Міністерство освіти і науки України
Одеська національна академія зв'язку ім. О.С. Попова

МАТЕРІАЛИ

VI Міжнародної науково-практичної конференції

"ПЕРСПЕКТИВНІ НАПРЯМИ ЗАХИСТУ ІНФОРМАЦІЇ"

02 – 06 вересня 2020 року

Одеса 2020

УДК 004.056.5
П 26

Перспективні няпрями захисту інформації: матеріали шостої
П 26 міжнародної наук.-пр. конф. – м. Одеса, 02 – 06 вересня 2020 р. –
Одеса: Бондаренко М.О., 2020. – 120 с.

ISBN 978-617-7829-61-3

Даний збірник містить тези матеріалів, що представлені на шосту всеукраїнську науково-практичну конференцію "**Перспективні няпрями захисту інформації**", що проводиться 02 – 06 вересня 2020 р. в Одеській національній академії зв′язку ім. О.С. Попова.

У збірник включені тези доповідей за такими напрямками:

- організаційно-правові методи захисту інформації;
- захист критичної інформаційної інфраструктури держави;
- кібербезпека, протидія кібертероризму та кіберзлочинності;
- управління інцидентами інформаційної безпеки;
- технології захисту хмарних обчислень;
- постквантова криптографія;
- технічні засоби виявлення каналів витоку інформації;
- засоби захисту інформації в інформаційних і телекомунікаційних системах;
- елементи і компоненти для систем захисту інформації;
- телекомунікаційні системи та мережі.

Робочі мови конференції – українська, російська, англійська.

УДК 004.056.5

ISBN 978-617-7829-61-3

Кононович В.Г.[1], Стайкуца С.В. [1], Кононович І.В.[2], Романюков М.Г.[3]

КОНТУРИ СИСТЕМ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ЦИФРОВІЗОВАНОГО СУСПІЛЬСТВА ТА КІБЕРНЕТИЗОВАНОГО ВИРОБНИЦТВА, БІЗНЕСУ Й УПРАВЛІННЯ

[1]Одеська національна академія зв'язку ім. О.С. Попова,
[2]Одеська національна академія харчових технологій,
[3]Одеський національний політехнічний університет
[1]vl_kononovich@ukr.net, [1]s.staikuca@gmail.com, [2]aS_8@i.ua, [3]kolyanr21@gmail.com

Анотація. Проблеми і задачі забезпечення інформаційної та кібербезпеки майже завжди виникали вже в процесі нестримного розвитку інформаційно-комунікаційних систем та технологій. Превентивні засоби і заходи захисту теж були предметом наукового дослідження, але прорив у цьому напрямі ще не сформувався. У даній роботі здійснюється превентивне формування методології системи забезпечення кібербезпеки в моделях результатів прийдешніх змін нашого буття. Дається короткий огляд змін суспільної організації, трансформації способів виробництва, цифрової економіки, соціальних і наносоціальних технологій. Формується каркас загальної ієрархічної системи забезпечення кібербезпеки. Пропонується принципи багаторівневої системи безпеки: внутрішньої кібербезпеки само організованих спільнот, зокрема методологія рейтингової системи кібербезпеки, заснованої на довірі, кібербезпеки взаємодії і співіснування між динамічно змінних у агональному часі спільнот, системи кібербезпеки технологій загального управління. Плодотворна полеміка в цих напрямах дозволить превентивно підвищити зрілість-ефективність системи забезпечення кібербезпеки як складової національної безпеки.

Ключові слова. Кібербезпека, цифрова економіка, рейтингова система кібербезпеки, інформаційно-телекомунікаційна мережа.

