УДК 004.056 DOI:10.31673/2412-4338.2021.017987

Гайдур Г.І., Гахов С.О. *Державний університет телекомунікацій, Київ*

ТЕОРЕТИЧНИЙ ПІДХІД ДО ВИРІШЕННЯ ПРОБЛЕМИ ВИЯВЛЕННЯ ШКІДЛИВИХ ПРОЦЕСІВ НА ОСНОВІ АНАЛІЗУ СТАНІВ ЛОГІЧНОГО ОБ'ЄКТА ІНФОРМАЦІЙНОЇ СИСТЕМИ

Анотація: *Сьогодні інформаційні системи організацій функціонують в умовах наявності вразливостей та їх експлуатації зловмисниками. Про це свідчать звіти світових компаній щодо аналізу інформації про загрози, а також пропозицій проведення відповідних заходів кібербезпеки. Незважаючи на застосовувані заходи забезпечення кібербезпеки даних систем, спостерігається постійне зростання числа виявлених вразливостей. Одним із шляхів вирішення даної проблеми є здійснення моніторингу стану безпеки функціональних компонентів інформаційних систем під час обробки даних та їх обміну.*

Встановлено причини виникнення шкідливих процесів функціонування інформаційних систем організацій. Головною причиною наявності вразливостей є властивості функціональних компонентів даної інформаційної системи.

Проведено аналіз існуючих методів виявлення вторгнень в інформаційні системи організацій. Застосування методу виявлення на основі аналізу станів протоколу надає можливості визначати і відслідковувати стан мережевих, транспортних і прикладних протоколів, які мають поняття стану.

Запропоновано теоретичний підхід до вирішення проблеми виявлення шкідливих процесів на основі аналізу станів логічного об'єкта інформаційної системи як частини системи забезпечення кібербезпеки інформаційної системи організації.

Реалізація даного теоретичного підходу дозволить правильно поставити та вирішити завдання виявлення шкідливих процесів на основі аналізу станів логічного об'єкта інформаційної системи в режимі реального часу та, у разі зміни стану безпеки даного логічного об'єкта під час впливу на нього деструктивних нецільових процесів, реагувати на такі події та відновлювати його безпечний стан.

Ключові слова: *вразливість інформаційної системи, безпека інформаційної системи, моніторинг стану логічного об'єкта інформаційної системи.*

Haidur H.I., Gakhov S.O. *State University of Telecommunications, Kyiv*

THEORETICAL APPROACH TO SOLVING THE PROBLEM OF DETECTING MALICIOUS PROCESSES BASED ON THE ANALYSIS OF THE STATES OF THE ENTITY OF THE INFORMATION SYSTEM

Abstract: *Today information systems of organizations operate in conditions of vulnerabilities and their exploitation by hackers. This is evidenced by the reports of global companies on the analysis of information on threats, as well as proposals for the implementation of appropriate cybersecurity measures. Despite the measures taken to ensure the cybersecurity of these systems, the number of identified vulnerabilities is constantly increasing. One of the ways to solve this problem is to monitor the security status of the functional components of information systems during data processing and exchange.*

The reasons for the occurrence of malicious processes in the functioning of information systems of organizations have been established. The main reason for the presence of vulnerabilities is the properties of the functional components of this information system.

The analysis of existing methods for detecting intrusions into information systems of organizations is carried out. The application of the discovery method based on the analysis of protocol states makes it possible to determine and monitor the state of network, transport and application protocols that have state concepts.

A theoretical approach to solving the problem of detecting malicious processes is proposed, based on the analysis of the states of the entity of an information system as part of the cybersecurity system of an organization's information system.

The implementation of this theoretical approach will make it possible to correctly formulate and solve the problem of detecting malicious processes based on the analysis of the states of the entity of the information system in real time. And in the event of a change in security, the state of this entity, when it is affected by destructive non-target processes, react to such events and restore its safe state.

