Так, наприклад, з початком повномасштабного вторгнення росії, Держспецзв'язком було створено телеграмканал Кібер Армія України [2]. Метою каналу є надання громадянам інформацію про те, як захиститися від кібератак рашистів. Було надано адреси чатботів, наприклад Кіберполіції та інших служб, куди можна повідомити про загрози, а також про важливі застосунки, які можна використовувати для унебезпечення особи. Так, було повідомлено, що за підтримки Служби безпеки України було створено додаток (YouControl: «Ти хто?») для перевірки підозрілих осіб, щоб не потрапити до диверсанта чи на підозрілу людину. Завдяки додатку можна перевірити дійсність фото з паспорта, перебування людини у державному розшуку та іншу інформацію [2].

Отже, проблеми кібербезпеки та кіберзахисту не зводяться до вирішення винятково технічних аспектів функціонування кіберпростору. Необхідно звертати на такі види захисту як правові, технічні, психологічні, інформаційні та організаційні. Особливо відкритим для громадян є питання самозахисту від кіберзлочинів. А отже, є нагальною потреба у формуванні культури кібербезпеки. Зокрема, закладам освіти, перш за все, потрібно переорієнтуватися на обов'язкове формування культури поведінки у кіберпросторі. Адже, соціалізація сучасного індивіда ускладнюється тим, що потрібно засвоювати певні соціальні норми та правила поведінки, цінності віртуального середовища, формування та набуття сталості яких відбувається тут і зараз.

1. Війна в Україні. Пульс кіберзахисту, серпень 2022. URL: https://www.ppl.org.ua/wp-content/uploads/2022/09/1662392024242416.pdf.

2. Кібер Армія України. URL: https://t.me/CyberArmUA.

3. Про основні засади забезпечення кібербезпеки України: Закон України № 2163-VIII від 05.10.2017 р. Відомості Верховної Ради. 2017. № 45. Ст. 403. URL: https://ips.ligazakon.net/document/TM059780.

4. Cavelty M. D. Cyberwar: concept, status quo, and limitations. URL: https://www.academia.edu/1058235/Cyberwar_Concept_Status_Quo_and_Limitations.

УДК 004
DOI: 10.31733/17-03-2023-532-534

Олександр КОСИЧЕНКО
доцент кафедри інформаційних технологій
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

ПРОБЛЕМИ БЕЗПЕКИ, ПОВ'ЯЗАНІ З МЕТАДАНИМИ ДОКУМЕНТІВ

Метадані – це дані про дані, інформація про інформацію. Іншими словами – це інформаційно-технічна інформація, що міститься в документах різних форматів, яку не видно при звичайному використанні. Метадані нерідко поміщаються у документ програмним чи апаратним засобом, з якого документ було створено. Так як цей процес автоматизований, користувач може залишатися необізнаним про наявність таких даних, і не вживати заходів для захисту цієї інформації, що нерідко має особливе значення.

Серед типів документів, що містять метадані – документи MS Office, Adobe PDF, Corel Word Perfect, зображення, створені Corel DRAW, Adobe Photoshop, створені або оброблені різними редакторами растрової графіки GIF і JPEG, аудіофайли MP3, відео файли, веб-сторінки, електронні листи.

Це найбільш поширені формати, які використовуються на різних офісних платформах
у повсякденній діяльності.

Метадані можуть включати ім'я автора документа, організацію, мітку програмного або апаратного засобу, історію модифікацій документа і так далі. В особливо складних випадках (MS Word) це може бути навіть текст, який колись входив у документ, але пізніше віддалений, але зберігається у файлі документа у вигляді метаданих. Метадані можуть також бути присутніми і у вихідному коді прикладних програм у вигляді коментарів

розробників, і у файлах, що виконуються.

Слід зазначити, що більшість користувачів вважають, що перетворення документа з MS Word в формат PDF знищує всі метадані в документі. Це не завжди так, і передбачливий автор документа повинен спочатку видалити метадані зі вихідного документа (для цього існують спеціальні програми), а потім конвертувати його в pdf формат. Подібні проблеми та методи їх вирішення також існують для інших форматів файлів.

