УДК 004.56(89) DOI: https://doi.org/10.32631/pb.2022.4.14

ІННА ПЕТРІВНА ХАВІНА,
кандидат технічних наук, доцент,
Харківський національний університет внутрішніх справ,
кафедра кібербезпеки та DATA-технологій;
https://orcid.org/0000-0002-1856-1186,
e-mail: inna.khavina25@gmail.com;

ЮРІЙ ВАЛЕРІЙОВИЧ ГНУСОВ,
кандидат технічних наук, доцент,
Харківський національний університет внутрішніх справ,
кафедра кібербезпеки та DATA-технологій;
https://orcid.org/0000-0002-9017-9635,
e-mail: duke6969@i.ua;

ОЛЕКСАНДР ОЛЕКСАНДРОВИЧ МОЖАЄВ,
доктор технічних наук, професор,
Харківський національний університет внутрішніх справ,
кафедра кібербезпеки та DATA-технологій;
https://orcid.org/0000-0002-1412-2696,
e-mail: mozhaev1957@gmail.com

РОЗРОБКА МУЛЬТИАГЕНТНОЇ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Запропоновано функціональну архітектуру системи управління інформаційною безпекою на основі мультиагентної системи для пошуку в реальному часі оптимальних рішень захисту інформації завдяки вибору за визначеними критеріями таких коаліцій агентів механізмів захисту, які дозволять побудувати оптимальний за обраними критеріями захист автоматизованої системи. Обґрунтовано та прийнято за основу модель із повним перекриттям загроз, яка дозволяє провести аналіз загальної ситуації та обрати стратегічно важливі рішення безпосередньо під час організації захисту інформації. Розкрито суть функціонування мультиагентних систем, що реалізують децентралізовану систему керування, засновану на роботі автономних агентів, які можуть бути реалізовано програмно. Визначено ролі агентів загроз, агентів ресурсів, агентів механізмів захисту та їх функціональне призначення. Узагальнено завдання пошуку множини коаліції агентів механізмів захисту для поточного стану автоматизованої системи як завдання оптимального пошуку за критерієм вартості захисту з урахуванням цінності інформації.

Ключові слова: *системи управління інформаційної безпеки, мультиагентні системи, коаліції агентів, модель із повним перекриттям загроз, оптимальний пошук механізмів захисту.*

Оригінальна стаття

ВСТУП. Із розвитком інформаційних технологій, наданням електронних послуг в Україні проєктуються та вводяться в експлуатацію все більше інформаційних систем (далі – ІС), до яких висуваються обов'язкові вимоги до захисту інформації (далі – ЗІ). Але зараз сучасні підприємства промисловості України все більше орієнтуються на створення автоматизованої системи (далі – АС), що ґрунтується на комплексному використанні технічних, математичних, інформаційних та організаційних засобів для управління складними технічними й економічними об'єктами, де частину функцій виконує людина. Водночас конфіденційні або критично важливі дані стають більш цінними і привабливими до крадіжки або злому, а протоколи кібербезпеки підприємства як частина стратегії захисту інформації стають все більші. Однак навіть провідні технологічні компанії світу, такі як Google чи Facebook, зазнають руйнівних порушень безпеки. Один нещодавній злом призвів до викрадення особистої інформації тридцяти мільйонів користувачів[1].

[1] Дані 30 мільйонів користувачів Google Chrome потрапили в руки хакерів, найбільший взлом в історії // Знай.UA : сайт. 19.06.2020. URL: https://znaj.ua/techno/318643-dani-30-milyoniv-koristuvachiv-google-chrome-potrapili-v-ruki-hakeriv-naybilshiy-vzlom-v-istoriji (дата звернення: 21.11.2022).

Питання створення системи захисту інформації у світі є дуже актуальними та виконується згідно з вимогами ISO/IEC 27001:2022 «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи управління інформаційною безпекою» та низкою інших.

Для боротьби з кібератаками та посилення безпеки в інформаційній сфері Президентом України було підписано Указ, яким уведено в дію рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України», де зазначаються виклики та загрози у сфері кібербезпеки, засади і шляхи розбудови національної системи кібербезпеки, пріоритети та стратегічні цілі держави у цій сфері суспільних відносин[1].

Тому одним з актуальних завдань є вирішення питань ефективного захисту інформації як від зовнішніх, так і від внутрішніх загроз завдяки створенню та впровадженню систем управління інформаційною безпекою (далі – СУІБ) в автоматизованих системах підприємств, що, серед іншого, потребує формалізації завдання захисту інформації для її наступної реалізації програмними та іншими засобами[2].

МЕТА І ЗАВДАННЯ ДОСЛІДЖЕННЯ. *Мета* статті – проаналізувати можливості розробки функціональної архітектури системи управління інформаційною безпекою на основі сучасних технологій штучного інтелекту – мультиагентного підходу. Для досягнення мети поставлені такі *завдання*: визначити основні проблеми систем захисту інформації та систем управління інформаційною безпекою; здійснити огляд існуючих підходів до побудови таких систем, сучасних закордонних прикладів розробок; виявити недоліки застосування технологій мультиагентних систем та методи їх усунення; запропонувати функціональну архітектуру системи управління інформаційною безпекою на основі мультиагентного підходу; формалізувати цільові функції агентів і критерії для пошуку оптимальних рішень захисту інформації завдяки вибору за визначеними критеріями таких коаліцій агентів механізмів захисту, які дозволять побудувати оптимальний за обраними критеріями захист автоматизованої системи на всіх етапах її життєвого циклу, та здійсненню моніторингу стану захисту в реальному часі.

МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ. Вирішення окреслених завдань здійснено за допомогою системи загальнонаукових і спеціальних методів пізнання. Використано такі методи, як аналізу і синтезу, індукції та дедукції, узагальнення. Також було застосовано системний підхід, елементами якого є структурний і функціональний методи. Структурний метод використано з метою висвітлення структури існуючих досліджень із заявленої проблематики, функціональний – для вивчення взаємозалежності окремих наукових результатів, їх взаємодії та взаємовпливу.

Застосування методу системно-функціонального аналізу дозволило розглянути систему управління інформаційною безпекою як сукупність етапів, у межах яких реалізують свої повноваження об’єкти інформаційного процесу. При мультиагентному підході можлива реалізація децентралізованого управління агентами, коли кожен агент системи самостійно приймає та реалізує рішення. Мультиагентна система (далі – МАС) будується як об’єднання агентів, що базуються на знаннях. Під агентом розуміється програмно або апаратно реалізована система, яка має такі властивості:

– *автономність* – здатність функціонувати без втручання людини і при цьому здійснювати самоконтроль над своїми діями і внутрішнім станом;

– *суспільна поведінка* – здатність функціонувати у співтоваристві з іншими агентами, обмінюючись з ними повідомленнями за допомогою деякої загальнозрозумілої мови комунікації;

– *реактивність* – здатність сприймати стан середовища і своєчасно реагувати на зміни, які в ньому відбуваються;

– *проактивність* – здатність агента брати на себе ініціативу, тобто здатність генерувати цілі та діяти раціонально для їх досягнення, а не тільки реагувати на зовнішні події.

