових рівнянь. Це дозволило перейти від нескінченної множини розв'язків до перебирання прийнятної кількості варіантів. Процеси як елементи систем управління інформаційною безпекою розглянуто в [8]. Запропоновано критерії та виокремлено основні процеси як основу їхнього розроблення і впровадження в організаціях. Це направлено на розмежування основних і допоміжних процесів, процесів управління і заходів забезпечення інформаційної безпеки. Формуванню проектних вимог

до систем управління інформаційною безпекою приділено увагу в [9]. Проведено їхню аналогію з системами масового обслуговування шляхом порівняння будови та функціональної структури. Завдяки такій аналогії встановлено можливість визначення ступеня важливості аспекту забезпечення інформаційної безпеки стосовно конкретної організації. Використання засобів забезпечення безпеки при розробленні систем управління інформаційною безпекою досліджено в [10]. Проаналізовано та класифіковано завдання їхнього реалізування в організаціях критичного сектору. До того ж описано залежності між засобами забезпечення безпеки та категоріями завдань.

Модель структуризування процесів систем управління інформаційною безпекою застосовано в [11]. На її основі запропоновано структуру комплексної системи безпеки кіберфізичних систем на рівні життєвого циклу інформації та багаторівневої моделі "кібернетичний простір – комунікаційне середовище – фізичний простір". Таке розширення систем управління інформаційною безпекою обумовлено використанням концепції "об'єкт – загроза – захист". Перспективи розроблення систем управління інформаційною безпекою описано в [12]. За основу взято врахування розвитку ринкових інновацій і технологій. Використання такого підходу сприяє адаптуванню організацій до мінливості внутрішніх і зовнішніх обставин діяльності. Як наслідок, гарантування зацікавленим сторонам належності управління ризиками інформаційної безпеки. Реалізування вимог до процесу розроблення систем управління інформаційною безпекою розкрито в [13]. Для цього запропоновано використання моделей зрілості процесів інформаційної безпеки. Серед них обрано найбільш застосовні, а саме: SSE-CMM, C2M2, NICE і O-ISM3.

Захищання персональних даних розробленням систем управління інформаційною безпекою висвітлено в [14]. Запропоновано систему вирівнювання вимог до збереження конфіденційності, цілісності та доступності інформації в організаціях. За її основу взято забезпечення узгодженості між Регламентом захисту персональних даних і міжнародним стандартом ISO/IEC 27001. Функції систем управління інформаційною безпекою визначено в [15]. Їх виокремлено на рівні структурних елементів (підсистем, комплексів, компонентів). Для цього встановлено мету, точку зору та розглянуто управління інформаційною безпекою як діяльність. Її відображено множиною ієрархічно взаємопов'язаних функцій. Стосовно кожної з них задано вхідні, вихідні дані, управління і механізми.

Отже, за результатами аналізування останніх досліджень і публікацій встановлено їхню орієнтованість на, по-перше, реалізування процесного підходу до розроблення систем управління інформаційною безпекою [7, 8, 11 – 13]. По-друге, встановлення можливостей визначення ступеня важливості аспектів забезпечення інформаційної безпеки стосовно конкретних організацій [9, 10]. По-третє, узгодження завдань захищання персональних даних і забезпечення інформаційної безпеки [14]. По-четверте, визначення ієрархічності функцій структурних елементів відповідно до встановленої мети та точки зору [15]. Однак, поза дослідженнями залишено аспект поведінки систем управління інформаційною безпекою. Для запобігання цьому запропоновано використання графічної нотації SysML [2]. Тому мета даної роботи формулюється як встановлення особливостей діяльності систем управління інформаційною безпекою методом синтезування їхньої поведінки.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Поведінка систем управління інформаційною безпекою синтезується за трьома аспектами. Насамперед послідовності дій структурних елементів, умов їхнього виконання, потоку об'єктів; часових особливостей передавання і приймання об'єктів між структурними елементами; змінення станів структурними елементами при настанні визначених умов. Моделювання такої поведінки зводиться до використання діаграм діяльності, послідовності та кінцевого автомату в графічній нотації SysML. Кожною зі зазначених діаграм синтезуються її особливості як окремих структурних елементів, так і систем управління інформаційною безпекою загалом [2, 4, 5, 16, 17].

