The essence of methods of responding to IS events and incidents and their processing, improving the processes of detection and processing of information security events and incidents, supporting the effective functioning of IS event monitoring systems is revealed.

The sequence of IS event and incident processing operations implemented at the stage of the IS incident management process using the algorithm of the first assessment and preliminary decision on events and the second assessment with confirmation of a possible information security incident is considered.

Particular attention is drawn to the fact that in the process of analyzing the potential or actual negative impact, it is necessary to confirm what consequences occurred for the organization's business as a result of the IS incident.

Practical recommendations are provided for improving the processes of identifying events and processing IS incidents, supporting the effective functioning of IS event monitoring systems, in particular, carrying out the following measures: ensuring the proper organization of the IS incident management process, which involves the development and implementation of IS incident management policies and procedures, training of personnel who will be responsible for identifying and responding to IS incidents; implementation of IS monitoring systems capable of detecting a wide range of IS events and incidents and ensuring effective processing of detected IS events and incidents; creation of an effective algorithm for responding to IS incidents, which will determine the order of actions that must be performed to eliminate detected IS events and incidents; holding regular exercises and trainings on detection and response to IS incidents, which will help staff acquire the necessary knowledge and skills to effectively detect and respond to IS incidents.

Key words: *a threat source, IS events and incidents, IS incident response process, event monitoring system, IS incident management system, event processing and correlation systems.*

DOI 10.51369/2707-7276-2024-1(37)-12
УДК 681.528.54

ДОМАРЄВ Валерій Валентинович
БОГУШ Володимир Михайлович

ВИКОРИСТАННЯ МАТЕМАТИЧНОГО АПАРАТУ НЕЧІТКИХ МНОЖИН ДЛЯ РОЗРОБЛЕННЯ МЕТОДІВ, ТЕХНОЛОГІЙ, МОДЕЛЕЙ БЕЗПЕКИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

Зростаюча складність і взаємопов’язаність сучасних інформаційно-комунікаційних систем (ІКС) створюють значні виклики для їхньої безпеки. Традиційні заходи безпеки, часто засновані на бінарній логіці та детермінованих моделях, є недостатніми

для протидії динамічному характеру сучасних кіберзагроз. У статті досліджено застосування математичного апарату нечітких множин для розроблення сучасних методів, технологій і моделей підвищення безпеки ІКС.

Використано принципи нечіткої логіки, щоби запропонувати інноваційні рішення для забезпечення безпеки, які адаптуються до мінливого ландшафту загроз. Ключові сфери застосування включають розроблення систем нечіткого виведення для виявлення загроз і реагування на них у режимі реального часу, адаптивних механізмів контролю доступу та надійних моделей оцінки ризиків.

Представлено нову нечітку модель безпеки, яка була емпірично підтверджена за допомогою симуляції та реальних прикладів. Результати демонструють значне покращання точності виявлення загроз, часу реагування й адаптивності системи порівняно з традиційними моделями безпеки.

Розглянуто впровадження нечіткої логіки в безпеку ІКС і потенціал цього підходу, який може революціонізувати існуючі практики та встановити нові стандарти кіберзахисту, а також проблеми впровадження та потенційні обмеження нечітких підходів до безпеки та надано практичні рекомендації щодо подолання цих бар'єрів.

Доведено, що, ураховуючи невизначеність і підвищуючи адаптивність, нечіткі методи, технології та моделі можуть значно підвищити надійність та ефективність систем безпеки ІКС, а інтеграція теорії нечітких множин у механізми безпеки інформаційно-комунікаційних систем є перспективним напрямом для вирішення багатогранних проблем сучасної кібербезпеки. Дослідження цієї проблематики сприяє теоретичному розвитку й практичному застосуванню нечітких множин у кібербезпеці, прокладаючи шлях до більш стійких та інтелектуальних рішень у сфері безпеки.

Ключові слова: *адаптивні моделі безпеки, безпека інформаційно-комунікаційних систем, виявлення загроз, кібербезпека, кіберзахист, оцінка ризиків, системи нечіткого виведення, теорія нечітких множин.*

Постановка проблеми. Безпека інформаційно-комунікаційних систем (далі – ІКС) стала першочерговою проблемою в цифрову епоху, коли обсяг, різноманітність і швидкість передачі даних постійно зростають. Традиційні заходи безпеки, засновані на бінарній логіці та детермінованих моделях, часто виявляються недостатніми для ефективного реагування на складну й динамічну природу сучасних кіберзагроз. Ландшафт загроз, що постійно змінюється і характеризується складними векторами атак, уразливостями «нульового дня» та сучасними постійними загрозами, потребує більш тонкого й адаптивного підходу до безпеки ІКС.

Однією з фундаментальних проблем безпеки ІКС є боротьба з невизначеністю та неоднозначністю. Кіберсередовища за своєю суттю є складними, із численними змінними, які можуть впливати на стан безпеки системи. Традиційні методи, які покладаються на чіткі бінарні відмінності між безпечними і небезпечними станами, неадекватні для моделювання та реагування на мінливий і невизначений характер цих середовищ. Така жорсткість обмежує здатність систем безпеки адаптуватися до нових і непередбачу-

ваних загроз, таким чином ставлячи під загрозу загальну стійкість ІСS.

Крім того, існуючим моделям безпеки часто не вистачає гнучкості, щоб ураховувати різні ступені ризику й загроз. У реальних сценаріях серйозність і ймовірність загроз не завжди є чорно-білими, а існують у спектрі. Бінарна логіка не здатна відобразити ці градації, що призводить до переоцінювання або недооцінювання ризиків, а також до неефективного розподілу ресурсів безпеки і робить потенційно системи вразливими.

Теорія нечітких множин, введена Лотфі Заде, пропонує багатообіцяюче рішення цих проблем. Ця теорія дає змогу представляти невизначеність і часткові значення істинності, забезпечуючи більш гнучку й реалістичну основу для моделювання складних систем. У контексті безпеки ІКС нечітка логіка може врахувати притаманні їй невизначеності та градації ризиків, що дає можливість розробляти точніші й адаптивніші заходи безпеки.

Включення нечіткої логіки в моделі безпеки дає можливість ефективніше представляти й управляти нюансами та градаціями рівнів ризику і загроз. Системи нечіткого виведення можуть обробляти неточні дані та приймати рішення з урахуванням контексту, підвищуючи точність і адаптивність механізмів виявлення загроз і реагування на них. Така гнучкість дає змогу розробляти більш деталізовані та динамічні заходи безпеки, які можуть адаптуватися до мінливого ландшафту загроз у режимі реального часу. Однак забезпечення функціонування ІКС в умовах виникнення непередбачуваних, зокрема катастрофічних, ситуацій потребує додаткових витрат і більшої кількості ресурсів. Постає необхідність розроблення нових підходів у дослідженнях систем безпеки інформаційних технологій.

Незважаючи на свій потенціал, застосування теорії нечітких множин до безпеки ІСS є ще недостатньо вивченим. Необхідні й комплексні дослідження для розроблення моделей, методів і технологій, які для підвищення безпеки ІКС використовують математичний апарат нечітких множин. Це передбачає створення нечітких протоколів безпеки, які можуть динамічно адаптуватися до мінливого ландшафту загроз, розроблення систем нечіткого виведення для виявлення загроз і реагування на них у режимі реального часу, а також розроблення моделей оцінки ризиків, які точніше відображають багатогранну природу кіберзагроз. Є потреба в емпіричній перевірці нечітких моделей безпеки за допомогою симуляції та тестування в реальних умовах для забезпечення їхніх ефективності та надійності.

