doi: https://doi.org/10.15407/visn2022.04.034

ЛЕТИЧЕВСЬКИЙ
Олександр Олександрович —
доктор фізико-математичних наук, завідувач відділу теорії цифрових автоматів Інституту кібернетики ім. В.М. Глушкова НАН України

НАУКОВІ ЗАСАДИ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Стенограма доповіді на засіданні Президії НАН України 9 лютого 2022 року

У доповіді обґрунтовано необхідність створення нових, більш ефективних засобів кібербезпеки для виявлення та аналізу зловмисної поведінки на основі методів штучного інтелекту та алгебраїчного підходу. В умовах гібридної війни це насамперед стосується кіберзахисту та кібербезпеки об'єктів критичної інфраструктури України. Інститут кібернетики ім. В.М. Глушкова НАН України завдяки знаній у світі школі академіків В.М. Глушкова — О.А. Летичевського є лідером з використання алгебраїчного підходу та методів штучного інтелекту для розроблення ефективних, критичних до безпеки систем і має великий досвід їх тестування та верифікації.

Шановні колеги!

Сьогодні я пропоную вашій увазі доповідь, присвячену науковим проблемам та дослідженням у галузі використання алгебраїчного підходу та методів штучного інтелекту для вирішення завдань кібербезпеки, зокрема завдань, пов'язаних із захистом об'єктів критичної інфраструктури.

Починаючи з 2014 р. Україна все частіше стикається з потужними кібератаками не лише на урядові ресурси, а й на об'єкти критичної інфраструктури. Так, 23 грудня 2015 р. відбулася атака на інфраструктурні об'єкти енергетичної галузі України, внаслідок чого було виведено з ладу автоматизовані системи управління технологічними процесами і сталося тимчасове масштабне відімкнення електроенергії в трьох регіонах (Прикарпаття, Київська та Чернівецька області). Найбільше постраждали споживачі Прикарпаттяобленерго — впродовж 1—6 годин було знеструмлено електромережі близько 30 підстанцій, понад 230 тис. мешканців залишилися без світла. Атаку було здійснено з використанням троянської програми BlackEnergy.

6 грудня 2016 р. хакерської атаки зазнали Державне казначейство, Міністерство фінансів, Пенсійний фонд та внутрішні мережі інших державних органів, що призвело до блокування бюджетних виплат, яке тривало кілька днів.

Уночі з 17 на 18 грудня 2016 р. стався ще один кібернапад на енергосистему України. Через збій автоматичного управління було повністю знеструмлено підстанції Київенерго та Київобленерго, а також Київської ГАЕС. Понад годину не було електроенергії у споживачів північної частини правобережного Києва та кількох прилеглих районів Київської області.

У ніч на 14 січня 2022 р. було здійснено кібератаку на урядові сайти. Постраждали близько 70 сайтів органів влади та державних установ, у тому числі й портал «Дія». На їх головних сторінках зловмисники розмістили повідомлення провокаційного характеру. Їм вдалося реалізувати цю атаку за допомогою програми-вайпера WhisperGate через вразливості в системі керування вмістом вебсайтів, яку використовувала компанія — розробник ІТ-продуктів для державних органів.

І хоча останніми роками ситуація у сфері кіберзахисту в Україні значно поліпшилася, в умовах сучасної кібервійни цього явно недостатньо. Постійне зростання кількості кіберінцидентів, несанкціонованих вторгнень, DDoS-атак, які можуть призвести до неможливості користування мережевими та комп'ютерними ресурсами, розміщення на офіційних сайтах провокаційних повідомлень, шифрування або знищення інформації, крадіжок персональних даних, свідчить про потребу підвищити ефективність засобів захисту для забезпечення своєчасного виявлення та ефективного блокування кібератак. Особливо це важливо для об'єктів критичної інфраструктури — серверів підприємств транспорту, енергетики, військових об'єктів тощо.