Діяльністю зі збереження конфіденційності, цілісності та доступності інформації в організаціях специфікується поведінка систем управління інформаційною безпекою через контрольовану послідовність дій структурних елементів. Характерною особливістю такого специфікування є орієнтованість на встановлення умов їхнього виконання. Водночас представлення об'єктів як вхідних і вихідних даних кожної дії. Тому діяльність розглядається як один з основних аспектів синтезування поведінки систем управління інформаційною безпекою і відображається відповідною діаграмою у графічній нотації SysML зі заголовком [5, 16, 17]:

act [різновид елементу моделі] ім'я діяльності [ім'я діаграми], наприклад [2, 17, 18], див. рис. 1:

act [activity] Ідентифікування ризиків [Поведінка структурного елементу].

При цьому дія тлумачиться елементарною одиницею специфікування поведінки. Це означає, що її неможливо розділити на інші дії або діяльність. Тому вона визначається окремим блоком (компонентом) систем управління інформаційною безпекою, скажімо (див. рис. 1): ідентифікування інформаційних активів, ідентифікування уразливостей. Виконанням дії реалізується його функція, зокрема, ідентифікуються наслідки реалізування загроз і/або конфіденційності, і/або цілісності, і/або доступності інформаційних активів у межах застосування систем управління інформаційною безпекою. Передумовами здійснення даної функції розглядаються наявність інформаційних активів, уразливостей і загроз. Умови виконання і послідовність дій визначаються потоком управління. Ним передаються маркери від вузла-передавача до вузла-приймача. Якщо розглянути "Ідентифікування ризиків" і "Визначення оцінок ризиків" як діяльності, то потоком управління між ними визначається виконання діяльності "Визначення оцінок ризиків" після завершення "Ідентифікування ризиків" [2, 5, 16, 17].

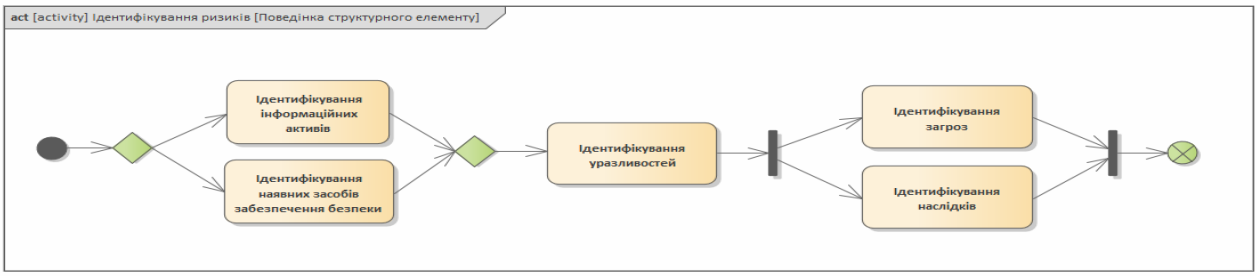

Рис. 1 Приклад специфікування поведінки окремого структурного елементу систем управління інформаційною безпековою діяльністю

Специфіка координування потоком управління відображається вузлами:

1) початковий – задається початок виконання діяльності. Маркер розміщується у даному;

2) вузлі та ним, наприклад, розпочинається "Визначення оцінок ризиків";

3) завершення потоку – завершується окремий потік у межах діяльності. Маркер передається до даного вузла та ним, наприклад, завершується "Оброблення ризиків";

4) завершення діяльності – завершуються усі потоки управління діяльністю. Маркер передається до даного вузла та ним, наприклад, припиняється "Управління ризиками".