Ускладнення технологій обробки інформації (інформаційних технологій) призвело до появи нових видів загроз процесам функціонування інформаційно-комунікаційних систем. Пошук ефективних шляхів адекватної протидії сучасним загрозам (атакам) в інформаційній сфері стає вкрай актуальною проблемою. Забезпечення безпеки ІКС в умовах непередбачуваних і навіть катастрофічних ситуацій стає все складнішим та ресурсомістким завданням. Для його вирішення необхід-

ні нові підходи й інновації, які дадуть змогу ІКС безперебійно виконувати свої функції навіть у разі виникнення небезпечних подій.

Процеси гарантування безпеки ІКС складаються із задач системного моделювання та аналізу (декомпозиції проблеми, комплексування проєктних рішень, побудови системних моделей різного класу, розроблення вимог до елементів системи управління інформаційною безпекою (далі – СУІБ), аналізу коректності й ефективності технологічних рішень). На нашу думку, поняття безпеки ІКС виділяється своїми відмінними властивостями, а саме:

– глобальною метою функціонування, пов'язаною з багаторівневим, складним комплексом спільних цілей;

– великою кількістю функціональних задач, що різняться за властивостями та комплексно взаємодіють, складаючи велику багаторівневу систему;

– складною, багаторівневою організацією матеріальних та інформаційних потоків взаємодії елементів структури ІКС;

– алгоритмами функціонування та управління системою безпеки з багаторівневим характером, складною динамікою.

Актуальним є вирішення завдання використання системного підходу в дослідженні наукових питань управління системами інформаційної безпеки великої розмірності й складної структури.

Процеси створення та впровадження СУІБ характеризуються великим ступенем випадковості, невизначеності, нестабільності, а їхнє відображення здійснюється за допомогою системи кількісних та якісних показників, які зазвичай подаються в лінгвістичній, нечітко заданій формі [2]. Так методи теорії нечіткості можуть стати найефективнішим інструментом для моделювання складних процесів безпеки ІКС.

Аналіз останніх досліджень і публікацій. Теоретичні основи нечітких множин і нечіткої логіки, а також математичного апарату теорії нечіткості заклав професор Лотфі Заде з Каліфорнійського університету, Берклі. Результати його досліджень були вперше опубліковані в 1965 році в журналі «Information and Control» [4]. У теорію нечіткої логіки та її використання в дослідженні складних систем, зокрема в системах безпеки інформаційних технологій, зробили значний внесок науковці з різних країн світу [5; 15; 17]. Можливості апарату нечіткої логіки як основи приблизних розрахунків і рішень визначено в роботах В. Бартолена, А. Болдуіна, Я. Мідзумото, М. Мукаідоно, Д. Циммермана й інших учених. Проблематику нечітких множин у системах управління та прийняття рішень вивчали Т. Желдак, Л. Коряшкіна, С. Ус [2], синтезу нечітких систем підтримки прийняття рішень для задач транспортної логістики – С. Енчева, Ю. Кондратенко, Є. Сіденко [3].

Водночас недостатньо вивчені питання застосування теорії нечітких множин до безпеки інформаційно-комунікаційних систем. Зокрема потрібне проведення комплексних досліджень для розроблення технологій, методів і моделей, які використовують

математичний апарат нечітких множин для підвищення безпеки таких систем, а також наукових розвідок за допомогою сучасної методології щодо подальшого розроблення системного та системно-процесного підходу до вирішення практичних завдань управління інформаційною безпекою.

Мета статті – дослідити використання теорії нечітких множин для розроблення передових методів, технологій і моделей безпеки інформаційно-комунікаційних систем, які дають змогу краще захистити ці системи від кіберзагроз, що постійно розвиваються. Результати цього дослідження сприятимуть теоретичному розвитку кібербезпеки та забезпечать практичні рішення для підвищення безпеки інформаційно-комунікаційних систем.

Виклад основного матеріалу. Безпека ІКС є критично важливою проблемою в сучасному цифровому ландшафті. Зі стрімким розвитком технологій і поширенням взаємопов'язаних пристроїв складність і масштаб ІКС зростають у геометричній прогресії. Це розширення супроводжується збільшенням складності та частоти кіберзагроз, що створює значні ризики для особистої конфіденційності, організаційної цілісності та національної безпеки. Потреба в надійних, адаптивних та інтелектуальних механізмах безпеки для захисту цих систем ще ніколи не була такою нагальною.

Сучасні ІКС охоплюють широкий спектр застосувань – від критичної інфраструктури й фінансових систем до охорони здоров'я та «розумних» міст. Ці системи, тісно пов'язані між собою, створюють складну мережу залежностей і взаємодій. Цей взаємозв'язок, хоча і є корисним для операційної ефективності й інновацій, також посилює уразливість. Порушення в одному компоненті може мати каскадний ефект, потенційно виводячи з ладу цілі мережі та завдаючи масштабної шкоди. Кіберзагрози еволюціонували від простих ізольованих інцидентів до дуже складних, скоординованих атак. Нині поширеними є Advanced Persistent Threats (APT), експлойти «нульового дня», програми-вимагачі та кібервійни [8]. Ці загрози характеризуються своєю непомітністю, наполегливістю та здатністю адаптуватися до контрзаходів. Традиційні заходи безпеки, які часто покладаються на статичні правила й бінарні рішення, погано пристосовані для протидії таким динамічним і витонченим загрозам.

Традиційні моделі безпеки здебільшого базуються на бінарній логіці, де стан системи є або безпечним, або небезпечним. Такий підхід не враховує невизначеності та неоднозначності, притаманні реальному кіберсередовищу. Через бінарну природу цих моделей застосовуються надмірно консервативні або недостатні захисні заходи, що призводить до неефективного розподілу ресурсів і потенційних прогалин у безпеці. Крім того, цим моделям бракує гнучкості для адаптації до нових і непередбачуваних загроз, що робить їх неадекватними щодо постійних змін кіберландшафту.

Теорія нечітких множин, запроваджена Лотфі Заде в 1965 році, про-

понує надійну основу для роботи з невизначеністю та частковими істинами [7]. На відміну від класичної теорії множин, яка оперує бінарною належністю (елементи або належать, або не належать множині), теорія нечітких множин допускає ступені належності. Ця характеристика робить її особливо придатною для моделювання складних, невизначених середовищ, подібних до тих, що є в ІКС.

У створенні систем безпеки ІКС зазвичай беруть участь фахівці з різних сфер, тому є певні вимоги стосовно координації їхньої діяльності. Водночас із практичної точки зору потрібні рекомендації щодо прийняття як оптимальних, так і достатньо ефективних рішень, що стосуються безпеки ІКС. Для забезпечення безпеки ІКС потрібне сумісне використання різних компонентів, які відрізняються своїми функціями та складом, таких як: заходи, методи, засоби, механізми, процедури й ін. Такі компоненти потребують об'єднання в систему безпеки ІКС та встановлення жорстких логічних і функціональних зв'язків між собою. Як видно із практики, саме якість зазначених зв'язків визначає рівень ефективності систем безпеки ІКС.

На відміну від об'єктного та комплексного підходів, у розробленні систем безпеки ІКС основну частину становлять завдання системного моделювання та аналізу. Ця тенденція потребує дослідження сучасних системних методів і моделей безпеки. Логіка методики дослідження питань безпеки ІКС полягає в такому [1]:

• Визначається предметна галузь знань із питань інформаційної безпеки.

• Проводиться системний аналіз та створюється логіко-лінгвістична модель безпеки ІКС.

• Розробляються методики й алгоритми використання моделі.