Отже, є необхідність у розробленні із залученням наукового потенціалу нових, більш ефективних засобів кібербезпеки. Сьогодні на часі створення інтелектуальних систем виявлення та аналізу зловмисної поведінки на основі методів штучного інтелекту та алгебраїчного підходу.

Чотири роки тому в Інституті кібернетики ім. В.М. Глушкова НАН України було розпочато роботи з розроблення алгебраїчних методів, призначених саме для вирішення завдань кібербезпеки, з використанням сучасних дедуктивних систем — розв'язувачів у різних теоріях та методів машинного навчання.

Алгебраїчний підхід переконливо довів свою ефективність ще в 2016 р., коли Агентство передових оборонних дослідницьких проєктів США (DARPA) організувало конкурс Cyber Grand Challenge, мета якого полягала у створенні систем автоматизованого кіберзахисту з можливістю швидкого, масштабованого виявлення атак і вразливостей програмного забезпечення та усунення недоліків у режимі реального часу. Перші три місця у змаганнях посіли компанії-розробники із США — Mayhem, Xandra і Mechanical Phish, які для виявлення вразливостей у бінарному коді запропонованих на конкурсі програм використали різновиди алгебраїчного моделювання. При цьому було зафіксовано рекорд з кількості виявлених вразливостей за одиницю часу.

В Інституті кібернетики ім. В.М. Глушкова НАН України алгебраїчні методи активно використовують для формальної верифікації, тестування та реінжинірингу критичних до безпеки систем. У цьому напрямі ми є послідовниками знаної у світі алгебраїчної школи Глушкова — Летичевського-старшого. В рамках цієї школи в 70-х — 80-х роках минулого століття було створено одну з перших у світі систем дедуктивного виведення — систему автоматичного доведення теорем. Сьогодні дедуктивні виведення тверджень зі знань є досить вагомою компонентою в методах штучного інтелекту, що в комбінації з індуктивною компонентою, основаною на машинному навчанні, генерації нейронних мереж та інших моделях класифікації, забезпечує достатньо потужний апарат для створення інтелектуальних систем.

Наприкінці 80-х — на початку 90-х років представники алгебраїчної школи розробили систему алгебраїчного програмування APS з вхідною мовою алгебраїчного програмування APLAN, а впродовж 90-х — 2000-х років активно розвивалася технологія алгебраїчного програмування, теорія агентів та середовищ, було створено систему інсерційного моделювання,

що є узагальненням теорії автоматів та транзитивних систем.

У контексті зазначених вище теорій було розроблено алгебру поведінок, за допомогою якої формалізується поведінка агента в певному середовищі. При цьому агентом може бути програма, пристрій апаратного забезпечення, зловмисник або інші сутності, які діють у кіберпросторі.

Отже, досвід Інституту з використання алгебраїчних методів становить близько пів століття, і ми сьогодні є лідерами в цьому напрямі.

За останні 20 років у рамках алгебри поведінок створено значну кількість формальних методів, які використовувалися у верифікації, тестуванні, реінжинірингу програмного та апаратного забезпечення, в аналізі моделей. Співпраця в галузі алгебраїчної верифікації критичних до безпеки систем з такими провідними компаніями, як «Моторола» (з алгебраїчної верифікації вимог та дизайну програмних та апаратних систем) та «Інтел» (з верифікації паралельних програм), підтвердила ефективність запропонованих нами формальних методів і забезпечила їх впровадження у програмну індустрію.

На українських підприємствах НВП «Радій» і НВП «Радікс», які розташовані у м. Кропивницький і є виробниками обладнання та сучасних автоматизованих систем управління технологічними процесами, зокрема систем захисту для підприємств атомної енергетики, було впроваджено формальні методи тестування та верифікації електронних проєктів модулів платформ, побудованих на основі технології FPGA.

У галузі верифікації моделей Інститут кібернетики ім. В.М. Глушкова НАН України плідно співпрацює з Національним аерокосмічним університетом ім. М.Є. Жуковського «Харківський авіаційний інститут».