Однак, при цьому унеможливлене передавання об'єктів і даних. Обмеження долається використанням потоку об'єктів для передавання відповідних маркерів. Як приклади діяльностей розглядаються "Оцінювання ризиків" та "Оброблення ризиків". Останньою можливе приймання "Неприйнятних оцінок ризиків" за результатами їхнього зіставлення з прийнятним рівнем. Цим прикладом демонструється використання об'єкту "Неприйнятна оцінка ризику". Потік об'єктів координується таким вузлами [2, 5, 17]:

1) розділення – розщеплюється вхідний потік об'єктів на декілька паралельних потоків. Отриманий ним маркер передається кожним з вихідних потоків. Наприклад, після завершення діяльності "Ідентифікування ризиків" даним вузлом передаються маркери управління потоком

об'єктів Ідентифіковані ризики" діям "Визначення оцінок вірогідності реалізації загрози" та "Визначення оцінок наслідків реалізації загрози";

2) з'єднання – синхронізуються декілька вхідних потоків об'єктів у один вихідний. Маркер передається за його доступності кожному вхідному потоку. Наприклад, після завершення дій "Визначення оцінок вірогідності реалізації загрози" та "Визначення оцінок наслідків реалізації загрози" маркер управління потоком об'єктів "Оцінка вірогідності" та "Оцінка наслідків" передається діяльності "Визначення оцінок ризиків";

3) рішення – вибирається один з вихідних потоків об'єктів. Маркер передається тільки одним з вихідних потоків. Наприклад, за результатами завершення діяльності "Оцінювання ризиків" можливе передавання маркеру управління потоку об'єктів "Прийнятні ризики" та/або "Неприйнятні ризики" одній з двох діяльностей: або "Визначення контексту (оточення)", або "Оброблення ризиків";

4) злиття – з'єднуються декілька альтернативних потоків у один вихідний потік об'єктів. Маркер передається вихідному потокові за його наявності хоча б на одному вхідному. Наприклад, після завершення однієї з діяльностей: або "Оцінювання ризиків", або "Оброблення ризиків", або "Контролювання і переглядання ризиків" можливе передавання маркеру діяльності "Визначення контексту (оточення)". Часові особливості передавання і приймання об'єктів між структурними елементами систем управління інформаційною безпекою відображаються через їхнє взаємодіяння. Основою такої взаємодії є встановлення послідовності обміну повідомленнями. Це можливе або між системами управління інформаційною безпекою і їхнім середовищем, або між структурними елементами на будь-якому рівні ієрархії. У цьому випадку як структурні елементи, так і системи управління інформаційною безпекою тлумачаться окремими сутностями – лініями життя. Взаємодіяння між ними представляється обміном повідомленнями.

Тому воно розглядається як окремий аспект синтезування поведінки систем управління інформаційною безпекою і специфікується діаграмою послідовностей у графічній нотації SysML зі заголовком [5, 16, 17]:

sd [різновид елементу моделі] ім'я взаємодії [ім'я діаграми], наприклад [2, 17, 18], див. рис. 2:

sd [package] Ідентифікування ризиків [Поведінка структурного елементу].

Лінії життя є основною структурною особливістю взаємодіяння елементів систем управління інформаційною безпекою. Ними відображаються час життя блоку протягом обміну повідомленнями. Зображується прямокутником з пунктирною лінією від його центру вниз, наприклад (див. рис.1): ідентифікування інформаційних активів, ідентифікування уразливостей, ідентифікування загроз. Їхня активність представляється при описанні взаємодії специфікаціями виконання. Дані специфікації зображуються зафарбованими вертикальними прямокутниками. Характеризуються настанням подій початку та завершення виконання.

Лінії життя є основною структурною особливістю взаємодіяння елементів систем управління інформаційною безпекою. Ними відображаються час життя блоку протягом обміну повідомленнями. Зображується прямокутником з пунктирною лінією від його центру вниз, наприклад (див. рис.1): ідентифікування інформаційних активів, ідентифікування уразливостей, ідентифікування загроз. Їхня активність представляється при описанні взаємодії специфікаціями виконання.

Дані специфікації зображуються зафарбованими вертикальними прямокутниками. Характеризуються настанням подій початку та завершення виконання.