Також передбачається, що агент додатково має низку ментальних властивостей, які доповнюють перелічені вище. Це:

– *знання* – постійна частина знань агента про себе, середовище та інших агентів, тобто та частина, яка не змінюється в процесі його функціонування;

[1] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447 Президент України : офіц. сайт. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 21.11.2022).

[2] Управління інформаційною безпекою : конспект лекцій : навч. посіб. / уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. Київ : КПІ ім. Ігоря Сікорського, 2021. 258 с. URL: https://ela.kpi.ua/bitstream/123456789/43377/1/Konspekt-Lektsii_UIB.docx (дата звернення: 21.11.2022).

– *переконання* – знання агента про середовище, зокрема про інших агентів; ті знання, які можуть змінюватися в часі і ставати неправильними, проте агент може не мати про це інформації і бути переконаним, що на них можна засновувати свої висновки;

– *бажання* – стани, ситуації, досягнення яких із різних причин є для агента бажаним, проте вони можуть бути суперечливими, тому агент не очікує, що всі вони будуть досягнуті;

– *наміри* – те, що агент або зобов'язаний зробити через свої зобов'язання стосовно інших агентів, або те, що випливає з його бажань;

– *цілі* – безліч конкретних кінцевих і проміжних станів, досягнення яких агент прийняв як поточну стратегію поведінки;

– *зобов'язання стосовно інших агентів* – завдання, які агент бере на себе за дорученням інших агентів у межах кооперативних цілей або цілей окремих агентів у межах співпраці.

МАС будується як об'єднання агентів, робота яких базується на знаннях. Для створення МАС за кожним об'єктом і компонентом, що бере участь у процесі АС, закріплюється свій програмний агент. При цьому мультиагентна система вважається об'єктом, де існують безліч агентів, здатних функціонувати в деяких середовищах та в певних відносинах один з одним. Агенти можуть формувати деякі коаліції та мають певні набори індивідуальних і спільних дій (стратегій поведінки), мають можливість комунікативних дій, а також можуть змінюватися.

Коаліцією вважається тимчасове об'єднання певної кількості агентів задля досягнення спільної мети, їх ресурси стають загальними. Коаліція забезпечує агентів можливістю домовитися та скласти спільний план дій щодо використання спільних ресурсів і засобів для узгодженого виконання всіх завдань.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ ТА ДИСКУСІЯ. Інформаційна система – це складна, розподілена у просторі система, що складається з безлічі зосереджених (локальних) підсистем (інформаційних вузлів), що розташовуються програмно-апаратними засобами реалізації інформаційних технологій, і безлічі засобів, що забезпечують з'єднання і взаємодію цих підсистем із наданими цілями, територіально видаленими користувачами широкого спектра набору послуг зі сфери інформаційного обслуговування (Маслова, 2008; Козюра та ін., 2019). Під системою захисту інформації розуміють єдину сукупність правових і морально-етичних норм, адміністративно-організаційних заходів, фізичних і програмно-технічних засобів, спрямованих на протидію загрозам АС з метою зведення до мінімуму можливості збитків. У цілому засоби забезпечення захисту інформації в частині запобігання навмисних дій залежно від способу реалізації поділяють на технічні, програмні й організаційні. Кожна із цих складових має переваги та недоліки.

Переваги *технічних засобів* пов'язані з їх надійністю, незалежністю від суб'єктивних факторів, високою стійкістю до модифікації. Недоліки: недостатня гнучкість, відносно великі обсяг і маса, висока вартість Перевагами *програмних засобів* є універсальність, гнучкість, надійність, простота установки, здатність до модифікації та розвитку; недоліками – обмежена функціональність, висока чутливість до випадкових або навмисних змін, залежність від типів комп'ютерів та їх апаратних засобів. *Організаційні засоби* прості в реалізації, швидко реагують на небажані дії, мають необмежені можливості модифікації та розвитку, але водночасмають високу залежність від суб'єктивних чинників, зокрема від загальної організації роботи в конкретному підрозділі[1].

Для виявлення вразливостей компонентів АС і недоліків політик безпеки проводять аналіз ризиків загальновідомими програмами, наприклад Facilitated Risk Analysis Process (FRAP), де за методикою ризики оцінюються на якісному рівні[2]. Компанія «RiskWatch» розробила власну кількісну методику, де ризик оцінюється через числове значення, наприклад розмір очікуваних річних втрат і оцінка повернення інвестицій[3]. Фірма «CRAMM» використовує комплексний підхід до оцінки ризиків, що поєднує кількісні та якісні методи аналізу[4]. Аналогічна змішана методика оцінки ризиків використовується і у продуктах компанії

[1] Переваги та недоліки різних видів заходів захисту // Skrippy : сайт. 02.02.2019. URL: http://www.skrippy.com/61328__119212_ (дата звернення: 21.11.2022).

[2] THE Facilitated Risk Analysis and Assessment (FRAAP) // Binus University : сайт. 26.07.2018. URL: https://student-activity.binus.ac.id/isgbinus/2018/07/the-facilitated-risk-analysis-and-assessment-fraap/ (дата звернення: 21.11.2022).

[3] Manage Risk Meet Compliance Improve Security // RiskWatch : сайт. URL: https://riskwatch.com/ (дата звернення: 21.11.2022).

[4] Cram // ENISA : сайт. URL: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html (дата звернення: 21.11.2022).

«Microsoft». Компанія «OCTAVE» застосовує методику поведінки оцінки ризиків, особливістю якої є те, що процес аналізу здійснюється працівниками організації; вона дає оцінку очікуваних збитків, але без оцінки ймовірності[1].

Формальне визначення політики безпеки називають математичною моделлю безпеки. Згідно з вимогами нормативних документів у галузі захисту інформації в інформаційних системах системи захисту інформації будують на основі математичних моделей захисту інформації, які дозволяють теоретично обґрунтувати відповідність системи захисту інформації вимогам заданої політики безпеки та прогнозувати її роботу. Зараз існує багато математичних моделей безпеки, які описують її та надають доказову теоретичну базу для побудови сучасних систем захисту інформації[2].

Захист інформації в АС ґрунтується на принципах системності, комплексності, безперервності захисту, розумної достатності, гнучкості управління і застосування, відкритості алгоритмів і механізмів захисту та простоти застосування захисних заходів і засобів (Козюра та ін., 2019). Основними компонентами моделі безпеки інформації є об'єкти загроз, загрози, джерела загроз, цілі загроз з боку зловмисників, джерела інформації, способи неправомірного оволодіння інформацією з обмеженим доступом, напрями захисту інформації, способи захисту інформації та засоби захисту інформації (Носенко, Півторак, Ліхоузова, 2014). Для аналізу такого значного набору джерел, об'єктів і дій доцільно використовувати методи математичного моделювання, формалізація яких дозволить провести прогнозування роботи СЗІ, оцінити її й обрати адекватні методи захисту.

