УДК 621.391:004.056.5

ПОШУК ВТОРГНЕНЬ У МЕРЕЖАХ В УМОВАХ НЕВИЗНАЧЕНОСТІ

Ахрамович Володимир Миколайович, Ахрамович Вадим Володимирович

Анотація. *У статті розглянуто проблему пошуку та виявлення вторгнень у комп'ютерних мережах в умовах невизначеності, що зумовлена неповнотою та неточністю даних, динамічністю мережевого трафіку, прихованим характером сучасних атак і використанням засобів шифрування. Показано обмеженість традиційних сигнатурних систем виявлення вторгнень, які не забезпечують належної ефективності за відсутності повного опису атак і призводять до зростання кількості хибних спрацювань та пропущених загроз.*

Запропоновано концептуальну модель гібридної системи виявлення вторгнень, що поєднує сигнатурний, аномалійний та нечітко-логічний підходи. Для формалізації невизначеності використано апарат нечітких множин, фазифікацію параметрів мережевого трафіку та дефазифікацію з отриманням інтегрального показника загрози. Введено коефіцієнт невизначеності, який дозволяє кількісно оцінити вплив неповної інформації на рівень ризику вторгнення. Запропоновано математичну модель залежності ризику від невизначеності та проаналізовано її властивості.

Підхід ґрунтується на використанні математичного моделювання та методів обробки неточної інформації, що дозволяє підвищити адаптивність систем виявлення вторгнень (IDS) та їхню здатність ефективно функціонувати в умовах невизначеності. Застосування нечіткої логіки, ймовірнісних моделей і алгоритмів машинного навчання створює підґрунтя для зменшення кількості хибних спрацювань і забезпечення більш точного визначення потенційних загроз.

Розроблено алгоритмічний підхід до побудови IDS з адаптивним порогом детекції, який змінюється залежно від рівня невизначеності середовища. Наведено методику оцінювання ймовірності виявлення атак та коефіцієнта хибних спрацювань на основі ROC-кривих, а також числові приклади, що демонструють ефективність запропонованого підходу. Отримані результати підтверджують, що використання нечіткої логіки та ймовірнісних моделей дозволяє підвищити точність виявлення вторгнень, зменшити кількість помилкових тривог і забезпечити адаптивність системи захисту до нових та невідомих сценаріїв атак.

Ключові слова: *виявлення вторгнень, інформаційна безпека, невизначеність, нечітка логіка, ризик, IDS, ROC-крива.*

Вступ

У сучасних умовах функціонування комп'ютерних мереж проблема забезпечення їхньої інформаційної безпеки набуває особливої актуальності. Зростання масштабів кіберзагроз, поява нових методів атак та збільшення обсягів мережевого трафіку роблять завдання виявлення вторгнень надзвичайно складним. Традиційні системи захисту, побудовані переважно на сигнатурному аналізі, виявляються недостатньо ефективними, оскільки вимагають повного та точного опису атак, який у реальних умовах часто відсутній.

Однією з ключових проблем є невизначеність, що виникає у процесі аналізу мережевої активності. Вона зумовлена кількома факторами: неповнотою або спотворенням даних, високою динамічністю поведінки мережі, прихованим характером сучасних атак, а також використанням шифрування, яке ускладнює ідентифікацію загроз. У таких умовах ефективність класичних підходів різко знижується, що призводить до зростання кількості як пропущених атак (false negatives), так і хибних спрацювань (false positives).

Для подолання зазначених обмежень необхідні нові математичні та алгоритмічні підходи, здатні працювати з неточною, частково суперечливою чи неповною інформацією. До таких підходів належать методи нечіткої логіки, ймовірнісні моделі (Баєсівські мережі, марковські процеси), машинне навчання та сценарне моделювання. Використання цих інструментів дозволяє не лише підвищити гнучкість систем виявлення вторгнень (IDS), а й забезпечити їхню адаптивність до нових типів загроз, які раніше не зустрічалися.

Таким чином, актуальною науковою задачею є розробка концептуальної моделі пошуку вторгнень у мережах в умовах невизначеності, яка поєднуватиме математичне моделювання ризиків, нечіткі методи обробки даних та алгоритмічні механізми зменшення кількості хибних спрацювань.

Постановка задачі

Системи виявлення вторгнень (IDS) працюють у середовищі, де: значна частина трафіку має невизначений характер (може бути як легітимним, так і аномальним); джерела атак та їх інтенсивність часто невідомі; поведінка мережі змінюється динамічно.

Традиційні сигнатурні IDS не здатні коректно працювати в таких умовах, оскільки вони вимагають точного опису атак. Необхідне створення моделей, що дозволяють працювати з неповною та неточною інформацією.

1. Аналіз останніх досліджень і публікацій.

В статті [1] проведено дослідження системи захищеності ком'ютера його складових в умовах невизначеності. Для цього складено: кортеж

нечітких множин із складових ком'ютера; проведено його моделювання; розраховані рівні ризиків; рівні захищеності ком'ютера, агрегація результатів, функції належності. Для обрахунків параметрів, використані методи трапеції та трикутника. Розрахунки ілюстровані графічним матеріалом.

В статті [2] досліджується система захисту соціальної мережі від компонентів мережі в умовах невизначеності. Основна увага приділяється нечіткості даних, побудові моделей нечітких множин, оцінці ризиків і рівня безпеки мережевих об'єктів. Запропонований підхід дозволяє розробляти ефективні рішення для прийняття управлінських рішень у контексті кібербезпеки. Представлено алгоритм для побудови кортежа параметрів захисту та їх моделювання за допомогою функцій членства. Методи агрегування результатів і розрахунків із використанням трапецієподібних і трикутних функцій розглядаються окремо. Для цієї мети було скомпільовано наступне: кортеж нечітких множин із компонентів мережі; Було проведено моделювання; Розраховувалися рівні ризику; рівні мережевої безпеки, агрегування результатів, функції членства.

В статті [3] представлено метод кількісного дослідження ризиків, що базується на аналізі й оцінюванні ризиків інформаційних систем. Запропонований підхід дозволяє використовувати широкий спектр параметрів, які забезпечують створення гнучких засобів оцінювання. Цей метод дає можливість розраховувати ризики як на основі статистичних даних, так і на основі експертних оцінок, зроблених в умовах невизначеності та слабкоформалізованого середовища.

Розроблені методи забезпечують представлення результатів у числовій і словесній формах. Наприклад, можливе використання лінгвістичних змінних, які часто застосовують для опису складних систем, що характеризуються параметрами не лише у кількісному, але й у якісному вигляді. Ризики інформаційних систем можуть бути описані через концептуальну модель нечітких множин, яка враховує невизначеність, неточність і суб'єктивність під час їхнього оцінювання.