Вирішення наукових завдань дослідження процесів створення систем безпеки ІКС потребує розроблення науково обґрунтованої моделі, адекватної сучасним викликам і загрозам. У дослідженнях систем безпеки ІКС запропоновано використання можливостей наукових методів і моделей теорії нечіткості [6]. Основою цієї теорії є апарат нечітких множин, що оперує нечітко детермінованими величинами, такими як: нечітка логіка, нечіткі лінгвістичні змінні, нечіткі відношення тощо. До того ж запропоновано логіко-лінгвістичну матричну модель безпеки ІКС (див. рис. 1) та алгоритм її використання (див. рис. 2) як науково-методичний апарат дослідження.

Моделювання систем безпеки ІКС у нечітких умовах передбачає використання методів формування функцій належності, тому визначення ступенів належності елементів множині та побудова на їхній основі функції належності – основне питання практичних реалізацій досліджень проблем створення систем безпеки ІКС. Зазначені елементи немовби частково належать тим чи іншим множинам. Нечіткі методи характеризуються використанням лінгвіс-

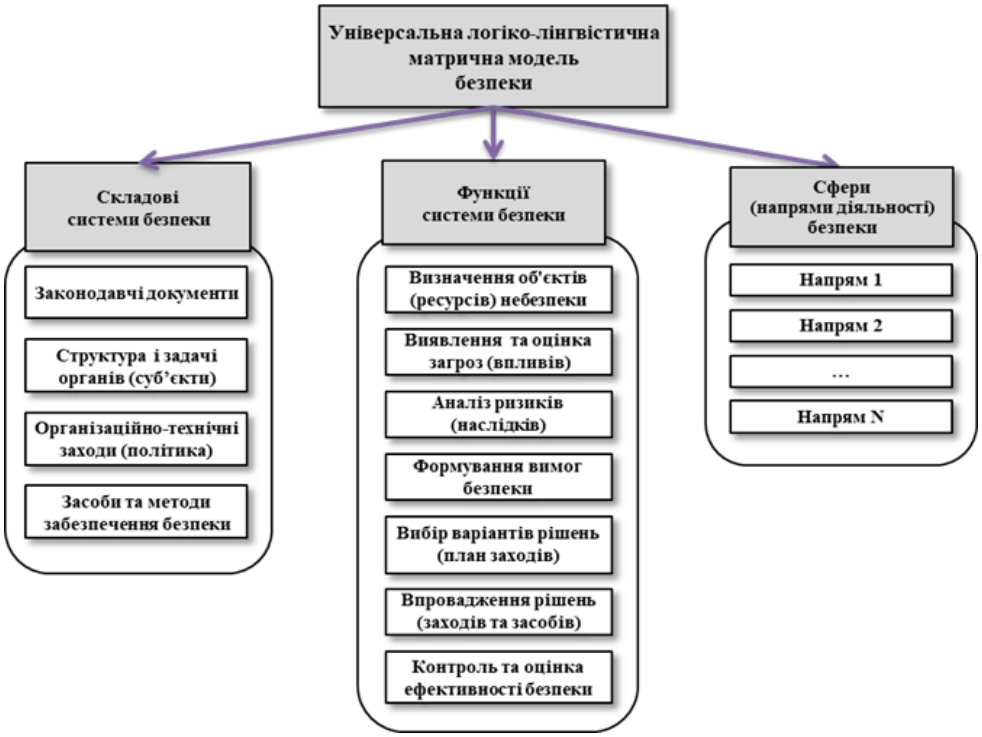

Рисунок 1 – Логіко-лінгвістична матрична модель загальної безпеки (складено авторами)

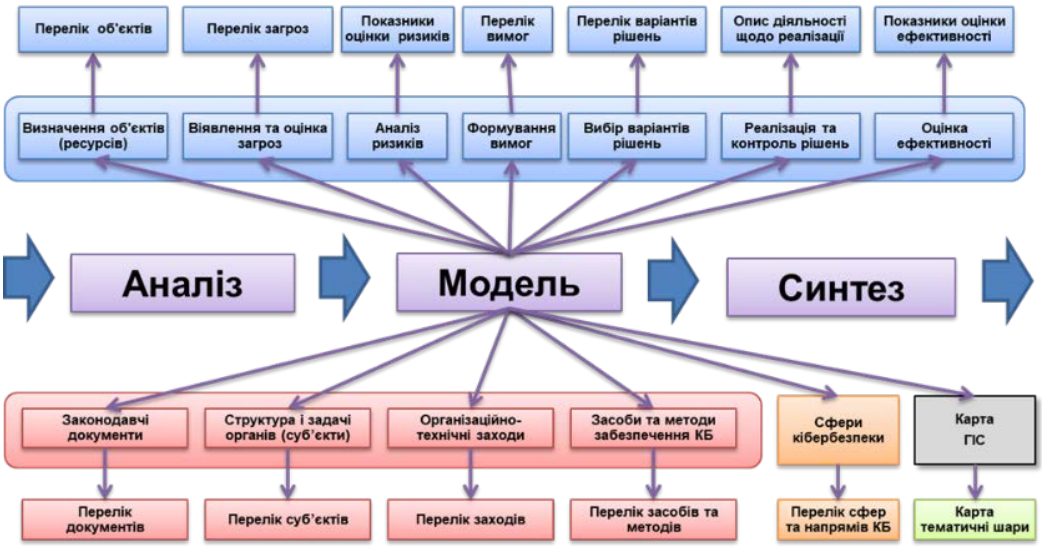

Рисунок 2 – Алгоритм використання логіко-лінгвістичної матричної моделі (складено авторами)

тичних змінних замість числових, коли функціонально-логічні зв'язки між лінгвістичними параметрами описуються за допомогою нечітких

висловлень або нечіткими алгоритмами.

Для формалізації функціональних зв'язків між лінгвістичними змінними, що характеризують стан безпеки ІКС, пропонується використати логіко-лінгвістичний підхід, що базується на поняттях нечітких і лінгвістичних змінних, які містять параметри, подані у вербальному вигляді.

Сукупність функціонально-логічних зв'язків логіко-лінгвістичної моделі систем безпеки ІКС у вигляді таблиці створює МАТРИЦЮ системи безпеки ІКС. Матриця системи безпеки ІКС – це інформаційно-методичний інструмент, який є простим, універсальним і ефективним засобом моделювання та реалізації процесів і систем безпеки ІКС.

Відповідні правила дозволяють швидко обробляти складні сполучення, що є важливою перевагою розмитої логіки. Тому моделі реальних систем, побудовані на основі нечітких множин, характеризуються великою гнучкістю, адекватністю реальному світу завдяки простоті використання нечітких операцій. Застосування теорії нечітких множин до безпеки ІКС має значні практичні наслідки та потенційні переваги (див. табл. 1):

Таблиця 1 – Практичні наслідки та потенційні переваги застосування теорії нечітких множин до безпеки ІКС (складено авторами)

Покращене виявлення загроз та реагування на них	
Системи на основі нечітких множин можуть аналізувати неоднозначні та неповні дані для більш точного виявлення потенційних загроз	Ця здатність зменшує кількість помилкових спрацьовувань і негативних результатів, що призводить до більш надійного і своєчасного виявлення загроз і реагування на них
Адаптивні моделі безпеки	
Нечітка логіка дозволяє розробляти адаптивні моделі безпеки, які можуть налаштовувати свої параметри залежно від поточного загрозливого середовища	Така адаптивність має вирішальне значення для підтримки надійної безпеки в умовах еволюції загроз
Покращена оцінка ризиків	
Теорія нечітких множин дозволяє створювати більш тонкі моделі оцінки ризиків, які можуть оцінювати загрози за ступенем серйозності та ймовірності	Такий підхід сприяє кращому визначенню пріоритетів для ресурсів безпеки та ефективнішому управлінню ризиками
Інтеграція з існуючими інфраструктурами	
Нечіткі рішення для забезпечення безпеки можуть бути інтегровані з існуючими інфраструктурами ІКС, розширюючи їхні можливості без необхідності повної перебудови	Така інтеграція має важливе значення для практичної реалізації та широкого впровадження

Управління системами безпеки ІКС розглядається як серія взаємопов'язаних безперервних дій, кожна з яких сама є процесом. Такі дії-процеси називають управлінськими функціями. Пропонується використання ментальної логіко-лінгвістичної матричної моделі безпеки ІКС як формалізованої сукупності взаємопов'язаних між собою процесів функціонування системи безпеки ІКС. Йдеться про універсальну логіко-лінгвістичну матричну модель, яку можна використовувати для дослідження будь-якої системи безпеки.

