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)

© Національний університет
«Одеська юридична академія», 2023

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

ЩЕРБИНА ЮРІЙ ВОЛОДИМИРОВИЧ

Національний університет «Одеська юридична академія», доцент кафедри інформаційних технологій, кандидат технічних наук, доцент

КАЗАКОВА НАДІЯ ФЕЛІКСІВНА

Національний університет «Одеська юридична академія», професор кафедри кібербезпеки, доктор технічних наук, професор

ПРОБЛЕМИ ЗАХИСТУ ВЕЛИКИХ ДАНИХ

Сучасні новітні технології роботи з великими даними широко використовуються у бізнес-процесах та управлінні складними системами. Під терміном «великі дані» розуміються інформаційні ресурси, які відрізняються великими об'ємами та швидкістю їх накопичення і оброблення. Зазвичай для роботи з ними власних ресурсів обчислювальної системи суб'єктам управління не вистачає і виникає необхідність користуватись ресурсами хмарних технологій [1].

Оскільки робота з великими даними, що являють собою великі структуровані або неструктуровані масиви інформації, вимагає використання програмного забезпечення, в якому реалізовані складні технології прогнозування, статистичного аналізу та підтримки прийняття рішень, виникають дві великі проблеми. Перша – це створення математичної теорії організації великих даних і, друга – організація захисту розподілених у просторі інформаційних процесів. Математичної теорії великих даних поки що не снує, не існує, навіть, узгодженого наукового визначення терміну «великі дані». Що ж стосується проблеми захисту інформаційних потоків, обумовлених обчислювальними процесами, пов'язаними з обробленням даних такого типу, то тут треба брати до уваги появу нових типів інформаційних загроз. Із цього витікає, що пошук наукових підходів до захисту технологій, орієнтованих на роботу з великими даними є актуальною науковою проблемою.

Формально, загальна теорія захисту інформаційних технологій була визначена у стандарті ISO-IEC 15408 «Критерії оцінки безпеки інформаційних технологій», виданому у грудні 1999 року [2-4].

Через відсутність сталого наукового обґрунтування проблем, пов'язаних з великими даними, розробники програмного забезпечення шукають рішення проблеми їх захисту в окремих обмежених предметних областях. Зважаючи на те, що захист даних – це область, яка важко піддається формалізації, єдиний, спосіб регулювання відносин між розробниками і замовниками захищених інформаційних технологій – це, створення відповідних стандартів. Суттєвий вклад в цю роботу внесли група WG9 під егідою комітету ISOJTC 1 і Big Data Working group від об'єднання Cloud Security Alliance. У США цією проблемою займається робоча група NIST Big Data (NBD-PWG). Міжнародна організація по стандартизації та Міжнародна електротехнічна комісія

(ISO/IEC) разом з Британським інститутом стандартів (BSI) також приєднались до цієї роботи.

На даний момент, результати сумісних зусиль всіх учасників цієї роботи викладені у таких документах NIST, як Визначення (Definitions) [5], Таксономія (Taxonomies) [6], Варіанти та вимоги (Use Cases and Requirements) [7], Безпека та конфіденційність (Security and Privacy) [8], Архітектура і документація (Architecture White Paper Survey) [9], Концептуальна модель архітектури (Reference Architecture) [10], Стандартна дорожня карта (Standards Roadmap) [11].

Згідно з концептуальною еталонною моделлю (NIST Big Data Reference Architecture) [12], архітектура захисту – це абстракція високого рівню, що розподілена на п'ять логічних функціональних компонентів, пов'язаних між собою відповідними інтерфейсами.

За визначення та інтеграцію дій по введенню даних у систему, відповідає головний компонент архітектури Big Data – системний менеджер (System Orchestrator – SO). Він виконує роль регулятора, який забезпечує контроль вимог і обмежень щодо дій з великими даними.

Контроль поповнення системи Big Data від джерел інформації через набір відповідних інтерфейсів новими даними виконує провайдер даних (Data Provider – DP).