Зараз існують системи аналізу захищеності, наприклад, що досліджують налаштування елементів захисту операційних систем робочих станцій і серверів, аналізують топологію мережі, шукають незахищені мережеві з'єднання, досліджують налаштування міжмережевих екранів. Ці системи дозволяють значно знизити ризик наявності невиявлених загроз у системі захисту мереж (Носенко, Півторак, Ліхоузова, 2014). Недоліком цих систем є те, що аналіз робиться практично вручну. У зв'язку із цим вони не підходять для моніторингу великих обсягів трафіку мереж масштабу міста. Рішенням цієї проблеми є застосування засобів моніторингу, здатних здійснювати аналіз великої кількості даних у режимі реального часу. До засобів моніторингу належать системи виявлення атак – це програмні засоби, процедури, правила та супутні документи і дані, що стосуються функціонування системи обробки інформації (Носенко, Півторак, Ліхоузова, 2014).

Аналіз існуючих публікацій, пов'язаних із проблемою проєктування систем захисту інформації свідчить про недостатнє висвітлення системних підходів до проблеми опису вразливостей систем захисту інформації (Сєвєрінов, Хрєнов, 2013; Бурячок, 2013; Поддубний, Сєвєрінов, 2020; Толюпа, Пархоменко, Штаненко, 2021). Як правило, це пов'язано з відсутністю єдиних засобів побудови СЗІ та механізмів, що дозволяють оцінювати захищеність і безпеку інформаційних систем. Надалі це призводить до виникнення труднощів для кількісної оцінки під час проєктування й експлуатації інформаційних систем. Захист інформації в АС під час її функціонування потребує не тільки дотримання політики безпеки, здійснення організаційних заходів чи технічного обслуговування засобів захисту, але й моніторингу, контролю та оцінки ризиків інформаційної безпеки (Поддубний, Сєвєрінов, 2020).

Також у роботах деяких науковців зазначено, що одним із перспективних напрямів є створення окремих систем виявлення загроз (системи виявлення атак, системи виявлення мережевих втручань тощо), але такий підхід не завжди може задовольнити принципи системності, комплексності, безперервності захисту, простоти та ін. (Поддубний, Сєвєрінов, 2020; Гвоздьов, Сєвєрінов, Караваєв, 2021).

Із зазначеного вище можливо зробити висновок, що актуальним завданням є розробка системи управління інформаційною безпекою, що буде відповідати вимогам сучасності й ISO 27001. Система управління інформаційною безпекою на основі стандарту ISO/IEC 27001 дає змогу:

– зробити більшість інформаційних активів найбільш зрозумілими для загального менеджменту організації;

– виявляти основні загрози безпеки для наявних бізнес-процесів;

– розраховувати ризики і приймати рішення на основі бізнес-цілей організації;

– забезпечити ефективне управління системою у критичних ситуаціях;

[1] Octave // ENISA : сайт. URL: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_octave.html (дата звернення: 21.11.2022).

[2] Захист інформації в комп'ютерних системах // Ужгородський національний університет : сайт. URL: https://uzhnu.edu.ua/en/infocentre/get/42935 (дата звернення: 21.11.2022).

– проводити процес виконання політики безпеки (знаходити і виправляти слабкі місця в системі забезпечення інформаційної безпеки);

– чітко визначити особисту відповідальність;

– досягти зменшення й оптимізації вартості підтримки системи забезпечення інформаційної безпеки;

– полегшити інтеграцію підсистеми безпеки в бізнес-процеси й інтеграцію з іншими стандартами на системи менеджменту;

– продемонструвати клієнтам, партнерам, власникам бізнесу свою прихильність до інформаційної безпеки;

– отримати міжнародне визнання і підвищення авторитету організації як на внутрішньому, так і на зовнішніх ринках;

– показати прозорість і чистоту бізнесу перед законом завдяки відповідності вимогам стандарту (Кожедуб, 2018).

Аналіз наукових публікацій свідчить, що при загальній різноманітності застосованих моделей та методів не визначено ефективних універсальних системних підходів для проєктування систем управління захисту інформації. Наприклад, у роботі І. Р. Опірського (2015) надано класифікацію моделей захисту інформації в інформаційних системах. Деякі науковці для оцінки ризиків інформаційної безпеки, аналізу вразливостей систем захисту інформації та для побудови систем виявлення атак пропонують алгоритми та методи штучного інтелекту (нечіткої логіки, штучних нейронних мереж), застосування яких має гарні результати (Замула, Северинов, Корниенко, 2014; Довбешко, Толюпа, Шестак, 2019).

Сьогодні в галузі управління великими розподіленими системами, зокрема в галузі захисту інформації, набувають більшого поширення відкриті мультиагентні системи. Основним практичним обмеженням відкритих МАС є безпека, оскільки сама відкритість таких систем суперечить деяким положенням безпеки інформації. Також ведуться дослідження технологій захисту у МАС і розробляються техніки протидії для деяких класів атак (Hedin, Moradian, 2015).

У роботах зарубіжних учених досліджується безпечний консенсусний контроль для багатоагентних систем, які зазнають атаки типу «відмова в обслуговуванні» (DoS), що викликають зміни в топології, руйнування каналів зв'язку, параліч мережі (Tian et al., 2022; Han et al., 2019; Yang et al., 2021; Ni et al., 2019; Sathishkumar, Liu, 2022; Cheng et al., 2020).

Кібератаки становлять серйозну загрозу для синхронізації мультиагентних систем. Оманна атака як типовий тип кібератаки може тихо обійти спостереження механізму виявлення атак, що призведе до великих втрат. Проблема кооперативного відстеження частково відомих кіберфізичних багатоагентних мережевих систем досліджується у роботах деяких зарубіжних науковців (Arafa, Tahoun, 2021).

Наведений огляд свідчить, що застосування МАС для розробки СУІБ є сучасним напрямом розвитку технологій систем захисту інформації. У зв'язку із цим виникає необхідність формалізації захисту інформаційної безпеки та СУІБ та визначення основних підходів у вивченні процесів, які виникають у частинах вразливостей систем захисту інформації під час впливу загроз. Для цього необхідно визначити місце і роль вразливостей у вигляді математичної моделі, класифікувати їх для подальшого використання системного підходу аналізу вразливостей систем захисту інформації в оцінках ефективності моделей, які будуються на етапі проєктування систем захисту інформації.

Основою для проведення аналізу є модель процесу захисту інформації з повним перекриттям загроз. Існують різні загальні методи оцінки ефективності функціонування СЗІ (Гапон, Федорченко, Полякова, 2020). У роботі прийнята за основу модель із повним перекриттям загроз, яка дозволяє провести аналіз загальної ситуації та прийняти стратегічно важливі рішення безпосередньо під час організації захисту інформації.

Метод захисту інформації з повним перекриттям загроз має такі етапи:

1) ідентифікація, класифікація та оцінка загроз;

2) визначення механізмів захисту, повноти їх реалізації та ступеня послаблення загрози;

3) визначення оцінки ефективності системи захисту, підготовка експертного висновку;

4) визначення рівня ризику для ресурсів системи з урахуванням механізмів захисту і висновку про ефективність системи захисту (Гапон, Федорченко, Полякова, 2020).