Забезпечення безпеки ІКС має важливе значення для захисту конфіденційних даних, підтримки операційної цілісності та забезпечення конфіденційності, цілісності й доступності інформації. У таблиці 2 подано шість основних методів забезпечення безпеки ІКС. Упроваджуючи ці методи, організації можуть значно підвищити безпеку своїх інформаційно-комунікаційних систем, забезпечуючи безпечну та надійну роботу критично важливої інфраструктури.

Таблиця 2 – Методи забезпечення безпеки ІКС
(складено авторами)

№	Метод	Характеристика		
		Опис	**Реалізація**	**Переваги**
1	Шифрування	Шифрування – це процес перетворення даних у закодовану форму для запобігання несанкціонованому доступу. Це гарантує, що навіть якщо дані перехоплені, вони не можуть бути прочитані без ключа розшифровки	***Data at Rest***	• Захищає дані від несанкціонованого доступу та зламу. • Забезпечує конфіденційність конфіденційної інформації. • Підвищує довіру та відповідність нормативним вимогам
			Шифруйте конфіденційні дані, що зберігаються на серверах, базах даних і пристроях зберігання	
			Дані в дорозі (Data in Transit)	
			Використовуйте такі протоколи як SSL/TLS для шифрування даних, що передаються мережею, включно з електронною поштою та вебтрафіком	

			Наскрізне шифрування	
			Впроваджуйте наскрізне шифрування для комунікацій, щоб гарантувати, що тільки сторони, які спілкуються, можуть читати повідомлення	
2	Контроль доступу	Механізми контролю доступу гарантують, що тільки авторизовані користувачі можуть отримати доступ до певної інформації та ресурсів. Це включає як фізичний, так і цифровий контроль доступу	***Автентифікація***	• Обмежує доступ до конфіденційних даних і систем. • Зменшує ризик внутрішніх загроз і несанкціонованого доступу. • Підвищує підзвітність та відстежуваність завдяки реєстрації та моніторингу спроб доступу
			Використовуйте надійні методи автентифікації, такі як багатофакторна автентифікація (MFA), для перевірки особи користувача	
			Авторизація	
			Впроваджуйте контроль доступу на основі ролей (RBAC), щоб призначати дозволи на основі ролей та обов'язків користувачів	
			Управління доступом	
			Регулярно переглядайте та оновлюйте дозволи доступу, щоб переконатися, що вони відповідають поточним ролям та обов'язкам	

3	Міжмережеві екрани та системи виявлення / запобігання вторгненням (IDPS)	Брандмауери та IDPS є критично важливими для захисту мереж від несанкціонованого доступу та виявлення потенційних загроз безпеці	***Брандмауери***	• Забезпечує першу лінію захисту від зовнішніх загроз. • Покращує видимість мережевої активності та потенційних інцидентів безпеки. • Дозволяє проактивно виявляти загрози та реагувати на них
			Розгортання брандмауерів для створення бар'єрів між різними сегментами мережі, контролюючи потік трафіку на основі заздалегідь визначених правил безпеки	
			Мережеві IDPS	
			Моніторинг мережевого трафіку для виявлення ознак зловмисної активності, таких як незвичні шаблони або відомі сигнатури атак	
			IDPS на основі хостів	
			Моніторинг активності окремих пристроїв на предмет ознак компрометації	
4	Моніторинг безпеки та реагування на інциденти	Безперервний моніторинг безпеки та чітко визначений план реагування на інциденти мають важливе значення для швидкого виявлення та реагування на інциденти безпеки	***Управління інформацією та інцидентами безпеки (SIEM)***	• Забезпечує швидке виявлення та реагування на інциденти безпеки. • Мінімізує вплив порушень безпеки на операційну діяльність. • Покращує загальну стійкість ICS
			Використовуйте системи SIEM для збору, аналізу та кореляції подій безпеки з різних джерел	
			План реагування на інциденти	
			Розробіть і регулярно оновлюйте план реагування на інциденти, який описує процедури виявлення, локалізації та відновлення після інцидентів безпеки	

			Навчання та тренування	
			Проводьте регулярні тренінги та симуляційні вправи, щоб переконатися, що команда реагування на інциденти готова до реагування на реальні інциденти	
5	Керування виправленнями	Управління виправленнями передбачає регулярне оновлення програмного забезпечення та систем виправлення безпеки для усунення відомих вразливостей. Це має вирішальне значення для підтримання безпеки та надійності ІКС	*Регулярні оновлення*: Заплануйте регулярні вікна технічного обслуговування для застосування виправлень безпеки й оновлень до програмного забезпечення та систем. *Тестування*: Тестуйте виправлення в контрольованому середовищі перед розгортанням, щоб переконатися, що вони не порушують роботу. *Резервне копіювання та відновлення*: підтримуйте актуальні резервні копії для швидкого відновлення в разі виникнення проблем під час встановлення патчів	• Знижує ризик використання відомих вразливостей. • Забезпечує захист систем від новітніх загроз. • Підтримує цілісність та надійність ICS
6	Політики та процедури безпеки	Встановлення комплексних політик та процедур безпеки має вирішальне значення для підтримки послідовного	***Розробка політики***	• Забезпечує структурований та послідовний підхід до безпеки ІКС.

		й ефективного підходу до безпеки ICS. Вони мають бути узгоджені з галузевими стандартами та найкращими практиками	Розробіть чіткі та обов'язкові до виконання політики безпеки, які охоплюють всі аспекти безпеки ICS, включаючи контроль доступу, мережеву безпеку та реагування на інциденти	• Гарантує, що всі зацікавлені сторони знають про свої обов'язки з безпеки. • Посилює загальний стан безпеки шляхом постійного вдосконалення
			Стандартні операційні процедури (СОП)	
			Створіть СОП, які містять детальні інструкції щодо впровадження заходів безпеки та реагування на інциденти	
			Відповідність та аудит	
			Регулярно перевіряйте дотримання політик і процедур безпеки, щоб виявити та усунути прогалини	

Розглядаючи моделі безпеки для інформаційно-комунікаційних систем, слід зауважити, що вони є критично важливими рамками, призначеними для захисту конфіденційності, цілісності та доступності даних. Ці моделі забезпечують структуровані підходи до захисту інформації від несанкціонованого доступу, розкриття, зміни та знищення. Оскільки сучасні інформаційні системи є складними, потрібні надійні моделі безпеки, які об'єднують різні теоретичні та практичні аспекти для протидії різним загрозам.