Винайдення алгебри поведінок дало змогу застосувати алгебраїчний підхід і методи штучного інтелекту до задач, пов'язаних з кібербезпекою, зокрема для пошуку вразливостей у програмних та апаратних системах.

Для цього вразливості, поведінку програми в разі вторгнення зловмисника, поведінку вірусної програми представляють у вигляді рівнянь алгебри поведінок. Такий підхід охоплює множину сценаріїв на відміну від традиційних інструментів, наприклад антивірусів, у яких сигнатура вірусів обмежена однією або дуже невеликою кількістю можливих поведінок вірусу. Алгебраїчний підхід дає змогу за допомогою рівнянь алгебри поведінок описати широкий клас сценаріїв вірусної поведінки для подальшого розпізнавання в комп'ютерному середовищі. Це стосується й опису вразливостей програми та її поведінки під час кібератаки.

Як працює антивірусна програма? В ній збирають вірусні сигнатури на основі коду всіх відомих вірусів. Однак вірусна сигнатура описує певні послідовності байтів. Якщо поміняти місцями кілька байтів, сигнатура вже не спрацює і, відповідно, антивірус не помітить загрози. На відміну від антивірусів, поведінкове рівняння описує не конкретні одиничні випадки, а множину потенційно можливих зловмисних дій. Тому за допомогою алгебраїчних сигнатур можна передбачити значно ширше коло дій хакерів.

Для того, щоб спрацювали формальні методи, необхідно мати поведінкову модель як самої програми, так і електронного пристрою. З цією метою використовують відповідні транслятори.

Таким чином, за допомогою поведінкових рівнянь можна представити бінарний код, у якому за допомогою алгоритмів його зіставлення з алгебраїчними сигнатурами і на основі розв'язання поведінкових рівнянь можна виявляти вразливу поведінку.

Інтегральна програмована плата FPGA може бути трансльована в поведінкову модель для подальшого використання формальних методів алгебри поведінок та виявлення вразливостей у побудові апаратного забезпечення (hardware).

Дизайн електронного пристрою, який описується формальними мовами, наприклад VHDL, також можна транслювати в поведінкові рівняння для подальшого їх використання в методах виявлення вразливостей.

В Інституті кібернетики ім. В.М. Глушкова НАН України спільно з Херсонським держав-

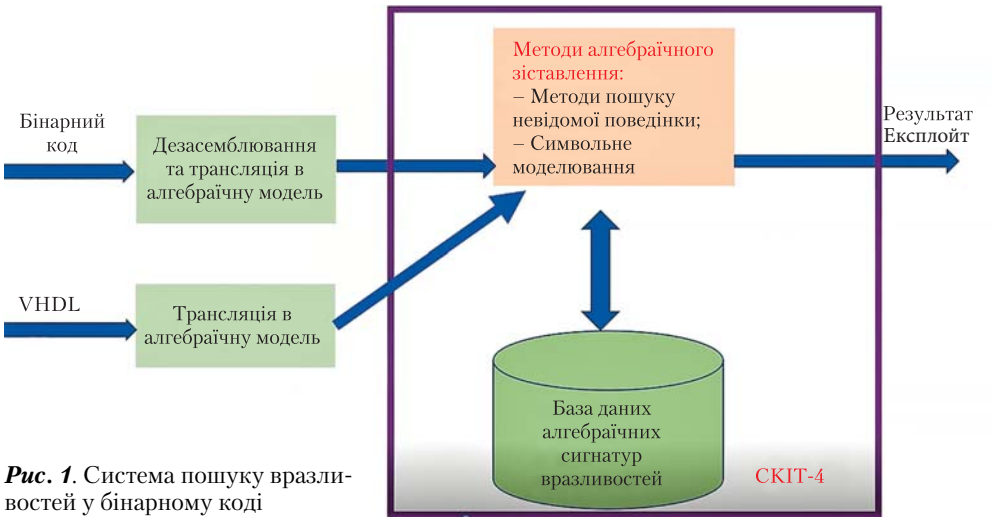


Рис. 1. Система пошуку вразливостей у бінарному коді

ним університетом створено прототип системи виявлення вразливостей у програмному забезпеченні на основі алгебраїчного підходу. В цій системі використано пошук вразливостей із застосуванням алгоритму алгебраїчного зіставлення. Вразливості представлено у вигляді алгебраїчних сигнатур, а їх пошук виконується на рівні бінарного коду. База даних алгебраїчних сигнатур має поповнюватися з різних джерел, зокрема з історичних даних про попередні кібератаки.

