ударом, як тільки буде запущений ефективний квантовий комп'ютер. Таким чином потрібна розробка нових квантово-криптографічних методів захисту інформації.

Інша загроза, якої можна уникнути, впроваджуючи квантово-криптографічні методи захисту інформації, це можливість переорієнтації великих обчислювальних потужностей, які вже обслуговують майнінг криптовалют, на переборні методи злому асиметричних (класичних) систем шифрування.

Квантові комп'ютери, коли їх можна буде використовувати масово, цілком змінять наш світ і стануть символом прогресу сучасних інформаційних систем.

УДК 343.9:159.9.075

ВОЛОДИМИР МИХАЛОВИЧ СТРУКОВ
кандидат технічних наук, доцент, професор кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ
ДМИТРО ЮРІЙОВИЧ УЗЛОВ
кандидат технічних наук, начальник Управління інформаційно-аналітичної підтримки ГУ НП в Харківській області, полковник поліції
ОЛЕКСІЙ ВЯЧЕСЛАВОВИЧ ВЛАСОВ
заступник начальника Управління інформаційного-аналітичної підтримки ГУНП в Харківській області, підполковник поліції

ПРОБЛЕМИ І ПЕРСПЕКТИВИ РОЗВИТКУ ТЕХНОЛОГІЙ ОБРОБКИ ДАНИХ В ПРАВООХОРОННІЙ СФЕРІ УКРАЇНИ

Дослідження, які щорічно проводяться в сфері обробки інформації, свідчать про те, що з моменту появи глобальних комп'ютерних мереж і, зокрема, Інтернету, лавиноподібне наростання кількості згенерованих і загальнодоступних даних є стійкою характерною тенденцією.

До 2020 р. прогнозується збільшення обсягу згенерованих доступних даних до 40 зеттабайт. (Якщо записати 40 зеттабайт даних на диски Blu-ray, загальна вага дисків (без паперової та пластикової упаковки) буде дорівнювати вазі 424 авіаносців.) Одним з основних чинників цього зростання є збільшення частки автоматично генеруємих даних: з 11% від загального обсягу у 2005 р. до понад 40% у 2020 р.

З усього океану інформації за оцінками фахівців менш 1% піддається аналізу. Разом з тим, реєстрація та зберігання інформації має сенс (тобто вона корисна) лише в тому випадку, якщо вона затребувана, тобто якимось чином обробляється. А на сьогоднішній день навіть сама елементарна обробка, така як простий перегляд, при величезному обсязі інформації людиною просто фізично неможлива.

Такий стан можна спостерігати і в правоохоронній сфері в Україні. Якщо ще зовсім недавно практичні всі накопичуювані і обробляємі дані

зберігалися в файлах системи «Інформаційний портал Національної поліції України» (ІП НПУ) в регламентованій строго структурованій формі, то зараз з інтенсивним впровадженням систем відеофіксації - це потокові відеодані, які в них реєструються і обробляються в реальному режимі часу (on-line). Причому кількість таких даних з введенням систем відеофіксації у всіх регіонах буде постійно зростати, і їх кількість у порівнянні зі строго структурованими даними переважатиме.

У свою чергу, інтеграція процесів зберігання і обробки інформації призводить до неефективності традиційних розподілених систем обробки даних і доцільності створення централізованих систем на основі комбінації технологій хмарних обчислень і клієнт-серверної технології і створення ЦОД (центрів обробки даних) на їх основі. Саме в цьому напрямку заплановано подальший розвиток системи інформаційного забезпечення НПУ (за матеріалами квітневого семінару керівників ДОАЗОР і ДІАП 2018 р. в м.Ужгороді).

Всі ці процеси призводять до явища, яке можна назвати як «криза перевиробництва інформації». Суть його полягає в тому, що люди фізично не в змозі засвоїти всю генеруєму все більш швидкими темпами інформацію або навіть усвідомити всі можливості її використання.

Мало того, що ми не встигаємо прочитати опубліковане, так ці дані швидко втрачають свою актуальність, а на їх місце приходять нові дані.