Наприклад, модель Белла – ЛаПадули (Bell-LaPadula, BLP), розроблена в 1970-х роках, є однією з фундаментальних моделей безпеки, що забезпечує конфіденційність даних [9]. Вона базується на двох основних принципах: простій властивості безпеки (не можна зчитувати) та *-властивості (не можна записувати). Проста властивість безпеки гарантує, що суб'єкти

(користувачі або процеси) із нижчим рівнем без-пеки не можуть читати дані з вищим рівнем безпеки, запобігаючи несанкціонованому доступу до конфіденційної інформації. Властивість *, навпаки, гарантує, що суб'єкти з вищим рівнем безпеки не можуть записувати дані до даних із нижчим рівнем безпеки, запобігаючи витоку конфіденційної інформації до менш захищених областей.

Модель BLP особливо ефективна в середовищах, де збереження конфіденційності інформації має першорядне значення, наприклад, у військових або урядових установах. Однак зосередженість на конфіденційності обмежує її застосування в комерційних умовах, де цілісність і доступність даних є не менш важливими.

Модель Biba, запропонована у відповідь на обмеження моделі BLP, забезпечує насамперед цілісність даних. Вона працює за принципами простої властивості цілісності (no write up) і *-властивості (no read down). Проста властивість цілісності гарантує, що суб'єкти не можуть записувати інформацію на вищий рівень цілісності, запобігаючи пошкодженню даних на вищих рівнях. Властивість * гарантує, що суб'єкти не можуть читати інформацію з нижчого рівня цілісності, підтримуючи достовірність даних, до яких мають доступ суб'єкти з високим рівнем цілісності. Модель Biba добре підходить для додатків, де цілісність даних має вирішальне значення, таких як фінансові системи або медичні записи [14]. Однак суворе дотримання цілісності може обмежити гнучкість, що потребує балансу між безпекою та зручністю використання.

Модель Кларка – Вілсона пропонує практичніший підхід до підтримки цілісності даних, зосереджуючись на чітко сформованих транзакціях і розподілі обов'язків [15]. Вона визначає набір правил і процесів сертифікації, які гарантують, що тільки авторизовані користувачі можуть виконувати певні транзакції і що ці транзакції зберігають цілісність даних. Модель використовує концепцію добре сформованих транзакцій, які є послідовністю операцій, що переводять систему з одного узгодженого стану в інший.

Модель Кларка – Вілсона широко застосовується в комерційних середовищах, де цілісність транзакцій є критично важливою, наприклад, у банківській справі та системах планування ресурсів підприємства (ERP). Вона забезпечує баланс між безпекою та зручністю використання, дає змогу гнучко контролювати транзакції.

Контроль доступу на основі ролей (RBAC) – це широко прийнята модель безпеки, яка спрощує управління доступом, призначаючи дозволи ролям, а не окремим користувачам. Користувачам призначаються ролі на основі їхніх обов'язків і посадових функцій. Ця модель полегшує адміністрування та масштабування в складних середовищах, зменшуючи ризик надмірних дозволів.

RBAC особливо корисна у великих організаціях із динамічною робочою силою, оскільки дає можливість ефективно управляти дозволами користувачів. Централізуючи контроль доступу навколо ролей, забезпечує послідовне застосування політик без-

пеки і спрощує дотримання нормативних вимог.

Контроль доступу на основі атрибутів (ABAC) розширює гнучкість RBAC, використовуючи атрибути, такі як характеристики користувачів, типи ресурсів та умови навколишнього середовища, для прийняття рішень щодо контролю доступу. Такий детальний підхід дає змогу створювати динамічні та контекстно залежні політики контролю доступу.

ABAC ідеально підходить для середовищ із різними вимогами до доступу, що швидко змінюються, таких як хмарні обчислення та системи інтернету речей (IoT). Забезпечує високий рівень деталізації та адаптивності, що дає можливість точно контролювати, хто і до яких ресурсів може отримати доступ за певних умов.

Модель нульової довіри – це сучасна парадигма безпеки, яка передбачає, що загрози можуть надходити як зсередини, так і ззовні мережі. Вона працює за принципом «ніколи не довіряй, завжди перевіряй», що означає, що жодному суб'єкту не можна довіряти за замовчуванням, незалежно від його місцезнаходження або облікових даних. Безперервна перевірка та суворий контроль доступу застосовуються на кожному рівні взаємодії. Нульова довіра особливо актуальна в сучасному ландшафті сучасних постійних загроз і витончених кібератак. Вона об'єднує різні технології безпеки, такі як багатофакторна автентифікація (MFA), мікросегментація та захист кінцевих точок, для створення комплексної стратегії захисту.

Ефективний захист інформаційно-комунікаційних систем часто потребує інтеграції декількох моделей безпеки для вирішення різних питань безпеки. Наприклад, поєднання моделей BLP і Biba може забезпечити як конфіденційність, так і цілісність, а от RBAC можна використовувати для ефективного управління контролем доступу.

Багаторівневий підхід до безпеки, або глибокий захист, передбачає впровадження засобів контролю безпеки на різних рівнях, зокрема на рівні мережі, додатків і даних. Така стратегія зменшує ймовірність виникнення єдиної точки відмови та підвищує загальну стійкість системи безпеки.

Моделі безпеки також повинні відповідати нормативним вимогам, визначеним у Загальному регламенті про захист даних (GDPR), Законі про переносимість і відповідальність за медичне страхування (HIPAA) і Стандарті безпеки даних індустрії платіжних карток (PCI DSS). Ці нормативні акти вимагають застосування спеціальних засобів контролю безпеки та процесів для захисту конфіденційних даних і забезпечення підзвітності.

Впровадження моделей безпеки, що відповідають регуляторним стандартам, допомагає організаціям уникнути юридичних санкцій і репутаційних втрат, забезпечуючи при цьому захист конфіденційної інформації.

Швидкий розвиток таких технологій як хмарні обчислення, інтернет речей та штучний інтелект створює нові виклики та можливості для моделей безпеки. Традиційні моделі безпеки можуть потребувати адаптації

або розширення, щоб упоратися з унікальними характеристиками та загрозами, пов'язаними з цими технологіями.

Наприклад, хмарні середовища потребують моделей безпеки, які можуть упоратися з динамічним розподілом ресурсів і багатокористувацьким використанням, тоді як системи інтернету речей потребують моделей, здатних захистити величезну кількість взаємопов'язаних пристроїв із різними можливостями. Штучний інтелект і машинне навчання можуть підвищити безпеку, надаючи розширені можливості виявлення загроз і реагування на них, але вони також створюють нові ризики, такі як ворожі атаки й упередженість моделей.

Розроблення нових технологій для забезпечення безпеки інформаційно-комунікаційних систем є багатогранною справою, яка охоплює широкий спектр методів і підходів. Ці технології спрямовані на захист конфіденційної інформації, забезпечення цілісності та доступності даних, а також захист від кіберзагроз, що постійно змінюються.

Технології безпеки інформаційно-комунікаційних систем охоплюють інструменти, протоколи й методи, призначені для захисту даних і підтримки функціональності систем. Ці технології спрямовані на досягнення різних цілей безпеки, зокрема: 1) забезпечення доступу до інформації лише авторизованим користувачам; 2) захист інформації від несанкціонованих змін; 3) забезпечення доступу до інформації та систем, коли це необхідно; 4) перевірка ідентичності користувачів і систем; 5) контроль доступу до ресурсів на основі ролей і дозволів користувачів; 6) забезпечення того, що дії або транзакції не можуть бути скасовані після того, як вони відбулися.

Наприклад, криптографія має фундаментальне значення для захисту інформаційно-комунікаційних систем. Вона передбачає перетворення читабельних даних (відкритого тексту) у нечитабельний формат (зашифрований текст) за допомогою алгоритмів і ключів. Ключові методи та їхні характеристики подано в таблиці 3.