Можна відзначити певні приховані уразливості, пов'язані з метаданими, у юридичній діяльності. Наприклад, ризик для адвоката полягає в тому, що, хоч би яким обережним він був, документ, переданий ним кудись в електронному вигляді, може містити метадані, які ворожі інтересам його клієнта або, у гіршому випадку, розкривають секрети або конфіденційну інформацію клієнта. Багато практикуючих у юристи в малих і середніх фірмах взагалі не знають, що таке метадані, або не розуміють можливих потенційних ризиків. У процесі підготовки остаточного документа юрист, який використовує всі інструменти обробки текстів або даних на своєму комп'ютері, проходить кілька етапів, всі вони нібито приховані в документі та невидимі для всіх, окрім самого юриста. Реальність, однак, така, що історія документа вбудована в його файли і фактично доступна для будь-якого, включаючи адвоката протилежної сторони, який отримує документ в електронному вигляді.

Незважаючи на всю свою специфічність, метадані розглядаються судами іноді як докази, в тому числі і при обґрунтуванні позиції у справі. Для цього тільки необхідно мати елементарні технічні навички. Дослідження метаданих також відіграє не останню роль у розслідуваннях випадків порушень авторських прав, виявленні плагіату чи спроб фальсифікації документів. Відомий факт використання EXIF тега як доказ у кримінальній справі.

Характерним прикладом апаратної (і не тільки апаратної) мітки може бути так званий EXIF тег (Exchangeable Image File Format teg). Він є схованою частиною файлу документа. Саме в цій частині містяться метадані. Слово tag перекладається саме як «мітка» або навіть «цінник, етикетка», що міститься у файлі фотографії у форматі JPEG (або в іншому форматі) цифровими камерами. У цих метаданих, серед інших, такі дані як дата, час, режим зйомки кадру та інше. EXIF тег дозволяє зберігати багато корисного: від параметрів зйомки до відомостей про те, в якій програмі і як відредаговано фотокадр з тією чи іншою метою. Інший цікавий приклад апаратного розміщення метаданих – нанесення кольоровими лазерними принтерами мітки на паперовій роздруківці.

Ризики, що виникають у зв'язку із застосуванням метаданих, можна розділити на дві основні групи: використання коду та розкриття значної інформації. Наприклад, метаданими електронної пошти називають характеристики повідомлень, які, не надаючи вмісту повідомлення, визначають адресатів листування та деякі інші обставини цього процесу. Точніше, до метаданих електронної пошти відносять: ім'я відправника, його поштову адресу,
його IP-адресу в Інтернеті, ім'я одержувача, унікальний ідентифікатор повідомлення та пов'язаних з ним повідомлень; дату, час та тимчасову зону відправлення та отримання повідомлення; формати заголовків повідомлення; тему листа; статус повідомлення; запит на підтвердження отримання та відкриття листа. Як видно, збір метаданих поштового сервісу може дати детальну картину діяльності деякого користувача, навіть якщо він шифрує свої повідомлення. При цьому зібрати дані досить просто.

По-перше, тому, що метадані телекомунікаційних сервісів – пошти, мобільного зв'язку, веб-сервісів та інших – законодавством більшості країн або зовсім не захищаються, або захищаються набагато меншою мірою, ніж зміст самих повідомлень сервісу. Тобто в той час, як розкриття вмісту листування в Інтернеті потребує рішення суду, збір метаданих не вважається атакою на інформаційну безпеку і може проводитися безперешкодно.

По-друге, метадані саме електронної пошти легше прив'язати до певного користувача. Метадані електронної пошти зберігаються на комп'ютерах відправника та одержувача (як і самі повідомлення), але що небезпечно для приватності користувачів, ще й у журналах поштових серверів, які передавали ці повідомлення. Метадані користувачів поштового сервісу набагато легше знайти на серверах провайдерів, ніж метадані користувачів веб-сервісу. провайдера готелю, вокзалу або кафе, де вони тимчасово перебувають, або через сервер публічної пошти, такий як Gmail. Користувач отримує пошту також через певний сервер, на якому у нього є обліковий запис. Ця ситуація не схожа на веб-сервіс, де користувач може відвідати будь-який сервер Інтернету, тому знайти сліди

його відвідувань шляхом перевірки серверів практично неможливо, навіть якщо користувач реєструвався на деяких з них.