З цього випливає, що людина повинна отримувати тільки потрібну і корисну «вижимку» з усіх даних, що підлягають аналізу, і в тому обсязі, в якому вона здатний її ефективно сприйняти. А весь препроцесінг (попередня обробка) повинен виконувати інтелектуальний робот-парсер. Причому, в ідеалі не тільки препроцессінг, але і прийняття рішень, оскільки часто час, що відводиться на прийняття рішення, обчислюється частками секунди, а людина просто фізично не в змозі це зробити.

Окремим напрямком, який останнім часом дуже інтенсивно розвивається, можна вважати обробку даних, що циркулюють у відкритих мережах. Це своєрідний океан різнотипних, здебільшого неструктурованих даних. З урахуванням вищесказаного про ефективну ручній обробці цієї категорії даних не може бути й мови. І на даний момент в світі вже розроблено кілька систем, які в автоматичному режимі обробляють такі потоки даних, зокрема продукти фірми Palantir.

Таким чином, розвиток подій в сфері обробки даних в останні роки призводить до неминучого висновку про те, що традиційні засоби обробки інформації двохтисячних років, зокрема інформаційно-пошукові системи, до яких належить пошуковик Google, а також ІП НПУ, представляють засоби минулого технологічного покоління. На передній план виходять інструментальні засоби наступного технологічного покоління - епохи четвертої промислової революції, які в своїй основі мають моделі і методи Data Science (Data Mining, Text Mining, Web Mining, Visual Mining) і штучного інтелекту на основі квазі-квантових і квантових обчислень і хмарних технологій.

Другий важливий висновок полягає в тому, що і зараз і в подальшому на інформаційному ринку будуть розвиватися все більш вузькі спеціалізації і відповідні потоки даних, і затребувані вузькі фахівці, які вміють ефективно працювати з ними. І це чудово розуміють керівники силових структур в США, Великобританії, Німеччини.

У розвинених країнах останні роки в розвитку і застосуванні сучасних технологічних інструментів обробки даних в правоохоронних структурах зроблений в буквальному сенсі прорив [1, 2]. Основними передумовами для такого прориву стали наступні фактори:

1) централізована (зверху) стимуляція і мотивація цих процесів на рівні керівництва силових структур;

2) активна співпраця силових структур з провідними науковими структурами (провідними університетами, провідними комерційними фірмами - світовими лідерами в передових сучасних галузях, в першу чергу, в IT-сфері та робототехніки) в найбільш перспективних технологічних напрямках;

3) потужне фінансування перспективних проектів.

Список використаних джерел:

1. Овчинский В. С. Криминология цифрового мира : учеб. Москва. Норма. ИНФРА–М, 2018. 352 с.

2. Gartner: Топ-10 стратегических трендов развития технологий в 2019 году. URL: https://ain.ua/2018/10/26/gartner-top-10-trendov-razvitiya-texnologij/.

УДК 681.3.06

ВЛАДИСЛАВ ВЛАДИСЛАВОВИЧ ГУДІЛІН
курсант 2 курсу факультету №4 Харківського національного університету внутрішніх справ
ВОЛОДИМИР МИХАЙЛОВИЧ СТРУКОВ
кандидат технічних наук, доцент, професор кафедри інформаційних технологій та кібербезпеки факультету №4 Харківського національного університету внутрішніх справ

ПРОБЛЕМИ ЗАХИСТУ ЗАШИФРОВАНИХ ДАНИХ В ЕПОХУ КВАНТОВИХ ТЕХНОЛОГІЙ

На сьогоднішній день більша частина інформації, яка передається по відкритих каналах передачі даних, шифрується з впровадженням криптографічних систем з відкритим ключем. Принцип роботи даних систем полягає у використанні двох ключів. Відкритий ключ кореспондента використовується при шифруванні вихідного повідомлення. Він публікується у відкритому доступі. Закритий або секретний ключ вживають при розшифровці отриманого повідомлення. З кінця 70-х років XX століття найбільш використовуваною системою з відкритим ключем є алгоритм RSA. Стійкість алгоритму RSA ґрунтується на тому, що факторизація великих