Таблиця 3 – Ключові методи криптографії в контексті захисту ІКС

Назва методу	***Характеристика***
Криптографія з симетричним ключем	Використовує один ключ як для шифрування, так і для розшифрування. Прикладами є Advanced Encryption Standard (AES) і Data Encryption Standard (DES). Симетричні алгоритми ефективні, але потребують безпечних механізмів розподілу ключів
Криптографія з асиметричним ключем	Використовує пару ключів: один для шифрування (відкритий ключ) і один для розшифрування (закритий ключ). Приклади: RSA і криптографія еліптичних кривих (ECC). Асиметричні алгоритми полегшують безпечний обмін ключами та цифровими підписами, але вони потребують великих обчислень

Хеш-функції	Генерують хеш-значення фіксованого розміру з вхідних даних. Такі хеш-функції як SHA-256 забезпечують цілісність даних і мають вирішальне значення для цифрових підписів і перевірки цілісності
Квантова криптографія	Використовує принципи квантової механіки для забезпечення безпеки комунікації. Квантовий розподіл ключів (QKD) забезпечує теоретично незламне шифрування, використовуючи властивості квантової заплутаності та суперпозиції

Мережева безпека зосереджена на захисті даних під час їх передачі через мережі. Контролюють вхідний і вихідний мережеві трафіки на основі заздалегідь визначених правил безпеки. Брандмауери можуть бути апаратними або програмними і є важливими для створення мережевих периметрів. Системи виявлення та запобігання вторгненням (IDPS) відстежують мережевий трафік на предмет підозрілих дій і вживають заходів для запобігання атакам [10]. IDPS можуть бути засновані на сигнатурах, аномаліях або гібридними. Віртуальні приватні мережі (VPN) створюють безпечні, зашифровані з'єднання через загальнодоступні мережі, забезпечуючи конфіденційність і цілісність даних, що передаються. Такі протоколи як SSL/TLS, IPsec і SSH забезпечують безпечні канали зв'язку через мережі, шифрування, автентифікацію та цілісність даних [11].

Безпека додатків передбачає захист програмних додатків від уразливостей і загроз. Безпечний життєвий цикл розробки програмного забезпечення (Software Development Life Cycle, SDLC) інтегрує практики безпеки протягом усього процесу розроблення програмного забезпечення – від проєктування до розгортання [12]. Практики включають моделювання загроз, безпечне кодування, перегляд коду та тестування безпеки. Брандмауери вебдодатків (WAF) захищають вебдодатки шляхом фільтрації та моніторингу HTTP/HTTPS-трафіку [13]. WAF запобігають таким атакам як SQL-ін'єкції, міжсайтовий скриптинг (XSS) і підробка міжсайтових запитів (CSRF). Статичне й динамічне тестування безпеки додатків (SAST/DAST) – це інструменти, які аналізують код і поведінку програми для виявлення вразливостей [16]. SAST перевіряє вихідний код, а DAST тестує запущені програми. Самозахист додатків під час виконання (RASP) вбудовує заходи безпеки в додатки для виявлення та запобігання атакам під час виконання.

Безпека кінцевих точок зосереджена на захисті окремих пристроїв, таких як комп'ютери, смартфони та планшети. Основні підходи включають: 1) антивірусне й антивірусне програмне забезпечення – виявлення та видалення шкідливого програмного забезпечення з пристроїв. Сучасні рішення використовують виявлення на основі сигнатур, евристики й аналізу поведінки; 2) виявлення та реагування на кінцевих точках (EDR) – надає можливості безперервного моніторингу та реагування на кінцеві пристрої. Рішення EDR виявляють підозрілі дії, проводять криміналістичний

аналіз і автоматизують реагування; 3) управління мобільними пристроями (MDM) – керує та захищає мобільні пристрої, забезпечуючи відповідність політикам безпеки та надаючи можливості віддаленого керування.

Системи IAM забезпечують доступ потрібних осіб до потрібних ресурсів у потрібний час. Ключові компоненти включають: 1) єдиний вхід (Single Sign-On, SSO) – дає можливість користувачам пройти автентифікацію один раз і отримати доступ до декількох додатків або систем [17]. SSO покращує взаємодію з користувачем і зменшує втому від введення паролів; 2) багатофакторна автентифікація (MFA) – вимагає декількох форм перевірки для автентифікації, таких як паролі, біометричні дані або токени безпеки. MFA значно підвищує безпеку, зменшуючи ризик атак на основі облікових даних; 3) управління привілейованим доступом (PAM) – контролює та відстежує доступ привілейованих користувачів до критично важливих систем і даних. Рішення PAM забезпечують дотримання принципу найменших привілеїв і створюють аудиторські сліди.

SIEM-системи збирають, аналізують і співставляють події безпеки з різних джерел, щоб забезпечити виявлення загроз і реагування на них у режимі реального часу. Можливості SIEM включають: 1) збирання та зберігання журналів із різних систем і додатків для аналізу; 2) виявлення взаємозв'язків між різними подіями безпеки для виявлення шаблонів, що вказують на потенційні загрози; 3) автоматизацію реагування на виявлені загрози, наприклад, ізоляцію уражених систем або сповіщення персоналу служби безпеки.

Штучний інтелект і машинне навчання трансформують технології безпеки, забезпечуючи просунуте виявлення загроз, предиктивну аналітику й автоматизоване реагування. Алгоритми ML можуть виявляти закономірності у великих масивах даних, аномалії та адаптуватися до нових загроз. Однак існують проблеми, пов'язані із забезпеченням стійкості моделей ML до ворожих атак та усуненням упереджень у навчальних даних.

Блокчейн пропонує потенціал для посилення безпеки завдяки децентралізованим і захищеним від несанкціонованого доступу обліковим записам. Застосування включає безпечний обмін даними, управління ідентифікацією та безпеку ланцюгів поставок. Однак масштабованість, відповідність нормативним вимогам та інтеграція з існуючими системами залишаються проблемами.

Із розвитком квантових обчислень існуючі криптографічні алгоритми можуть стати вразливими. Постквантова криптографія спрямована на розроблення алгоритмів, стійких до квантових атак. Тривають дослідження для визначення та стандартизації квантово-стійких алгоритмів, які можуть бути розгорнуті в практичних системах.

Захист пристроїв інтернету речей створює унікальні виклики через їхні обмежені ресурси, різноманітні архітектури та широкомасштабне розгортання. Підходи включають легкі криптографічні протоколи, механізми безпечного завантаження й автентифікацію пристроїв. Забезпечення

інтероперабельності й управління життєвим циклом пристроїв інтернету речей є критично важливими сферами.

Кіберфізичні системи, такі як промислові системи управління та інтелектуальні мережі, потребують надійної безпеки для захисту фізичної інфраструктури й операцій. Підходи включають моніторинг у реальному часі, виявлення аномалій і безпечні протоколи зв'язку. Конвергенція IT-середовищ і середовищ операційних технологій має важливе значення для комплексної безпеки CPS.

Нечітка теорія множин розширює класичну теорію множин, дозволяючи елементам мати різні ступені належності до множини, а не бінарну умову належності. У класичній теорії множин елемент або належить до множини, або ні (значення належності 1 або 0). На відміну від цього, теорія нечітких множин вводить функцію належності $\mu_A(x)$, яка ставить у відповідність кожному елементу x значення між 0 та 1, що представляє ступінь, до якого x належить до нечіткої множини A.

Системи виявлення вторгнень (IDS) є критично важливими компонентами для захисту інформаційно-комунікаційних систем. Традиційні IDS часто покладаються на заздалегідь визначені правила та порогові значення, які можуть бути жорсткими й не виявляти нові або складні атаки. IDS на основі нечіткої логіки можуть розширити можливості виявлення, ураховуючи невизначеність і розмитість даних мережевого трафіку.