В статті [4] запропоновано метод оцінювання ймовірності виникнення атак у MANET, що базується на апараті нечіткої логіки. Метод включає побудову кортежу нечітких множин, який описує основні параметри мережі (вразливості вузлів, рівень довіри, поведінкові аномалії тощо), моделювання ризиків з урахуванням експертних оцінок, визначення функцій належності та агрегування результатів для отримання інтегрального показника захищеності.

В статті [5] проведено дослідження системи захисту корпоративної мережі з урахуванням її архітектурних та функціональних складових в умовах часткової або повної невизначеності Для досягнення поставленої мети було побудовано кортеж нечітких множин, що описують найважливіші аспекти функціонування та захисту корпоративної мережі. У кортеж включено як технічні характеристики (наприклад, інтенсивність інформаційного потоку, рівень захисту, параметри витоку даних, активність фаєрволу, роботу системи резервного копіювання тощо), так і організаційні складові (розмежування доступу, політика автентифікації, ідентифікація користувачів, аудит тощо). Кожен з параметрів отримав відповідну нечітку інтерпретацію у вигляді лінгвістичних змінних: "низький", "середній", "високий" рівень.

В статті [6] представлено підхід до аналізу безпеки інформації в корпоративних та локальних мережах в умовах невизначеності на основі теорії нечітких множин. Запропоновано методику, що поєднує математичне моделювання, експертні оцінки та інструменти нечіткої логіки для оцінювання ефективності системи захисту. Розглянуто вплив параметрів внутрішніх складових мережі та зовнішніх факторів, проведено оцінку їх значущості за допомогою методів PRCC та Sobol-аналізу. Наведено приклади обчислень, графічні ілюстрації та рекомендації щодо підвищення рівня захищеності інформації. Результати підтверджують доцільність застосування нечітких множин як інструменту для прийняття рішень у сфері кіберзахисту в умовах невизначеності.

В статті [7] відмічається, що один з актуальних напрямків, що розвиваються в області інформаційної безпеки, пов'язаний з використанням Honeypots (віртуальних приманок, онлайн-пасток), а вибір критеріїв для визначення найбільш ефективних Honeypot і їх подальшої класифікації є актуальним завданням. Представлені основні продукти, в яких реалізовані технології віртуальної приманки. Вони часто використовуються для вивчення поведінки, підходів і методів, які використовує стороння сторона для отримання несанкціонованого доступу до ресурсів інформаційної системи. Онлайн-хуки можуть імітувати будь-який ресурс, але частіше вони виглядають як справжні продакшн-сервери та робочі станції.

В статті [8] розглядається один із нових та перспективних підходів до вирішення проблеми оцінювання кібербезпеки на об'єктах критичної інфраструктури з використанням теорії нечітких множин, наприклад, для оцінки ризиків інформаційної безпеки. На практиці трапляються ситуації, коли на розрахунок кінцевих результатів істотно впливають невідповідності висновків або помилки експертів. Тому, щоб мінімізувати такі похибки, пропонується методи фазирування інтервалів шляхом перетворення їх у нечіткі числа.

В статті [9] для моделювання ризику інформаційної безпеки підприємства запропоновано нечіткі моделі надавати у вигляді нечітких мереж. Модель містить бази правил і дозволяє проводити лінгвістичний аналіз ризиків, які несуть потенційні загрози і збиток організації. Використовуваний в методиці механізм отримання оцінок ризику на основі нечіткої логіки дозволяє отримати чисельне значення ризику, лінгвістичний опис ступеня ризику, а також рівень впевненості експерта у виникненні ризикової події.

Монографія [10] присвячена теоретико-методологічним і практичним аспектам розробки методів ідентифікації аномальних станів та методології побудови систем виявлення вторгнень. У роботі проведено аналіз засобів виявлення зловживань та аномалій. Значну увагу приділено формалізації процесу створення mi-вимірних параметричних, атакуючих, еталонних, поточних та детекційних середовищ. Це є підґрунтям для створення засобів, які дозволять автоматизувати процес детектування в слабоформалізованому нечітко визначеному середовищі аномальний стан, що породжується кібератаками, у заданий проміжок часу шляхом контролю поточного стану множини визначених параметрів.

Монографія [11] присвячена теоретико-методологічним і практичним аспектам оцінювання ризиків інформаційної безпеки. У роботі проведено аналіз базових понять, методів, моделей, засобів та міжнародних нормативних документів, пов'язаних з оцінюванням і управлінням ризиками. Значну увагу приділено розробленню методів модифікації порядку лінгвістичної змінної при перевизначенні еталонів параметрів, а також оцінювання ризиків безпеки ресурсів інформаційних систем в реальному часі з використанням CVSS метрик, які містяться у відкритих базах даних уразливостей.

В статті [12] відзначається, що одним з методів оцінки ризиків інформаційної безпеки є обґрунтований вибір і здійснення протидії загрозам. Ситуативна нечітка модель OWA багатокритеріальна. Вирішення проблеми вибору заходів протидії зниженню інформаційної безпеки пропонуються ризики. Запропонована модель дає можливість модифікувати пов'язані ваги критеріїв на основі інформаційної ентропії щодо ситуації агрегації. Перевагою модель полягає в постійному вдосконаленні вагових коефіцієнтів критеріїв і агрегації експертів. думки в залежності від параметра, що характеризує ситуацію агрегації.

В роботі [13] досліджується поєднання оцінку ризику (RA) і нечіткої логіки (FL), де: «Оцінка ризику – це загальний процес ідентифікації, аналізу та оцінки ризику. Ідентифікація ризику включає розуміння джерел ризику, сфер впливу, подій та їх причини та можливі наслідки. Мета полягає в тому, щоб створити вичерпний перелік ризиків, включаючи ризики, які можуть бути пов'язані з втраченими можливостями, і ризики, пов'язані з прямим контролем організації. Комплексний огляд дозволяє повністю розглянути потенціал вплив ризику на організацію».

У статті [14] розроблено підхід на основі аналізу оболонок даних (DEA) для вирішення MOSPP з нечіткими параметрами (FMOSPP) для врахування реальних ситуацій, коли вхідні-вихідні дані включають невизначеність трикутної форми членства. Цей підхід до встановлення зв'язку між MOSPP і DEA є більш гнучким для реального практичного застосування. У зв'язку з цим кожна дуга в FMOSPP розглядається як одиниця прийняття рішень з безліччю нечітких входів і виходів. Потім отримують дві нечіткі оцінки ефективності, що відповідають кожній дузі. Ці нечіткі оцінки ефективності об'єднані для визначення унікальної нечіткої відносної ефективності.

