УДК 004.056.5:621.3.01:656.1/.5

Лахно Валерій Анатолійович
доктор технічних наук, професор, професор кафедри комп'ютерних систем, мереж та кібербезпеки,
Національний університет біоресурсів та природокористування України
ORCID: https://orcid.org/0000-0001-9695-4543
E-mail: lva964@nubip.edu.ua

Касаткін Дмитро Юрійович
кандидат педагогічних наук, доцент, завідувач кафедри комп'ютерних систем, мереж та кібербезпеки,
Національний університет біоресурсів та природокористування України
ORCID: https://orcid.org/0000-0002-2642-8908
E-mail: d.kasatkin@nubip.edu.ua

ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ РОЗПІЗНАВАННЯ КІБЕРЗАГРОЗ, ЯК СКЛАДОВА СИСТЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

Анотація. *Транспортна галузь, зокрема й залізничний транспорт (ЗТ) все більше використовує комп'ютеризовані системи для управління, що робить його вразливим до кібератак. Для захисту інформаційної та кібернетичної безпеки на транспорті стають важливими інтелектуальні системи розпізнавання загроз. Забезпечення кібербезпеки для інформаційних систем та автоматизованих систем керування на транспорті є важливим завданням для забезпечення національної безпеки України. Це дозволяє запобігти можливим кібератакам, зберегти конфіденційність інформації, забезпечити надійну роботу транспортної системи та зберегти безпеку громадян. Розвиток та впровадження ефективних заходів кібербезпеки є необхідними кроками для забезпечення стійкості і надійності транспортних систем та збереження національної безпеки в Україні. Ця стаття описує метод інтелектуального розпізнавання загроз для інформаційних систем керування на транспорті (на прикладі залізничного транспорту – ЗТ). Метод ґрунтується на дискретних процедурах та використанні логічних функцій та нечітких множин.*

Ключові слова: *транспорт, автоматизовані системи керування, кібернетична безпека, розпізнавання загроз, інтелектуальні системи.*

Вступ. Забезпечення кібербезпеки для інформаційних систем (ІС) та автоматизованих систем керування (АСК) на транспорті має вирішальне значення в контексті забезпечення національної безпеки України.

По-перше, транспортна система є однією з найважливіших інфраструктурних сфер у країні. Вона забезпечує транспортування людей, вантажів та інших ресурсів, що є необхідними для економічного розвитку та функціонування суспільства. В разі порушення кібербезпеки в транспортних системах можуть виникнути серйозні наслідки, включаючи аварії, перерви у роботі та збитки. Такі події можуть призвести до загрози для громадської безпеки, економічних збитків та навіть загрози для життя і здоров'я громадян. По-друге, ІС та АСК транспортом включають в себе значну кількість критичних інфраструктурних об'єктів, таких як мережі зв'язку, системи диспетчеризації, системи безпеки та контролю, системи керування рухом транспорту тощо. Ці системи містять велику кількість конфіденційної інформації, включаючи дані про рух транспортних засобів, розклади, пасажирську інформацію та інше. Несанкціонований доступ до цих систем може призвести до крадіжки даних, розкриття конфіденційної інформації або навіть зловживання владою. Такі ситуації можуть мати серйозні наслідки для безпеки країни та забезпечення національних інтересів. По-третє, у зв'язку зі швидким розвитком технологій та поширенням Інтернету ризики кібератак на транспортні системи зростають. Зловмисники можуть використовувати різні методи, такі як вторгнення в мережу, фішинг, віруси, шкідливі програми та інші, для отримання несанкціонованого доступу до систем керування та завдання шкоди. Ефективне забезпечення

кібербезпеки вимагає розробки та впровадження сучасних заходів захисту, моніторингу та виявлення вторгнень, контролю доступу та навчання персоналу з питань кібербезпеки.

Залізничний транспорт (ЗТ) є однією з найбільш важливих інфраструктурних галузей економіки України. Він забезпечує безперебійне перевезення вантажів і пасажирів, а також є важливим фактором безпеки держави.

У сучасних умовах транспорт є все більш уразливим до кібератак. Кіберзлочинці можуть використовувати різні методи для порушення роботи транспортної інфраструктури, наприклад, щоб: викликати затримки або скасовування рейсів; пошкодити обладнання або інфраструктуру; викрадати або підробляти важливу інформацію; та ін.

