З КАФЕДРИ ПРЕЗИДІЇ НАН УКРАЇНИ

doi: https://doi.org/10.15407/visn2022.09.009

НОВІКОВ
Олексій Миколайович —
член-кореспондент
НАН України, директор
Фізико-технічного інституту
Національного технічного
університету України
«Київський політехнічний
інститут імені Ігоря Сікорського»

КІБЕРНЕТИЧНИЙ ЗАХИСТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Стенограма доповіді на засіданні Президії НАН України 13 липня 2022 року

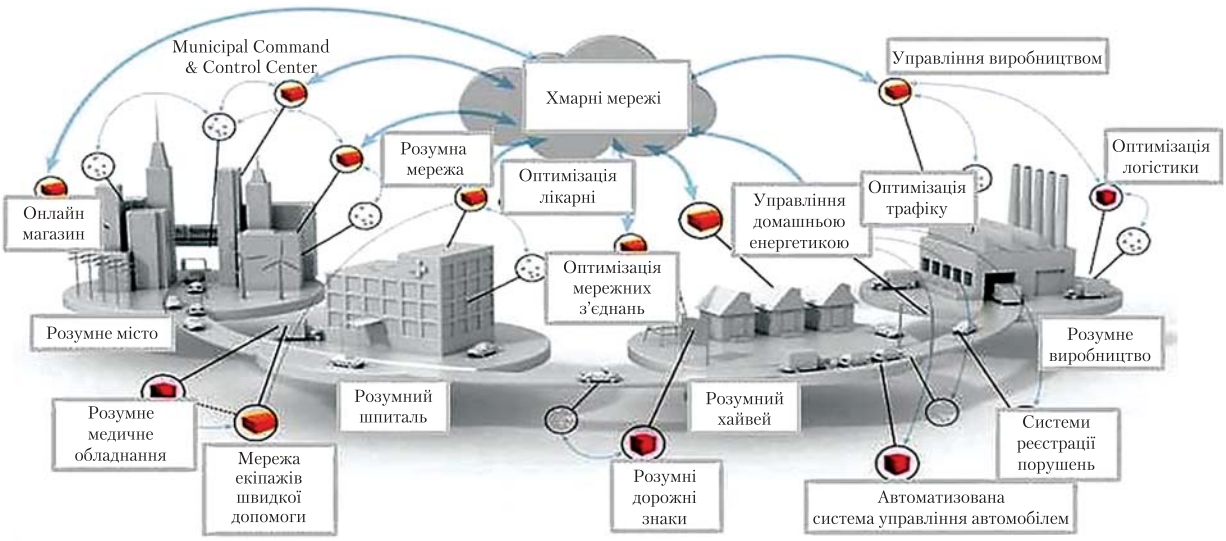
У доповіді наголошено, що одним з пріоритетних завдань для науки є зміцнення кібернетичної безпеки держави, зокрема кібернетичного захисту об'єктів критичної інфраструктури України. Наведено приклади деяких розробок у галузі інформаційної та кібернетичної безпеки, виконаних в останні роки у Фізико-технічному інституті Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Акцентовано на продуктивній співпраці з профільними установами НАН України.

Шановний Анатолію Глібовичу!
Шановні члени Президії!
Шановні присутні!

Сучасний світ характеризується стрімким поширенням інформаційно-комунікаційних технологій у всіх сферах життєдіяльності людства, зростанням можливостей інформаційного обміну даними в режимі реального часу, який уже наближається до необмеженого. З року в рік світовий інформаційний простір усе більш глобалізується, про що свідчить світова динаміка використання інтернет-ресурсів.

Так, згідно з результатами дослідження Міжнародного союзу електрозв'язку (International Telecommunication Union — ITU), у 2021 р. налічувалося 4,9 млрд інтернет-користувачів, що становить 63 % чисельності людства. Україна посідає 79-те місце зі 193 країн у рейтингу підключення до Інтернету; в нашій країні інтернет-послугами користується 67 % населення.