В статті [15] розглядаються різнітипи шкідливих атак, такі як електронні віруси, шкідливе програмне забезпечення, шкідливий код, та інші кіберзагрози, в першу чергу, які впливають на інформаційні системи. Системні адміністратори не знають типу та рівня атаки. Коли зловмисники зламують комп'ютерні системи, і вони не впевнені в діях, які необхідно вжити для захисту. Тому – наукові цілі визначити ці типи кібератак за допомогою теорії нечітких множині випустити попередження для адміністраторів, спонукаючи їх до вжиття необхідних дій.

В статті [16] описується кібербезпека промислової системи управління яка є дуже складна і складна тема дослідження, з огляду на інтеграцію цих систем у національні критичні

інфраструктури. Системи управління зараз з'єднані між собою в промислові мережі і часто підключені до Інтернет. У цьому контексті вони стають мішенями різних кібератак зловмисників таких як хакери, промислові шпигуни тощо та розвідувальні служби. Автори пропонують спосіб моделювання профілів зловмисників і оцінки рівня успіху нападу, проведений у заданих умовах. Автори використовують нечіткий підхід для створення профілів зловмисників на основі атрибутів зловмисника, такі як знання, техресурсів і мотивації.

В літературних джерелах [1,3,7,8,10 – 16] не розглядаються пошук вторгнень у мережах в умовах невизначеності, що являється недоліком, в [2] розглядаються окремий тип мереж-соціальні, в [4] розглядаються окремий тип мереж – MANET, в [5] проведено дослідження системи захисту корпоративної мережі, в [6] – в корпоративних та локальних мережах в [9] для моделювання ризику інформаційної безпеки підприємства запропоновано нечіткі моделі надавати у вигляді нечітких мереж. Загальним недоліком [2,4,5,10] являється використання одного типу математичних моделей та розгляд якогось конкретного типу мереж.

2. Мета статті

Розробити концептуальну модель пошуку вторгнень у комп'ютерних мережах, що функціонує в умовах невизначеності, та обґрунтувати використання математичних інструментів для зменшення кількості хибних спрацювань.

3. Основний матеріал

3.1 Математичне моделювання

Введення функцій ризику R(t), що залежить від ступеня захищеності системи та ймовірності атаки. Використання нечітких множин для опису станів «нормальний трафік», «підозрілий», «атака». Застосування функцій приналежності для гнучкого прийняття рішень.

3.2 Методи обробки невизначеності

Фазифікація даних мережевого трафіку (пакети, затримки, відхилення від нормальних моделей). Дефазифікація – отримання інтегрального показника загрози. Використання ймовірнісних методів (Баєсівський підхід) для обчислення апостеріорної ймовірності атаки.

3.3. Алгоритмічний підхід

Побудова гібридної IDS з двома модулями: сигнатурним і адаптивним (fuzzy/ML). Використання сценарного моделювання атак з урахуванням неповних даних. Адаптація параметрів моделі в реальному часі.

Проміжні висновки

Пошук вторгнень у мережах в умовах невизначеності вимагає комплексного підходу, що поєднує математичне моделювання, нечітку логіку та алгоритми машинного навчання. Це дозволяє підвищити точність виявлення атак, знизити кількість хибних спрацювань та забезпечити адаптивність систем захисту до нових сценаріїв загроз.

3.4. Математична модель

Функція ризику вторгнення

$$R = f(P_a, C_s, U)$$

де: P_a – ймовірність атаки, C_s – коефіцієнт стійкості системи, U – коефіцієнт невизначеності. Приклад:

$$R = P_a(1 - C_s)(1 + U)$$

3.5 Методи обробки невизначеності

Фазифікація параметрів трафіку:

Виділяємо три лінгвістичні змінні:

- Швидкість аномалій (A): низька, середня, висока;
- Відхилення від нормальної поведінки (D): мале, середнє, значне;
- Ймовірність атаки (P): низька, середня, висока (табл. 1).

Таблиця 1. Приклад правил фазифікації

Значення P	Функція μ(P)
0–0.3	"низька"
0.2–0.7	"середня"
0.6–1.0	"висока"

Функції приналежності (приклад для P,A,D – рис. 1-3):

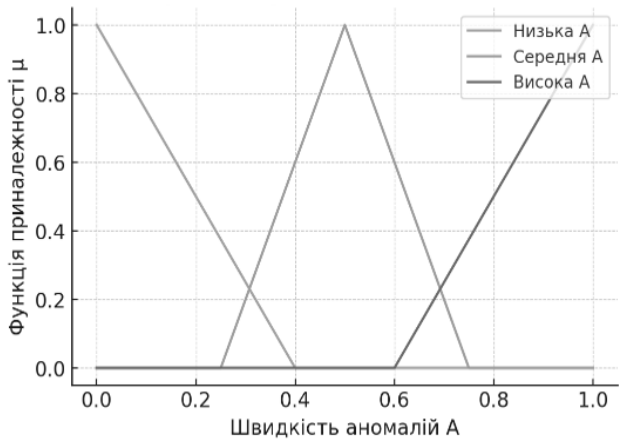

Рисунок 1. Функції приналежності для ймовірності атаки P

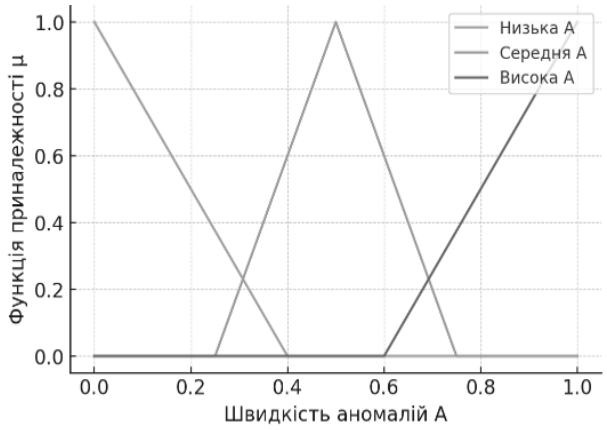

Рисунок 2. Функції приналежності для швидкості аномалій A

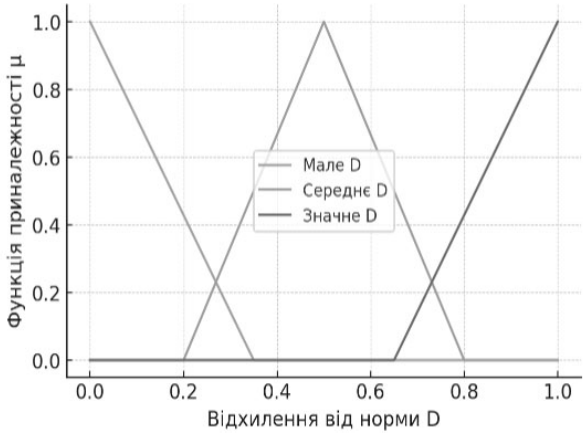

Рисунок 3. Функції приналежності для відхилення D

Аналіз впливу невизначеності (табл. 2).