Keywords: *vulnerability of the information system, security of the information system, monitoring the state of the entity of the information system.*

Гайдур Г.И., Гахов С.А. *Государственный университет телекоммуникаций, Киев*

ТЕОРЕТИЧЕСКИЙ ПОДХОД К РЕШЕНИЮ ПРОБЛЕМЫ ОБНАРУЖЕНИЯ ВРЕДОНОСНЫХ ПРОЦЕССОВ НА ОСНОВЕ АНАЛИЗА СОСТОЯНИЙ ЛОГИЧЕСКОГО ОБЪЕКТА ИНФОРМАЦИОННОЙ СИСТЕМЫ

Аннотация: *Сегодня информационные системы организаций функционируют в условиях наличия уязвимостей и их эксплуатации злоумышленниками. Об этом свидетельствуют отчеты мировых компаний по анализу информации об угрозах, а также предложений проведения соответствующих мер обеспечения кибербезопасности. Несмотря на применяемые меры обеспечения кибербезопасности данных систем, наблюдается постоянный рост числа выявленных уязвимостей. Одним из путей решения данной проблемы является осуществление мониторинга состояния безопасности функциональных компонентов информационных систем во время обработки данных и их обмена.*

Установлены причины возникновения вредных процессов функционирования информационных систем организаций. Главной причиной наличия уязвимостей являются свойства функциональных компонентов данной информационной системы.

Проведен анализ существующих методов обнаружения вторжений в информационные системы организаций. Применение метода обнаружения на основе анализа состояний протокола предоставляет возможности определять и отслеживать состояние сетевых, транспортных и прикладных протоколов, которые имеют понятия состояния.

Предложено теоретический подход к решению проблемы обнаружения вредоносных процессов на основе анализа состояний логического объекта информационной системы как части системы обеспечения кибербезопасности информационной системы организации.

Реализация данного теоретического подхода позволит правильно поставить и решить задачу обнаружения вредоносных процессов на основе анализа состояний логического объекта информационной системы в режиме реального времени и, в случае изменения состояния безопасности данного логического объекта при воздействии на него деструктивных нецелевых процессов, реагировать на такие события и восстанавливать его безопасное состояние.

Ключевые слова: *уязвимость информационной системы, безопасность информационной системы, мониторинг состояния логического объекта информационной системы.*

1. Вступ

Вразливості інформаційних систем організацій та їх експлуатація зловмисниками становлять серйозну проблему для сучасних організацій різних галузей. Так, за даними IBM Security X-Force сканування і використання вразливостей інформаційних систем стали основним вектором їх зараження в 2020 році та складав 35 відс. загального числа інцидентів [1].

В [1] зазначається, що протягом 2020 року зловмисники частіше використовували вразливості виявлені раніше, що ймовірно пов’язано з труднощами постачальників програмних продуктів та організацій, які їх застосовують, в їх виправленні. Причиною широкого застосування зловмисниками сканування та використання вразливостей є те, що проведення такого роду атак зазвичай вимагає небагато ресурсів, їх можна автоматизувати та масштабувати для охоплення найрізноманітніших інформаційних систем [1].

За даними Microsoft [2] невиправлені вразливості є причиною кожного третього порушення у всьому світі. В результаті незахищених та невиправлених вразливостей організації терплять великих збитків. Як приклад, у 2017 році атака програма-вимагач WannaCry заразила більше 200 000 комп’ютерів в 150 країнах, завдавши збитків від сотень

мільйонів до мільярдів доларів. Хоча Microsoft випустила виправлення для закриття експлойта, велика частина поширення WannaCry припала на організації, які ще не встигли їх застосували [2].

За останні п'ять років загальна кількість вразливостей в продуктах Microsoft зросла на 181 відс. – до 1268 вразливостей у 2020 році [2]. Тому, у міру збільшення кількості вразливостей зловмисники отримують доступ до постійно зростаючого "каталогу експлойтів", що приводе до експоненціального збільшення поверхні атаки з року в рік [2].

Фахівці зазначають, що вразливості програмного забезпечення, які входять у The 2021 CWE Top 25 [3], небезпечні тому, що їх часто легко знайти та використати для досягнення злочинних цілей.

Отже, наявність та зростання числа вразливостей інформаційних систем організацій є серйозним викликом як для фахівців з кібербезпеки, так і організацій в цілому. Тож констатуємо, що існує проблема виявлення та усунення вразливостей. Ця проблема є складною та немає остаточного вирішення на даний момент.

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.

2. Аналіз літературних даних і постановка задачі

В рекомендаціях NIST [4] 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 [4].

Для виявлення та запобігання вторгненням в інформаційних системах організацій розробляються та застосовуються відповідні системи кібербезпеки: системи SIEM (Security Information and Event Management), системи EDR (Endpoint Detection and Response), системи виявлення й запобігання вторгненням, міжмережеві екрани з функціями виявлення й запобігання вторгненням тощо.