Якщо розглядати програмне забезпечення у вигляді бінарного коду, то його можна сканувати і далі транслювати у відповідну алгебраїчну модель, яка і є входом для системи виявлення вразливостей. На виході отримуємо виявлення слабких місць та згенеровані експлойти, тобто послідовності вхідних даних, які можуть використати виявлену вразливість програмного забезпечення для проведення атаки (рис. 1).

Розгортання такої системи на багатопроцесорному комплексі суперкомп'ютера СКІТ-4 дасть змогу провести повномасштабну перевірку програмних комплексів об'єктів критичної інфраструктури щодо наявності в них вразливостей. Ці роботи перебувають уже на завершальній стадії. Планується здійснити верифікацію програмного забезпечення, яке використовується на таких об'єктах критичної інфраструктури, як Укрзалізниця, аеропорт «Бориспіль», розподільчі енергетичні компанії, банківські установи тощо.

Отже, використовуючи алгебраїчні методи та методи штучного інтелекту, ми отримуємо доказове (на відміну від тестування, імітаційного моделювання і симуляції) підтвердження, що програмне забезпечення, встановлене на об'єктах критичної інфраструктури, має певну стійкість до атак.

В Інституті кібернетики ім. В.М. Глушкова НАН України започатковано також дослідження із застосуванням комбінованого способу виявлення в реальному часі атак на мережеве оточення методами штучного інтелекту. В цьому методі поєднано використання згенерованих за допомогою машинного навчання моделей класифікації та дедуктивних засобів. Поведінка трафіку мережі обробляється спочатку в моделі класифікації (зокрема, нейронною мережею), а потім підозріла поведінка зіставляється з алгебраїчними шаблонами (рис. 2). У рамках моделі класифікації на основі початкових даних певної поведінки трафіку можна визначити початок підозрілої діяльності. Модель класифікації працює швидше, ніж алгебраїчне зіставлення, але точність її нижча. Тому в разі якщо модель класифікації виявить підозрілу поведінку, далі алгебраїчне зіставлення починає аналізувати відповідні атрибути і остаточно встанов-

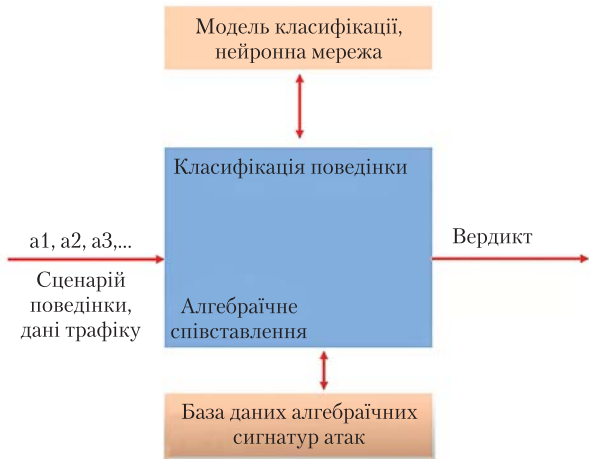


Рис. 2. Використання комбінації технологій машинного навчання та алгебраїчного підходу

лює, чи є ця поведінка справжньою атакою, чи ні, і якщо так, то сигналізує про це в систему. Таким чином, зовнішній трафік аналізується в режимі реального часу.

Тренування моделі класифікації методами машинного навчання може відбуватися за такими напрямами:

• аналіз логів попередніх атак, отриманих із системи обміну інформації, що містить також інформацію від наших союзників — Європейського Союзу, США та Великої Британії;

• моделювання дій зловмисника;

• використання міжнародних сховищ поведінок зловмисників (датасетів).