При цьому виділяються три категорії взаємодій [2, 5, 17]:

– надсилання та отримання повідомлень, наприклад: обмін ідентифікованими інформаційними активами між лініями життя "Ідентифікування ризиків" (передавач повідомлення) та "Ідентифікування уразливостей" (приймач повідомлення);

– початок та кінець виконання дій і поведінки, наприклад: поведінка структурного елементу "Ідентифікування ризиків" починається за наяв-

ності вхідних даних про сферу, межі застосування систем управління інформаційною безпекою, критерії прийнятності та метод оцінювання ризиків. Завершується отриманням ідентифікованих ризиків у встановлених межах застосування систем управління інформаційною безпекою. Отримані дані відображаються повідомленням, що може передаватися між лініями життя "Ідентифікування ризиків" та "Аналізування ризиків";

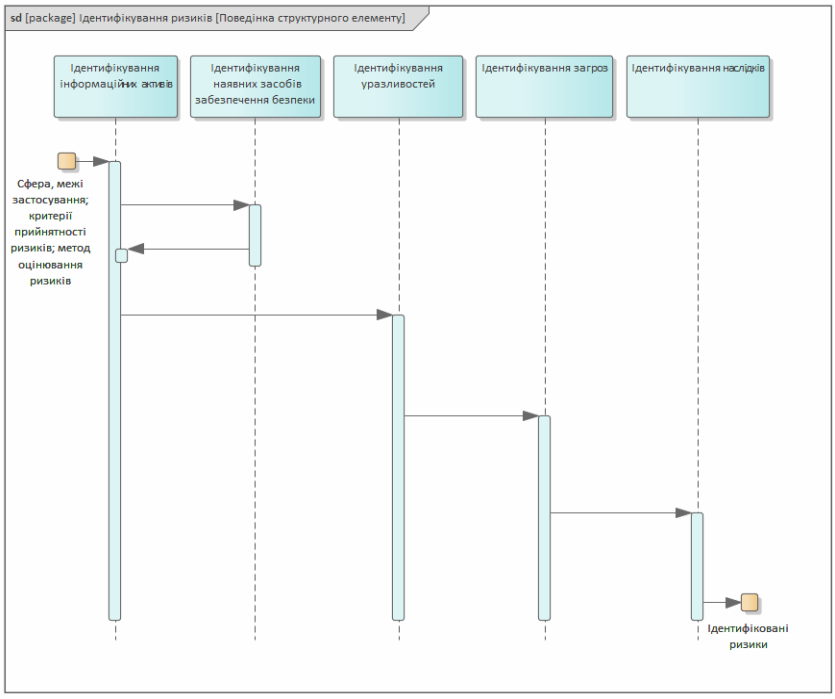

Рис. 2 Приклад специфікування поведінки структурних елементів систем управління інформаційною безпековою взаємодією

– створення і знищення екземплярів, наприклад: лінії життя "Ідентифікування наявних засобів забезпечення безпеки" з огляду на їхню відсутність при розробленні систем управління інформаційною безпекою.

Взаємодіяння між лініями життя відображається повідомленнями. Для їхнього зображення використовуються лінії зі стрілками на кінці (див. рис. 1). Ними спонукається або до передавання і приймання сигналів, або до початку виконання дій (діяльності). Водночас при ініціюванні виконання дії аргументи повідомлення можуть визначатися як передавачем, так і приймачем. У цьому випадку здебільшого очікується отримання відповіді від приймача [5, 16]. Наприклад (див. рис. 1), передаванням повідомлення від лінії життя "Ідентифікування інформаційних активів" ініціюється виконання дій лінією життя "Ідентифікування наявних засобів забезпечення безпеки". За результатами отримується повідомлення про наявні засоби забезпечення безпеки.

Це дозволяє продовжити проявляння поведінки "Ідентифікування інформаційних активів" стосовно лінії життя "Ідентифікування уразливостей". Загалом виокремлюються два різновиди повідомлень – синхронні та асинхронні.