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

виявлення на основі сигнатур (Signature-Based Detection);

виявлення на основі аномалій (Anomaly-Based Detection);

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

Сутність методу виявлення на основі сигнатур полягає в порівнянні сигнатур із характеристиками подій, які спостерігаються, для виявлення можливих інцидентів. В рекомендаціях NIST [4] зазначається, що метод виявлення на основі сигнатур є дуже ефективним при реалізації відомих загроз, але в значній мірі є неефективним при реалізації раніше невідомих загроз, загроз, які замасковані за допомогою методів ухилення, та різних варіантів відомих загроз.

В [4] зазначається, що "технології виявлення на основі сигнатур погано сприймають процеси функціонування за мережевими або прикладними протоколами і не можуть відстежувати та ідентифікувати стан їх складних зв'язків". У них також відсутня можливість запам'ятовувати попередні запити при обробці поточного запиту. Ці недоліки методу виявлення на основі сигнатур не дозволяють виявляти атаки, що складаються з декількох подій, якщо жодна з подій не містить чіткої ознаки даної атаки [4].

Сутність методу виявлення на основі аномалій полягає в порівнянні ознак того, яка активність вважається нормальною, з характеристиками подій, які спостерігаються, для виявлення значних відхилень. Система виявлення й запобігання вторгненням, в якій реалізується метод виявлення на основі аномалій, має профілі, які відображають ознаки нормальної поведінки таких сутностей, як користувачі, хости, мережеві з'єднання або додатки.

Профілі розробляються за результатами спостереження характеристик типової

активності в інформаційній системі протягом певного періоду часу. В системі виявлення вторгнень застосовуються статистичні методи для порівняння характеристик поточної активності з граничними значеннями профіля та, у разі їх перевищення, відбувається попередження адміністратора про аномалії [4]. Профілі можуть бути розроблені за багатьма поведінковими ознаками, які мають місце, таких як кількість електронних листів, відправлених користувачем, кількість невдалих спроб входу в систему для хоста і рівень використання процесора хоста в заданий період часу тощо.

Основна перевага методу виявлення на основі аномалій полягає в тому, що він може бути дуже ефективним при виявленні реалізацій нових загроз, наприклад, зараження невідомим шкідливим програмним забезпеченням та його активність, яка значно відрізнятися від визначених профілів нормальної активності для конкретної інформаційної системи. Необхідно підкреслити, оскільки системи і мережі змінюються з часом, відповідні характеристики нормальної поведінки також змінюються, що викликає необхідність корегування або створення нових профілів нормальної поведінки системи.

Недоліком методу виявлення на основі аномалій є його слабкість щодо виявлення шкідливої активності низької інтенсивності, а також існує можливість випадкового включення шкідливої активності під час визначення характеристик початкових профілів, що призведе до неможливості її не визначення системою виявлення у подальшому.

Унікальна поведінка інформаційної системи організації зумовлює складність точного визначення профілю у методі виявлення на основі аномалій та, як наслідок, наявність великої кількісті помилкових спрацьовувань при застосуванні такої системи виявлення.

Інша проблема використання методу виявлення аномалій полягає в тому, що ознаки аномалії є загальними показниками поведінки інформаційної системи організації, наприклад, середнє значення частоти подій в секунду протягом однієї хвилини або пікове значення об’єму потоку протягом однієї хвилини. Даний момент ускладнює роботу аналітиків безпеки у визначенні причин та дійсності (хибності) виявленої системою аномалії.

Сутність методу виявлення на основі аналізу станів протоколу полягає у порівнянні попередньо визначених профілів загальноприйнятих визначень правильної роботи протоколу для кожного його стану з подіями, які спостерігаються, для виявлення відхилень [4]. На відміну від методу виявлення на основі аномалій, в якому використовуються профілі, які специфічні для хоста або мережі, метод виявлення на основі аналізу станів протоколу базується на універсальному профілі розробленому постачальником [4].

По-перше, застосування методу виявлення на основі аналізу станів протоколу надає можливості визначати і відслідковувати стан мережевих, транспортних і прикладних протоколів, які мають поняття стану [4]. У [4] зазначається, що виконання більшості команд в нерозпізнаному стані буде вважатися підозрілою активністю, але в розпізнаному стані протоколу виконання більшості команд вважається нешкідливим.