Проведений вище огляд свідчить, що сучасним напрямом реалізації таких складних розподілених систем керування в режимі реального часу є застосування методів штучного інтелекту у вигляді мультиагентних систем, що характеризуються гнучкістю, оскільки динамічно реагують на зміну середовища, модульністю – системи незалежно, тому що є можливість розширювати архітектуру незалежно від уже існуючої та постійно покращувати рішення в реальному часі.

Під час агентного моделювання будь-яку систему розглядають як систему, що складається

з безлічі інтелектуальних агентів, кожен з яких відповідає за одну або кілька дій, взаємодіє з іншими агентами для планування та здійснення своїх цілей і використовує наявні знання. Агент є автономною, орієнтованою на конкретну ціль програмною одиницею, яка працює асинхронно, спілкується та координує дії з іншими агентами (Khavina, Lymarenko, 2019).

Агент є інкапсульованою комп'ютерною системою, яка знаходиться в певному виконавчому середовищі і може гнучко й автономно діяти в цьому середовищі відповідно до функціональних вимог. Агента визначають як програму:

– в якій сформульоване завдання з чітко окресленими граничними умовами та інтерфейсами;

– розміщену (вбудовану) в конкретне виконавче середовище, де агент через сенсори отримує вхідні дані щодо стану цього середовища і впливає на нього через механізми, що забезпечують дію;

– спроєктовану для виконання спеціальної ролі: їй вказані приватні цілі, яких необхідно досягти, і вона має особливі можливості (служби) вирішення завдань, що дозволяють довести виконання необхідного запиту до кінця і без «зависання»;

– автономну – вона керує як своїм внутрішнім станом, так і своєю поведінкою;

– здатну виявляти гнучкість у виконанні запроєктованої ролі; агенту необхідно бути як реактивним (здатним своєчасно реагувати на зміни, що відбуваються в його середовищі), так і проактивним (здатним вигідно вибирати приватні цілі та виявляти ініціативу).

Здебільшого агенти діють або виконуючи запити, що надходять від імені персон, або як частина більш потужного «вирішувача проблем», що аналогічно концепції віртуальної організації. Отже, під час взаємодії агентів має місце певний основний організаційний контекст, який визначає відносини поміж них. Щоб охоплювати такі зв'язки, агентські системи зазвичай наділяють точними інструкціями для моделювання відносин між організаціями чи ролями, наприклад рівнів менеджера або члена команди. Здебільшого ці відносини безперервно змінюються: соціальні взаємодії припускають, що існуючі відносини еволюціонують (наприклад, команда, що складається з рівних, може вибрати лідера) або створюються нові відносини (наприклад, низка агентів може утворити віртуальну організацію, щоб надавати особливе обслуговування, яке жоден індивід не може запропонувати). У тимчасовому аспекті сфера цих відносин також може змінюватися: від зв'язків, достатніх для того, щоб одночасно надавати конкретні послуги, до постійних зв'язків.

Незалежно від характеру процесу спілкування агентів є дві особливості, які якісно відрізняють взаємодії агентів від тих, що відбуваються в інших комп'ютерних моделях. По-перше, це тенденція до зростання складності взаємодій між агентами порівняно з іншими контекстами, що мають, наприклад, справу з уявленнями співпраці, координації та переговорів. По-друге, агенти є гнучкими «вирішувачами проблем», що оперують у виконавчому середовищі, стан якого вони можуть контролювати й оглядати лише частково. Тому взаємодії необхідно обробляти так само гнучким способом, крім того, агентам потрібен програмний апарат для того, щоб реалізовувати контекстно залежні рішення про характер і межі їх взаємодій, а також щоб ініціювати (або відповідати на) взаємодії, які не були передбачені під час проєктування. Однак недолік такої автономії та гнучкості виявляється в тому, що при цьому важко гарантувати проведення бажаної глобальної дисципліни. З цією метою часто застосовуються засоби (наприклад, закріплення навички, навчання, спеціальні програми й апаратура), які сприяють перевірці та підтримці більшого порядку.

Архітектуру агентної системи можна розділити на три функціональні частини: засоби моделювання; синхронізація часу та контролю; частина, що здійснює аналітичні розрахунки та візуалізацію. Як агентів представляють всі найважливіші об'єкти та компоненти системи. На рис. 1 показана можлива структура агента.

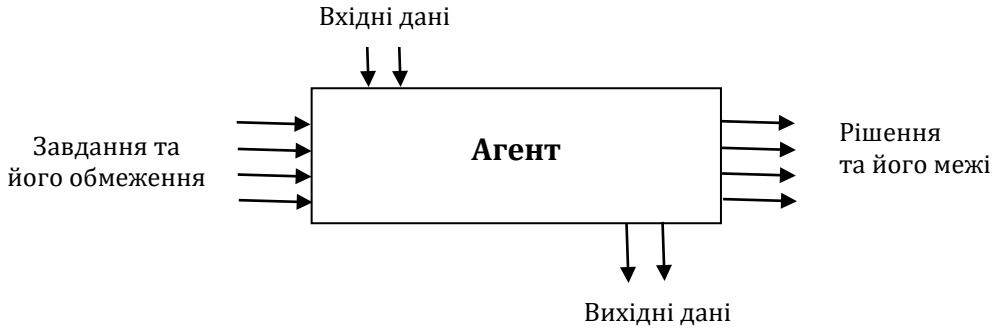


Рис. 1. Агент як одиниця системи

Агентні технології забезпечують високу гнучкість і модульність архітектури. Концепція агентного підходу дозволяє використовувати існуюче програмне забезпечення, технічні й апаратні рішення та людські ресурси. Мультиагентна система може бути реалізована за допомогою Java Agent Development Framework – програмного середовища розробки мультиагентних систем, що підтримує стандарти FIPA для інтелектуальних агентів[1].

Для роботи в реальному часі децентралізованої структури МАС системи захисту та реалізації асинхронної роботи агентів існує алгоритм життєвого циклу агента, згідно з яким агент закінчує свій життєвий цикл тільки тоді, коли здійснено доручені йому завдання.

Колектив або мультиагентна система – це набір інтелектуальних систем (агентів), які діють разом для досягнення спільних цілей (рис. 2.), де *N* – кількість агентів у колективі.