Особливості використання кожного з них визначаються очікуваністю/неочікуваністю отримання відповіді від приймача [17]. Це унеможливлює проявляння поведінки лініями життя при передаванні синхронних повідомлень допоки не отримується відповідь на них.

Змінення станів структурними елементами або системами управління інформаційною безпекою при настанні визначених умов відображається кінцевими автоматами. Їхнє використання орієнтоване на описання поведінки за схемою "стан – перехід". Це супроводжується створенням і знищенням

об'єктів, зміненням значень їхніх атрибутів, генеруванням повідомлень між ними.

Тож поведінка представляється послідовним проходженням вершин графу кінцевого автомату. Направленість відношення між ними задається дугами переходів.

Тому змінення станів розглядається як окремий аспект синтезування поведінки систем управління інформаційною безпекою і специфікується діаграмою кінцевих автоматів у графічній нотації SysML зі заголовком [5, 16, 17]:

stm [різновид елементу моделі] ім'я кінцевого автомату [ім'я діаграми], наприклад [2, 17, 18], див. рис. 3:

stm [StateMachine] Ідентифікування ризиків [Поведінка структурного елементу].

Стан структурних елементів або систем управління інформаційною безпекою відображається вершинами графу кінцевого автомату.

Для їхнього зображення на діаграмі використовується прямокутник зі заокругленими кутами (див. рис. 3), наприклад: ідентифікування уразливостей, ідентифікування загроз, ідентифікуванн аслідків. Кожним станом можуть визначатися такі варіанти поведінки: входження/завершення, виконання. Останній варіант можливий за умови входження у стан і триває до його завершення. Крім цього поширене використання допоміжних вершин або псевдо станів. Серед них зображення початкового псевдо стану.

Цією вершиною відображається стан-джерело з якого починається представлення поведінки структурних елементів або систем управління інформаційною безпекою. Для завершення змінення станів використовується кінцевий псевдо стан. Однак, їхнім використанням обмежується представлення альтернативних (наприклад, або прийняти, або обробити ризики) і паралельних (наприклад, ідентифікувати загрози та наслідки) варіанів поведінки кінцевого автомату. Дані обмеження долаються завдяки зображенню вершин вибору/з'єднання і розділення/злиття.

Першою парою реалізується можливість представлення вхідного переходу двома або більше альтернативними шляхами, а другою – представлення вхідного переходу двома або більше паралельними шляхами.

Змінення станів структурних елементів або систем управління інформаційною безпекою визначається переходами. Характерною особливістю такого визначення є можливість виконання наступної події після завершення поточної.

Це означає, що вразливості ідентифікуються після визначення інформаційних активів і наявних засобів забезпечення безпеки в межах застосування систем управління інформаційною безпекою.

Для врахування даних особливостей використовуються від одного до декількох тригерів. Ними визначаються умови переходу з одного стану в інший, а саме:

1. Подія сигналу вказує на надходження асинхронного повідомлення. Вона може супроводжуватися визначенням аргументів переходу. Наприклад, перехід від стану "Ідентифікування інформаційних активів" до "Ідентифікування уразливостей" без потреби відправлення відповіді.

2. Подія часу вказує на проміжок часу від настання поточного стану. Насамперед відносно моменту його введення. Наприклад, визначення часового проміжку перебування структурного елементу "Ідентифікування ризиків" в одному зі станів як-от "Ідентифікування загроз".