Проблеми і задачі забезпечення інформаційної та кібербезпеки майже завжди виникали з запізненням вже в процесі нестримного розвитку інформаційно-комунікаційних систем і технологій. Превентивні засоби і заходи захисту теж були предметом науково-практичного дослідження, але прорив у цьому напрямі ще не сформувався. На поточний момент багато вчених і футурологів (виділимо з них лише Василя Стуса та Сергія Переслегіна) відмічають перехід від сингулярних моделей розвитку людства (яскраве дослідження належить Сергію Капіца [1]) до аутопоезних (Олена Князева), синергетичних (Сергій Курдюмов, Георгій Малинецький) моделей динамічного хаосу – не стохастичного, а детермінованого хаосу, відкритого М. Фейгенбаумом і який, у найпростішому вигляді, якісно демонструється нелінійною динамічною системою, що описується математичним виразом:

$$x_{n+1} = x_n - px_n^2 + x_{input} \tag{1}$$

де: x_{input} – вхідний потік даних системи (відбір вхідної інформації, консолідація, переробка); x – динамічна змінна, яка має смисл інтенсивності інформаційних елементів потоку на етапах обробки інформації; p – управляючий перехідний коефіцієнт, що характеризує степінь зворотного зв'язку з наступним етапом обробки інформації; причому $p = const \in (0,1)$, $\{x\} \in R$, $x_{input} \in R^+$. Конкретна фізична інтерпретація моделі залежить від виду системи і може застосовуватись до широкого кола соціальних, біологічних, технічних, психічних процесів тощо. Незважаючи на свою простоту, модель (1) ілюструє само організоване виникнення коливань, біфуркації з подвоєнням періоду, ускладнення форми (спектру) коливань і детермінований хаос (хаосоподібні коливання). Важлива властивість детермінованого хаосу полягає в тому, що під час біфуркації малий вплив визначає значні зміни у виборі подальшої траєкторії процесу. Огляд застосування ряду нелінійних

динамічних моделей для опису процесів забезпечення кібербезпеки надано у [2]. У роботі В. Лепского «представлені результати досліджень з актуальних науково-практичних напрямах; рефлексивні механізми управління складністю; етичні аспекти управління; управління саморозвитком рефлексивно-активними середовищами; еволюція технологій управління в інформаційних війнах; розвитку кібернетики від класичної та кібернетики другого порядку до кібернетики третього порядку на основі постнекласичної наукової реальності та транс дисциплінарного підходу [3]» а також наївно елементарні підходи до їх безпеки. Численні періодичні видання містять описи можливого майбутнього. Наприклад, Лариса Колесова наводить дослідження «агонального часу» [4], а багато авторів описують майбутню «цифрову економіку», наприклад [5]. У переважній більшості цих робіт мало або зовсім не приділяється увага до проблем кібербезпеки.

Мета даної роботи полягає в окресленні шляхів вирішення проблеми кібербезпеки в соціальних, економічних, технічних аспектах найближчого майбутнього. Поставлена проблема почала вирішуватись авторами в роботі [6], де на базі поточної фіксації нових тенденцій розвитку суспільства і технологій обґрунтовується та пропонується інноваційна ієрархічна система категоріювання інформаційних ресурсів. Дана робота є нарисом формування системи кібербезпеки з врахуванням того факту, що Україна і весь світ вже перейшли в фазу хаосу і глобальні трансформації суспільства вже починають здійснюватись.

Зауважимо, що у вирішенні задачі забезпечення кібербезпеки інформаційно-комунікаційних систем (ІКС) і технологій, зокрема Інтернет, досягнуто серйозні успіхи в частині організаційних заходів, апаратно-програмних засобів кібербезпеки, криптографічних методів захисту і контролю доступу. Але, залишилася неблагополучна ситуація з людським фактором. Його доля в кількості порушень та інцидентів з кібербезпекою на сьогодні складає більше 80%. Відповідно до цього, теорії і методи кібербезпеки повинні включати в себе такі категорії, як індивідуальна та колективна свідомість та підсвідомість; соціальні та наносоціальні технології. Кібернетична безпека і національна безпека, в цьому смислі вирішують спорідненні проблеми.