По-друге, застосування методу виявлення на основі аналізу станів протоколу надає можливості ідентифікувати несподівані послідовності команд, наприклад, багаторазовий запуск однієї і тієї ж команди або видачу команди без видачі попередньої команди, від якої вона залежить.

У методах виявлення на основі аналізу станів протоколу використовуються моделі, в основі яких покладено стандарти протоколів від постачальників програмного забезпечення і органів стандартизації (наприклад, Internet Engineering Task Force (IETF), Request for Comments (RFC)) [4].

Багато стандартів не є вичерпними для пояснення деталей протоколу, що викликає розбіжності між реалізаціями [4]. Крім того, багато постачальників або порушують стандарти, або додають пропрієтарні функції, деякі з яких можуть замінювати функції, які визначені відповідними стандартами. Про пропрієтарні протоколи іноді недоступна повна інформація, що ускладнює проведення всебічного і точного аналізу для реалізацій у системах виявлення інцидентів.

В [4] зазначається, що моделі протоколів також зазвичай враховують 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.

Основним недоліком методів виявлення на основі аналізу станів протоколу є те, що вони потребують багато обчислювальних ресурсів через складність аналізу та необхідність відстеження стану для багатьох одночасних сеансів [4]. Інша серйозна проблема полягає в тому, що методи виявлення на основі аналізу станів протоколу не можуть виявляти атаки, які не порушують характеристики загальноприйнятої поведінки протоколу, наприклад, виконання множини безпечних дій за короткий період часу, що викликають відмову в обслуговуванні [4]. Ще одна проблема полягає в тому, що модель протоколу, що використовується системою виявлення, може конфліктувати зі способом реалізації протоколу в конкретних версіях конкретних програм і операційних систем або з тим, як взаємодіють різні клієнтські і серверні реалізації протоколу [4].

Існуючі проблеми щодо виявлення вторгнень в інформаційних системах організацій, недоліки існуючих методів виявлення визначають їх актуальність та спонукають нас до подальшого дослідження даних питань.

3. Мета і задачі дослідження

Під час вирішення проблеми забезпечення кібербезпеки необхідно передбачати в яких умовах буде застосовуватися інформаційна система організації. Наявність відомих та невідомих (невиявлених на даний момент часу) вразливостей, а також потенційна можливість їх експлуатації зловмисниками є реаліями застосування інформаційних систем організацій. Одним із шляхів вирішення даної проблеми є виявлення шкідливих процесів на основі аналізу станів функціональних компонентів інформаційних систем. Тому, визначаємо за мету даної роботи розроблення теоретичного підходу до вирішення проблеми виявлення шкідливих процесів на основі аналізу станів логічного об’єкта інформаційної системи.

4. Результати дослідження

Для сучасних інформаційних систем організацій характерні структурна масштабованість; територіальна і часова рознесеність; функціональна розширюваність; різноманітність цілей їх створення, користувачів, інформаційних ресурсів і технологій, що визначає все зростаючу їх складність [5]. Необхідно підкреслити, що інформаційну систему організації необхідно розглядати як цілісну систему – окрему сутність в кіберпросторі, яка повинна виконувати функції за призначенням та проявляти властивості функціональної стійкості в умовах деструктивних кібернетичних впливів.

Інформаційна система організації має динамічний, постійно змінюваний, мінливий характер. Інформаційну систему організації можна уявити як множину функціональних компонентів, які з’єднуються між собою відповідними зв’язками для реалізації складної функції обробки та обміну даними, що становить зміст відповідної інформаційної технології для задоволення різноманітних потреб людей та бізнесу. Те, як реалізується відповідна інформаційна технологія в інформаційній системі організації має визначальне значення для забезпечення кібербезпеки даної системи та процесів її функціонування.

Необхідно підкреслити, що *вразливість* є необхідною умовою виникнення шкідливого процесу в середовищі інформаційної системи організації. Носієм даного шкідливого процесу будуть функціональні компоненти самої інформаційної системи, та, необов’язково, функціональні компоненти, які втілені зловмисником в дану інформаційну систему. При цьому, шкідливий процес, який виникає, змінює стан інформаційної системи та переводить його з безпечного в небезпечний.