Мета статті полягає в аналізі та порівнянні засобів для захисту ІС та АСК транспорту від кібератак, використовуючи комплексні заходи, включаючи: фізичний захист інфраструктури; запровадження стандартів і процедур безпеки; підвищення кваліфікації персоналу.

Результати дослідження та їх обговорення. У статті запропонований **метод** інтелектуального розпізнавання загроз, який базується на дискретних процедурах та використанні логічних функцій та нечітких множинах, пропонується з метою підвищення ефективності розпізнавання загроз для автоматизованих систем керування на транспорті, наприклад, залізничному, автомобільному та ін.

Одним із ключових елементів захисту ІС та АСК від кібератак є використання інтелектуальних систем кібербезпеки.

Інтелектуальні системи кібербезпеки використовують штучний інтелект (ШІ) для виявлення і реагування на кібератаки. Вони відрізняються від звичайних систем захисту інформації наступними особливостями:

– інтелектуальні системи кібербезпеки можуть виявляти кібератаки набагато швидше, ніж звичайні системи. Це дозволяє швидко реагувати на атаки та запобігти їх поширенню.

– інтелектуальні системи кібербезпеки можуть виявляти кібератаки з більш високою точністю, ніж звичайні системи. Це дозволяє уникати помилкових спрацьовувань і не блокувати законний трафік.

– інтелектуальні системи кібербезпеки можуть адаптуватися до нових загроз і атак. Це дозволяє забезпечувати ефективний захист залізничного транспорту в умовах постійно мінливих кіберзагроз.

Крім зазначених переваг, використання інтелектуальних систем кібербезпеки, наприклад, на ЗТ транспорті може також мати наступні позитивні наслідки:

Зниження витрат на кібербезпеку. Інтелектуальні системи кібербезпеки можуть допомогти оптимізувати витрати на кібербезпеку, оскільки вони дозволяють автоматизувати деякі завдання та підвищити ефективність роботи персоналу.

Покращення іміджу компанії. Впровадження інтелектуальних систем кібербезпеки свідчить про те, що компанія піклується про безпеку своїх систем і даних. Це може позитивно вплинути на імідж компанії і її конкурентоспроможність.

З розвитком інформаційних технологій (ІТ) ЗТ став все більш залежним від них. Це призвело до зростання актуальності проблеми інформаційної безпеки (ІБ) ЗТ, яка є складовою державної безпеки України. ІБ ЗТ полягає в забезпеченні схоронності, конфіденційності та цілісності інформації, яка використовується на залізничному транспорті. Ураховуючи різноманітність потенційних загроз у кіберпросторі, складність їх структури та функцій, а також участь людей в технологічних процесах на ЗТ, забезпечення ІБ ЗТ, зокрема АСК ЗТ, вимагає створення комплексних систем захисту (КСЗІ). КСЗІ повинні містити заходи, спрямовані на захист ІС та АСК ЗТ від усіх видів релевантних кіберзагроз.

Проблеми кібербезпеки в ІС та АСК ЗТ мають важливе значення з кількох причин, зокрема:

1) *Вразливість до кібератак*. ІС та АСК можуть стати об'єктом атак через підключення до мереж, використання застарілих програмних засобів або вразливостей у мережевих протоколах.

2) *Інфраструктурна вразливість*. Збільшення автоматизації на ЗТ призводить до більшої вразливості мереж і систем до атак та збільшує ризик порушення нормальної роботи.

Для України питання захисту інформації та забезпечення інформаційної (кібернетичної) безпеки (далі ІБ) для ІС та АСК ЗТ мають особливе значення. Причина цього полягає в тому, що Україна є великою країною з геополітично важливим розташуванням.. Приклади несанкціонованого втручання зловмисників (хакерів) в роботу ІС та АСК ЗТ було наведено у роботах [1, 2, 3]. Разом із тим, завдання визначення ризиків кібератак на ІС та АСК ЗТ, належним чином не розглядається та, у найкращому випадку, підмінюється на етапі проектування СЗІ якісним аналізом надійності системи й можливих наслідків проникнення до неї [3].

Захист від кіберзагроз та кібератак атак звичайних інформаційних систем (ІС) на ЗТ дещо відрізняється від захисту від АСК ЗТ.