Окреслимо основні риси майбутнього суспільства з нашої точки зору. Перш за все, розглянемо причини перетворень і змін. Ми вже вказували [6], що грандіозні зміни у людства відбуваються не вперше. Так, перехід від феодалізму до капіталізму проходив під тиском нового економічного укладу і супроводжувався прийняттям нових законів, юридичної системи, нового рівня свободи і відповідальності людини, культури, світогляду і багато іншого. Подібні новації у наш час будуть більш масштабними і також незвичними. Інформаційний товар, інформаційний засіб виробництва, інформаційна сировина для виробництва, взаємодія і взаємовідносини за допомогою ІКС зовсім не схожі на їх фізичні аналоги. Їх цінність і спосіб використання визначаються зовсім по іншому. Інформація здебільшого безплатна, а її значення і вплив все посилюються. Інформаційний світ своєю віртуальною реальністю стає панувати над фізичним світом. Виділимо декілька аспектів, важливих для методології систем кібербезпеки.

Знання перестає бути силою. Знання швидко старіє. За одне покоління змінюється декілька технологій і люди змушені все життя вчитись і переучуватись, що не є легкою працею. Силою стало уміння мислити. Вже сьогодні від бізнесмена вимагається вміння сприймати нове. Креативність стала головнішою, ніж розумність.

Наука втрачає своє значення. Точніше – у абсолютному вимірі потреба у наукових (науково-практичних) дослідженнях зростає, а у відносному, у порівнянні з іншими засобами досягнення прогресу – падає. У віртуальному світі та світі програмування аналітику може замінити простий перебір варіантів. Кожен з варіантів легко і дешево запрограмувати і порівняти з попереднім. Крім того, наука дискредитувала себе, бо мало дбає про наукову безпеку. Наука не змогла вирішити проблему раціональної швидкості прогресу. Ми викидаємо на смітник транзистори, інтегральні схеми, мікропроцесори і комп'ютери, хоча вони фізично ще не виробили свій ресурс. Наука допустила забруднення у масштабах планети і ще багато чого. Наука повинна створити і запровадити систему власної безпеки.

Тут можна знайти багато спільного з кібербезпекою кібер середовища. Обидві мають глобальний характер, обидві засновані на широкому обміні інформації, обидві користуються віртуальними інструментами.

Самоорганізація стає провідним чинником. Вона завжди була одною з невід'ємних рис сапієнсу – сім'я, плем'я, тейп, держава, цивілізація… . Навіть при плановому господарстві, коли самоорганізація жорстко контролювалась, пробивались її впливи у вигляді кооперативів, профспілок, спільнот у трудових колективах, професійних спільнот. У постіндустріальну епоху їм на зміну приходять інші – «мережні спільноти, у яких люди ніяк не пов'язані один з одним місцем роботи, зате мають більш високий рівень політизації, ніж суспільство в цілому (цитата із сайту Олександра Скопова)». Деякий час здавалось, що почалась атомізація і розпилення спільнот. Але, як казав відомий класик: «Перш ніж поєднатись треба роз'єднатись». Автономні особистості звільняються від залежності від усіляких угрупувань і вступають у новий світ горизонтальної самоорганізації таких автономних особистостей (вільний переклад з рос.). У майбутньому осередки самоорганізації будуть інші. Більш детально рушійні сили самоорганізації та використання її в системах забезпечення кібербезпеки наведені далі.

Ієрархічна система кібербезпеки. Спираючись на результати використання ієрархічної системи категоріювання, що описана в [6], доцільно будувати систему забезпечення кібербезпеки, відповідно, за принципом ієрархії. На зміну державної системи кібербезпеки з єдиною державною нормативно-правовою базою може прийти ієрархічна система кібербезпеки зі своїми принципами на кожному з рівнів. Це рішення випливає з того факту, що змінюється організація державного устрою. Вертикальна система прийняття рішень замінюється на мережні структури з горизонтальними взаємодіями. Ієрархічна система забезпечення кібербезпеки може мати наступну структуру: рівень системи кібербезпеки державного управління, місцевого самоврядування та надавання державних послуг з вертикальними зв'язками; рівень взаємодії та співпраці самоорганізованих спільнот та угрупувань; рівень самоорганізованих мережевих структур з горизонтальними взаємодіями. На практиці система може бути складнішою при комбінуванні вертикальних та горизонтальних зв'язків. Далі розглянемо детально побудову системи забезпечення кібербезпеки 3-го рівня, коротко оглянувши системи кібербезпеки першого та другого рівня.

