САВЧУК
Михайло Миколайович — член-кореспондент НАН України, виконувач обов'язків завідувача кафедри математичних методів захисту інформації Фізико-технічного інституту Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»

ЗАХИСТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА КІБЕРБЕЗПЕКА

Стенограма наукової доповіді на засіданні Президії НАН України 25 вересня 2019 року

У доповіді висвітлено низку найважливіших досліджень з розроблення методів захисту інформації, інформаційних технологій, математичного апарату криптографії та криптоаналізу, стеганографії, а також технічних засобів та правових засад кібернетичної безпеки. Підкреслено необхідність подальшого розвитку цього напряму в Україні та актуальність підготовки висококваліфікованих кадрів у сфері захисту інформації та безпеки кіберпростору.

Шановний Борисе Євгеновичу!
Шановні учасники засідання!
За дорученням Президії НАН України я маю честь доповісти про стан і шляхи розвитку такого наукового напряму, як захист інформаційних технологій і кібербезпека.

Як відомо, рівень розвитку людської цивілізації залежить від кількості інформації, якою можуть активно користуватися різні соціальні прошарки населення, від вміння її ефективно зберігати, швидко обробляти та передавати. Останніми роками у світі спостерігається перехід суспільства на принципово новий рівень розвитку, що пов'язано зі стрімким зростанням обсягів інформації, істотним збільшенням швидкості її обробки, розширенням можливостей комутацій для миттєвого обміну повідомленнями з метою комунікації, управління, реагування тощо.

Проте одночасно з неймовірними перспективами, які відкривають людству новітні інформаційні технології, все більшого масштабу набувають проблеми забезпечення конфіденційності, цілісності, автентичності, доступності та невідстежуваності інформації, неможливості нав'язування та розповсюдження шкідливої інформації. Масова доступність засобів обчислювальної техніки, насамперед персональних ЕОМ, сучасного високошвидкісного інтернету зумовила поширення комп'ютерної грамотності серед широких кіл населення та значне збільшення

кількості користувачів комп'ютерних мереж та їх можливостей. У свою чергу, це спричинило зростання можливостей і для потенційних порушників та призвело до численних спроб втручання в роботу державних і комерційних систем, як зі злими намірами, так і зі «спортивного інтересу». Деякі з цих спроб виявилися успішними і завдали чималої шкоди власникам інформації та обчислювальних систем. Саме на протидію таким несанкціонованим втручанням і спрямовано розвиток методів та засобів захисту інформації та кіберпростору.

Підвищення ефективності, надійності та стійкості систем захисту інформації, інформаційних технологій, захисту кіберпростору нині є першочерговими завданнями для кожної організації та галузі в будь-якій країні світу. Для захисту інформаційних технологій створено низку криптографічних, стеганографічних, технічних методів з розвиненими науковими обґрунтуваннями та відповідними технічними засобами. Однак бурхливий розвиток як нових інформаційних систем, так і нових видів кібератак потребує подальших широкомасштабних наукових досліджень. Складність проблеми вимагає комплексного підходу із залученням найсучасніших наукових досягнень та ретельного дослідження реальних систем обробки, передачі та захисту інформації, систем та комплексів керування технологічними процесами.

Розвиток сучасного кіберпростору нерозривно пов'язаний з появою нових загроз безпеці інформації та інформаційним технологіям. Поширення новітніх ІТ-технологій, зокрема так званого «інтернету речей», криптовалют, криптобірж, систем електронних виборів, «розумних контрактів» тощо, кардинально змінює кіберпростір. При цьому зростає кількість кібератак на глобальні критичні інфраструктури: системи електропостачання, керування банківськими та комерційними структурами, транспортом, зокрема аеропортами, глобальні бази даних. Усі ви, мабуть, добре пам'ятаєте, якої шкоди 27 червня 2017 р. завдала в Україні хакерська атака з використанням різновиду вірусу Petya.

Сучасні «інтелектуальні» атаки в кіберпросторі вирізняються тим, що мають «латентний» період, який може тривати досить довго, впродовж кількох місяців, а це значно ускладнює процес їх виявлення. Тому сьогодні є нагальна потреба у розробленні нових підходів до захисту телекомунікаційних мереж, об'єктів критичної інфраструктури, систем керування, в тому числі цілими галузями. Ефективного забезпечення кібербезпеки можна досягти лише завдяки комплексному і безперервному застосуванню нових теоретичних напрацювань, організаційно-правових, криптографічних, технічних методів захисту.