Було встановлено, що основними причинами наявності вразливостей та виникнення шкідливих процесів функціонування інформаційних систем організацій є [5]:

– властивості функціональних компонентів даної інформаційної системи;

– властивості впроваджених зловмисником функціональних компонентів в дану інформаційну систему;

– переходи інформаційної системи в небезпечний стан внаслідок ненавмисних дій

користувачів.

Концептуальну основу побудови систем моніторингу стану безпеки та реагування на інциденти безпеки інформаційної системи організації становить еталонна модель взаємодії відкритих систем, яка представляє собою визначені базові елементи відкритих систем і основні рішення, пов'язані з їх організацією і функціонуванням [6].

Відповідно до концепції взаємодії відкритих систем реальна система являє собою комп'ютер або сукупність декількох комп'ютерів, відповідного програмного забезпечення, периферійного обладнання, терміналів, операторів, фізичних процесів, засобів передачі даних тощо, що утворює повністю автономну систему, здатну обробляти дані та обмінюватися ними [6].

У реальній відкритій системі *прикладний процес* являє собою застосування сукупності ресурсів, які задіяні для реалізації функцій, пов'язаних з обробкою даних та їх обміном. Також, прикладний процес може утворювати свої взаємозв'язки з іншими прикладними процесами для досягнення часткової мети обробки даних [6].

Відповідно до [6], під *протоколом* розуміється набір правил і форматів (семантичних і синтаксичних), що визначають процедури зв'язку логічних об'єктів при виконанні ними функцій. Тому, назва "stateful protocol analysis methods", на наш погляд, є не зовсім коректною. У той же час, 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 функціональний компонент системи, що реалізує множину функцій, певних для даного рівня.

Розглядаючи процеси функціонування інформаційної системи організації можна виділити рівні обробки даних та обміну даними, а також можливі способи кібернетичного впливу зловмисника з точки зору окремого *i*-го хоста даної системи. Характерні процеси функціонування інформаційної системи організації, носіями яких виступають відповідні утворювані функціональні системи, та типові способи атаки зловмисника, які породжують відповідні шкідливі процеси схематично представлено на рис. 1.