Система забезпечення кібербезпеки державного управління та державних послуг. Як найбільш консервативна система забезпечення кібербезпеки держави (кібербезпеки вертикального управління та кібербезпека державних послуг, включно до місцевих органів влади) може бути заснована на існуючій системі кібербезпеки та єдиній державній нормативно-правовій базі. Тим паче, що ця система активно розвивається. На доданок до системи цифрового підпису, розвивається системи безпечного надавання державних послуг, електронного документообігу і всієї системи безпеки «Електронного уряду». Продовжується вдосконалення системи криптографічного захисту інформації.

Система забезпечення кібербезпеки загальнодержавної системи взаємодії та співпраці самоорганізованих спільнот та угрупувань включаючи взаємодію та співпрацю з державними підприємствами, установами та органами. Це найбільш відповідальна частина системи кібербезпеки, від якої залежить сталість і ефективність функціонування суспільства, інформаційна безпека держави та національна безпека. Основу системи кібербезпеки на цьому рівні складають засоби кібербезпеки ІКС, які на сьогодні вже перетворились на інформаційно-комунікаційне середовище. В його скла входить і глобальна мережа – Інтернет. Наприклад, банкомати успішно і безпечно працюють через Інтернет. Є задача забезпечити базову кібербезпеку всього інформаційно-комунікаційне середовища.

Система забезпечення кібербезпеки функціонування самоорганізованих децентралізованих мережевих структур з горизонтальними взаємодіями. Організацію системи кібербезпеки проведемо на базі децентралізованих кооперативних мереж (ДКМ) у відновлювальній медицині [7]. Уточнимо термінологію, маючи за зразок дану роботу. «У широкому смислі мережа є система із елементів (вузлів), які з'єднані лініями (зв'язками,

ребрами)». У вузькому смислі «мережева структура – це децентралізована (що не має єдиної управляючої ланки) структура з елементів, які кооперують між собою у реалізації певної діяльності [7]» (реалізують горизонтальну взаємодію). Мережева структура протиставляється системі з вертикальними зв'язками, де є управляюча ланка – лідер, керівник, домінант тощо. До даної структури не відносяться також ринкові структури, бо їх складові елементи не кооперують, а конкурують між собою. Децентралізована мережева структура утворюється в результаті самоорганізації, хоча її члени не приєднується стохастичним чином, а в процесі динамічного хаосу, тобто в процесі «добровільного» приєднання.

Рушійною силою самоорганізації децентралізованої мережевої структури є потреба у реалізації певної цілі, яку можна досягти лише об'єднаними силами. Такого типу поведінку мають на рівні інстинктів багато видів живих істот, а людям вона притаманна з часів первісного світу. Тут відіграє свою «колективне народне підсвідоме, аморфне, спонтанне, яке поступово звіріє і втрачає почуття страху, яке не направляється, схоже, ніким і нічим, окрім загального усвідомлення, що жити так більше не можна».