Опис цієї технології нещодавно було презентовано в Національному координаційному центрі кібербезпеки при РНБО України, і фахівці позитивно оцінили ці роботи. Відповідну доповідь було також представлено на саміті Національного кластера кібербезпеки, який відбувся 16 грудня 2021 р. Наприкінці поточного року ми плануємо перше випробування прототипу системи, яка працюватиме з використанням зазначеного підходу.

Ще одна технологія, яку ми розробляємо з використанням методів штучного інтелекту, — це нечітке тестування. Суть його полягає в тестуванні програмного забезпечення на вразливості, в тому числі й невідомі, за допомогою генерації неочікуваних або критичних входів. Після певного аналізу бінарного коду, який потрібно протестувати, з використанням алгебраїчного підходу тести генеруються більш цілеспрямовано, звужуючи простір пошуку для виявлення вразливостей (рис. 3).

За ефективністю ця технологія завдяки більш змістовному аналізу може конкурувати з інструментом нечіткого тестування American Fuzzing Lop, розробленим компанією «Гугл».

Крім того, ми проводимо роботи з вивчення бекдорів. Бекдор — це недокументована особливість функціональності продукту, яка дозволяє несанкціоноване проникнення в роботу апаратного чи програмного забезпечення з метою зловмисних дій. Виявлення бекдорів дуже важливе у критичних до безпеки системах військового призначення, у ядерній енергетиці, авіоніці та в інших подібних сферах. По суті, бекдори є способом обходу автентифікації або інших засобів контролю безпеки для доступу до комп'ютерної системи або даних, що містяться в цій системі. Бекдор працює як створений розробником-зловмисником таємний вхід у систему або програму.

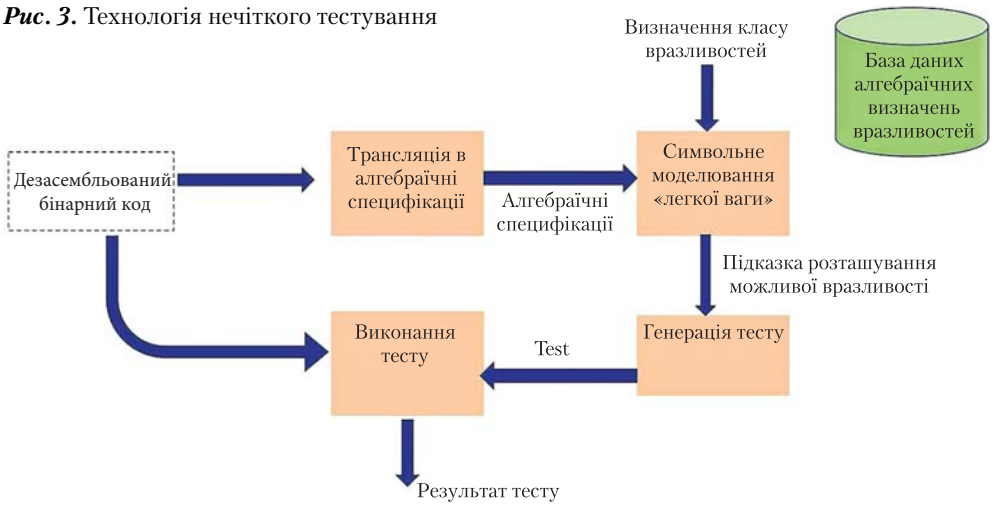
Як приклад використання бекдору можна навести хакерську атаку 2017 р., коли через популярну програму електронного документообігу MEDoc комп'ютерні системи майже 80 % підприємств України, у тому числі й критичної інфраструктури, було вражено вірусом-хробаком NotPetya. Потім вірус поширився й на інші країни. Саме бекдор на досить тривалий час дав зловмисникам доступ до інформації цих підприємств. Інфікування відбулося під час оновлення програмного забезпечення, тобто захисник Windows або інший встановлений антивірус дав попередження: «Чи довіряєте ви джерелу оновлення?». Оскільки це був сайт виробника, користувач погоджувався із записом оновлення на свій комп'ютер. Сам виробник і не знав, що оновлення інфіковане або хтось із його команди вчинив злочин, вставивши зловмисний код.