Слід зазначити, що широко вживані терміни «захист інформації», «захист інформаційних технологій» і «захист кіберпростору» мають дещо відмінний один від одного сенс. Дещо спрощено можна сказати, що захист інформації — це сукупність методів і засобів, які забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру; безпека інформаційних технологій містить у собі ще й захист і забезпечення працездатності технічної частини, зокрема під час кібератак, а захист кіберпростору передбачає безпеку комунікаційних систем, об'єктів критичної інформаційної інфраструктури, комунікацій та систем керування.

В Україні активні дискусії щодо кібербезпеки розпочалися більш як 10 років тому. Перше чітке розділення інформаційної безпеки та кібербезпеки було зафіксовано в оновленій Стратегії національної безпеки України 2015 р. Потім, 05.10.2017 р. було прийнято Закон України «Про основні засади забезпечення кібербезпеки України», 08.07.2018 р. набрали чинності Закон України «Про національну безпеку України» від 21.06.2018 та нова редакція Закону України «Про основні засади забезпечення кібербезпеки України», у ст. 6 якого записано, що «критерії та порядок віднесення об'єктів до об'єктів критичної інфраструктури, перелік таких об'єктів, загальні вимоги до їх кіберзахисту, в тому числі щодо застосування індикаторів кіберзагроз, та вимоги до проведен-

ня незалежного аудиту інформаційної безпеки затверджуються Кабінетом Міністрів України, а в банківській системі України — Національним банком України».

У системах захисту інформаційних технологій істотну роль відведено криптографічним механізмам. Необхідність розвитку криптологічних досліджень у НАН України ще на початку 70-х років минулого століття добре усвідомлювали академіки Б.Є. Патон і В.М. Глушков. За їх ініціативою в 1973 р. в Інституті кібернетики АН УРСР було створено науково-дослідний підрозділ, який під керівництвом тоді ще члена-кореспондента, а нині — академіка НАН України І.М. Коваленка займався розв'язанням математичних задач, зумовлених запитами криптографії.

Так, в Інституті кібернетики розроблено математичний апарат для дослідження дискретних схем, комбінаторно-ймовірнісних алгоритмів, імовірнісно-алгебраїчних моделей та розв'язання прикладних задач захисту інформаційних технологій. Розроблені математичні моделі, методи, алгоритми та отримані результати застосовано для вирішення актуальних завдань криптографічного захисту інформації та криптоаналізу, визначення статистичних характеристик і оцінювання якості дискретних пристроїв, складних технічних і керуючих комплексів, а також надійності, стійкості та ефективності криптографічних систем.

Після здобуття Україною незалежності дослідження в галузі відкритої криптографії продовжували активно розвиватися. Співробітники Інституту кібернетики ім. В.М. Глушкова НАН України зробили значний внесок у становлення в Україні криптології як науки, яка не лише розробляє теоретичний апарат криптографії та криптоаналізу, а й впроваджує результати досліджень у практичну діяльність. Розроблено та у 2002 р. введено в дію Державний стандарт України ДСТУ 4145-2002, який встановлює механізм цифрового підпису, оснований на властивостях груп точок еліптичних кривих над скінченними полями характеристики 2, та правила застосування цього механізму до повідомлень, які пересилаються каналами зв'язку та/або обробляються в комп'ютеризованих системах загального призначення. Зокрема, багато уваги приділялося гармонізації європейських криптографічних стандартів для використання їх в умовах української нормативної бази з урахуванням наявних технічних і організаційних можливостей. Відповідно до планів державної стандартизації України в 2004–2009 рр. було розроблено і гармонізовано 8 стандартів ISO/IEC з метою їх прийняття в Україні.

В Інституті кібернетики розроблено також структуру цифрового конверта та протоколи його формування і декодування на основі вітчизняних криптографічних алгоритмів. У 2013 р. в Києві створено сертифікаційний центр з українським профілем X-509, який є основним елементом підтримки сучасних технологій електронного документообігу. До речі, це саме ті технології, розроблення яких ще на початку 1970-х років започаткував академік В.М. Глушков, назвавши їх «безпаперовими технологіями».

У результаті робіт, виконаних в Інституті кібернетики групою науковців під керівництвом академіка І.М. Коваленка (в 2015–2016 рр. ці роботи здійснювалися за оборонним замовленням, а з 2019 р. — за замовленням Державної служби спеціального зв'язку і захисту інформації України), було створено сучасні методи криптоаналізу потокових шифрів. Ці потужні новітні методи криптоаналізу поставили під сумнів стійкість деяких систем, наприклад бездротового зв'язку, які потребують заміни наявних алгоритмів потокового шифрування на нові, більш сучасні.