Завдяки таким властивостям децентралізованих мережевих структур їх кібербезпека може отримати, так би мовити, «друге дихання». Людський фактор може стати лояльним і благо сприятливим до системи кібербезпеки. Людина змінюється. Дійсно, протестуюча людина – «це людина, чия національна ідея – вільна країна, де на чолі законність і право. Це людина, яка усвідомлює себе громадянином і цінить права співгромадян. Поважає їх право недоторканність власності і тому навіть під час протесту не дозволить собі нікому причинити збиток. Ця людина готова відстоювати свої права навіть не маючи особливої надії на перемогу – просто тому, що почуття власної гідності не дозволяє йому поступати інакше. … Величезна новопридбана солідарність, почуття ліктя та спільності – вона куди більш заразніше короновірусу і моментально просочилась повсюди (переклад з рос. - вільний)». Тобто, можливо стверджувати, що методами соціальних і наносоціальних технологій можна досягти такого психологічного настрою у мережевій структурі, яка сприяє чіткому дотриманню правил кібербезпеки та свідомого їх вдосконалення. Крім того, можна створити систему кібербезпеки, яка створює і підтримує відповідні умови. Розглянемо цю систему докладніше.

Рейтингова система кібербезпеки, заснована на довірі. Така система була відома раніше у, модних десятиліття назад, піринговых мережах (ITU-T Recommendation X.1162, X.1162. Security architecture and operations for peer-to-peer networks.). До речі, пірингові комунікації створювались користувачами якраз за принципами самоорганізації. Розглянемо стандартні функції безпеки для задоволення вимог до кібербезпеки піринговых комунікацій.

Щоб досягти виконання вимог кібербезпеки піринговых комунікацій при виконанні піринговою мережею її примітивних операцій можуть використовуватися наступні *стандартні функції безпеки*: шифрування; обмін ключами; контроль доступу; механізм цілісності даних; безпека маршрутизації; механізм контролю трафіку. До стандартних функцій безпеки додають *спеціальні функції безпеки*: цифровий підпис; управління довірою; обмін автентифікацією; нотаризація; призначення ідентифікатора (ІД).

Сукупно стандартні і спеціальні функції безпеки можуть бути використані для гарантування стандартних вимог безпеки: (автентифікація користувача; приватність; цілісність даних; конфіденційність даних; контроль доступу; готовність; доступність; не зречення) і спеціальних вимог безпеки: (анонімність; спостережність з'єднань; контроль трафіку). Зауважимо, що вимоги «приватність» в українській нормативній нема. Замість цього права суб'єкта захищаються Законом «Про захист персональних даних користувача».

Примітивні операції піринговой мережі тісно пов'язані з функціями безпеки. Коли виконуються примітивні операції, то адміністратор безпеки домену повинен використовувати відповідні функції безпеки, які відповідають вимогам інформаційної безпеки. До примітивних операцій піринговой мережі відносяться: приєднання; від'єднання; пошук; чат (бесіда); маршрутизація; вставка, поправка; оновлення, вилучення; мультикастинг. Розглянемо докладніше функція, пов'язану з використанням довіри.

Управління довірою поділяється на такі задачі:

- **рекомендоване обмеження локальною мережею.** Величина довіри одного користувача визначається дослідженням обмеженого числа інших користувачів. У цьому випадку широко використовується простий метод місцевої широкомовної передачі. Звичайно обмежуються P2P мережею малого масштабу, як наприклад маленькою локальною обчислювальною мережею. Для більшої мережі оцінки величини довір'я часто стають істотно неточними.

- публічна інфраструктура ключів. У цій інфраструктурі є декілька центральних вузлів, які контролюють всю мережу і регулярно сповіщають щодо зміни вузлів. Законність і ефективність цих центральних вузлів гарантована атестатами відповідності чинним нормативно-правовим документам. Така роду системи мають залежність від центра і певні проблеми, наприклад, із здатністю розширення та аспектами законності окремих вузлів.

- репутація. Величина довіри пір вузлів обчислюється через зворотний зв'язок транзакцій з кожним із них. Величина довіри користувачу обчислюється після оцінки і статистичного аналізу такого зворотного зв'язку.