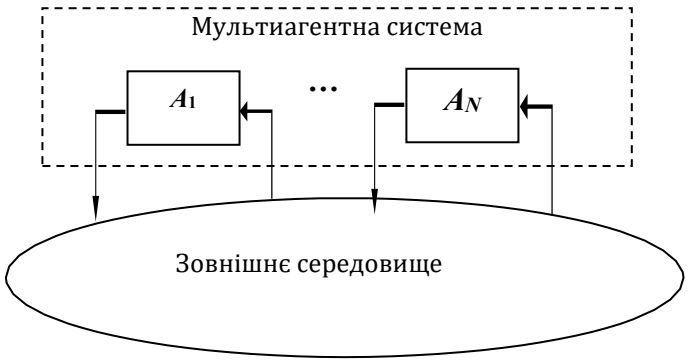


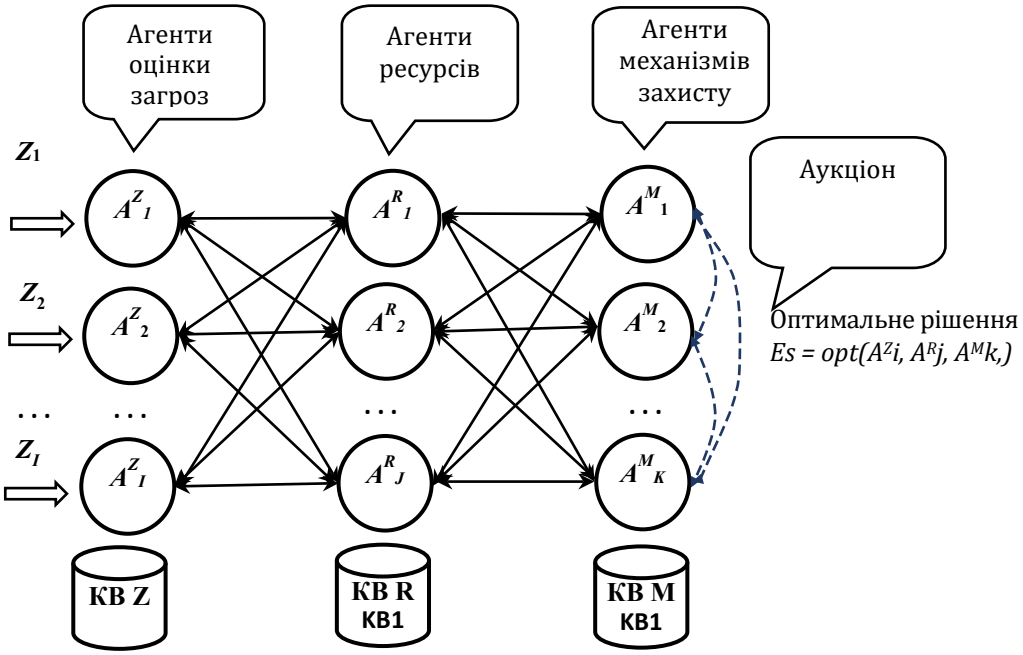
Рис. 2. Взаємодія колективу агентів із середовищем

Колектив – це набір з N інтелектуальних систем (агентів), які діють разом для досягнення спільних цілей. Центр (користувач) – той, хто ставить завдання колективу.

Функціональна цілісність системи передбачає такий тип внутрішньої взаємодії її елементів, за якого властивості цілого (тобто всієї системи) не можна звести до суми властивостей елементів. Принцип колективної дії – гіпотеза про перевагу колективної дії над індивідуальними (за певних умов): колективними діями можна досягти кращих результатів, ніж індивідуальними.

Роботу МАС СУІБ можливо уявити як взаємодію (суцільна лінія) в реальному часі безлічі агентів, що відповідають за різні функції захисту, які реалізовані через їх поведінку в системі, формалізовані у вигляді відповідних цільових функцій та обмежень і визначають оптимальну дію на основі аукціонів, що здійснюються за допомогою переговорів (пунктирна лінія) (рис. 3).

[1] JAVA Agent Development Framework is an open source platform for peer-to-peer agent based applications // Jade : сайт. URL: https://jade.tilab.com/ (дата звернення: 21.11.2022).



Умовні позначки

⇒ – атаки; ↔ – взаємодія між агентами;

$\{A_1^Z, \ldots, A_I^Z\}$ – множина агентів оцінки загроз;

$\{A_1^R, \ldots, A_J^R\}$ – множина агентів ресурсів;

$\{A_1^M, \ldots, A_K^M\}$ – множина агентів механізмів захисту;

КВ Z, КВ Z, КВ Z – бази знань відповідних агентів;

⌣ – аукціон між агентами захисту;

Es – оптимальне рішення на поточний час.

Рис. 3. Архітектура системи МАС СУІБ

Процес роботи МАС захисту інформації представлено такими етапами (рис. 2).

1. Ідентифікація загроз $\{Z_1, \ldots, Z_I\}$, де I – кількість загроз, що надійшли за наперед заданий фіксований період часу, здійснюється множиною агентів оцінки загроз $\{A_1^Z, \ldots, A_I^Z\}$, де I – кількість загроз.

Ідентифікація оцінки загроз і вразливостей полягає в послідовному виконанні таких кроків: визначення загроз для ресурсів організації та рівня реалізації загроз без використання механізмів захисту.

База знань КВ Z містить знання для забезпечення роботи множини агентів оцінки загроз $\{A_1^Z, \ldots, A_I^Z\}$.

2. Множина агентів ресурсів $\{A_1^R, \ldots, A_J^R\}$, де J – кількість ресурсів АС згідно з політикою безпеки, встановлюють відповідний рівень конфіденційності, цілісності, доступності і спостережності для кожного ресурсу організації та ризики і їх пріоритети.

Рівень конфіденційності визначається ступенем важливості ресурсу і наслідками розголошення відповідної інформації, рівень цілісності ресурсу – ступенем пошкодження, фінансових втрат і можливістю відновлення, рівень доступності ресурсу – значенням максимального часу, протягом якого недоступність ресурсу не впливає негативно на діяльність організації, рівень спостережності – ступенем повноти, якості і контролю використання ресурсу з боку авторизованих користувачів.

База знань КВ R містить знання для забезпечення роботи множини агентів ресурсів $\{A_1^R, \ldots, A_J^R\}$.

3. Множина агентів захисту $\{A_1^M, \ldots, A_K^M\}$, де K – кількість механізмів захисту, визначають механізми захисту, що протидіють загрозам та входять до складу СЗІ, визначають рівень, з яким механізми захисту зменшують загрозу, що діє на систему, і вартість механізму захисту з урахуванням цінності інформації, що захищається в поточний час.

База знань КВ M містить знання для забезпечення роботи множини агентів ресурсів $\{A_1^M, \ldots, A_K^M\}$.

Наступним етапом після того, як були визначені загрози і вразливості для системи та встановлені ризики та їх пріоритети, є розробка впорядкованої й економічно обґрунтованої стратегії захисту. На рис. 4 показано варіанти можливих дій агентів механізмів захисту згідно з можливостями захисту ресурсу R_2 від усіх діючих у поточний момент загроз та можливі коаліції агентів захисту.

Виникає питання: як обрати найкращу множину агентів захисту – коаліцію з оптимальним захистом за критерієм вартості захисту та з урахуванням цінності інформації?

Для визначення коаліції агентів захисту *K* з множини всіх можливих механізмів захисту $\{A_1^M, \ldots, A_K^M\}$, що протидіють загрозі, та оцінки рівня захисту запропоновано застосувати аукціон агентів для пошуку оптимального складу множини коаліції агентів механізмів захисту за критерієм вартості захисту *Es* та з урахуванням цінності інформації, що дозволить упорядкувати дії захисту і протистояти всім поточним загрозам:

$$E_s = opt\left(A_i^Z, A_j^R, A_i^M\right) m = 1, \ \ldots, \ \mathbf{M},$$

де M – кількість коаліцій, що були відібрані для роботи МАС.