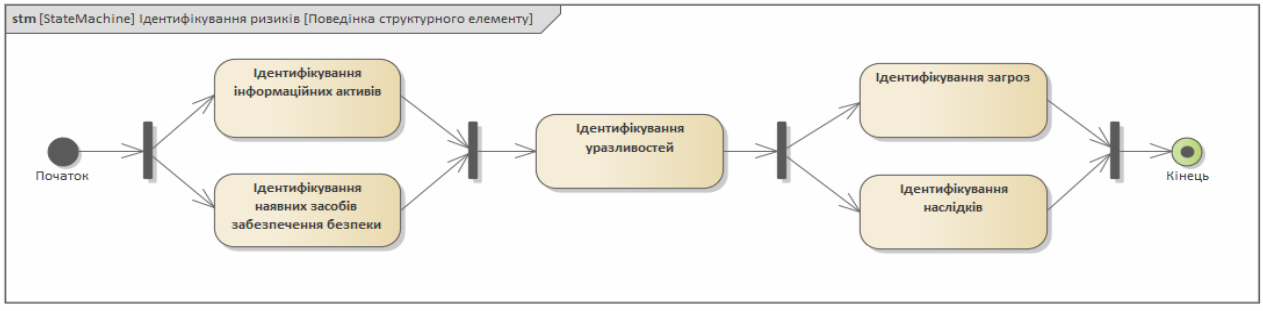

Рис. 3 Приклад специфікування поведінки структурних елементів систем управління інформаційною безпекою кінцевим автоматом

3. Подія змінення вказує на виконання певної умови за якої можливе змінення станів. При цьому припускається існування множини значень атрибутів такого переходу. Наприклад, за умови перевищення оцінками ризику їхнього прийнятного значенням здійснюється перехід від стану "Зіставлення оцінок ризиків" до "Оброблення ризиків".

4. Подія виклику вказує на надсилання запиту ініціювання переходів і, як наслідок, потрібних дій. Нею можливе оброблення як синхронних, так і асинхронних запитів. Наприклад, ініціювання синхронним запитом переходу в стан "Ідентифікування наявних засобів забезпечення безпеки". Це спонукає до отримання відповіді про їх наявність або відсутність.

ВИСНОВКИ

Отже, встановлено особливості діяльності систем управління інформаційною безпекою методом синтезування їхньої поведінки. Виокремлено три аспекти її прояву, зокрема: послідовності дій структурних елементів, умов їхнього виконання, потоку об'єктів; часових особливостей передавання і приймання об'єктів між структурними елементами; змінення станів структурними елементами при настанні визначених умов. Моделювання такої поведінки зведено до використання діаграм діяльності, послідовності та кінцевого автомату в графічній нотації SysML.

Діаграмою діяльності специфіковано поведінку зі збереження конфіденційності, цілісності та доступності інформації в організаціях через контрольовану послідовність дій. Часові особливості передавання і приймання об'єктів між структурними елементами відображено завдяки їхньому взаємодіянню.

Воно зведено до встановлення послідовності обміну повідомленнями між лініями життя як окремими сутностями. Тоді як змінення станів описано за схемою "стан – перехід" і представлено послідовним проходженням вершин графу кінцевого автомату направленими дугами переходів.

ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У перспективах подальших досліджень планується розробити метод визначення зрілості систем управління інформаційною безпекою. Завдяки окресленню відповідних рівнів можливе встановлення спроможності організацій до їхнього розроблення і, як наслідок, гарантування зацікавленим сторонам належності поводження з ризиками.

ЛІТЕРАТУРА

[1] ISO/IEC 27001:2013. *Information technology. Security techniques. Information security management systems. Requirements*. [Second edition 2013-09-25; confirmed 2019-06-03]. [Електронний ресурс] – Режим доступу до ресурсу: https://www.iso.org/standard /54534.html.

[2] Мохор В. В., Цуркан В. В. Поведінкові аспекти системи управління інформаційною безпекою. *Інформаційна безпека та інформаційні технології : тези доповідей міжнар. наук.-практ. конф.*, м. Кропивницький, 2–3 квіт. 2020 р. Кропивницький, 2020. С. 18.

[3] *OMG Systems Modeling Language* (OMG SysML™). [Version 1.6 2019-11-01]. [Електронний ресурс] – Режим доступу до ресурсу: https://sysml.org/res/docs/specs/OMGSysML-v1.6-19-11-01.pdf.

[4] Ларман К. *Применение UML 2.0 и шаблонов проектирования. Практическое руководство*. Москва: ООО "И.Д. Вильямс", 2013.- 736 с.

[5] Леоненков А. В. *Самоучитель UML 2*. Санкт-Петербург: БХВ-Петербург, 2007. - 576 с.