Звичайні ІС на ЗТ використовуються для виконання різних завдань, таких як управління фінансами, персоналом, логістикою та маркетингом. Вони, як правило, мають меншу критичність для безпеки руху поїздів, ніж АСК ЗТ.

Автоматизовані системи керування (АСК) на ЗТ використовуються для управління рухом поїздів, залізничною інфраструктурою та іншими критичними системами. Вони мають високий рівень критичності для безпеки руху поїздів, тому до їхнього захисту пред'являються особливі вимоги.

Основні відмінності між захистом від кіберзагроз та кібератак ІС на ЗТ та захистом АСК ЗТ є:

Критичність. АСК ЗТ мають вищий рівень критичності для безпеки руху поїздів, ніж звичайні ІС. Тому до їхнього захисту пред'являються особливі вимоги.

Вплив на безпеку руху поїздів. Кіберзагрози та кібератаки, спрямовані на АСК ЗТ, можуть призвести що найменш до серйозних порушень безпеки руху поїздів. Тому захист АСК ЗТ від кіберзагроз та кібератак є життєво важливим для забезпечення безпеки ЗТ.

Складність. АСК ЗТ, як правило, мають більш складну архітектуру, ніж звичайні ІС. Тому їхній захист вимагає більших ресурсів.

Для ІС та АСК ЗТ характерними є наступні види елементів: бортові засоби (наприклад: електронні датчики, які вимірюють різні фізичні величини; камери, які забезпечують відеоспостереження за навколишнім середовищем; засоби обробки інформації; системи комп'ютерного зору, які використовують для обробки даних, отриманих відеокамер; системи розпізнавання образів, які використовують для розпізнавання об'єктів на залізничному шляху; системи радіозв'язку, які використовуються для обміну інформацією між рухомим складом та іншими об'єктами на залізничному шляху; та ін.); засоби, що встановлюються на стаціонарні об'єкти інфраструктури ЗТ (наприклад, системи: автоблокування, сигналізації та ін.); дистанційно керовані виконавчі та індикаційні пристрої (наприклад, системи: управління гальмуванням; управління дверима; управління освітленням та ін.); сервери для опрацювання та зберігання інформаційних масивів (ІМ); ситуаційні центри, диспетчерські центри керування ЗТ; засоби забезпечення різноманітного зв'язку; інформаційно-телекомунікаційні системи та ін.

Неповнота інформації про загрози ІБ для АСК ЗТ може проявлятися двома способами. По-перше, ми можемо не мати повної інформації про структуру об'єкта кібератаки, навіть на базовому рівні. Особливо якщо цей об’єкт має складну архітектуру. По-друге, ми можемо не бути в змозі повністю спостерігати за об'єктом кібератаки й розпізнавати всі кіберзагрози та атаки, які він може зазнати.

Для побудови ефективної СЗІ АСК ЗТ, вибору та впровадженню адекватних технічних засобів кібербезпеки повинен передувати опис, аналіз і моделювання загроз й уразливостей АСК ЗТ. Також потрібен ретельний розрахунок й аналіз ризиків ІБ для АСК ЗТ. Отже, очевидним є те, що спочатку кожна загроза повинна бути впізнана й ідентифікована.

Сучасні системи виявлення та протидії кібератакам (СВАП) на залізничному транспорті у країнах ЄС, США, Японії, Південної Кореї використовують методи, які є ефективними лише

в тому випадку, якщо відомо, які кібератаки або загрози ІБ можуть бути реалізовані зловмисниками.

Саме тому, нові дослідження, пов'язані з методами інтелектуального розпізнавання загроз, мають вирішальне значення для забезпечення ІБ в ІС або АСК ЗТ. Це, зокрема обумовлено можливостями забезпечити:

Реактивний та прогностичний підхід. Методи інтелектуального розпізнавання дозволяють не лише реагувати на вже відомі загрози, але й прогнозувати нові атаки на основі аналізу попередніх моделей або аномальних відхилень, що підвищує рівень захисту ІС або АСК ЗТ;

Виявлення нових загроз. Застосування інтелектуального розпізнавання дозволяє виявляти навіть раніше невідомі атаки, загрози або аномалії в поведінці ІС або АСК ЗТ, що важливо для запобігання їхнього розвитку та поширення;