Таблиця 2. Залежність ризику від коефіцієнта невизначеності U

U (невизначенність)	R (ризик)
0.0	0.180
0.2	0.216
0.4	0,252
0.6	0.288
0.8	0.324

Пояснення до табл. 2

У таблиці ризик R явно зростає прямо пропорційно до коефіцієнта невизначеності U.

Перевіримо приріст:

$$R(0.2)-R(0.0)=0.216-0.180=0.036,$$
$$R(0.4)-R(0.2)=0.252-0.216=0.036,$$
$$R(0.6)-R(0.4)=0.288-0.252=0.036,$$
$$R(0.8)-R(0.6)=0.324-0.288=0.036$$

Отже, кожні +0.2 U дають +0.036 R. Це лінійна залежність.

Формула. Можна припустити, що вона має вигляд:

$$R(U)=a+b\cdot U$$

Підставимо значення: при U=0, R=0.180, a=0.18; при U=0.2, R=0.216 ($0.180+b\cdot 0.2=$ $= 0.216$ b=0.18)

Перевіримо інші точки:

$$R(0.4)=0.180+0.18\cdot 0.4=0.180+0.072=$$
$$= 0.252, R(0.8)=0.180+$$
$$+0.18\cdot 0.8 =0.180+0.144=0.324$$

Отже:

$$R(U)=0.180+0.18\cdot U$$

Таким чином, значення у табл. 2 визначені за лінійною моделлю залежності ризику від коефіцієнта невизначеності, де початковий ризик при нульовій невизначеності = 0.180, а коефіцієнт приросту = 0.18 (рис. 4).

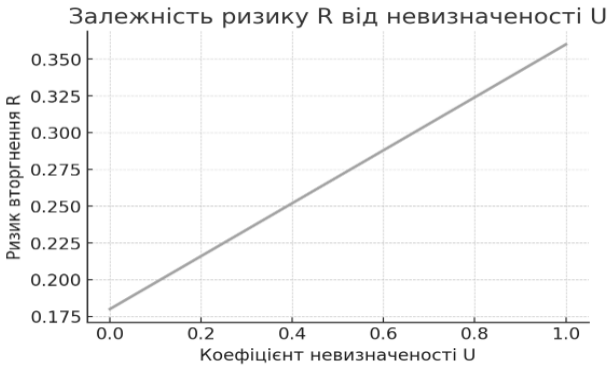

Рисунок 4. Залежність ризику R від коефіцієнта невизначеності U

З графіка видно, що збільшення невизначеності прямо пропорційно підвищує інтегральний ризик.

Дефазифікація – інтегральний показник загрози (T) (табл. 3).

$$T = \frac{\sum \mu_i x_i}{\sum \mu_i}$$

де x_i – центр відповідного нечіткого інтервалу.

Таблиця 3. Приклад фазифікації параметрів трафіку

Параметр	Значення	Нечіткий стан	μ
Аномалії A	0.55	середня	0.6
Відхилення D	0.7	високе	0.8
Ймовірність P	0.6	середня/висока	0.5 / 0.5

Після дефазифікації отримуємо T = 0.62 (середній рівень загрози).

Проміжний висновок. В умовах невизначеності ризик вторгнень зростає навіть при відносно високому рівні стійкості мережі. Поєднання фазифікації параметрів трафіку з ймовірнісними моделями дозволяє більш гнучко оцінювати рівень загрози. Використання коефіцієнта невизначеності U у моделі дозволяє кількісно оцінити вплив неповної інформації на результати аналізу. Запропонований підхід може стати основою для побудови гібридних IDS нового покоління.

3.6 Алгоритмічний підхід

Основа для того, щоб зв'язати математичні графіки та нечітку модель із реальною системою виявлення вторгнень (IDS).

Вхідні параметри IDS. Швидкість аномалій (A) – кількість підозрілих пакетів за певний інтервал часу. Відхилення (D) – наскільки поведінка користувача чи вузла відрізняється від «нормального профілю». Ймовірність атаки (P) – агрегований показник із сигнатурного аналізу (збігів з базою атак).Ці дані IDS отримує з сенсорів: моніторингу трафіку, журналів подій, поведінкової аналітики.

Нечітка логіка в IDS. Графіки функцій приналежності (які ми побудували для P, A, D – рис. 1-3) задають «м'які межі» замість жорстких порогів. Наприклад, якщо аномалії A=0.55, система не одразу каже «атака», а визначає, що це 60% середнього рівня. Це знижує кількість хибних спрацювань (false positives). Інтегральний показник загрози (T). Система обчислює значення T (після дефазифікації). Якщо $T < 0.3 \rightarrow$ нормальний стан, $0.3 \leq T < 0.6$ – підозрілий стан (IDS піднімає попередження), $T \geq 0.6$ – висока загроза (IDS генерує сигнал тривоги або запускає IPS-правило).

Вплив невизначеності (U)

IDS часто працює з неповними даними (пакети втрачаються, трафік шифрований, джерело неідентифіковане). Коефіцієнт U у нашій моделі якраз враховує цей фактор. Як показує графік R=f(U) (рис.4), навіть при середній загрозі невизначеність може «підняти» рівень ризику, тому IDS має адаптивно змінювати політику реагування.

Архітектурна інтеграція (рис. 5)

Сигнатурний модуль – дає базові значення P. Аномалійний модуль – рахує A та D. Модуль нечіткої логіки – комбінує ці параметри у показник T. Модуль ухвалення рішень – формує дії (лог, сповіщення, блокування).

Таким чином, графіки (функції приналежності та R(U)) ілюструють, як IDS може працювати в умовах невизначеності: не за принципом «чорне/біле», а за принципом «ступеня ризику».

Схема архітектури IDS з модулем нечіткої логіки. Мережевий трафік (вхідні дані). Сигнатурний аналіз (P) – перевірка на збіги з відомими атаками. Аномалійний аналіз (A, D) – виявлення відхилень від нормальної поведінки. Модуль нечіткої логіки (T) – обробка P, A, D з урахуванням функцій приналежності. Модуль ухвалення рішень – інтегральна оцінка ризику. Дії системи – логування, сповіщення, блокування.