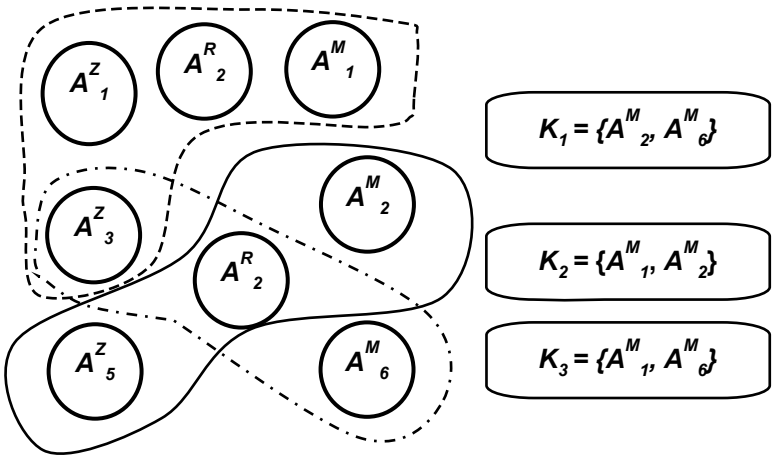


Рис. 4. Варіанти можливих коаліцій агентів механізмів захисту

Отже, мультиагентна система захисту інформації має таку структуру:

$$MAS = < \{A_1^Z, \ \ldots, \ A_I^Z\}, \{A_1^R, \ \ldots, \ A_J^R\}, \{A_1^M, \ \ldots, \ A_K^M\}, \{KE_s = (K_1, K_2, \ldots, K_M), KB_1, \ldots, KB_M\}, m = 1, \ \ldots, \ M,$$

де A^Z – множина агентів загроз; A^R – множина агентів ресурсів; A^M – множина агентів механізмів захисту; $\{K_1, \ \ldots, \ K_M\}$ – множина створених коаліцій агентів захисту під час роботи МАС, де *M* – кількість створених коаліцій; $\{KB_1, \ \ldots, \ KB_M\}$ – бази даних та знань для роботи МАС.

Взаємодія безлічі агентів, що відповідають за різні функції системи, реалізована через їх поведінку в системі та формалізована у вигляді відповідних цільових функцій та обмежень, які визначають оптимальну дію на основі аукціонів, що здійснюються за допомогою переговорів. Це буде оптимальне рішення для поточного стану АС. Через деякий час, коли відбудеться зміна середовища (сцени), здійсняться нові атаки, і МАС зробить перерахунок нової коаліції механізмів захисту K_m за подібним сценарієм для вже нових умов.

Висновок про ефективність системи захисту E_s робиться за рахунок глобального оптимального рішення за часом і складається з множини сукупної дії всіх коаліцій *Km*:

де *M* – кількість коаліцій, що за поточний час були обрані як кращі за визначеними критеріями щодо коаліції.

Зважаючи на можливості та здібності агентів до моделювання загроз, процесу виявлення, прогнозування та визначення загроз на рівні підприємства, в майбутньому агент може приймати проактивні, а не реактивні рішення щодо безпеки Це допоможе активізувати необхідні засоби захисту даних ще на ранніх стадіях процесу захисту інформації. За такого підходу множина агентів, що працює в режимі реального часу, може протистояти векторним атакам завдяки великій кількості агентів та можливостей їх навчання.

ВИСНОВКИ. У роботі запропоновано функціональну архітектуру системи захисту інформації автоматизованої системи на основі мультиагентної системи для пошуку в реальному часі оптимальних рішень захисту інформації завдяки вибору за визначеними критеріями

таких коаліцій агентів механізмів захисту, які дозволять побудувати оптимальний захист АС. Обґрунтовано та прийнято за основу модель із повним перекриттям загроз, тому що вона дозволяє провести аналіз загальної ситуації та прийняти стратегічно важливі рішення безпосередньо під час організації захисту інформації. Розкрито суть функціонування мультиагентних систем, що реалізують децентралізовану систему керування, засновану на роботі автономних агентів, які можуть бути реалізовано програмно. Визначено ролі агентів загроз, агентів ресурсів, агентів механізмів захисту та їх функціональне призначення. Узагальнено завдання пошуку множини коаліції агентів механізмів захисту для поточного стану АС як завдання оптимального пошуку за критерієм вартості захисту та з урахуванням цінності інформації.

Завдяки модульності МАС подальша робота буде направлена на деталізацію компонентів МАС та її вдосконалення.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Бурячок В. Л. Сучасні системи виявлення атак в інформаційно-телекомунікаційних системах і мережах. Модель вибору раціонального варіанта реагування на прояви стороннього кібернетичного впливу. *Інформаційна безпека.* 2013. № 1 (9). С. 33–40.
2. Гапон А. О., Федорченко В. М., Поляков А. О. Підходи до побудови загроз для аналізу безпеки відкритого програмного кода. Системи обробки інформації. 2020. Вип. 1 (160). С. 128–135. DOI: https://doi.org/10.30748/soi.2020.160.17.
3. Гвоздьов Р. Ю., Сєвєрінов О. В., Караваєв В. М. Методика формального проектування комплексних систем захисту інформації в інформаційно-телекомунікаційних системах // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління : тези доп. XI міжнар. наук.-тех. конф. (м. Харків, 8–9 квіт. 2021 р.) / Нац. тех. ун-т «Харківський політехнічний інститу». Харків, 2021. С. 44.
4. Довбешко С. В., Толюпа С. В., Шестак Я. В. Застосування методів інтелектуального аналізу даних для побудови систем виявлення атак. *Сучасний захист інформації.* 2019. № 1. С. 56–62. DOI: https://10.31673/2409-7292.2019.010615.
5. Замула А. А., Северинов А. В., Корниенко М. А. Анализ моделей оценки рисков информационной безопасности для построения системы защиты информации. *Розвиток радіотехнічного забезпечення, АСУ та зв'язку Повітряних Сил*. 2014. № 2. С. 133–138.
6. Кожедуб Ю. Функціональна модель системи забезпечення інформаційної безпеки. *Information Technology and Security.* 2018. Vol. 6, Iss. 2 (11). Pp. 29–42.
7. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / В. Д. Козюра, В. О. Хорошко, М. Є. Шелест та ін. Ніжин : Орхідея, 2019. 144 с.
8. Маслова Н. О. Методи оцінки ефективності систем захисту інформаційних систем. *Штучний інтелект*. 2008. № 4. С. 253–264.
9. Носенко К. М., Півторак О. І., Ліхоузова Т. А. Огляд систем виявлення атак в мережевому трафіку. *Адаптивні системи автоматичного управління.* 2014. № 1 (24). С. 67–75.
10. Опірський І. Р. Класифікація моделей захисту інформації в інформаційних мережах держави. *Науковий вісник НЛТУ України*. 2015. Т. 25, № 10. С. 329–335. DOI: https://doi.org/10.15421/40251050.
11. Поддубний В. О., Сєвєрінов О. В. Менеджмент вразливостей з використанням формалізованого опису. *Радіотехніка*. 2020. Вип. 203. С. 121–125. DOI: https://doi.org/10.30837/rt.2020.4.203.11.
12. Сєвєрінов О. В., Хрєнов А. Г. Аналіз сучасних систем виявлення вторгнень. *Системи обробки інформації*. 2013. Вип. 6 (122). С. 122–124.
13. Толюпа С. В., Пархоменко І. І., Штаненко С. С. Модель системи протидії вторгненням в інформаційних системах. *Інфокомунікаційні технології та електронна інженерія*. 2021. № 1 (1). С. 39–50. DOI: https://doi.org/10.23939/ictee2021.01.039.
14. Arafa M., Tahoun A. Cooperative control for cyber-physical multi-agent networked control systems with unknown false data-injection and replay cyber-attacks. *ISA Trans.* 2021. Vol. 110. DOI: https://doi.org/10.1016/j.isatra.2020.10.002.
15. Cheng Z., Yue D., Hu S., Ge H., Chen L. Distributed event-triggered consensus of multi-agent systems under periodic DoS jamming attacks. *Neurocomputing*. 2020. Vol. 400. Pp. 458–466.
16. Han J., Zhang H., Liang X., Wang R. Distributed impulsive control for heterogeneous multi-agent systems based on event-triggered scheme. *Journal of the Franklin Institute*. 2019. Vol. 356, Iss. 16. Pp. 9972–9991. DOI: https://doi.org/10.1016/j.jfranklin.2019.01.055.
17. Hedin Ya., Moradian E. Security in Multi-Agent Systems. *Procedia Computer Science*. 2015. Vol. 60. Pp. 1604–1612. DOI: *https://doi.org/10.1016/j.procs.2015.08.270.*
18. Khavina I. P., Lymarenko V. V. DSS controlling a machine manufacturing // General and complex problems of technical sciences: experience of EU countries and implementation in the practice of Ukraine : collective monograph. Riga : Baltija Publishing, 2019. Pp. 319–337.