Бекдори можуть бути реалізовані як:

• прихована функціональність;

• спеціальні облікові дані (для входу);

Рис. 3. Технологія нечіткого тестування



• маніпуляція критичними параметрами безпеки;
• непередбачена мережева активність;
• вбудовані команди;
• руткіти (схованки);
• годинникова бомба;
• самомодифікований код.

Усі ці різновиди бекдорів можуть бути наявні як у програмному, так і в апаратному забезпеченні, і вносяться, як правило, завербованими кіберзлочинцями.

Боротьбу з бекдорами та кібершпигунством проводять або методами тестування на еквівалентність, якщо природа бекдору невідома, або скануванням і алгебраїчним зіставленням з відомими можливими поведінками зловмисника під час входу через бекдор. Наприклад, при аналізі моделі поведінки спрацьовує шаблон бекдору, якщо є змога зайти не лише через автентифікацію, а й ще в якийсь спосіб.

Нещодавно ми подали на конкурс проєкт у рамках програми НАТО, в якому пропонували сканувати підозрілі пристрої способом ламінографії та аналізувати потім просканову схему на основі відомих моделей бекдорів, використовуючи алгебраїчний підхід.

Ще кілька експериментів було проведено в напрямі створення алгебраїчного антивірусу — виявлення в мережах підозрілих процесів та файлів. Ці процеси та файли можна сканувати безпосередньо в мережі або з відповідного пристрою процесора і переводити в поведінкові рівняння та аналізувати за допомогою алгебраїчного сервера із зіставленням з алгебраїчними сигнатурами вірусів з відповідної бази даних (рис. 4).

На відміну від традиційних інструментів-антивірусів, алгебраїчний антивірус здійснює пошук множин зловмисних поведінок за їх алгебраїчними сигнатурами. Такий алгебраїчний антивірус досить точно може виявляти зловмисні дії в підозрілих процесах у мережі та в підозрілих файлах — так званих троянах.

Отже, навіть у разі дотримання правил кібербезпекової гігієни, зокрема під час оновлення програмного забезпечення, завантажені програми потрібно сканувати та аналізувати на предмет зловмисних дій. Тут можна знову згадати кібератаку на Прикарпаттяобленерго, внаслідок якої непомічений троян призвів до знеструмлення 30 підстанцій. Вчасне сканування на зловмисні дії могло б запобігти цій атаці.

Ще одним напрямом кіберзахисту є протидія DDoS-атаці — атаці типу «відмова в обслуговуванні». І це загалом нетривіальне завдання. Така атака здійснюється із заражених комп'ютерів — ботнетів. Саму DDoS-атаку передбачити і зупинити складно, хоча інструменти з її нейтралізації є. Однак можна виявити джерело такої атаки та позбавитися мережі