- основна роль. У заснованій на ролі моделі довіри P2P, величиною довіри певного пір вузла визначається його статус користувача мережі, і за статусом користувача можуть плануватись його відношення з іншими користувачами. Нормально, у такій модель застосовується функція для обчислення величини довіри кожного вузла. Також застосовується простий, мало затратний алгоритм, який дозволяє користувачу перевірити асиметричність довіри у взаємовідносинах між двома користувачами.

Призначення ідентифікатора (ID). Для того, щоб відрізняти кожен пір та інформацію, всім пір та інформації призначаються унікальні ідентифікатори (ID). Тому, що у чистих моделях пірингових послуг немає ніяких централізованих серверів, то такі ідентифікатори призначаються за згодою пір (за договором).

Якщо механізм призначення ID не захищений, то зловмисний пір може атакувати пірингові комунікації, використовуючи підроблені ID. Безпечна функція призначення ID використовується для захисту проти неправильного вживання призначених ID і зловживання нелегальними ідентифікаторами.

Висновок. У даній роботі сформована методологія ієрархічної системи забезпечення кібербезпеки. Пропонується принципи трьохрівневої системи кібербезпеки: внутрішньої кібербезпеки само організованих спільнот, кібербезпеки взаємодії між само організованих спільнотами; кібербезпеки технологій загального управління. Детально обґрунтована методологія рейтингової системи кібербезпеки, заснованої на довірі, яка дозволить підвищити ефективність системи забезпечення кібербезпеки як складової національної безпеки.

Литература

1. Капица С.П. Модель роста населения земли и предвидимое будущее цивилизации // Вопросы экономики. 2000. No 12, – С. 22 – 43. [Електронний ресурс]: http://ecsocman.hse.ru/data/291/971/1219/2002 _n3_p22-43.pdf.
2. Кононович В. Г. Математичні моделі процесів забезпечення соціально-психологічної кібербезпеки / В.Г. Кононович, І.В. Кононович, М.Г. Романюков // Науково-технічний збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». – Випуск 2 (32), 2016. С. 49 – 55.
3. Лепский В. Е. Методологический и философский анализ развития проблематики управления / В.Е. Лепский – М.: Когито-Центр, 2019. – 340 с.
4. Колесова Л. Агональные времена / Лариса Колесова // Сайт С.А. Курдюмова [Електронний ресурс]: http://spkurdyumov.ru/networks/agonalnye-vremena.

5. Гохберг Л. М. Что такое цифровая экономика? Тренды, компетенции, измерение [Текст]: докл. к XX Апр. междунар. науч. конф. по проблемам развития экономики и общества, Москва, 9–12 апр. 2019 г. / Г. И. Абдрахманова, К. О. Вишневский, Л. М. Гохберг и др. – М.: Изд. дом Высшей школы экономики, 2019. – 82 с.

6. Кононович В. Г. Адаптивні підходи до забезпечення кібербезпеки розподілених систем / В. Г. Кононович, С.В. Стайкуца, І. В. Кононович, Ю.В. Копитін, М.Г. Романюков // Безпека інформації. – Київ: НАУ, 2016. – Том 22, № 3. – С. 255 - 260.

7. Олескин А.В. Роль децентрализованных кооперативных сетей (ДКС) в восстановительной медицине / А.В. Олескин // Вестник восстановительной медицине, № 2, 2018. – С. 21-36.

МАТЕРІАЛИ

VI Міжнародної науково-практичної конференції

“ПЕРСПЕКТИВНІ НАПРЯМИ ЗАХИСТУ ІНФОРМАЦІЇ”

02 – 06 вересня 2020 року

Підписано до друку 24.08.2020.
Формат 60×90/8. Папір офсетний. Гарнітура Times New Roman.
Друк цифровий. Ум. друк. арк. 13,5. Наклад 50 прим.

Надруковано у ФОП Бондаренко М.О.
Свідоцтво про внесення суб’єкта видавничої справи до державного реєстру видавців
ДК № 4684 від 13.02.2014 р.
м. Одеса, вул. В. Арнаутська, 60,
т. +38 0482 35 79 76, info@aprel.od.ua