Сьогодні інформаційно-комунікаційні технології (ІКТ) відіграють важливу роль у розвитку різних галузей економіки, системи охорони здоров'я, у побуті. Значущість ІКТ особливо підвищилася з поширенням так званого Інтернету речей (IoT), технології якого сприяють розвитку розумних міст, безпілотного транспорту, моніторингу показників здоров'я людей та інших соціально важливих напрямів. Сьогодні ІКТ інтегровано в такі продукти, які раніше традиційно функціо-



Зростання впливу інформаційних і комунікаційних технологій на життя людства

нували без них, наприклад в автомобілі, будинки, людські організми (див. рис.). Згідно з результатами аналізу компанії IoT Analytics, упродовж 2021 р. до мережі Інтернет додатково було підключено 12,3 млрд активних точок IoT, тобто по 2,5 підключення на кожного інтернет-користувача.

Однак зі зростанням впливу ІКТ на життя людей зростає і кількість загроз із кібернетичного простору.

За інформацією такої авторитетної установи, як A. James Clark School of Engineering (University of Maryland), у 2021 р. у світі сталося понад 800 тис. кібератак, тобто в середньому 2,2 тис. атак на добу. У звіті Norton Cyber Safety Insights Report зазначено, що минулого року 300 млн користувачів у 10 провідних країнах світу зазнали нападів кіберзлочинців. За даними, опублікованими у журналі Cybersecurity Ventures, збитки від глобальної кіберзлочинності у 2021 р. становили 6 трлн дол. США і мають тенденцію до зростання (приблизно на 15 % щороку); очікується, що у 2025 р. збитки сягнуть 10,5 трлн дол. США.

Загрози у кібернетичному просторі мають свою історію, постійно еволюціонують та удосконалюються. Зазвичай виділяють чотири групи носіїв загроз у кібернетичному просторі:

1) *неорганізовані аматори* (ентузіасти, зловмисники, шахраї) — діють з 1975 р.; їхні мотиви — цікавість, ентузіазм, матеріальний зиск;

2) *організовані хакерські угруповання* — діють з 1980—1990-х років; їхньою метою є отримання матеріальної вигоди злочинним шляхом;

3) *кіберзлочинні угруповання, які фінансуються державами*, — діють з 1998 р.; їх діяльність спрямована на порушення конфіденційності й цілісності інформації та доступності комп'ютерних даних і систем;

4) *кібервійська* — діють з 2010 р.; застосовують кіберзброю з метою заподіяння руйнівної шкоди супротивнику, зокрема у фізичному просторі.

Згідно зі звітом корпорації «Майкрософт» щодо загроз у кібернетичному просторі за період II півріччя 2020 р. — I півріччя 2021 р., найбільше хакерських атак було зафіксовано з Російської Федерації (58 %), Північної Кореї (23 %), Ірану (11 %) та Китаю (8 %). Більшість хакерських атак було спрямовано проти Сполучених Штатів Америки (46 %), України (19 %), Великої Британії (9 %), Бельгії, Японії, Німеччини (по 3 %), Ізраїлю (2 %).

За останні 10 років Україна зазнала та відбила десятки потужних кібератак. Найбільш відомими з них були такі:

• грудень 2013 р. — під час масових протестів атаковано інформаційні системи приватних підприємств та державні установи України;

• травень 2014 р. — атаковано інформаційну систему «Вибори» під час виборів Президента України;

• грудень 2015 р. — кібератака за допомогою троянської програми BlackEnergy на три енергопостачальні компанії України: «Прикарпаттяобленерго», «Чернівціобленерго» та «Київобленерго»;

• грудень 2016 р. — атаковано підстанцію «Північна» НЕК «Укренерго», що призвело до часткового знеструмлення правобережної частини Києва та області;

• квітень-травень 2017 р. — атака з ураженням бекдором від програми M.E.Doc;

• червень 2017 р. — масштабна атака хробаком-винищувачем NotPetya, внаслідок чого постраждали ресурси майже 80 % підприємств України;

• жовтень 2020 р. — DDoS-атака на мережу НТУУ «КПІ імені Ігоря Сікорського» з боку 200 тис. інфікованих вузлів.