[6] ISO/IEC 27000:2018. *Information technology. Security techniques. Information security management systems. Overview and vocabulary*. [Fifth edition 2018-02-07]. [Електронний ресурс] – Режим доступу до ресурсу: https://www.iso.org/standard/73906.html.

[7] Безштанько В. М., Зінченко Я. В. Методи розв'язання лінійних діофантових рівнянь в задачах моделювання процесів в компонентах системи управління інформаційної безпеки. *Сучасний захист інформації*, 2015. № 1. С. 10–18.

[8] Haufe K., Colomo-Palacios R., Dzombeta S., Brandis K., Stanchev V. ISMS core processes : A study. *Procedia Computer Science*. 2016. Vol. 100. pp. 339–346.

[9] Мохор В., Бакалинский А., Богданов А., Цуркан В. Дескриптивный анализ аналогий между системами управления информационной безопасностью и массового обслуживания. *Захист інформації*. Том 19, № 2. С. 119–126.

[10] Sirisom P., Payakpate J., Wongthai W. A System

Design for the Measurement and Evaluation of the Communications Security Domain in ISO 27001:2013 Using an Ontology / K. Kim, N. Joukov (eds). Information Science and Applications. ICISA 2017 : *Lecture Notes in Electrical Engineering. Vol. 424. Springer*, Singapore, 2017. pp. 257–265.

[11] Дудикевич В. Б., Микитин Г. В., Ребець А. І. До проблеми управління комплексною системою безпеки кіберфізичних систем. *Вісник Національного університету "Львівська політехніка". Серія: Інформаційні системи та мережі*. 2018. № 901. С. 10–21.

[12] Humphreys E. The Future Landscape of ISMS Standards. *Datenschutz Datensich*. 2018. Vol. 42, iss. 7. pp. 421–423.

[13] Коломыцев М., Носок С., Тоцкий Р. Сравнительный анализ моделей оценки зрелости информационной безопасности. *Захист інформації*. 2019. Том 21, № 4. С. 224–232.

[14] Diamantopoulou V., Tsohou A., Karyda M. General Data Protection Regulation and ISO/IEC 27001:2013: Synergies of Activities Towards Organisations' Compliance / S. Gritzalis, E. Weippl, S. Katsikas, G. Anderst-Kotsis, A. Tjoa, I. Khalil (eds). Trust, Privacy and Security in Digital Business. TrustBus 2019 : *Lecture Notes in Computer Science*. Vol. 11711. Springer, Cham, 2019. pp. 94–109.

[15] Цуркан В. В. Метод функціонального аналізування систем управління інформаційною безпекою. *Кібербезпека: освіта, наука, техніка*. 2020. Том 4,№ 8. С. 192–201.

[16] *OMG Systems Modeling Language (OMG SysML™)*. [Version 1.6 2019-11-01]. [Електронний ресурс] – Режим доступу до ресурсу: https:// sysml.org/.res/docs/specs/OMGSys ML-v1.6-19-11-01.pdf.

[17] Moore A., Steiner R. A *Practical Guide to SysML*. The Systems Modeling Language. Waltham: Elsevier, 2015. 640 p.

[18] *Model based systems engineering with Sparx Systems Enterprise Architect*. [Електронний ресурс] – Режим доступу до ресурсу: https:// sparxsystems.com/ resources/user-guides /.

