МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет «Одеська юридична академія»

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ В УМОВАХ ВІЙНИ ТА ГЛОБАЛЬНИХ ВИКЛИКІВ XXI СТОЛІТТЯ: СИНЕРГІЯ НАУКОВИХ, ОСВІТНІХ ТА ТЕХНОЛОГІЧНИХ РІШЕНЬ

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

19 травня 2023 року

У двох томах

Том 1

Видавництво
«Юридика»
2023

УДК 005.332.2(4):316.42(477)"364""20"(062.552)
Є24

Рекомендовано до друку Вченою радою
Національного університету «Одеська юридична академія»
(протокол № 3 від 16.06.2023 р.)

За загальною редакцією **С. В. Ківалова.**

Відповідальний за випуск **М. Р. Аракелян.**
Матеріали видано в авторській редакції.

Є24 **Європейські** орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень : у 2 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 19 травня 2023 р.) / за загальною редакцією С. В. Ківалова. – Одеса : Видавництво «Юридика», 2023. – Т. 1. – 790 с.

ISBN 978-617-8263-39-3

Матеріали Міжнародної науково-практичної конференції «Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень». У першому томі збірника містяться наукові напрацювання вчених, практиків, військовослужбовців у теоретичній та емпіричній площині в умовах повномасштабного військового вторгнення у сферах філософських основ, загальної теорії та історичних досліджень держави і права, актуальних проблем світових соціально-політичних процесів, соціології та психології. Висвітлено питання загроз національній безпеці в їхньому конституційному вимірі, у рамках міжнародного та європейського права, трудового права та права соціального забезпечення, земельного, аграрного та екологічного права, пов'язані з функціонуванням економіки та підприємництва в умовах європейського вибору України. Розглянуто проблеми інформатизації та цифровізації суспільства, захисту інформації та кібербезпеки в умовах військового вторгнення, питання методики викладання іноземних мов, теорії та практики перекладу, проблеми лінгвістики та журналістики.

Збірник розраховано на наукових та науково-педагогічних працівників, здобувачів вищої освіти, практичних працівників у сферах юридичної, економічної, соціологічної, політологічної, психологічної, філологічної наук, журналістики та кібербезпеки тощо.

УДК 005.332.2(4):316.42(477)"364""20"(062.552)

ISBN 978-617-8263-37-9 (у 2 т.)
ISBN 978-617-8263-39-3 (т. 1)

СЕКЦІЯ 13
КІБЕРБЕЗПЕКА ОСОБИ, СУСПІЛЬСТВА ТА ДЕРЖАВИ ЯК ФУНДАМЕНТАЛЬНИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ ОБОРОНОЗДАТНОСТІ УКРАЇНИ

3. How To Perform A Vulnerability Assessment [Електронний ресурс]. – Режим доступу до ресурсу: https://www.intruder.io/guides/vulnerability-assessment-made-simple-a- step-by-step-guide

Ключові слова: Веб-сервер, безпека, заходи, вразливості, оцінка.
Key words: Web server, security, measures, vulnerabilities, assessment.

ЧЕПУРНА ОЛЕНА ЄВГЕНІВНА

Національний університет «Одеська юридична академія», доцент кафедри кібербезпеки, кандидат фізико-математичних наук, доцент

КУЛЕШОВА ЄВГЕНІЯ РОМАНІВНА

Національний університет «Одеська юридична академія», аспірант кафедри кібербезпеки

СУЧАСНІ МАТЕМАТИЧНІ МЕТОДИ ОПТИМІЗАЦІЇ ЗАХОДІВ КІБЕРБЕЗПЕКИ

Сучасний світ можна назвати світом інформаційно-комунікаційних технологій. Кожну долю секунди народжується інформаційна одиниця, здійснюється інформаційний обмін. Глобалізація сучасного світу, розвиток новітніх технологій передачі інформації породжує нові загрози її викрадення, маніпуляцій та порушень. Впровадження ефективних заходів кібербезпеки є серйозним викликом для фахівців, зважаючи на те, що кількість і технічний рівень приладів зростає, а рівень кіберзлочинів і кіберзлочинців росте з їх розвитком [1].

Згідно з «Глобальним дослідженням інформаційної безпеки», що його провела компанія EY, 55 % організацій не розглядають захист інформації як частину загальної бізнес-стратегії. Водночас 87 % організацій мають обмежений бюджет на забезпечення необхідного рівня кібербезпеки. Однак бюджети на кібербезпеку зростають – великі компанії витрачають на кібербезпеку більше вже в цьому (63 %) і наступних роках (67 %), менші компанії – 50 % і 66 % відповідно [2]. З огляду на нагальні потреби в розвитку ефективних систем захисту інформації як особистої, так і організацій різних форм власності, постає задача застосування осучаснених методів і систем кіберзахисту, та оптимізація вже існуючих.

Підвищення ефективності захисту інформації можливе за наступними напрямками :

– заміна обладнання на більш сучасне;
– оптимізація програмного забезпечення вже існуючого обладнання;
– застосування хмарних технології в обробці і зберіганні інформації;
– застосування математичних методів в різних сферах організації кіберзахисту.

Кожний з напрямків оптимізації систем і заходів захисту заслуговує на окреме дослідження як з точки зору організації (передбачення критичності ризиків, фінансування), так із використання додаткових методів аналізу, математичних зокрема.