З початком гострої фази воєнної агресії РФ проти України масштаб кібератак істотно збільшився. Служба безпеки України 4 квітня 2022 р. повідомила, що в ніч на 24 лютого росіяни здійснили рекордну кількість хакерських атак на українські інформаційні системи, вони планували знищити весь кіберзахист України. В інтерв'ю виданню Liga.Tech від 29 червня 2022 р. голова Державної служби спеціального зв'язку та захисту інформації України Юрій Щиголь зазначив, що від початку війни РФ здійснила 796 кібератак проти України, що втричі більше, ніж за аналогічний період минулого року, проте якість кібератак почала знижуватися. За його словами, 90 % російських хакерських угруповань, які беруть участь у кібервійні проти України, належать до силових структур, таких як Головне розвідувальне управління Генштабу Збройних сил РФ, Федеральна служба безпеки, Служба зовнішньої розвідки РФ.

У звіті корпорації «Майкрософт» від 27 квітня 2022 р. «Гібридна війна в Україні» зазначено, що підготовка до проведення кібернападу на Україну розпочалася ще за рік до повномасштабного вторгнення — у березні 2021 р. Фахівці компанії зафіксували щонайменше 6 хакерських угруповань, пов'язаних з РФ, які здійснили 237 кібератак проти українських підприємств та державних установ: 32 % атак було спрямовано на українські органи державної влади різних рівнів, 40 % — на організації критичної інфраструктури.

Незважаючи на всі зусилля росіян з організації масованих кібератак, національна система кібербезпеки України виявила високу стійкість, продемонструвала здатність ефективно реагувати на комп'ютерні надзвичайні події в країні, що засвідчило професійність кадрового складу та успішність у боротьбі в умовах жорсткої інтелектуальної конфронтації. Запланованого ворогом цифрового армагедону в Україні не відбулося.

Успішність України в кібервійні з росіянами стала результатом багаторічної праці з побудови та зміцнення національної системи кібербезпеки України. Створення потужної системи інформаційної безпеки держави було закріплено в Законі України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017. У травні 2021 р. РНБО України ухвалила Стратегію кіберзахисту України на наступні п'ять років, у серпні 2021 р. Указом Президента України було прийнято рішення про створення кібервійськ у складі Міністерства оборони України, а фінальний етап розроблення законодавчих нормативних актів щодо структури кібервійськ завершився у лютому 2022 р.

Завдяки системній роботі з розбудови національної системи кібербезпеки Україна посідає високі позиції у світових рейтингах з кібербезпеки: 24-те місце серед 160 проіндексованих країн у рейтингу Академії електронного управління Естонії (National Cyber Security Index — NCSI) за 2020—2021 рр.; 78-ме місце серед 193 проіндексованих країн у GCI (Global Cybersecurity Index) Міжнародного союзу електрозв'язку (International Telecommunication Union — ITU) за 2020 р.

Президент НАН України академік Б.Є. Патон та ректор НТУУ «КПІ імені Ігоря Сікорського» академік М.З. Згуровський вручають магістерські дипломи випускникам Фізико-технічного інституту. 2001 р.

Слід наголосити, що розбудова й ефективне функціонування національної системи кібербезпеки України, які забезпечили успішне стримування кіберагресії РФ, стали можливими завдяки активній участі наукових установ і колективів фахівців з інформаційних технологій, збільшенню кількості і якості їхніх розробок у сфері кібербезпеки. Так, Фізико-технічний інститут Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», який я представляю, має багаторічний досвід проведення науково-технічних робіт у галузі інформаційної та кібернетичної безпеки.