19. Ni H., Xu Z., Cheng J. Robust Stochastic Sampled-data-based Output Consensus of Heterogeneous Multi-agent Systems Subject to Random DoS Attack: A Markovian Jumping System Approach. *International Journal of Control, Automation and Systems*. 2019. Vol. 17. Pp. 1687–1698. DOI: https://doi.org/10.1007/s12555-018-0658-9.

20. Sathishkumar M., Liu Ye.-C. Resilient Memory Event-triggered Consensus Control for Multi-agent Systems with Aperiodic DoS Attacks. *International Journal of Control, Automation and Systems*. 2022. Vol. 20, No. 6. Pp. 1800–1813. DOI: https://doi.org/10.1007/s12555-021-0380.

21. Tian Yu., Tian S., Li H., Han Q., Wang X. Event-Triggered Security Consensus for Multi-Agent Systems with Markov Switching Topologies under DoS Attacks. *Energies*. 2022. Vol. 15, Iss. 15. DOI: https://doi.org/10.3390/en15155353.

22. Yang Yi., Liu F., Yang H., Li Yu., Liu Yu. Distributed Finite-Time Integral Sliding-Mode Control for Multi-Agent Systems with Multiple Disturbances Based on Nonlinear Disturbance Observers. *Journal of Systems Science and Complexity*. 2021. Vol. 34. Pp. 995–1013.

Надійшла до редакції: 23.11.2022

Прийнята до опублікування: 20.12.2022

REFERENCES

1. Arafa, M., & Tahoun, A. (2021). Cooperative control for cyber-physical multi-agent networked control systems with unknown false data-injection and replay cyber-attacks. *ISA Trans, 110*. https://doi.org/10.1016/j.isatra.2020.10.002.

2. Buryachok, V. L. (2013). Modern systems of intrusion detection in information and telecommunication systems and networks. The selection model of rational variant of responding to the occurrence of extraneous influence cybernetic. *Informational Security, 1*(9), 33-40.

3. Cheng, Z., Yue, D., Hu, S., Ge, H., & Chen, L. (2020). Distributed event-triggered consensus of multi-agent systems under periodic DoS jamming attacks. *Neurocomputing, 400*, 458-466.

4. Dovbeshko, S. V., Toliupa, S. V., Shestak, Ya. V. (2019). Application of intelligent data analysis methods for building attack detection systems. *Modern Information Protection, 1*, 56-62. https://10.31673/2409-7292.2019.010615.

5. Han, J., Zhang, H., Liang, X., & Wang, R. (2019). Distributed impulsive control for heterogeneous multi-agent systems based on event-triggered scheme. *Journal of the Franklin Institute, 356*(16), 9972-9991. https://doi.org/10.1016/j.jfranklin.2019.01.055.

6. Hapon, A. O., Fedorchenko, V. M., & Polyakov, A. O. (2020). Approaches to the construction of the threat model for analysis of security of the open software code. *Information Processing Systems, 1*(160), 128-135. https://doi.org/10.30748/soi.2020.160.17.

7. Hedin, Ya., & Moradian, E. (2015). Security in Multi-Agent Systems. *Procedia Computer Science, 60*, 1604-1612. *https://doi.org/10.1016/j.procs.2015.08.270.*

8. Hvozdov, R. Yu., Sievierinov, O. V., & Karavaiev, V. M. (2021, April 8-9). *Methodology of formal design of complex information protection systems in information and telecommunication systems* [Conference presentation abstract]. XI international scientific and technical conference "Modern trends in the development of information and communication technologies and management tools", Kharkiv, Ukraine.

9. Khavina, I. P., & Lymarenko, V. V. (2019). DSS controlling a machine manufacturing. In *General and complex problems of technical sciences: experience of EU countries and implementation in the practice of Ukraine* (pp. 319-337). Baltija Publishing.

10. Kozhedub, Yu. (2018). Functional model of the information security system. *Information Technology and Security, 6*(2), 29-42.

11. Koziura, V. D., Khoroshko, V. O., Shelest, M. Ye. et al. (2019). *Complex information protection systems in information and telecommunication systems.* Orchid.

12. Maslova, N. O. (2008). Methods for evaluating the effectiveness of systems for protection of information systems. *Artificial Intelligence, 4*, 253-264.

13. Ni, H., Xu, Z., & Cheng, J. (2019). Robust Stochastic Sampled-data-based Output Consensus of Heterogeneous Multi-agent Systems Subject to Random DoS Attack: A Markovian Jumping System Approach. *International Journal of Control, Automation and Systems, 17*, 1687-1698. https://doi.org/10.1007/s12555-018-0658-9.

14. Nosenko, K. M., Pivtorak, O. I., & Likhouzova, T. A. (2014). Overview of systems for detecting attacks in network traffic. Interdepartmental scientific and technical collection. *Adaptive Automatic Control Systems, 1*(24), 67-75.

15. Opirsky, I. R. (2015). Classification models of information security in information networks of the state. *Scientific Bulletin of UNFU, 25*(10), 329-335. https://doi.org/10.15421/40251050.

16. Poddubnyi, V. O., & Sievierinov, O. V. (2020). Vulnerability management using a formalized description. *Radio Engineering, 203*, 121-125. https://doi.org/10.30837/rt.2020.4.203.11.