Виходячи з цього, слід розробити IDS, які використовують системи на основі нечітких правил для класифікації поведінки мережі як нормальної або аномальної. Ці системи використовують нечіткі правила у вигляді «ЯКЩО умова, ТО дія», де умови і дії виражені в нечітких термінах. Наприклад: ЯКЩО (мережевий трафік високий І активність порту незвична), ТО (рівень потенційної загрози високий).

Нечіткі умови (наприклад, «високий мережевий трафік») визначаються за допомогою функцій належності, які дають змогу поступово переходити від нормального до аномального стану. Впровадження адаптивних порогів із використанням нечіткої логіки необхідне для динамічного налаштування чутливості IDS. На відміну від фіксованих порогів, нечіткі пороги можна налаштовувати на основі контекстної інформації та історичних даних, покращуючи виявлення нових загроз без збільшення помилкових спрацьовувань.

Системи контролю доступу визначають: хто може отримати доступ, до яких ресурсів, за яких умов. Традиційні моделі, такі як Role-Based Access Control (RBAC), не можуть упоратися з нюансами й залежністю від контексту реальних вимог до контролю доступу. Теорія нечітких множин може привнести гнучкість і врахування контексту в рішення щодо контролю доступу.

Зважаючи на це, слід удосконалити RBAC шляхом включення нечітких множин для управління різними рівнями дозволів доступу. У FRBAC ролі та дозволи визначаються за допомогою нечітких функцій належності, що дозволяє часткове призначення ролей і нюансовані рівні доступу.

Наприклад: користувач може мати 0,7 належності до ролі «менеджер» і 0,3 належності до ролі «супервайзер», що точніше відображає його обов'язки й потреби в доступі. Слід упроваджувати контекстно залежні механізми контролю доступу з використанням нечіткої логіки для оцінювання динамічних умов, таких як час доби, місцезнаходження та пристрій, що використовується. Наприклад: ЯКЩО (роль користувача – менеджер, час доступу – робочий час, пристрій захищений), ТО (рівень доступу – високий).

Ефективне оцінювання та управління ризиками мають вирішальне значення для забезпечення безпеки інформаційно-комунікаційних систем. Традиційні методи оцінювання ризиків часто покладаються на точні оцінки ймовірності та впливу, які може бути складно отримати і які можуть неточно відображати реальну невизначеність. Варто розробити нечіткі матриці ризиків, у яких імовірність загроз і наслідки їх виникнення представлені за допомогою нечітких множин. Такий підхід дає можливість проводити гнучкіше та реалістичніше оцінювання ризиків, де ймовірності та наслідки виражаються не точними значеннями, а нечіткими числами.

Практичною, на нашу думку, є пропозиція застосовувати нечіткі методи MCDM для визначення пріоритетів та управління ризиками безпеки. Такі критерії як імовірність загрози, серйозність впливу та витрати на пом'якшення наслідків можуть бути змодельовані за допомогою нечітких множин, що дає змогу особам, які приймають рішення, ураховувати декілька неточних факторів одночасно. Наприклад, можна використовувати такі методи як процес нечіткої аналітичної ієрархії (FAHP) для зважування та ранжування ризиків безпеки на основі нечітких критеріїв.

Уже згадувана нами криптографія є наріжним каменем інформаційної безпеки, забезпечуючи конфіденційність, цілісність та автентичність даних. Теорія нечітких множин може вдосконалити криптографічні методи, додавши їм гнучкості та стійкості до невизначеностей. Слід розробити схеми нечіткого управління ключами, які використовують нечітку логіку для управління розподілом і відкликанням ключів у динамічних і невизначених середовищах. Наприклад, можна визначити нечіткі правила для розподілу ключів на основі таких факторів як рівень довіри користувачів, контекст використання та історична поведінка. Це допоможе зменшити ризики, пов'язані з компрометацією ключів і несанкціонованим доступом.

Розумні мережі являють собою критично важливу інфраструктуру, де безпека має першорядне значення через інтеграцію інформаційних технологій з енергетичними системами. Упровадження IDS на основі нечіткої логіки в інтелектуальних мережах може значно покращити виявлення кібер-фізичних атак. Ідейною пропозицією може стати визначення нечітких правил на основі шаблонів зв'язку в інтелектуальних мережах та експлуатаційних параметрів. Наприклад, ЯКЩО (коливання напруги високе І затримка передачі даних ненормальна), ТО (потенційна кібер-фізична атака). Слід упроваджувати адаптивні нечіткі пороги для налаштування чут-

ливості IDS на основі даних у реальному часі й історичних тенденцій. Цей підхід допоможе виявити тонкі аномалії, що вказують на сучасні постійні загрози, не перевантажуючи операторів помилковими тривогами.

Відомо, що хмарні обчислення потребують гнучких і масштабованих механізмів контролю доступу. Нечіткі системи контролю доступу можуть упоратися з динамічним і контекстно залежним характером вимог до доступу до хмари. Зважаючи на це, варто розробити систему FRBAC, у якій ролі та дозволи визначаються за допомогою нечітких множин. Наприклад: користувач хмари може мати нечітку належність до декількох ролей (наприклад, 0,6 належності до «адміністратора» і 0,4 належності до «користувача»), що дає змогу приймати деталізованіші рішення щодо контролю доступу.

Необхідно впроваджувати контекстно залежні політики доступу з використанням нечіткої логіки для оцінювання таких умов як місцезнаходження користувача, безпека пристрою та час доступу. Наприклад: ЯКЩО (роль користувача – адміністратор, час доступу – неробочий час, пристрій захищений), ТО (надати частковий доступ адміністратора).

Застосування теорії нечітких множин для розроблення методів захисту інформаційно-комунікаційних систем є перспективним напрямом досліджень із численними можливостями для інновацій. Нечітка логіка може впоратися з невизначеностями в даних, тоді як машинне навчання може ідентифікувати складні патерни й підвищити точність виявлення. Слід розробити протоколи безпеки, які включають нечітку логіку для обробки невизначеностей у комунікаційних середовищах, таких як бездротові мережі та системи інтернету речей. Ці протоколи можуть підвищити стійкість і надійність захищених комунікацій. Також перспективним убачаємо дослідження використання нечітких множин у системах управління довірою для оцінювання та управління довірчими відносинами в децентралізованих мережах, таких як блокчейн та однорангові системи. Нечіткі моделі довіри можуть забезпечити більш нюансовані й адаптивні оцінки довіри.

Висновки. Моделі безпеки для інформаційно-комунікаційних систем є важливими рамками, у межах яких упроваджуються засоби контролю безпеки для захисту даних від широкого спектру загроз. Їхній спектр – від класичних моделей, таких як Bell-LaPadula і Biba, що зосереджені на конфіденційності й цілісності, до сучасних – таких як RBAC, ABAC і Zero Trust, які пропонують гнучкість і адаптивність. Ці моделі забезпечують основу для захисту складних і динамічних середовищ.

Доведено, що інтеграція декількох моделей безпеки, дотримання нормативних вимог та адаптація до нових технологій мають вирішальне значення для підтримки надійної безпеки в сучасному взаємопов'язаному світі. Постійно розвиваючись і вдосконалюючи моделі безпеки, організації можуть краще захиститися від кіберзагроз, що постійно змінюються, і забезпечити захист своїх критично важливих інформаційних активів.