В Інституті кібернетики розроблено методи побудови диференціальних атак збоїв на різні схеми потокових шифрів. Для національного стандарту ДСТУ ГОСТ 28147:2009 у режимі потокового шифрування запропоновано нову атаку збоїв та досліджено її ефективність для різних можливостей криптоаналітика. Розглянуто загальну модель алгебраїчних атак за побічними каналами, для дослідження потокових шифрів застосовано кубічні атаки. Використовуючи алгебраїчний підхід, побудовано

атаку за побічним каналом на потоковий шифр Hitag-2. Досліджено криптографічні атаки на протоколи реалізації алгоритмів шифрування. Побудовано загальні моделі протоколів захищеного обміну повідомленнями для мобільних систем миттєвого обміну повідомленнями. Проведено криптоаналіз алгоритмів «легкої» криптографії. Розроблено бібліотеку програм для проведення криптографічного аналізу та оцінок стійкості систем криптографічного захисту.

У 1996 р. в Інституті кібернетики під керівництвом нині академіка В.К. Задираки було започатковано новий науковий напрям — комп'ютерну стеганографію. Нині цей напрям дуже динамічно розвивається.

Мета стеганографії полягає в тому, щоб замаскувати, приховати сам факт наявності або передачі конфіденційної інформації. Стеганографічні методи забезпечують неможливість виявлення конкретної інформації завдяки її прихованому вбудовуванню за спеціальними математичними алгоритмами, як правило, з використанням секретних ключів, у масиви або потоки іншої інформації — у так звані контейнери (зазвичай у тексти, зображення, аудіо- чи відеофайли, неперервні потоки). Прикладом такого маскування є цифрові «водяні знаки», ідентифікаційні номери, інша прихована інформація.

Результати досліджень, проведених в Інституті кібернетики за цим напрямом, дали змогу побудувати узагальнену модель функціонування стеганографічних систем, розробити спектральні стеганографічні методи маркування аудіосигналів, підійти до розв'язання задач захисту інформації на паперових носіях за допомогою стеганографічних технологій, удосконалити методи стеганоаналізу аудіосигналів на основі матриці суміжності та SVM-класифікації, а також на базі атаки контрольним вкрапленням.

Було розроблено пакет програм для реалізації алгоритмів арифметики багаторозрядних чисел, який за швидкодією перевершує найкращі світові зразки. Реалізовано стеганоаналітичні модифікації, які здатні з високою точністю виявляти стеганоконтейнери, створені програмами Hide4PGP, S-Tools 4.0, Steganos Privacy Suite 2012, JPHide 0.5 та JSteg. Результати досліджень впроваджено у Службі безпеки України, у виробничій діяльності ТОВ «Торговий дім «Сек» та компанії «Твінфілд Україна», зокрема для перевірки цілісності мультимедійних об'єктів і автентифікації джерел даних.

Інститут кібернетики ім. В.М. Глушкова НАН України проводить також спільні дослідження в галузі захисту інформації та інформаційних технологій з Інститутом проблем математичних машин і систем НАН України, з факультетом кібернетики Київського національного університету імені Тараса Шевченка, з Фізико-технічним інститутом (який підпорядковується МОН і НАН України) Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». У 2000 р. за ініціативою академіків НАН України М.З. Згуровського та І.М. Коваленка у Фізико-технічному інституті НТУУ «КПІ» було створено факультет інформаційної безпеки, на якому відкрито три нові кафедри:

- кафедра математичних методів захисту інформації;
- кафедра інформаційної безпеки;
- кафедра фізико-технічних засобів захисту інформації.

Освітню діяльність факультету спрямовано на підготовку фахівців високо рівня в галузі криптографічного і технічного захисту інформації, захисту інформації в комп'ютерних системах та побудови комплексних систем захисту інформації, а основними напрямами наукових досліджень та розробок є такі:

- розроблення методів криптоаналізу;
- криптографічний аналіз систем та комплексів захисту інформації;
- побудова та синтез якісних криптографічних перетворень, стійких криптографічних алгоритмів і протоколів;
- дослідження складності алгоритмів у класичній та квантовій моделі обчислень із застосуванням у криптографії;

• створення і дослідження алгоритмів стеганографічного захисту інформації;

• моделювання та аналіз кіберзагроз, дослідження систем сучасного антивірусного програмного забезпечення.