Автоматизація аналізу великих обсягів даних. Методи інтелектуального розпізнавання дозволяють ефективно обробляти та аналізувати великі обсяги інформації, що важливо для вчасного виявлення аномалій та загроз для ІС або АСК ЗТ;

Підвищення швидкості реагування. Завдяки автоматизації процесу аналізу та розпізнавання, можливо швидше реагувати на потенційні загрози та вчасно приймати заходи щодо їх запобігання чи мінімізації впливу;

Адаптація до змін у загрозах ІБ. Методи інтелектуального розпізнавання дозволяють ІС або АСК ЗТ адаптуватися до нових видів атак та загроз, та змінювати стратегії захисту в реальному часі.

Оцінка можливості реалізації конкретної загрози для ІБ ІС або АСК ЗТ залежить від багатьох факторів. Загроза, яка може завдати шкоди, є потенційно небезпечною і тому повинна бути оцінена. Оцінка загрози для ІС та/або АСК ЗТ передбачає формування моделі загроз, яка описує потенційні способи реалізації загрози та її наслідки.

Методи та моделі. Нижче зупинимося на запропонованому у [1, 2, 3] методі і моделі інтелектуального розпізнавання загроз для безпеки ІС та АСК ЗТ, заснованих на побудові покриттів класів загроз ІБ.

Нехай існує ряд загроз об'єкту інформаційної безпеки (ОІБ у нашому випадку АСК ЗТ) (загальна класифікація загроз наведена у [1]). Рівень загрози для АСК ЗТ залежить від того, наскільки система захищена. Фактори, які можуть призвести до порушення безпеки АСК ЗТ – це фактори ризику. Фактори, які сприяють підвищенню безпеки АСК ЗТ, будемо називати факторами захищеності.

Як було показано в роботах [2, 3] апарат нечіткої логіки виявляється перспективним напрямом для створення систем інтелектуального розпізнавання загроз ІБ ІС або АСК ЗТ. Цьому сприяють наступні фактори [2, 3]:

Робастність до невизначеності. Нечітка логіка дозволяє враховувати та обробляти нечіткі або невизначені дані, що дозволяє аналізувати та розпізнавати аномальні патерни, коли точні значення невідомі або неоднозначні;

Адаптивність до змінних умов. Системи розпізнавання загроз ІБ, що базуються на нечіткій логіці, можуть легше адаптуватися до змінних умов роботи та нових видів загроз, що важливо у контексті кібербезпеки, де атаки постійно еволюціонують.

Менша чутливість до шуму в даних. Нечітка логіка може працювати ефективно при наявності шуму або неточностей у вхідних даних, що дозволяє покращити точність розпізнавання загроз при обробці реальних даних з ІС або АСК ЗТ.

Використання апарату нечіткої логіки вимагає математичного моделювання нечітких множин, розробки нечітких правил та алгоритмів, які можуть бути використані для аналізу даних та прийняття рішень у системах інтелектуального розпізнавання загроз. Для кожного із співвідношень дерева висновку в [1] побудовані нечіткі бази знань (див. табл. 1, показано частину бази знань), які представляють сукупність нечітких правил «ЯКЩО-ТОДІ», що визначають взаємозв'язок між вхідними та вихідною змінними, див. табл. 1. За нечіткими базами знань складені логічні рівняння, див. табл. 2.

Таблиця 1 – Фрагмент бази знань для розпізнавання загроз ІБ для ІС та АСК ЗТ (об'єкту інформаційної безпеки (ОІБ), аналогічно складається для інших ІС на транспорті)