3.7 Ймовірність знаходження вторгнень (Detection Probability) для пропонованої IDS. Загальна ідея. Система ухвалює рішення на основі дефазифікованого інтегрального показника загрози $T \in [0,1]$. Приймаємо просте правило: IDS сигналізує про вторгнення, якщо $T \geq \theta$, PD= = θ? де: θ – поріг детекції

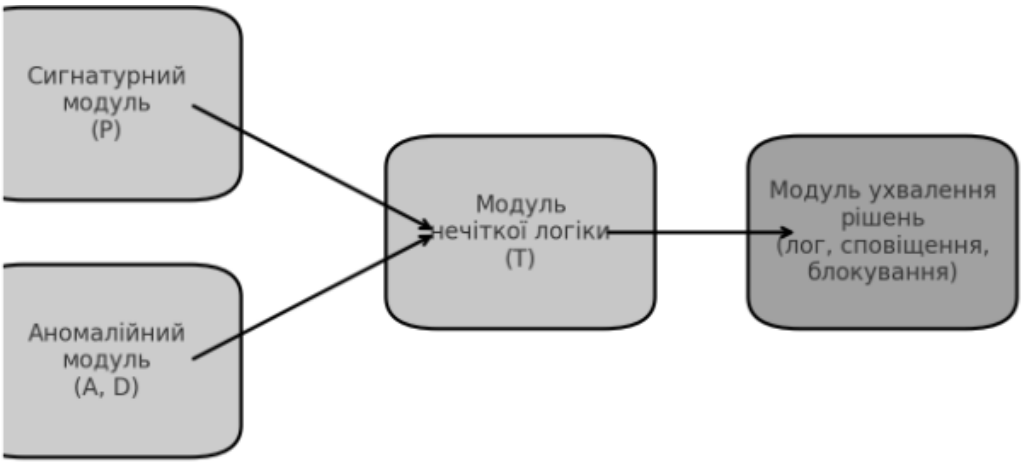

Рисунок 5. Схема архітектурної інтеграції: сигнатурний та аномалійний модулі подають дані у блок нечіткої логіки, який формує показник T, а далі рішення приймає модуль дій (логування, сповіщення, блокування).

(threshold). IDS (система виявлення вторгнень) подає сигнал про атаку, якщо: T≥ θ?. де: T – інтегральний показник підозрілості (обчислений модулем нечіткої логіки на основі параметрів P,A,D); θ – поріг детекції (threshold), тобто мінімальне значення показника T, після якого вважається, що в мережі відбулася атака.

Складові поняття "порогу атаки". Поріг θ формується з урахуванням кількох складових: ймовірнісна частина (P). Результати сигнатурного модуля: чи відповідає подія відомим шаблонам атаки. Дає базове значення ризику.

Аномальна частина (A, D). A – ступінь відхилення від "нормальної" поведінки (аномалія трафіку, користувачів тощо), D – динаміка відхилень (наскільки швидко наростає підозрілий тренд), P – вказує, наскільки ймовірно, що спостережувана поведінка є шкідливою, навіть без точного сигнатурного збігу.

Нечітка інтеграція.Модуль нечіткої логіки комбінує P,A,D у єдиний показник T. Це дозволяє враховувати невизначеність: навіть слабкі сигнали можуть підняти T, якщо вони збігаються.

Поріг θ**.** Встановлюється адміністратором або обчислюється адаптивно (залежно від навантаження, історії атак, профілю користувачів). Якщо зробити θ занадто низьким – буде багато false positives (помилкових тривог). Якщо занадто високим – є ризик **false negatives** (атака пройде непоміченою).

Інтерпретація умови. Якщо T< θ – IDS вважає подію нормальною. Якщо T≥ θ – IDS сигналізує: спрацьовує логування, надсилається сповіщення чи блокується сесія (рис. 6).

Точка перетину: при U≈0.50U інтегральний показник T досягає порога θ=0.27. Саме з цього моменту IDS починає сигналізувати про вторгнення.

3.8 Модель шумів / невизначеності. Моделюємо отриманий T як детерміновану частину + шум, що залежить від невизначеності U:

$$T = \mu_T + \varepsilon, \quad \varepsilon \sim N(0, \sigma_T^2(U)),$$

де μ_T — середнє дефазифіковане значення при поточному стані (інтрузія або норма), а $\sigma_T(U)$ — стандартне відхилення помилки, що зростає з U. Часто зручно взяти просту залежність:

$$\sigma_T(U) = \sigma_0 + kU, k > 0$$

де: σ_0 - базова похибка визначення T (при U =0), $k > 0$ – коефіцієнт 2.

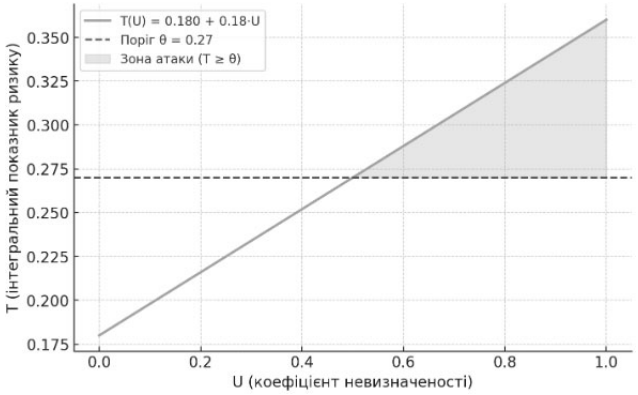

Рисунок 6. IDS сигналізує: спрацьовує логування, надсилається сповіщення чи блокується сесія

Аналітичний вираз для P_D (при нормальному шумі):

$$P_D = 1 - \Phi(\frac{\theta - \mu_{T,}атак}{\sigma_T, атак}),$$

$$FPR = 1 - \Phi(\frac{\theta - \mu_{T,}norm}{\sigma_T, norm}),$$

де: Φ – стандартна нормальна функція розподілу, $\mu_{T,}norm$ та $\mu_{T,}атак$ – середні T у двох класах, а σ_T – відповідні стандартні відхилення.

Числовий приклад (кроки обчислення)

Візьмемо прикладні значення: при атаці: μ_T =0.72, при нормі: μ_T norm=0.25, базова похибка σ_0 =0.08, вплив невизначеності k=0.12, поточна невизначеність U=0.3.

Спочатку обчислюємо σ_T**:** k·U=0.12×0. =0.0360. Додаємо σ_0, σ_T =0.08+0.036=0.116. Отже σ_T ,attack= σ_T ,norm=0.116 (для простоти припускаємо однакову похибку).

Візьмемо поріг θ=0.60. Тепер обчислюємоP_D: Знайдемо z-значення:

$$z_D = \frac{\theta - \mu_{T,}атак}{\sigma_T} = \frac{0.60 - 0.72}{0.116} \approx -1.03448$$

Так як Φ(−1.03448)≈ ≈0.1506\ Φ (-1.03448). то P_D≈1−0.1506=0.8494P_≈ 84.9%.

Тепер FPR:

$$z_{FP} = \frac{\theta - \mu_{T,}norm}{\sigma_T} = \frac{0.60 - 0.15}{0.116}) \approx 0.9987,$$

отже FPR=1−0.9987=0.- ≈ 0.13%.