17. Sathishkumar, M., & Liu, Ye.-C. (2022). Resilient Memory Event-triggered Consensus Control for Multi-agent Systems with Aperiodic DoS Attacks. *International Journal of Control, Automation and Systems, 20*(6), 1800-1813. https://doi.org/10.1007/s12555-021-0380.

18. Severinov, O. V, & Khrenov, A. G. (2013). Analysis of modern intrusion detection systems. *Information Processing Systems, 6*(122), 122-124.

19. Tian, Yu., Tian, S., Li, H., Han, Q., & Wang, X. (2022). Event-Triggered Security Consensus for Multi-Agent Systems with Markov Switching Topologies under DoS Attacks. *Energies, 15*(15). https://doi.org/10.3390/en15155353.

20. Tolyupa, S. V., Parkhomenko, I. I., & Shtanenko, S. S. (2021). Model of intrusion detection system in information system. *Information and communication technologies, electronic engineering, 1*(1), 39-50. https://doi.org/10.23939/ictee2021.01.039.

21. Yang, Yi., Liu, F., Yang, H., Li, Yu., & Liu, Yu. (2021). Distributed Finite-Time Integral Sliding-Mode Control for Multi-Agent Systems with Multiple Disturbances Based on Nonlinear Disturbance Observers. *Journal of Systems Science and Complexity, 34*, 995-1013.

22. Zamula, A. A., Severinov, A. V., & Kornienko, M. A. (2014). Analysis of information security risk assessment models for building a data protection system *Development of Radio Technical Support, ACS and Communication of the Air Force, 2*, 133-138.

Received the editorial office: 23 November 2022

Accepted for publication: 20 December 2022

ИННА ПЕТРОВНА ХАВИНА,
кандидат технических наук, доцент,
Харьковский национальный университет внутренних дел,
кафедра кибербезопасности и DATA-технологий;
ORCID: https://orcid.org/0000-0002-1856-1186,
e-mail: inna.khavina25@gmail.com;

ЮРИЙ ВАЛЕРЬЕВИЧ ГНУСОВ,
кандидат технических наук, доцент,
Харьковский национальный университет внутренних дел,
кафедра кибербезопасности и DATA-технологий;
ORCID: https://orcid.org/0000-0002-9017-9635,
e-mail: duke6969@i.ua;

АЛЕКСАНДР АЛЕКСАНДРОВИЧ МОЖАЕВ,
доктор технических наук, профессор,
Харьковский национальный университет внутренних дел,
кафедра кибербезопасности и DATA-технологий;
ORCID: https://orcid.org/0000-0002-1412-2696,
e-mail: mozhaev1957@gmail.com

РАЗРАБОТКА МУЛЬТИАГЕНТНОЙ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Предложена функциональная архитектура системы управления информационной безопасностью на основе мультиагентной системы для поиска в реальном времени оптимальных решений защиты информации за счет выбора по определенным критериям таких коалиций агентов механизмов защиты, которые позволят построить оптимальную по выбранным критериям защиту автоматизированной системы. Обоснована и принята за основу модель с полным перекрытием угроз, позволяющая провести анализ общей ситуации и выбрать стратегически важные решения непосредственно во время организации защиты информации. Раскрыта суть функционирования мультиагентных систем, реализующих децентрализованную систему управления, основанную на работе автономных агентов, которые могут быть реализованы программно. Определены роли агентов угроз, агентов ресурсов, агентов механизмов защиты и их функциональное назначение. Обобщено задание поиска множества коалиции агентов механизмов защиты для текущего состояния АС как задание оптимального поиска по критерию стоимости защиты с учетом ценности информации.

Ключевые слова: *системы управления информационной безопасностью, мультиагентные системы, коалиции агентов, модель с полным перекрытием угроз, оптимальный поиск механизмов защиты.*

INNA PETRIVNA KHAVINA,
Candidate of Technical Sciences, Associate Professor,
Kharkiv National University of Internal Affairs,
Department of Cyber Security and DATA Technologies;
ORCID: https://orcid.org/0000-0002-1856-1186,
e-mail: inna.khavina25@gmail.com;

YURII VALERIIOVYCH HNUSOV,
Candidate of Technical Sciences, Associate Professor,
Kharkiv National University of Internal Affairs,
Department of Cyber Security and DATA Technologies;
ORCID: https://orcid.org/0000-0002-9017-9635,
e-mail: duke6969@i.ua;

OLEKSANDR OLEKSANDROVYCH MOZHAIEV,
Doctor of Technical Sciences, Professor,
Kharkiv National University of Internal Affairs,
Department of Cyber Security and DATA Technologies;
ORCID: https://orcid.org/0000-0002-1412-2696,
e-mail: mozhaev1957@gmail.com

DEVELOPMENT OF MULTI-AGENT INFORMATION SECURITY MANAGEMENT SYSTEM

The issue of creating an information security system is very relevant in the world today. One of the urgent tasks is to solve the issues of effective protection of information from both external and internal threats through the creation and implementation of information security management systems in automated systems of enterprises, which, among other things, requires the formalization of the task of protecting information for its subsequent implementation by software and other means. Now there are security analysis systems, for example, that examine the security elements settings of workstations and servers operating systems, analyze the network topology, look for unprotected network connections, examine the settings of firewalls. The disadvantage of these systems is that they are not suitable for monitoring large volumes of network traffic. The solution to this problem is the use of monitoring tools capable of analyzing large amounts of data in real time. Therefore, a significant place in the article is given to the review of developments based on artificial intelligence technologies, namely multi-agent systems, review of information security models, threat risk assessment in automated systems.

The functional architecture of the information security management system based on a multi-agent system has been proposed to search in real time for information security optimal solutions through the selection of such coalitions of protection mechanisms agents that will allow to build the optimal protection of the automated system according to the selected criteria. The model with complete overlapping of threats has been substantiated and adopted as a basis, which allows to analyze the overall situation and choose strategically important decisions directly during the organization of information security. The essence of of multi-agent systems functioning that implement a decentralized control system based on the work of autonomous agents that can be implemented programmatically has been revealed. The role of threat agents, resource agents, agents of protection mechanisms and their functional purpose have been defined. The problem of searching a set of protection mechanisms agents coalition for the current state of the automated system as a problem of optimal search by the criterion of protection cost, taking into account the value of information, has been generalized. Due to the modularity of the multi-agent system, the further work will be aimed at detailing its components and perfection.

Key words: *information security management systems, multi-agent systems, coalitions of agents, model with complete overlap of threats, optimal search for protection mechanisms.*

Цитування (ДСТУ 8302:2015): Хавіна І. П., Гнусов Ю. В., Можаєв О. О. Розробка мультиагентної системи управління інформаційною безпекою. *Право і безпека*. 2022. № 4 (87). С. 171–183. DOI: https://doi.org/10.32631/pb.2022.4.14.

Citation (APA): Khavina, I. P., Hnusov, Yu. V., & Mozhaiev, O. O. (2022). Development of multi-agent information security management system. *Law and Safety, 4*(87), 171–183. https://doi.org/10.32631/pb.2022.4.14.