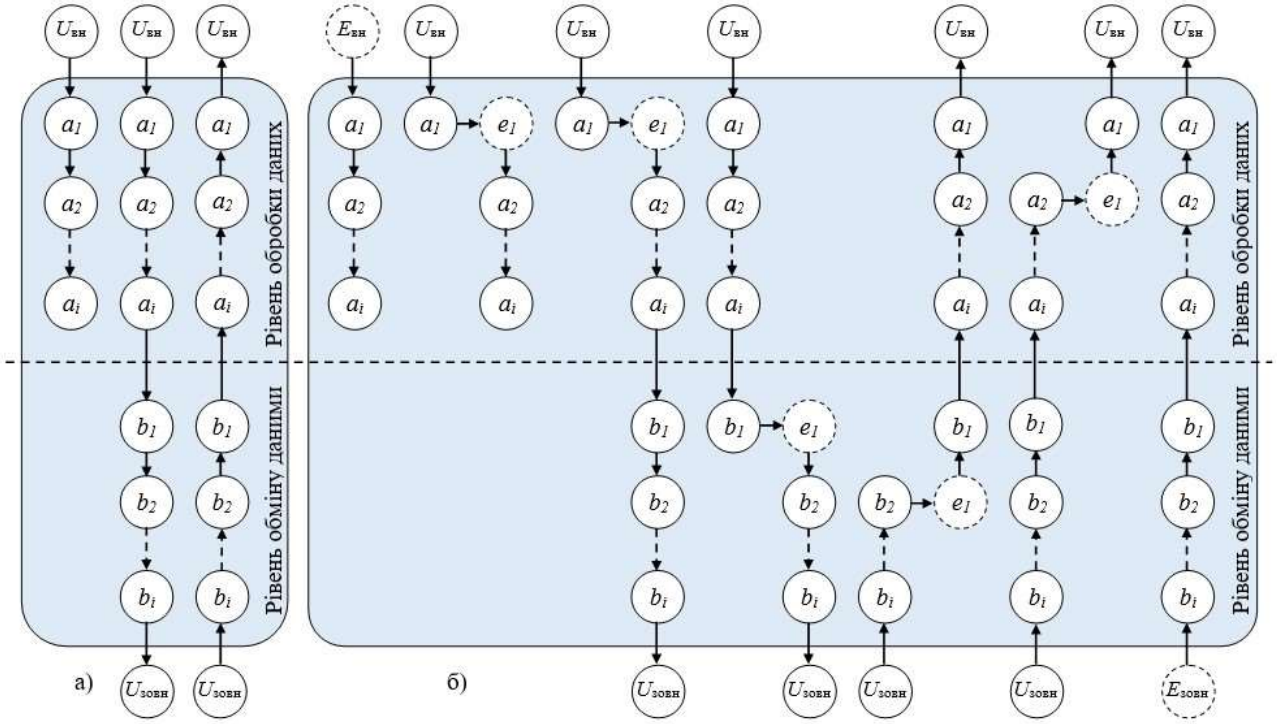

Рис. 1. Характерні процеси функціонування *i*-го хоста інформаційної системи організації (а) та можливі типові способи атаки зловмисника на процеси функціонування *i*-го хоста (б)

Позначки на рис. 1 застосовуються у такому значенні: $U_{вн}$ – внутрішній користувач

системи (людина, яка безпосередньо знаходиться за комп'ютером, розглядається як функціональний компонент системи), a_i – функціональний компонент системи рівня обробки даних, b_i – функціональний компонент системи рівня обміну даними, $U_{\text{зовн}}$ – зовнішній користувач системи (розглядається як функціональний компонент системи, який не входять до складу даного *i*-го хоста інформаційної системи організації), $E_{\text{вн}}$ – внутрішній зловмисник системи (людина, яка безпосередньо знаходиться за комп'ютером, розглядається як функціональний компонент системи), $E_{\text{зовн}}$ – зовнішній зловмисник системи (розглядається як функціональний компонент системи, який не входять до складу даного *i*-го хоста інформаційної системи організації), e_i – функціональний компонент, втілений зловмисником.

Отже, необхідно забезпечувати функціонування інформаційної системи організації в умовах кібернетичних впливів таким чином, щоб у ній утворювалися тільки ті функціональні системи та виникали тільки ті процеси, які відповідають цілям створення даної системи. Якщо у функціональному компоненті системи (логічному об'єкті) виникають тільки процеси, які відповідають цілям створення даної системи, то компонент буде перебувати у дозволеному стані – стані безпеки.

Перебування логічного об'єкта у дозволеному стані визначає його стан безпеки. У свою чергу, стан безпеки інформаційної системи визначається станом безпеки її функціональних компонентів.

Необхідно підкреслити, що не можливо оцінити в рамках самої системи в якому стані перебуває функціональний компонент системи. Дане завдання можна вирішити шляхом моніторингу стану безпеки функціональних компонентів системи. Для цього необхідно розробити та створити зовнішню (тобто ту, яка не входить до функціональної системи, що реалізує певну інформаційну технологію) *систему моніторингу стану безпеки*.

Необхідно відмітити, що під час дослідження інформаційної системи та процесів її функціонування, у тому числі компонентів системи, які реалізують функції захисту, необхідно чітко визначати кожну мету її функціонування. Під час реалізації даних цілей утворюються відповідні функціональні системи (рис. 2), які складають певні специфічні множини функціональних компонентів (логічних об'єктів).

Виконання функцій ідентифікації та діагностування стану логічних об'єктів покладається на відповідні функціональні компоненти, які будемо називати агентами моніторингу (рис.2.) На агент моніторингу стану логічного об'єкта буде надходити вхідна послідовність даних, які відображають поточний стан обраного логічного об'єкта інформаційної системи та процесів його функціонування. Агент має реалізувати відповідну функцію, результатом якої є вихідна послідовність даних, яка буде відображати процес реагування на можливий деструктивний вплив.

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*. На рис. 2. показано можливі варіанти вирішення даного завдання з використанням автономних автоматичних агентів (зовнішніх систем), а саме:

– децентралізований моніторинг стану окремих визначених логічних об'єктів інформаційної системи (варіант а));

– централізований моніторинг стану визначеної множини логічних об'єктів окремого хоста інформаційної системи (варіант б));

– централізований моніторинг стану визначеної множини логічних об'єктів хостів інформаційної системи (варіант с)).