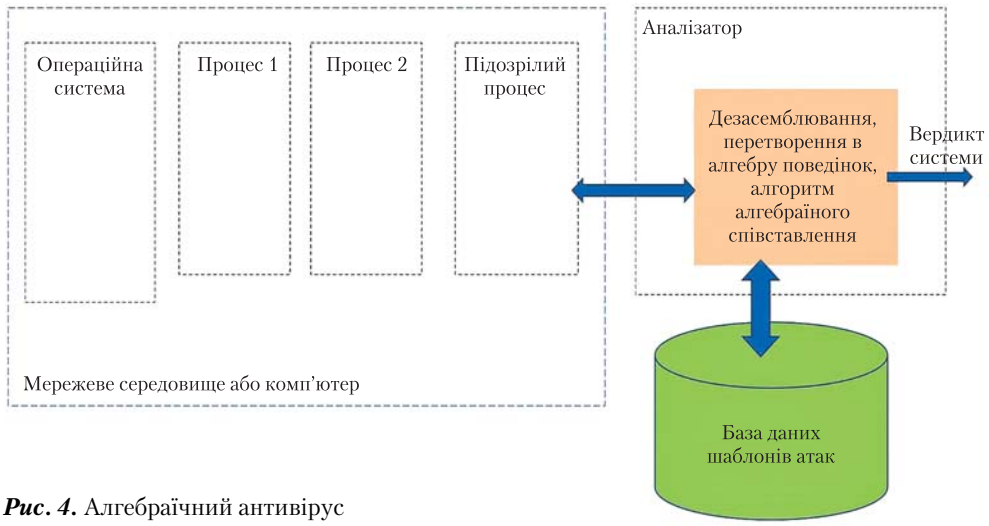


Рис. 4. Алгебраїчний антивірус

ботнетів. За ініціативою молодих аспірантів в Інституті кібернетики ім. В.М. Глушкова НАН України започаткували роботи з виявлення ботнетів за допомогою нейронних мереж. Поки що ці роботи перебувають на початковій стадії, але невдовзі заплановано виконати кілька експериментів, за результатами яких буде сформовано пропозиції щодо побудови нової системи захисту.

Отже, сьогодні як ніколи гостро постає потреба у використанні результатів фундаментальних досліджень для створення інтелектуальних систем, що аналізують, класифікують, виявляють аномалії в поведінці агентів у кіберпросторі. Такі системи мають поєднувати дві компоненти: індуктивну — машинне навчання та моделі класифікації — і дедуктивну, тобто здатність системи до виведення тверджень із конкретних фактів.

Саме поєднання фундаментальної науки та інженерного досвіду в тісній співпраці з білими (етичними) хакерами дозволить зробити якісний перехід до більш надійних систем кіберзахисту проти дій зловмисників.

На сьогодні залишається ще досить велика кількість математичних проблем, які потрібно вирішити для того, щоб алгебраїчні методи усталилися в кібербезпеці і набули широкого використання для оптимізації, підвищення ефективності алгоритмів аналізу та виявлення зловмисної чи вразливої поведінки.

Застосування формальних методів можна поширити на такі напрями, як моделювання масштабованих кіберударів по противнику, кіберрозвідка, автоматична корекція вразливих точок, блокування атак.

На особливу увагу заслуговує налагодження постійного обміну інформацією з нашими союзниками та НАТО, що є необхідною умовою для поповнення бази даних алгебраїчних сигнатур зловмисних та вразливих поведінок.

Якщо оцінювати наших кіберпротивників, зокрема «Лабораторію Касперського» чи групи чорних хакерів, то здебільшого їх вміння та засоби ґрунтуються на досить тонких інженерних рішеннях щодо створення засобів вторгнення. Проте вони не є алгебраїстами, а тому потрібно використати нашу перевагу у володінні алгебраїчними методами.

Дякую за увагу!

За матеріалами засідання підготувала О.О. Мележик

Oleksandr O. Letychevskyi
ORCID: https://orcid.org/0000-0003-0856-9771

V.M. Glushkov Institute of Cybernetics of the National Academy of Sciences of Ukraine, Kyiv, Ukraine

SCIENTIFIC PRINCIPLES OF CYBERSECURITY OF CRITICAL INFRASTRUCTURE OBJECTS

Transcript of the report at the meeting of the Presidium of NAS of Ukraine, February 9, 2022

The report substantiates the need to create new, more effective cybersecurity tools for detecting and analyzing malicious behavior based on artificial intelligence methods and algebraic approach. In the conditions of hybrid war, this primarily concerns cyberdefense and cybersecurity of Ukraine's critical infrastructure. V.M. Glushkov Institute of Cybernetics of the NAS of Ukraine, thanks to the world-famous school of academicians V.M. Glushkov – O.A. Letychevskyi, is a leader in the use of algebraic approach and artificial intelligence methods to develop effective, security-critical systems and has extensive experience in their testing and verification.