Стрімке зростання машинного навчання і штучного інтелекту для боротьби з кібератаками потребує все більшого залучення математичних методів дослідження і моделювання.

Теорія ймовірностей та математична статистика, лінійне та нелінійне програмування, динамічне програмування, диференціальна геометрія і топологія та її спеціальна частина – інформаційна геометрія стають інструментами вдосконалення систем захисту інформації.

Застосування ймовірнісних та статистичних методів в організації кіберзахисту обумовлено в першу чергу тим, що будь яка загроза чи вже здійснене втручання є випадковою величиною, яка розподілена за відповідним законом, має свої характеристики. Будь яке відхилення від характерного розподілу буде свідчити, наприклад, про аномальну активність та потребує уваги. Статистичні дослідження допомагають зробити прогнозування майбутніх втручань, оцінити значущість факторів впливу на інформаційні системи. На основі статистичних досліджень будується ймовірнісна функція оцінки кібернетичної загрози або кібернетичної безпеки, досліджується комплексна модель кіберзагроз й оцінка та прогнозування сценаріїв потенційних вторгнень. Застосовуючи моделі дослідження операцій можливо синтезувати системи захисту інформації з оптимальними характеристиками [3].

Якщо розглядати порушника як антагоніста фахівцю з кіберзахисту, можливо застосування методів теорії ігор, яка моделює поведінку контрагентів, відповідні стратегії та фіксує взаємодію між ними (прості антагоністичні некооперативні ігри з нульовою сумою) [4].

Складність і багатомірність сучасних інформаційних систем та баз даних сприяла розвитку спеціального розділу диференціальної геометрії – інформаційної геометрії, яка народилася з математичної цікавості розгляду параметричного сімейства ймовірнісних розподілів, яке називається статистичною моделлю, як рімановий многовид з тензором Фішера. Інформаційна геометрія вирішує проблеми, використовуючи поняття диференціальної геометрії (наприклад, кривини) з тензорним численням для вивчення проблем класифікації та перевірки гіпотез у статистиці щодо характеру розподілу випадкових величин (кіберінцидентів або кіберзагроз) [5].

Сучасні методи математичного моделювання й аналізу виграють значну роль в оптимізації засобів кіберзахисту та мають достатній науковий потенціал щодо подальших наукових досліджень і практичного застосування.

Список використаних джерел:

1. Дослідження Check Point: кібератаки зросли на 50 % у порівнянні з минулим роком. URL: https://www.bdo.ua/uk-ua/blog-2/consulting/march-2020/cybersecurity- for-ceo

2. Результати Глобального дослідження EY. URL: https://eba.com.ua/rezultaty-globalnogo-doslidzhennya-ey-z-informatsijnoyi-bezpeky-pokazuyut-shho-kiberbezpeka-zalyshayetsya-vazhlyvym-pytannyam-poryadku-dennogo-organizatsij/
3. Моделі та методи кібернетичного захисту інформаційно-комунікаційних систем на основі логіко-ймовірнісного підходу / О. М. Новіков, А. М. Родіонов, А. О. Тимошенко. – Київ : НТУУ «КПІ» Вид-во «Політехника», 2015. – 276 с.
4. Fighting Cyber Attacks with Game Theory. URL: https://www.sciencedirect. com/science/article/abs/pii/B9780128205433000134?via%3DihubShun-ichiA mari
5. Information Geometry and Its Applications. Applied Mathematical Sciences, Springer, 2016.

Ключові слова: кібербезпека, теорія ймовірностей, математичне моделювання, інформаційна геометрія.

Key words: cyber security, probability theory, mathematical modeling, information geometry.

БАЛАНДІНА НАТАЛІЯ МИКОЛАЇВНА

Національний університет «Одеська юридична академія», старший викладач кафедри кібербезпеки

АЛГЕБРАЇЧНА НЕЛІНІЙНІСТЬ S-БЛОКІВ КОНСТРУКЦІЇ НІБЕРГ ПРИ ЇХ ПРЕДСТАВЛЕННІ ФУНКЦІЯМИ БАГАТОЗНАЧНОЇ ЛОГІКИ

Криптографічний S-блок є основним компонентом сучасних шифрів, який визначає їх ефективність. На сьогоднішній день в літературі відомо чимало методів синтезу S-блоків, які відповідають критеріям криптографічної якості. При цьому серед основних критеріїв криптографічної якості дослідники виділяють алгебраїчну нелінійність, відстань нелінійності, критерій розповсюдження помилки і критерій кореляційного імунітету. Зважаючи на останні наукові дослідження, зазначені критерії криптографічної якості мають застосовуватися не тільки до компонентних булевих функцій S-блоків [1], але і до їх компонентних функцій багатозначної логіки [2].

На сьогоднішній день, однією з найбільш затребуваних та застосовуваних конструкцій побудови S-блоків є конструкція Ніберг [3], що пропонує побудову елементів S-блока за допомогою мультиплікативного обернення над розширеним полем Галуа.

Дослідженню відповідності S-блоків конструкції Ніберг критеріям криптографічної якості як при її представленні булевими функціями, так і функціями багатозначної логіки присвячено чимало досліджень, наприклад [4, 5]. Тим не менш, алгебраїчна нелінійність S-блоків конструкції Ніберг при їх можливому представленні 4-функціями та 16-функціями лишається недослідженою.