Цінність метаданих добре розуміють і використовують спецслужби та поліція деяких країн. Такі технології реалізують масовий збір та аналіз метаданих користувачів мобільного зв'язку. При цьому закони, що охороняють приватність, забороняють прослуховування телефонних розмов, але не забороняють збирати метадані клієнтів мобільного зв'язку.

Слід зазначити, що взагалі загрози та вразливості в обробці метаданих ще недостатньо досліджені фахівцями з кібербезпеки. Із загальним гігантським зростанням обсягів інформації метадані набувають все більшого поширення як засіб індексування даних (спосіб прискорення пошуку інформації в інформаційних системах). Як наслідок, виникають і нові (або будуть виявлені вже існуючі), уразливості, розробляються нові методології впровадження коду.

До іншої групи ризиків відноситься розкриття інформації, що міститься серед метаданих. Це може бути конфіденційна, або яка стосується комерційної таємниці інформація, адреси електронної пошти, шляхи до файлів на системі, на якій було створено або оброблено документ, інша інформація про автора та його програмне та апаратне забезпечення.

Витік інформації через метадані в документах MS Office дав основу деяким інцидентам, які набули міжнародного розголосу. В одному випадку це був документ, підписаний прем'єр-міністром однієї з країн, що стосувався міжнародної ситуації. Дослідження файлу показало віддалений із нього текст, що містив інформацію, не призначену для відкритого доступу. Інший випадок доповнив собою велику літопис позову однієї з фірм до багатьох інших компаній. Аналіз позовної заяви, складеної юридичною компанією, що представляє інтереси фірми, показав, що з тексту видалено назву одного з великих банків – отже, банк був однією з мішеней позову, але з якихось причин юристи фірми утрималися від пред'явлення претензій до банку. Для обізнаної та зацікавленої людини це – важлива інформація.

Висновок зі сказаного вище простий – використанню та захисту метаданих слід приділяти більше уваги у всіх видах діяльності, де використовуються документи, що містять важливу інформацію. При цьому слід зазначити, що взагалі захисту метаданих немає. Шифрування не допомагає їх приховати. Існують методи, що дозволяють видаляти метадані документів перед їх використанням або надсиланням. На жаль, як в юридичній, так і в діловій практиці цьому не завжди приділяється увага, що призводить до різних проблем. Аналіз метаданих став повсякденною практикою для юристів розвинутих країн. На жаль, у питаннях безпеки метаданих в Україні поки що залишається в кращому разі відкритим, швидше – ще не поставленим належним чином. Можливо, у майбутньому законодавство в галузі захисту особистих даних буде суворішим, і метадані як і персональні дані стануть більш захищеними у правовому відношенні.

_____-

1. Baca M. Introduction to Metadata (3rd edition). URL: https://www.getty.edu/publications/intrometadata/
2. Is Metadata a Threat to Your Online Security? URL: https://fastestvpn.com/blog/is-metadata-a-threat-to-your-online-security.
3. Are Your Documents Leaking Sensitive Information? Scrub Your Metadata! Authors: Michael Spiegel. URL: https://er.educause.edu/blogs/2017/1/are-your-documents-leaking-sensitive- information-scrub-your-metadata.
4. Kosychenko O., Rybalchenko L. Peculiarities of using visual means of information and analytical acticiti in legal and law enforcement sphere. Philosophy, Economics and Law Review. 2022. Vol. 2 (1). Pp. 162-169.
5. Rybalchenko L. V., Kosychenko O. O., Klinitskyi I. I. Ensuring economic security of enterprises taking into account the peculiarities of information security. Philosophy, Economics and Law Review. 2022. Vol. 2 (1). Pp. 96-102.