де: Φ=(θ−μ attack)/σ).

Висновок для прикладу: при заданих параметрах θ=0.60 система має PD≈85% і FPR≈0.13%. Результати сильно залежать від μ-значень (тобто від того, як побудовані функції приналежності, як проведена дефазифікація) та

від σ_T (вплив невизначеності). Зі збільшенням U зростає σ_T (припущення), отже розподіли класів «атака/норма» більше накладаються – за фіксованого порога θ знижується і одночасно може зрости FPR (залежить від відстані між μ). Можна зробити адаптивну стратегію: змінювати поріг θ в залежності від U — наприклад знижувати θ, коли U великий, щоб бути більш консервативним ("ловити" більше атак), або підвищувати θ, якщо важливо тримати низький FPR.

Приклад адаптивного правила (проста лінійна політика):

$$\theta(U) = \theta_0 - \beta U \qquad \beta \in [0,1]$$

де: θ_0 – базовий поріг, β = налаштування «консервативності»

Це надає простий контроль компромісу $P_D \leftrightarrow FPR$

3.9 Практичні кроки для оцінки і налаштування IDS. Калібрування μ-значень**:** для кожного класу (атака/норма) зберіть вибірку сигналів (P, A, D), пропустіть через нечіткий модуль і отримаєте емпіричні розподіли T. Оцініть μ та σ для кожного класу (наприклад, методом максимальної правдоподібності).

Побудова ROC-кривої: варіюємо θ від 0 до 1, для кожного θ обчислюйте PD_i FPR – отримаємо R. Вибираємо робочу точку залежно від бізнес-втрат (витрати на пропущену атаку, витрати на хибні тривоги).

Врахування U у режимі реального часу: оцінимо U (наприклад, частка втрачених пакетів, кількість зашифрованого трафіку, якість логів). Модифікуємо σ_T або θ відповідно до значення U.

Валідація та stress-test: Виконуємо симульовані сценарії (DoS, розгалужені сканування, складні мультистадійні атаки) і визначаємо, як змінюється P_D при різних U.

Резюме. Детекція базується на T (дефазифікованому показнику) і порозі θ. Якщо моделювати шум як нормальний з дисперсією, що зростає з U, то P_D аналітично виражається через нормальний розподіл: $P_D=1-\Phi(\theta-\mu\ attack)/\sigma)$..

3.10 Оцінка ефективності системи виявлення вторгнень за допомогою ROC-кривої

Вступ. Для оцінки ефективності системи виявлення вторгнень (IDS) використовують дві ключові метрики: ймовірність виявлення (Detection Probability, PD) – частка реальних атак, які система успішно виявляє. Коефіцієнт помилкових спрацьовувань (False Positive Rate, FPR) – частка нормального трафіку, помилково класифікованого як атака.

Зміна порогового параметру θ впливає на обидві метрики: при зниженні θ зростає PD, але також зменшується FPR, і навпаки. Графічне відображення залежності цих метрик від порогу дає ROC-криву (Receiver Operating Characteristic), яка є стандартним інструментом оцінки IDS (рис. 7).

Формули. Ймовірність виявлення PD та FPR можна обчислити за формулами:

$$P_D(\theta,U) = \frac{N_{\det ected}(\theta,U)}{N_{attacks}},$$

$$FPR(\theta,U) = \frac{N_{false\ positive}(\theta,U)}{N_{normal}}$$

де: $N_{\det ected}$ – кількість атак, які система виявила; $N_{attacks}$ – загальна кількість атак;

$N_{false\ positive}$ – кількість нормальних подій, помилково класифікованих, як атаки;

N_{normal} – загальна кількість нормальнимх подій: U – параметр середовища або інтенсивності трафіку

Числовий приклад. Розглянемо систему IDS, яка аналізує 100 подій, з яких 40 — атаки, 60 — нормальний трафік. Вибір порогів θ=[0.2,0.4,0.6,0.8] та параметрів U=[0.5,0.7,1.0] дає такі результати (табл. 4).

Таблиця 4. P_D та FPR для різних порогів θ і U

θ	N_detected	N_false positive	U	P_D	FPR
0.2	0.7	39	20	0.975	0.33
0.4	0.7	37	14	0.925	0.23
0.6	0.5	32	6	0.80	0.10
0.8	0.5	28	3	0.70	0.05
0.6	0.7	33	7	0.825	0.12
0.8	0.7	29	4	0.725	0.07
0.2	1.0	40	22	1.00	0.37
0.4	1.0	38	15	0.95	0.25
0.6	1.0	34	8	0.85	0.13
0.8	1.0	30	5	0.75	0.08
0.2	0.5	38	18	0.95	0.30
0.4	0.7	37	14	0.925	0.23

Пояснення: збільшення U (наприклад, навантаження мережі) підвищує як ймовірність виявлення PD , так і FPR.

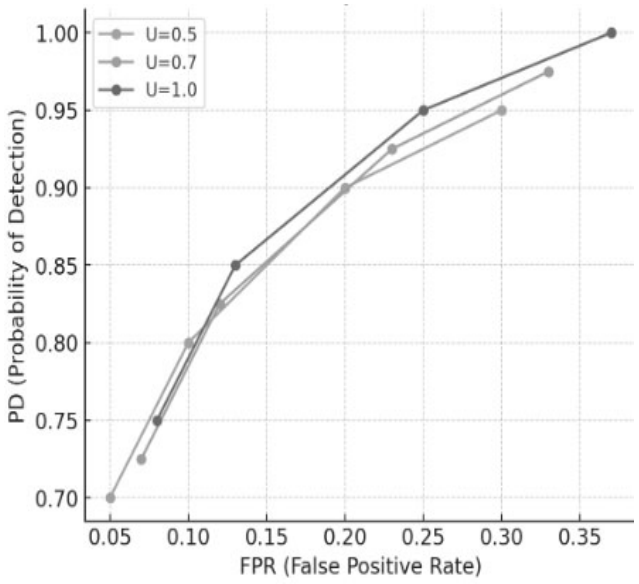

Рисунок 7. ROC-крива IDS для різних порогів θ та параметрів U.

ROC-крива та графіки. На основі таблиці будується ROC-крива: вісь X — FPR, вісь Y — PD.. Додатково можна побудувати графіки залежності PD(θ) та FPR(θ) для наочного аналізу (рис. 8,9).

ROC-крива IDS**.** На графіку показано залежність ймовірності виявлення P_D від коефіцієнта помилкових спрацьовувань FPR для різних порогів θ і значень параметра середовища U. Кожна крива відповідає певному значенню U. ROC-крива дозволяє оцінити баланс між чутливістю системи та частотою помилкових спрацьовувань, а також обрати оптимальний поріг θ.