Класи загроз ІБ		**Атрибути**		**Ознаки** $\{p_{ax1}, \dots, p_{axn}\}$	**Універ-сум**	**Терми для лінгвістичної оцінки**
Можливі загрози ІС та АСК ЗТ	**Відомі загрози**	KL_1	Відмова в обслугову-ванні	1 – Стандартні компоненти АСК ЗТ не функціонують; 2 – ін.	[0,1], у. о.	• не представляє значної загрози для ІБ АСК ЗТ (не критичний – нкр), • представляє значну загрозу (критичний – кр)
		KL_2	Викрадення компонентів	1 – фактичні ознаки (наприклад, поява конфіденційної інформації у ЗМІ); 2 – необ'єктивні ознаки; 3 – ін.	[0,1], у. о.	• знайдені в рамках моніторингу ІБ (виявлені – в), • не повністю вивчена (частково не зафіксовані / невиявлені – чв), • не знайдені (нв)
		KL_3	Привласнен-ня особистості	1 – фактичні ознаки (наприклад, було виявлено спроби несанкціонованого доступу до АСК ЗТ під чужим обліковим записом.); 2 – необ'єктивні ознаки; 3 – ін.	[0,1], у. о.	• знайдені в рамках моніторингу ІБ (в), • не повністю вивчені (чв), • не знайдені (нв)
Інше ….						
Стани ІС або АСК в контексті забезпечення ІБ						
S_1 – встановлене ПЗ та оновлення до нього; S_2 – в АСК ЗТ присутні мережеві сервіси; S_3 – АСК ЗТ підтримує багатозадачність; S_4 – підтримка багатокористувацького режиму; S_5 – встановлені пристрої введення / виводу; S_6 – наявність пристроїв «гарячої заміни»; S_7 – наявність зовнішніх каналів зв'язку; S_8 – наявність системи відеоспостереження, яка з'єднана з АСК ЗТ; S_9 – наявність системи супутникової навігації, яка з'єднана з АСК ЗТ; S_{10} – наявність ЗЗІ.						
Методи протидії загрозам та атакам						
D_1 – ідентифікація і аутентифікація; D_2 – блокування безконтрольного доступу; D_3 – захист від шкідливого програмного забезпечення; D_4 – контроль цілісності даних; D_5 – знищення залишкових даних; D_6 – захист ПЗ та інформаційних масивів ІС та АСК ЗТ від дослідження; D_7 – резервування інформації ІС та АСК ЗТ; D_8 – відновлення і самовідновлення компонентів ІС та АСК ЗТ; D_9 – перевірка сертифіката безпеки; D_{10} – блокування запуску ПЗ; D_{11} – криптографічний захист; D_{12} – ін.						

Таблиця 2 – Фрагмент бази знань у вигляді правил

Правила			
PR1	*IF* $(KL_1 \vee S_1 \vee S_7)$ *THEN* D_2	*PR10*	*IF* $(KL_9 \vee S_1)$ *THEN* D_8
PR2	*IF* $(KL_1 \vee S_2 \vee S_7)$ *THEN* D_2	*PR11*	*IF* $(KL_{10} \vee S_7)$ *THEN* D_7
PR3	*IF* $(KL_2 \vee S_4 \vee S_7)$ *THEN* D_2	*PR12*	*IF* $(KL_{11} \vee S_4 \vee S_7)$ *THEN* D_2
PR4	*IF* $(KL_3 \vee S_4)$ *THEN* D_8	*PR13*	*IF* $(KL_{11} \vee S_5)$ *THEN* D_7
PR5	*IF* $(KL_4 \vee S_1)$ *THEN* D_4	*PR14*	*IF* $(KL_{11} \vee S_4 \vee S_7)$ *THEN* D_2
PR6	*IF* $(KL_5 \vee S_3)$ *THEN* D_6	*PR15*	*IF* $(KL_5 \vee S_7)$ *THEN* D_2
PR7	*IF* $(KL_6 \vee S_1)$ *THEN* D_3	*PR16*	*IF* $(KL_5 \vee KL_8 \vee KL_{11} \vee S_5 \vee S_7)$ *THEN* D_{10}
PR8	*IF* $(KL_7 \vee S_4 \vee S_5 \vee S_6 \vee S_7)$ *THEN* D_5	*PR17*	*IF* $(KL_3 \vee KL_9 \vee KL_4)$ *THEN* D_9
PR9	*IF* $(KL_8 \vee S_4)$ *THEN* D_1	*PR18…PR*$_{nm}$	*Інші*

Якщо істинність умови логічного рівняння більша за нуль, тоді правило активується. В базах знань для об'єднання умов в правилах використовуються нечіткі логічні операції, такі як нечітка кон'юнкція, нечітка диз'юнкція, нечітка відмова та інші.

Запропоновано метод, дозволяє формувати вирішальні правила для дискретних процедур розпізнавання загроз, на прикладі, АСК ЗТ. Метод базується на аналізі критичності окремих елементів АСК ЗТ.