Забезпечення виконання програмними продуктами певного набору сервісів оброблення інформації, що відповідають вимогам SO, здійснює розробник і постачальник системи (Big Data Application Provider – BDAP). Він повинен реалізувати інкапсуляцію бізнес-логіки і функціональних можливостей архітектури Big Data.

Структура, що реалізує логіку великих даних і підтримує захист даних називається постачальником інфраструктури великих даних (Big Data Framework Provider – BDFP). Вона забезпечує управління інфраструктурою (віртуальною або фізичною), структурою обробки інформації, обробкою даних для підтримки системи Big Data та надає служби для забезпечення зв'язку і управління ресурсами.

Останній компонент системи Big Data, це споживачі даних (Data Consumer – DC). Це кінцеві споживачами або інші системи та надані їм інтерфейси.

У документі NIST Special Publication 1500-4, під назвою "Security and Privacy" [8] визначаються аспекти забезпечення захисту і конфіденційності та надається класифікація основних напрямів захисту. Відповідальність за безпеку покладається на структуроване середовище захисту Security and Privacy Fabric, що охоплює усі компоненти архітектури NBDRA.

На даний час, розробники методів та засобів захисту великих даних пропонують варіанти архітектури систем захисту орієнтованих на роботу у конкретних предметних областях. Такі відомі розробники і виробники як Apache Software Foundation, Informatica, HPE, Gemalto, Imperva та інші, пропонують свої унікальні варіанти підходу до автоматизації операцій, пов'язаних з аналізом великих об'ємів інформації як у структурованому, так і у неструктурованому вигляді. Варіативність проєктів реалізації підходів до способів оцінки захисту великих даних

і його організації буде мати місце до тих пір, поки не буде створено науково обґрунтованої концептуальної моделі великих даних як це сталося, наприклад, з моделлю побудови реляційних баз даних.

Можна сподіватись, що досвід, накопичений розробниками і аналітиками робочих груп WG9, NBD-PWG, BSI, ISO/IEC у перспективі приведе до створення науково обґрунтованої моделі даних і стандартів, що визначають усі етапи розроблення і реалізації систем захисту великих даних.

Список використаних джерел:

1. Min Chen, Shiwen Mao, Yin Zhang, Victor C.M. Leung. Big Data Related Technologies, Challenges and Future Prospects. SpringerBriefs in Computer Science. 2014. P. 100.
2. ISO/IEC 15408-1:1999 – Information technology – Security techniques – Evaluation criteria for IT security – Part1: Introduction and general model.
3. ISO/IEC 15408-2:1999 – Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements.
4. ISO/IEC 15408-3:1999 – Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements.
5. NIST Special Publication 1500-1. NIST Big Data Interoperability Framework: Volume 1, Definitions.
6. NIST Special Publication 1500-2. NIST Big Data Interoperability Framework: Volume 2, Big Data Taxonomies.
7. NIST Special Publication 1500-3. NIST Big Data Interoperability Framework: Volume 3, Big Data Cases and General Requirement.
8. NIST Special Publication 1500-4. NIST Big Data Interoperability Framework: Volume 4, Big Data Security and Privacy.
9. NIST Special Publication 1500-5. NIST Big Data Interoperability Framework: Volume 5, Big Data Architectures White Paper Survey.
10. NIST Special Publication 1500-6. NIST Big Data Interoperability Framework: Volume 6, Big Data Reference Architecture.
11. NIST Special Publication 1500-7. NIST Big Data Interoperability Framework: Volume 7, Big Data Standards Roadmap.
12. NIST Special Publication 1500-9. NIST Big Data Interoperability Framework: Volume 8, Big Data Reference Architecture Interfaces.

Ключові слова: великі дані, модель захисту і конфіденційності, таксономія великих даних, провайдери даних, провайдери платформ, інтерфейс взаємодії.

Key words: big data, cyber security, privacy and security model, taxonomy of great data, data providers, platform providers, interfacing.