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 станів обраного логічного об'єкта інформаційної системи необхідно поставити та розв'язати низку задач, а саме:

– розробити метод побудови динамічної моделі функціонування логічного об'єкта за

відповідним протоколом, який забезпечить точність моделі функціонування обраного логічного об'єкта;

– розробити динамічну модель функціонування логічного об'єкта за відповідним протоколом та визначити його закон функціонування;

– розробити метод ідентифікації та діагностування стану безпеки логічного об'єкта інформаційної системи на основі його динамічної моделі;

– на основі закону функціонування логічного об'єкта поставити та розв'язати задачі ідентифікації та діагностування його стану безпеки;

– обґрунтувати вимоги до процесів функціонування агента моніторингу стану обраного логічного об'єкта та реагування на його зміни.

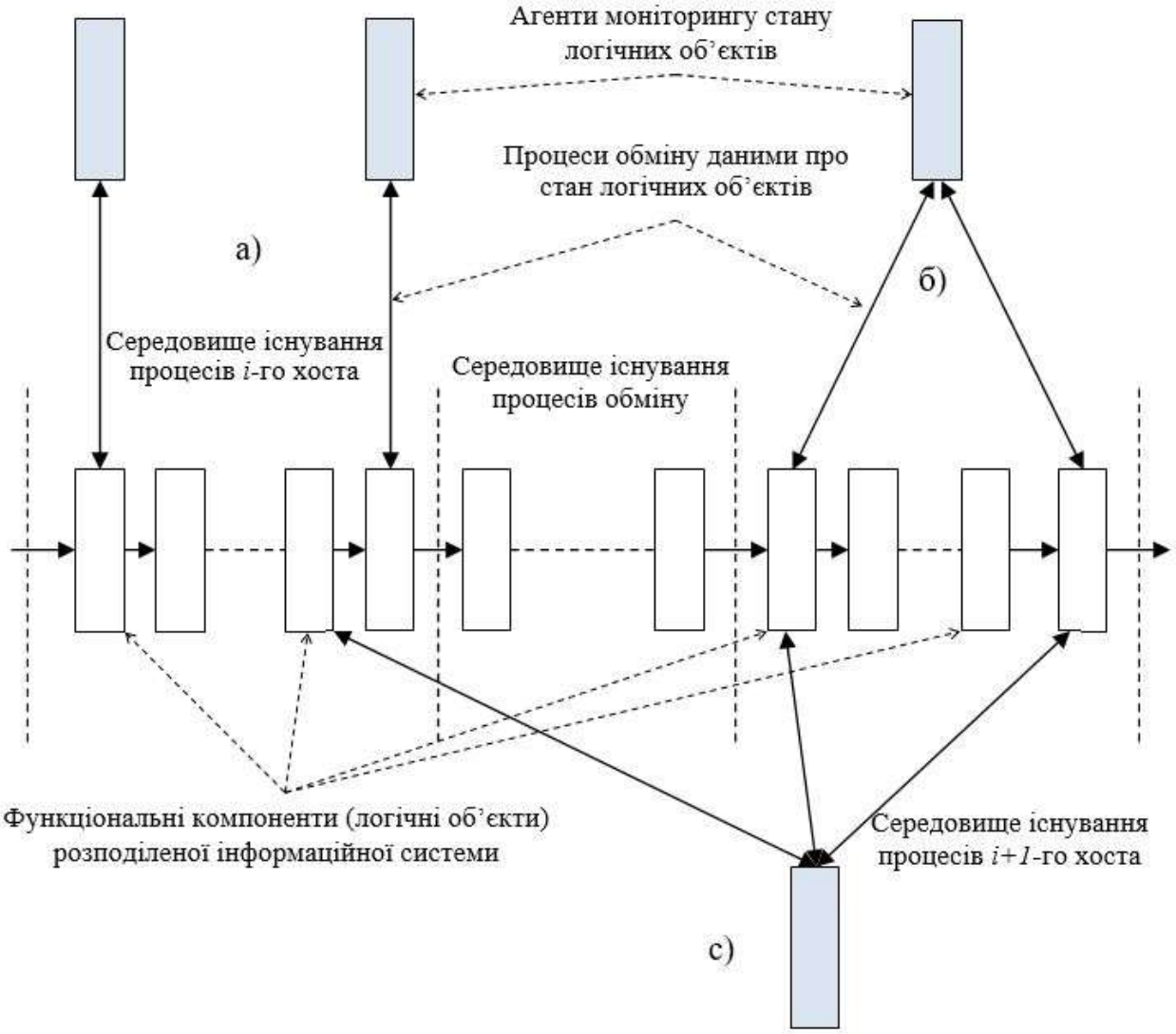

Рис. 2. Схема процесу функціонування розподіленої інформаційної системи та варіанти розміщення агентів моніторингу стану логічних об'єктів