Розробка нових технологій для забезпечення безпеки інформаційно-комунікаційних систем є динамічною і мультидисциплінарною галуззю. Вона включає в себе широкий спектр методів і підходів – від базових криптографічних методів до передових технологій виявлення загроз на основі штучного інтелекту. Оскільки ландшафт загроз змінюється і з'являються нові технології, постійні дослідження й інновації мають вирішальне значення для розв'язання поточних проблем і загалом підвищення безпеки інформаційних систем. Інтегруючи надійні практики безпеки, використовуючи нові технології та зберігаючи проактивну позицію, організації можуть краще захистити свої критичні інформаційні активи та забезпечити відмовостійкість своїх комунікаційних систем.

Застосування теорії нечітких множин для розроблення методів захисту інформаційно-комунікаційних систем пропонує потужний підхід до подолання невизначеності та складності, притаманних сучасним викликам у сфері безпеки. Використовуючи гнучкість і надійність нечіткої логіки, дослідники й практики можуть розробляти адаптивніші, контекстно залежні та стійкі рішення для забезпечення безпеки. Постійні дослідження й інновації в цій галузі мають потенціал для значного посилення безпеки інформаційно-комунікаційних систем, захисту критично важливих даних та інфраструктури від постійно мінливого ландшафту загроз.

Беручи до уваги сучасні тенденції розвитку ІКС, потрібні дослідження питань їхньої безпеки з використанням системного підходу, теорії нечіткої логіки та математичного апарату нечітких множин. Моделі систем безпеки ІКС, побудовані на основі нечітких множин, характеризуються великою гнучкістю, адекватністю реальному світу завдяки простоті використання нечітких операцій.

Запропоновано логіко-лінгвістичну матричну модель безпеки ІКС та алгоритм її використання як науково-методичного апарату дослідження методів, технологій, моделей і систем інформаційної безпеки, які з використанням математичного апарату нечітких множин дають можливість ефективно вирішувати завдання створення та впровадження СУІБ.

Подальше дослідження питань безпеки ІКС із використанням системного підходу та математичного апарату нечітких множин дасть змогу визначити нові методичні шляхи створення ефективних СУІБ, які раціонально об'єднуватимуть різні за властивостями засоби, заходи й методи протидії загрозам ІКС. Запропоновану ментальну логіко-лінгвістичну матричну модель безпеки ІКС та алгоритм аналізу й синтезу системних знань із питань інформаційної безпеки зараз використано в навчальному процесі Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії СБ України. Запропоновані системно-процесний підхід і логіко-лінгвістична матрична модель можуть використовуватися як інструмент взаємодії та координації діяльності науковців, експертів і викладачів для формування системних знань із питань інформаційної та кібербезпеки.

Список використаних джерел

1. Домарєв В. В. Система ситуаційного управління: теорія, методологія, рекомендації. Київ : Знання України, 2017. 347 с.

2. Желдак Т. А., Коряшкіна Л. С., Ус С. А. Нечіткі множини в системах управління та прийняття рішень : навчальний посібник / М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». Дніпро : НТУ «ДП», 2020. 387 с.

3. Кондратенко Ю., Енчева С., Сіденко Є. Синтез нечітких систем підтримки прийняття рішень для задач транспортної логістики. *Технічні вісті*. 2010. № 1 (31). С. 61–66.

4. Zadeh L. Fuzzy sets. *Information and Control*. 1965. № 8 (3). P. 338–353.

5. Kaufmann A., Gupta M. Introduction to Fuzzy Arithmetic: Theory and Applications. Van Nostrand Reinhold Company. New York, 1985.

6. Fuzzy Logic Toolbox. User's Guide. The MathWorks, Inc. 1999. 134 p.

7. Fuzzy Sets by Lotfi A. Zadeh. Manhattan Rare Book Company. URL: https://www.manhattanrarebooks.com/pages/books/1652/lotfi-a-zadeh/fuzzy-sets?soldItem=true (дата звернення: 23.02.2024).

8. Advanced persistent threat (APT). Imperva. URL: https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/ (дата звернення: 12.03.2024).

9. Difference between bell lapadula and biba. Study X. Best AI Homework Helper & Homework AI Tutor. URL: https://studyx.ai/homework/100587682-difference-between-bell-lapadula-and-biba-model (дата звернення: 14.03.2024).

10. IDP rights: what can internally displaced persons claim? Visit Ukraine : Service portal about Ukraine 24/7. URL: https://visitukraine.today/blog/1624/idp-rights-what-can-idps-claim (дата звернення: 13.03.2024).

11. IPsec vs SSL/TLS vs SSH (Secure Shell). CCNA-Classes. URL: https://ccna-classes.com/ccna-study-resources/ipsec-vs-ssl-tls-vs-ssh-secure-shell/ (дата звернення: 13.03.2024).

12. The Seven Phases of the Software Development Life Cycle. Split. URL: https://www.split.io/blog/software-development-life-cycle-phases/ (дата звернення: 18.03.2024).

13. Why is HTTP not secure? HTTP vs. HTTPS. Cloudflare. URL: https://www.cloudflare.com/ru-ru/learning/ssl/why-is-http-not-secure/ (дата звернення: 18.03.2024).

14. Biba Model. ScienceDirect. URL: https://www.sciencedirect.com/topics/computer-science/biba-model (дата звернення: 18.03.2024).

15. Ahmed L. The Clark-Wilson Model. URL: https://www.studynotesandtheory.com/single-post/the-clark-wilson-model (дата звернення: 25.03.2024).

16. Phadke A. SAST vs. DAST: What's the Difference? Synopsys Blog. URL: https://www.synopsys.com/blogs/software-security/sast-vs-dast-difference.html#:~:text=Get%20Newsletter-,What%20are%20SAST%20and%20DAST?,organization's%20applications%20susceptible%20to%20attack. (дата звернення: 25.03.2024).

17. Teravainen T. What is Single Sign-On (SSO) and How Does It Work? Security. URL: https://www.techtarget.com/searchsecurity/definition/single-sign-on (дата звернення: 25.03.2024).

Стаття надійшла до редакції 12.04.2024

UDC 681.528.54

Domariev V. V., Bohush V. M.

FUZZY SET THEORY IN THE DEVELOPMENT OF METHODS, TECHNOLOGIES, MODELS FOR INFORMATION SECURITY OF INFORMATION AND COMMUNICATION SYSTEMS

The increasing complexity and interconnectedness of modern information and communication systems (ICS) pose significant challenges to their security. Traditional security measures, often based on binary logic and deterministic models, are insufficient to counter the dynamic nature of modern cyber threats. This article explores the use of the mathematical apparatus of fuzzy sets to develop modern methods, technologies and models for improving ICS security. Fuzzy logic principles have been used to propose innovative security solutions that adapt to the changing threat landscape. Key applications include the development of fuzzy inference systems for real-time threat detection and response, adaptive access control mechanisms, and robust risk analysis models.

A new fuzzy safety model that has been empirically validated with simulations and real-world examples is presented. The results demonstrate significant improvements in threat detection accuracy, response time, and system adaptability compared to traditional security models.

The implementation of fuzzy logic in ICS security and the potential of this approach, which can revolutionize existing practices and set new standards for cyber defense, as well as the challenges of implementation and potential limitations of fuzzy approaches to security are considered and practical recommendations for overcoming these barriers are provided. Consequences are also considered.

It is proved that taking into account the uncertainty and increasing adaptability, fuzzy methods, technologies and models can significantly increase the reliability and efficiency of ICS security systems, and the integration of the theory of fuzzy sets into the security mechanisms of information and communication systems is a promising direction for solving multifaceted problems of modern cybersecurity. Research on this topic contributes to the theoretical development and practical application of fuzzy sets in cybersecurity, paving the way for more sustainable and intelligent security solutions.

Key words: *adaptive security models, security of information and communication systems, threat detection, cybersecurity, cyber defense, risk assessment, fuzzy inference systems, fuzzy set theory.*