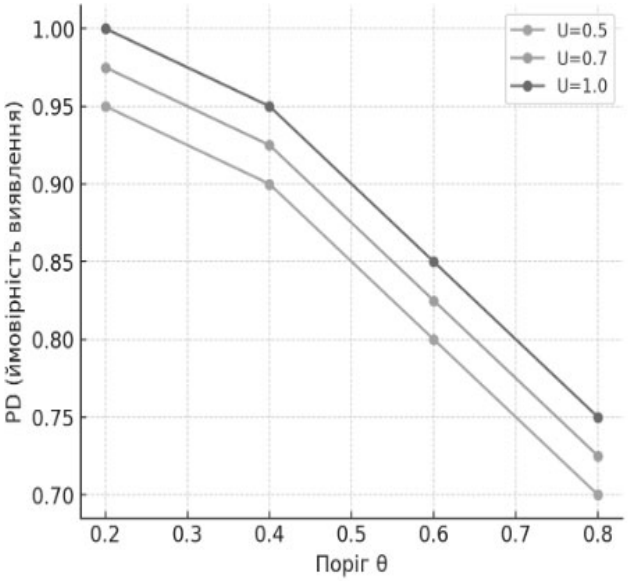

Рисунок 8. P_D від θ при різних U

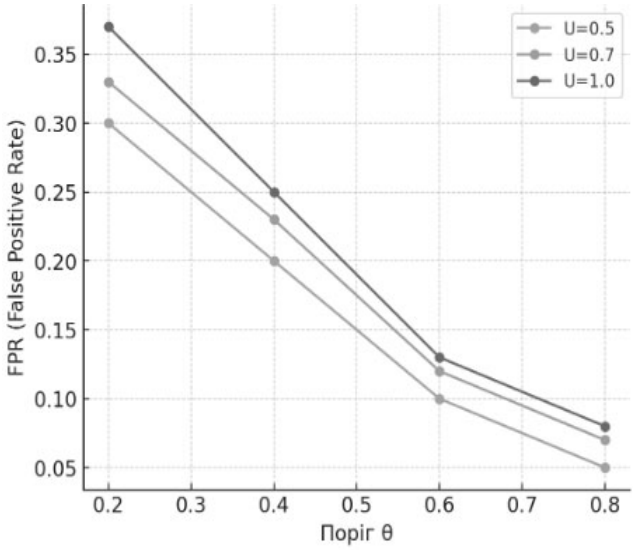

Рисунок 9 Залежність FPR(θ) для різних U

На графіку відображено зміну ймовірності виявлення атак IDS при різних порогах θ для трьох значень параметра U. Зменшення порогу підвищує P_D, однак одночасно може зростати FPR (рис.9).

На графіку показано зміну коефіцієнта помилкових спрацьовувань при різних порогах θ та значеннях U. Зменшення порогу θ збільшує FPR, що демонструє необхідність компромісного вибору порогу для балансування чутливості системи та кількості помилкових спрацьовувань. Блок- схема, яка показує, як фактори невизначеності впливають на IDS (рис. 10)

Рисунок 10 Вплив факторів невизначенності на IDS

Висновки. У ході аналізу встановлено, що проблема виявлення вторгнень у комп'ютерних мережах значною мірою ускладнюється впливом факторів невизначеності, серед яких основними є неповнота даних, варіативність мережевої поведінки та динамічність загроз.

Традиційні сигнатурні методи, які базуються на точному описі атак, не забезпечують

належного рівня захисту в сучасних умовах, що призводить до підвищення ймовірності як пропуску атак, так і хибних спрацювань.

Запропонований підхід ґрунтується на використанні математичного моделювання та методів обробки неточної інформації, що дозволяє підвищити адаптивність систем виявлення вторгнень (IDS) та їхню здатність ефективно функціонувати в умовах невизначеності. Застосування нечіткої логіки, ймовірнісних моделей і алгоритмів машинного навчання створює підґрунтя для зменшення кількості хибних спрацювань і забезпечення більш точного визначення потенційних загроз.

Таким чином, формування концептуальної моделі IDS, здатної враховувати невизначеність, є перспективним напрямом розвитку систем кіберзахисту корпоративних та локальних мереж.

Треба відмітити, що: виявлення вторгнень у мережах ускладнене через невизначеність (неповнота даних, варіативність поведінки, динамічність загроз). Традиційні сигнатурні методи мають обмеження: підвищують ризик пропуску атак та кількість хибних спрацювань. Використання математичного моделювання та методів обробки неточної інформації підвищує адаптивність IDS. Нечітка логіка, ймовірнісні моделі, машинне навчання зменшують кількість хибних спрацювань та покращують точність визначення загроз.

Перспективним є розробка концептуальної моделі IDS, здатної враховувати невизначеність у корпоративних та локальних мережах. Зниження порогу θ підвищує ймовірність виявлення атак, але одночасно зростає FPR. Збільшення параметра U (інтенсивності трафіку або навантаження мережі) зміщує криву вгору, що може призводити до більшої кількості помилкових спрацьовувань. ROC-крива дозволяє візуально оцінити баланс між чутливістю IDS та кількістю помилкових спрацьовувань, а також обрати оптимальний поріг θ.

Література

[1]. Вадим Ахрамович, Володимир. Ахрамович. Метод розрахунку показника захисту інформації ком'ютера в умовах невизначеності. Information Technology and Security.January-June2025. Vol. 13. Iss. 1(24) pp. 55-68. DOI 10.20535/2411-1031.2025.13.1.328898.

[2]. Володимир Ахрамович, Олександр Лаптєв, Анна Ільєнко, Вадим Ахрамович. Метод розрахунку захисту інформації у соціальних мережах в умовах нечітких множин. Безпека інформації, Том 30 № 3 (2024): с. 358-364.

[3]. Володимир Ахрамович, Вадим Ахрамович, Микола Браіловський, Юрій Пепа, Тетяна Лаптєва. Кількісне дослідження ризиків методом нечітких множин. Information Systems and Technologies Security, № 1(9)/2025 – с. 18-25

[4]. Володимир. Ахрамович, Вадим. Ахрамович. Метод розрахунку можливості появи атак в мережі MANET в умовах невизначеності. Information Technology and Security. July-December 2025. Vol. 13. Iss.2(25)pp. 334-345. DOI 10.20535/2411-1031.2025.13.1.328898.

[5]. Анна Ільєнко, Вадим Ахрамович. Метод розрахунку захисту корпоративної мережі в умовах невизначеності. Кібербезпека:освіта, наука техніка. № 1 (29), 2025. -с. 480-492.

[6]. Володимир Ахрамович, Вадим Ахрамович. Аналіз безпеки інформації в корпоративних та локальних мережах в умовах нечітких множин // Безпека інформації, Том 31 № 1 (2025): с. 15-22.