Автоматизація процесів ідентифікації та діагностування стану безпеки логічного об'єкта інформаційної системи базується на алгоритмізації даних процесів. Це вимагає детального аналізу процесів функціонування логічного об'єкта, які будуть визначати зміст необхідних та достатніх умов ідентифікації та діагностування його стану безпеки. Тому, основою для постановки та розв'язку задач ідентифікації та діагностування стану безпеки логічного об'єкта є динамічна модель функціонування логічного об'єкта та визначення закону його функціонування.

Для одержання логічного виведення необхідні відповідні правила виведення, які враховують можливості математичної моделі логічного об'єкта та мету, яка переслідується.

Алгоритмізація процесів ідентифікації та діагностування стану безпеки логічного об'єкта інформаційної системи буде визначати передумови для створення саме автоматичного агенту для вирішення даних завдань.

Висновки

Для ефективної протидії кібернетичним впливам на інформаційні системи організацій необхідні інструменти автоматичного моніторингу, ідентифікації, діагностування та реагування на події безпеки. Ми вважаємо, що дана робота є корисною за умови передбачення та допущення наявності відомих та невідомих (невиявлених) вразливостей інформаційних систем організацій та їх функціональних компонентів.

В той же час, існує інший підхід до забезпечення стану безпеки інформаційних систем організацій та їх компонентів, який спирається на постановку та вирішення завдання проектування та створення саме безпечних компонентів та систем, тобто, які не мають вразливостей.

Застосування вищезгаданих підходів забезпечить створення та застосування якісно нових інформаційних систем організацій, які можна буде назвати саме захищеними.

Напрямками подальших досліджень щодо вирішення проблеми виявлення шкідливих процесів на основі аналізу станів обраного логічного об'єкта інформаційної системи є завдання поставлені в даній статті.

Список використаної літератури

1. X-Force Threat Intelligence Index 2021. IBM Security. 2021. https://www.ibm.com/downloads/cas/M1X3B7QG.

2. Microsoft Vulnerabilities Report 2021. Evolving Threats, The Dangers of Admin Rights & How To Address Them. BeyondTrust. 2021. https://www.beyondtrust.com/assets/documents/BeyondTrust-Microsoft-Vulnerabilities-Report-2021.pdf.

3. 2021 CWE Top 25 Most Dangerous Software Weaknesses. https://cwe.mitre.org/top25/archive/2021/2021_cwe_top25.html#methodology.

4. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-94. February 2007. p. 127. https://doi.org/10.6028/NIST.SP.800-94.

5. Гахов С. О. Застосування положень імунології в теорії захищених інформаційних систем. Сучасний захист інформації. 2018. № 2. С. 59 – 64.

6. ISO/IEC 7498-1:1994. Information Technology. Open Systems Interconnection. Basic Reference Model: The Basic Model. International Telecommunication Union, 1994, 07. 59 p.

References

1. X-Force Threat Intelligence Index 2021. IBM Security. 2021. https://www.ibm.com/downloads/cas/M1X3B7QG.

2. Microsoft Vulnerabilities Report 2021. Evolving Threats, The Dangers of Admin Rights & How To Address Them. BeyondTrust. 2021. https://www.beyondtrust.com/assets/documents/BeyondTrust-Microsoft-Vulnerabilities-Report-2021.pdf.

3. 2021 CWE Top 25 Most Dangerous Software Weaknesses. https://cwe.mitre.org/top25/archive/2021/2021_cwe_top25.html#methodology.

4. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-94. February 2007. p. 127. https://doi.org/10.6028/NIST.SP.800-94.

5. Gakhov S.O. The application of the principal propositions of immunology in the secure information systems theory. Modern Information Security. 2018. № 2. P. 59 – 64.

6. ISO/IEC 7498-1:1994. Information Technology. Open Systems Interconnection. Basic Reference Model: The Basic Model. International Telecommunication Union, 1994, 07. 59 p.