МЕТОД СИНТЕЗИРОВАНИЯ ПОВЕДЕНИЯ СИСТЕМ УПРАВЛЕНИЯ ІНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Определено поведение систем управления информационной безопасностью через деятельность по сохранению конфиденциальности, целостности и доступности информации в организациях. Охарактеризовано ее со стороны структурных элементов последовательностью действий относительно обращения с рисками. Установлено предусловия такой деятельности. Среди них выделены определения внешних и внутренних обстоятельств деятельности организаций, потребности и ожидания заинтересованных сторон, сферы и границ применения систем управления информационной безопасностью, установление критериев приемлемости и выбор метода оценивания рисков. Предложено синтезирование поведения систем управления информационной безопасностью в трех аспектах. Для этого использованы диаграммы деятельности, последовательности и конечного автомата в графической нотации SysML. Каждой из обозначенных диаграмм синтезировано ее особенности как отдельных структурных элементов, так и систем управления информационной безопасностью в целом. Диаграммой деятельности специфицировано поведение через контролируемую последовательность действий. Характерной особенностью такой спецификации является ориентированность на установление условий их выполнения. В тоже время представление объектов как входных и выходных данных каждого действия. Временные особенности передачи и приема объектов между структурными элементами систем управления информационной безопасностью отображено диаграммой последовательности через их взаимодействие. Основой такого взаимодействия является установление последовательности обмена сообщениями. Его осуществление возможно либо между системами управления информационной безопасностью и их средой, либо между структурными элементами на любом уровне иерархии. В этом случае как структурные элементы, так и системы управления информационной безопасностью толкуются отдельными сущностями – линиями жизни. Взаимодействие между ними представляется обменом сообщениями. Изменение состояний при наступлении определенных условий отображено диаграммой конечного автомата. Ее использование ориентировано на описание поведения по схеме "состояние – переход". Это сопровождается созданием и уничтожением объектов, изменением значений их атрибутов, генерацией сообщений между ними. Таким образом, поведение представлено последовательным прохождением вершин графа конечного автомата направленными дугами. Благодаря этому установлены особенности деятельности систем управления информационной безопасностью в организациях методом синтезирования их поведения.

Ключевые слова: система управления информационной безопасностью, поведение, синтезирование поведения, деятельность, взаимодействие, конечный автомат, SysML.

METHOD OF INFORMATION SECURITY MANAGEMENT SYSTEMS BEHAVIOR SYNTHESIZING

The behavior of information security management systems is determined due to activities to keep the confidentiality, integrity, and availability of information in organizations. It is characterized by a sequence of risk management actions on the part of structural elements. The prerequisites for such activities have been established. Among them, definitions of external and internal factors of organizations' activities, needs, and expectations of stakeholders, scope and limits of information security management systems application, the establishment of acceptability criteria, and selection of risk assessment methods are highlighted. Taking this into account, it was proposed to synthesize the behavior of information security management systems in three aspects. To do this, the activity, sequence, and state machine diagrams in SysML graphic notation are used. Each of the above diagrams synthesized its features as individual structural elements, and information security management systems in general. Activity diagrams specify behavior through a controlled sequence of actions. The characteristic feature of this specification is the orientation towards the establishment of conditions for their implementation. At the same time, represent objects as inputs and outputs of each action. Time features of transmission and reception of objects between structural elements of information security management systems are reflected in the sequence diagram through their interactions. The basis of such interaction is to establish a sequence of message exchange. It is possible either between information security management systems and their environment or between structural elements at any hierarchy level. In this case, both structural elements and information security management systems are interpreted by individual entities – lifelines. The interaction between them is represented by the exchange of messages. The change in states when certain conditions occur is reflected in the state machine diagram. Its use is aimed at describing the behavior according to the "state–transition" scheme. This is accompanied by the creation and destruction of objects, change of their attribute values, generation of messages between them. Therefore, the behavior is represented by the sequential passage of the vertices of a finite automaton graph by directed arcs. Due to this, the activity features of information security management systems in organizations by synthesizing their behavior were established.

Keywords: information security management systems, behavioral, behavior synthesizing, activity, interaction, state machine, SysML.

Цуркан Василь Васильович, кандидат технічних наук, доцент, старший науковий співробітник, Інститут проблем моделювання в енергетиці імені Г.Є. Пухова Національної академії наук України.
E-mail: v.v.tsurkan@gmail.com.
Orcid ID: 0000-0003-1352-042X.
Цуркан Василий Васильевич, кандидат технических наук, доцент, старший научный сотрудник, Институт проблем моделирования в энергетике имени Г.Е. Пухова Национальной академии наук Украины.
Tsurkan Vasyl, candidate of technical sciences, associate professor, senior researcher, Pukhov Institute for Modeling in Energy Engineering of National Academy of Sciences of Ukraine.