[7]. A. Korchenko, V. Breslavskyi, S. Yevseiev, N. Zhumangalieva, A. Zvarych, S. Kazmirchuk, O. Kurchenko, O. Laptiev, O. Sievierinov, S. Tkachuk, Development of a method for constructing linguistic standards for multi-criteria assessment of honeypot efficiency, EasternEuropean Journal of Enterprise Technologies, 2021. Vol.111. №.3/9. pp. 63-83. DOI:10.15587/1729-4061.2021.225346, https://www.researchgate.net /publication /349850679_Development_of_a_method_for_constructing_linguistic_ standards _for_multi-criteria_assessment_of_honeypot_efficiency

[8]. С. П. Євсеєв, О. В. Шматко, Н. В. Ромащенко, Алгоритм оцінювання ступеня ризику інформаційної безпеки, що базується на нечіткомножинному підході, Сучасні інформаційні системи, 2019. Т. 3, № 2. С. 73-79. DOI: 10.18372/2225-5036.29.18068, https://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/18068

[9]. О. В. Кочетков, Т. О. Гаур, В. М. Машін, Система оцінки ризиків інформаційної безпеки підприємства на основі нечіткої логіки, Наукові праці ОНАЗ ім. О.С. Попова. 2019., № 1. С. 97-104. DOI 10.33243/2518-7139-2019-1-1-97-104, https://ojs.suitt.edu.ua › index.php › article › view

[10]. А.О. Корченко, Методи ідентифікації аномальних станів для систем виявлення

вторгнень, Монографія, Київ, ЦП «Компринт», 2019, 361 с. https://nubip.edu.ua/sites/default/files/u34/monografiya_korchenko_anna_1.pdf

[11]. Security Risk Management. Automatic Control and Computer Sciences, 2021, Vol. 45, No. 1, pp. 20-28. https://www.researchgate.net/publication/265520240_Fuzzy_Owa_ Model_for_ Information_Security_Risk_Management_YN_Imamverdiyev_SA_Derakshande_Automatic_Control_and_Computer_Sciences_45_1_20-28

[12]. Arnold F. Shapiro. Risk Assessment Applications of Fuzzy Logic. Casualty Actuarial Society, Canadian Institute of Actuaries, Society of Actuaries, All Rights Reserved. https://translate.google.com/?sl=en&tl=uk&text=%20Casualty %20Actua rial%20Society %2C%20Canadian%20Institute%20of%20Actuaries%2C% 20Society%20of%20Actuaries%2C%20All%20Rights%20Reserved&op=translate

[13]. M. Bagheri, Ali Ebrahimnejad, S. Razavyan, F. Hosseinzadeh, N. Malekmohammadi. Solving fuzzy multi-objective shortest path problem based on data envelopment analysis approach. Complex & Intelligent Systems (2021) 7:pp. 725-740 https://doi.org/10.1007/s40747-020-00234-4

[14]. Sastry VN, Janakiraman TN, Mohideen SI (2003) New algorithms for multi objective shortest path problem. Opsearch 40(4): pp. 278-298https://www.researchgate.net/publication /265545561_New_Algorithms_For_Multi_Objective_Shortest_Path_Problem.

[15]. Emil Pricop, Sanda Florentina Mihalache. Fuzzy approach on modelling cyber attacks patterns on data transfer in industrial control systems. ECAI 2019 – International Conference – 7th Edition Electronics, Computers and Artificial Intelligence 25 June -27 June, 2019, pp.-1-6. Bucharest, ROMÂNIA

[16]. Saša D Milić. Fuzzy-Decision Algorithms for Cyber Security Analysis of Advanced SCADA and Remote Monitoring Systems. Chapter 7. DOI: 10.4018/978-1-7998-2910-2.ch007. www.igi-global.com/chapter/fuzzy-decision-algorithms-for-cyber-security analysis-of-advanced-scada-and-remote-monitoring.

INTRUSION DETECTION IN NETWORKS UNDER CONDITIONS OF UNCERTAINTY

Abstract. The article addresses the problem of intrusion detection in computer networks under conditions of uncertainty caused by incomplete and inaccurate data, the dynamic nature of network traffic, the concealed character of modern attacks, and the use of encryption mechanisms. The limitations of traditional signature-based intrusion detection systems are demonstrated, as they fail to provide sufficient effectiveness in the absence of complete attack descriptions and lead to an increased number of false positives and missed threats.

A conceptual model of a hybrid intrusion detection system is proposed, combining signature-based, anomaly-based, and fuzzy-logic approaches. To formalize uncertainty, fuzzy set theory is employed, including fuzzification of network traffic parameters and defuzzification to obtain an integral threat indicator. An uncertainty coefficient is introduced, enabling a quantitative assessment of the impact of incomplete information on the level of intrusion risk. A mathematical model describing the dependence of risk on uncertainty is proposed and its properties are analyzed.

The approach is based on mathematical modeling and methods for processing imprecise information, which enhances the adaptability of intrusion detection systems (IDS) and their ability to operate effectively under uncertainty. The application of fuzzy logic, probabilistic models, and machine learning algorithms provides a foundation for reducing false alarms and achieving more accurate identification of potential threats.

An algorithmic approach to constructing an IDS with an adaptive detection threshold that varies according to the level of environmental uncertainty is developed. A methodology for evaluating the probability of attack detection and the false positive rate using ROC curves is presented, along with numerical examples demonstrating the effectiveness of the proposed approach. The results confirm that the use of fuzzy logic and probabilistic models improves intrusion detection accuracy, reduces the number of false alarms, and ensures the adaptability of protection systems to new and previously unknown attack scenarios.

Keywords: intrusion detection, information security, uncertainty, fuzzy logic, risk, IDS, ROC curve.

Ахрамович Володимир Миколайович,
д.т.н., проф., професор кафедри кібербезпеки Державного університету «Київський авіаційний інститут»
ORCID: https://orcid.org 0000-0002-0086-9131,
E-mail: 12z@ukr.net

Akhramovych Volodymyr Mykolaiovych,
Doctor of Technical Sciences, Professor,
Professor of the Department of Cybersecurity,
State University "Kyiv Aviation Institute",
ORCID: 0000-0002-0086-9131,
E-mail: 12z@ukr.net

Ахрамович Вадим Володимирович
завідувач комп'ютерним центром Національна академія статистики, обліку та аудиту, Київ, Україна
ORCID ID: 0009-0003-2787-8745
E-mail 12zstzi@ukr.net

Akhramovych Vadym Volodymyrovych
head of the computer center National Academy of Statistics, Accounting and Audit, Kyiv, Ukraine
ORCID ID: 0009-0003-2787-8745
E-mail 12zstzi@ukr.net