Фізико-технічний інститут НТУУ «КПІ імені Ігоря Сікорського» було засновано в 1995 р. рішенням Президії НАН України та МОН України за ініціативою академіків НАН України Б.Є. Патона і М.З. Згуровського. Перший випуск магістрів відбувся в 2001 р.

Зараз у Фізико-технічному інституті налічується понад 100 викладачів і більш як 1000 студентів. Ми працюємо не лише за двома традиційними фізтехівськими напрямами — прикладна фізика і прикладна математика, а й за напрямом інформаційної безпеки, який тепер має назву «кібербезпека». Впродовж двох останніх десятиліть науково-технічні проєкти в галузі інформаційної та кібернетичної безпеки успішно виконують співробітники трьох підрозділів Фізико-технічного інституту:

• *кафедра математичних методів захисту інформації* — створена в 2000 р. на базі наукової школи криптоаналізу академіка НАН України Ігоря Миколайовича Коваленка; основні напрями наукової діяльності: криптологія і криптографія; розроблення математичних методів захисту інформації на базі фундаментальних курсів математичного аналізу, алгебри, загальної алгебри, теорії алгоритмів та математичної логіки, дискретної математики, теорії імовірності та математичної статистики;

• *кафедра інформаційної безпеки* — створена в 1999 р. на базі наукової школи моделювання та безпеки складних систем академіка НАН України Михайла Захаровича Згуровського; основні напрями наукової діяльності: математичні методи моделювання і проєктування систем захисту інформації; системний аналіз безпеки складних систем; безпека інформаційно-комунікаційних систем; розв'язання задач, пов'язаних з прийняттям рішень в умовах невизначеності та конкурентної взаємодії;

• *команда білих хакерів* — науково-технологічна лабораторія під керівництвом доцента Миколи Ільїна; протягом останніх 10 років ця команда впевнено входить до першої десятки світового змагання CTF, а у 2016 р. посіла 1-ше місце серед 12 600 команд — учасниць цього конкурсу; бере активну участь у виконанні наукових розробок Фізико-технічного інституту та проведенні тренінгів.

За останні 10 років співробітники Фізико-технічного інституту НТУУ «КПІ імені Ігоря Сікорського» виконали десятки робіт за державним оборонним замовленням за такими напрямами, як теорія і практика комп'ютерного моделювання; моніторинг, аналіз стану та проєктування систем кібернетичного захисту; створення моделей, описів, новітніх сценаріїв кібернетичного захисту; розроблення методів протидії зовнішнім атакам; створення зразків програмних засобів тощо. Лише в 2021 р. за державним оборонним замовленням було виконано п'ять робіт з обсягом фінансування близько 4 млн грн. Оскільки більшість цих робіт мають

обмеження на поширення інформації, я розповім лише про дві «відкриті» розробки.

По-перше, це створення *програмно-апаратного комплексу для аналізу комп'ютерних програм та їх оновлень на відсутність недокументованих функцій*. Актуальність цієї розробки визначається необхідністю довіри до відсутності вразливостей у програмних системах.

Так, Агентство з кібербезпеки та захисту інфраструктури США (Cybersecurity and Infrastructure Security Agency — CISA) у 2020 р. зафіксувало в програмних продуктах 17 500 вразливостей з тенденцією до їх зростання на 2 % за рік. Висока довіра до використовуваних програм є ключовою вимогою, особливо для застосування їх у системах критичної інфраструктури країни та інформаційних системах національного рівня.

У 2020 р. Держспецзв'язок України оголосив конкурс, який проводився в рамках програми реформування системи захисту інформації в Україні. В основі зазначеного реформування лежить перехід від директивної системи, що ґрунтується на необхідності впровадження та атестації комплексної системи захисту інформації на об'єкті інформаційної діяльності, до декларативної системи, в якій власник інформації самостійно визначає спосіб її захисту та відповідає за захист цієї інформації. Отже, відповідальність власників інформації за її захист посилюється, але при цьому Держспецзв'язок України має вивести на ринок країни сучасні системи забезпечення кібербезпеки та її аудиту (сканери безпеки та ін.), з використанням яких власники інформації на місцях можуть забезпечити її захист.