Дещо детальніше зупинюся на діяльності кафедри математичних методів захисту інформації. Ядро кафедри становлять представники школи теорії надійності, криптографії та криптоаналізу академіка І.М. Коваленка, а до викладання спеціальних дисциплін залучено як колишніх, так і нинішніх співробітників Інституту кібернетики ім. В.М. Глушкова НАН України. Наукова діяльність кафедри пов'язана насамперед з розвитком методів криптоаналізу та синтезу симетричних блокових і потокових криптосистем, криптоаналізу асиметричних криптосистем та побудови стійких криптографічних протоколів з новими функціями та властивостями, також з розробкою математичних, ймовірнісних моделей і математичного апарату для аналізу, проектування та побудови систем криптографічного захисту інформації, забезпечення безпеки інформаційно-комунікаційних систем з урахуванням як класичної, так і квантової моделі обчислень.

На сьогодні на кафедрі математичних методів захисту інформації вже виконано 27 науково-дослідних робіт, спрямованих переважно на створення більш ефективних і стійких систем криптографічного захисту інформаційних технологій. Ці роботи виконувалися на замовлення НАН України, МОН України, Служби безпеки України, Служби зовнішньої розвідки України, Міністерства оборони України, Державної служби спеціального зв'язку та захисту інформації України, ТОВ «Самсунг Електронікс Україна Компані» (Samsung Electronics Ukraine Company).

Зокрема, за останні три роки отримано результати світового рівня, а саме: розроблено методи обчислення аналітичних оцінок стійкості немарковських симетричних блокових шифрів для диференціального криптоаналізу, які дозволяють за чіткими формалізованими алгоритмами швидко виконувати практично важливі оцінки їх стійкості; вперше доведено критерії існування ефективного розв'язку в квантовій моделі обчислень чотирьох спеціальних задач абстрактної алгебри, які важливі при розробці криптосистем після винаходу масштабованого квантового комп'ютера.

На кафедрі інформаційної безпеки Фізико-технічного інституту за останні 7 років було проведено аналіз та моделювання вразливих місць у сучасних інформаційних і програмно-обчислювальних системах; розширено функціональність автоматизованого робочого місця для функціонального аналізу програмного коду; виконано аналіз та моделювання сучасних загроз безпеці операційних систем сімейства Windows; розроблено технології протидії сигнатурним та евристичним системам сучасного антивірусного програмного забезпечення з використанням механізмів антивіртуалізації, антиемуляції та захисту від відлагоджування для платформи ОС Windows; досліджено системи раннього прогнозування на основі штучного інтелекту. На кафедрі фізико-технічних засобів захисту інформації ФТІ постійно проводяться дослідження в галузі технічного та стеганографічного захисту інформації.

З 2001 р., згідно з рішенням Президії НАН України, на базі НТУУ «КПІ» регулярно проводиться науковий семінар «Проблеми сучасної криптології», роботу якого високо оцінюють фахівці з криптографічного захисту інформаційних технологій.

Однак, незважаючи на значні досягнення і напрацювання в установах Академії та університетах у галузі криптографічного захисту інформації, залишається низка актуальних проблем, які потребують нагального вирішення. Серед них можна виокремити такі:

• деякі фундаментальні питання теорії алгоритмів, абстрактної алгебри, теорії чисел, від розв'язання яких залежать характеристики якості та стійкості криптографічних алгоритмів;

• розв'язання нових прикладних задач криптографії, стеганографії, криптоаналізу, кібербезпеки;

• необхідність створення нових надійних та ефективних систем захисту інформації з урахуванням постійно зростаючих обчислюваль-

них та телекомунікаційних можливостей потенційних порушників систем інформаційної безпеки;

• розроблення алгоритмів і систем захисту інформації, стійких у квантовій моделі обчислень;

• пошук нових підходів до вирішення проблем кібербезпеки з використанням статистичних даних, теоретичних напрацювань, математичного та статистичного моделювання, машинних обчислень;

• розроблення математичного, алгоритмічного апарату, програмного забезпечення, технічних засобів для швидкого реагування на інциденти та загрози, які постійно виникають у системах захисту;

• вдосконалення та поліпшення нормативно-правової бази для створення сучасної ефективної структури захисту інформаційних технологій і кібербезпеки в державі.

Для забезпечення високого рівня захисту інформаційних технологій необхідно продовжити та посилити дослідження і розробки в галузі криптографічного, стеганографічного та технічного захисту інформації. На наш погляд, стратегія та принципи створення національної системи кібербезпеки потребують змін, доповнень та уточнень. Для модернізації і підтримки системи кібербезпеки на належному рівні потрібне створення ефективної нормативно-правової бази та постійне проведення інтенсивних комплексних наукових досліджень із залученням професіоналів-практиків.

Дякую за увагу!

За матеріалами засідання підготувала О.О. Мележик