Суть методу полягає у визначенні кон’юнкцій за покриттям класів загроз ІБ, та який відрізняється від наявних методів застосуванням дискретних процедур із використанням апарату логічних функцій та нечітких множин ознак атак на АСК ЗТ, що дозволяє створювати ефективні програмні, аналітичні та схемотехнічні рішення для систем кібернетичної безпеки АСК ЗТ.

Також запропоновано метод формування вирішального правила для дискретних процедур розпізнавання загроз ІБ АСК ЗТ, який базується на процедурі аналізу критичності окремих елементів АСК ЗТ, та на відміну від наявних, забезпечує можливість виконувати інтелектуальне розпізнавання загрози з мінімальною кількістю помилок та ураховувати нетипові ознаки кібератак.

Висновки і перспективи Будь який транспорт, використовує значну кількість комп'ютеризованих систем для управління, що робить його уразливим перед кібератаками. Інтелектуальні системи можуть моніторити та виявляти потенційні загрози безпеці автоматизованих систем керування на транспорті. У сфері кібернетичної безпеки (КБ), інтелектуальні системи розпізнавання загроз стають ключовим елементом захисту. Ці системи дозволяють автоматично виявляти аномальну поведінку та потенційні загрози в мережах та автоматизованих системах керування на транспорті, сприяючи швидкому реагуванню та запобіганню можливим атакам. Запропонований у статті метод інтелектуального розпізнавання загроз, який базується на дискретних процедурах та використанні логічних функцій та нечітких множинах, пропонується з метою підвищення ефективності розпізнавання загроз для автоматизованих систем керування на транспорті, наприклад, залізничному, автомобільному та ін.

Список використаних джерел

1. Lakhno V.A., Petrov O.S., Hrabariev A.V., Ivanchenko Y.V., Beketova G.S. Improving of information transport security under the conditions of destructive influence on the information-communication system (2016) Journal of Theoretical and Applied Information Technology, 89 (2), pp. 352 – 361.
2. Lakhno V., Mohylnyi H., Donchenko V., Smahina O., Pyroh M. A model developed for teaching an adaptive system of recognising cyberattacks among nonuniform queries in information systems (2016) Eastern-European Journal of Enterprise Technologies, 4 (9), pp. 27 – 36. DOI: 10.15587/1729-4061.2016.73315
3. Lakhno V. Creation of the adaptive cyber threat detection system on the basis of fuzzy feature clustering (2016) Eastern-European Journal of Enterprise Technologies, 2 (9), pp. 18 – 25. DOI: 10.15587/1729-4061.2016.66015

Lakhno Valeriy
Doctor of Technical Sciences, Professor of the Department of Computer systems, networks and cybersecurity,
National University of Life and Environmental Sciences of Ukraine,
ORCID: https://orcid.org/0000-0001-9695-4543
E-mail: lva964@nubip.edu.ua

Kasatkin Dmytro
PhD, Associate Professor, Head of the Department of Computer systems, networks and cybersecurity,
National University of Life and Environmental Sciences of Ukraine
ORCID: https://orcid.org/0000-0002-2642-8908
E-mail: d.kasatkin@nubip.edu.ua

INTELLIGENT CYBER THREATS RECOGNITION SYSTEMS AS A COMPONENT OF THE INFORMATION SECURITY SYSTEM IN TRANSPORT

Abstract. *The transport industry, in particular the railway transport (RT), is increasingly using computerized systems for management, which makes it vulnerable to cyber attacks. Intelligent threat recognition systems are becoming important for the protection of information and cyber security in transport. Ensuring cyber security for information systems and automated control systems in transport is an important task for ensuring the national security of Ukraine. This makes it possible to prevent possible cyber attacks, preserve the confidentiality of information, ensure the reliable operation of the transport system and preserve the safety of citizens. The development and implementation of effective cyber security measures are necessary steps to ensure the stability and reliability of transport systems and the preservation of national security in Ukraine. This article describes the method of intelligent recognition of threats for information systems of transport management (on the example of railway transport – TZ). The method is based on discrete procedures and the use of logical functions and fuzzy sets.*

Keywords: *transport, automated control systems, cyber security, threat recognition, intelligent systems*.