Фізико-технічний інститут НТУУ «КПІ імені Ігоря Сікорського» виграв згаданий вище конкурс Держспецзв'язку і розробив відповідний програмно-апаратний комплекс, за допомогою якого можна оцінити рівень впевненості у відсутності недокументованих функцій у досліджуваному програмному продукті. В основу розробки було покладено ідею щодо використання зворотного інжинірингу (платформа Ghidra) та аналізу програмного коду з використанням найбільш відомих у світі баз вразливостей інформаційної безпеки CVE (Common Vulnerabilities and Exposures) та бази помилок програмного забезпечення різного рівня критичності CWE (Common Weakness Enumeration).

Перевагами комплексу є його обчислювальна ефективність, яка дає змогу здійснювати аналіз реального програмного забезпечення великого обсягу (понад 1 млн інструкцій), зокрема вихідних кодів ядра операційної системи, прошивки складних мережевих пристроїв тощо, за прийнятний час (від 1 хв до кількох діб) на комерційно доступних робочих станціях середнього рівня, а також можливість його тиражування та розповсюдження в масштабах усієї країни.

Тестування комплексу проводили з використанням набору програм, запропонованих замовником, у режимі «чорної скриньки». Тестові програми містили 65 дефектів, незадекларованих функцій та вразливостей. У результаті було виявлено 90 % проблемних місць, і в 2021 р. Держспецзв'язок України прийняв комплекс в експлуатацію.

Друга наша розробка — це створення методу та процедури проєктування систем кібернетичного захисту інформаційно-комунікаційних систем, на основі яких розроблено *програмний комплекс проєктування системи кібернетичного захисту інформаційно-комунікаційних систем*.

Метод ґрунтується на логіко-ймовірнісній моделі успішності кібератаки на інформаційно-комунікаційну систему з урахуванням множини загроз та механізмів захисту; процедура проєктування — на оптимізаційному підході, застосованому до систем кібернетичного захисту з визначенням топології мережі, місць розміщення та міцності механізмів захисту. При побудові комплексу, який ґрунтується на послідовності етапів створення комплексних систем захисту інформації, ми врахували всі вимоги відповідних нормативних документів Держспецзв'язку України.

Використання зазначеної розробки дозволяє скоротити час проєктування та зменшити вартість механізмів захисту інформації. На

сьогодні діє прототип програмного комплексу проєктування системи кібернетичного захисту інформаційно-комунікаційних систем.

Важливим етапом впровадження результатів виконуваних проєктів є підвищення кваліфікації персоналу замовників — фахівців з інформаційної та кібернетичної безпеки. Останніми роками викладачі Фізико-технічного інституту провели десятки тренінгів для співробітників організацій-замовників.

На завершення слід зазначити, що Фізико-технічний інститут НТУУ «Київський політехнічний інститут імені Ігоря Сікорського» плідно співпрацює в галузі кібернетичного захисту інформаційних систем і технологій з установами Відділення інформатики НАН України, зокрема з Інститутом кібернетики ім. В.М. Глушкова, Інститутом проблем реєстрації інформації, Інститутом космічних досліджень НАН України і ДКА України.

Дякую за увагу!

За матеріалами засідання підготувала О.О. Мележик

Oleksii M. Novikov

National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Kyiv, Ukraine

CYBER DEFENSE OF INFORMATION TECHNOLOGIES

Transcript of scientific report at the meeting of the Presidium of NAS of Ukraine, July 13, 2022

The report emphasizes that one of the priority tasks for science is to strengthen the cyber security of the state, in particular, to ensure the cyber protection of critical infrastructure objects of Ukraine. Examples of some developments in the field of information and cyber security carried out in recent years at the Institute of Physics and Technology of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" are given. Emphasis is placed on productive cooperation with specialized institutions of the NAS of Ukraine.