ДИГИТАЛИЗАЦИЯ НА КУЛТУРНОТО НАСЛЕДСТВО КАТО ЧАСТ ОТ СИСТЕМАТА ЗА КИБЕРСИГУРНОСТ

Проф. д.н. Мария Нейкова [*]

Резюме: *Дигитализацията на културното наследство (КН) традиционно се разглежда като технологичен и културно-политически процес, избор на обекти, заснемане/сканиране, описание с метаданни, съхранение и предоставяне на достъп. В съвременната среда, дигитализацията се превръща и в елемент от системата за киберсигурност и киберустойчивост на институциите, които управляват културни ценности (музеи, библиотеки, архиви, научни и административни звена). Причината е двупосочна – цифровите копия и свързаните с тях метаданни са високостойностни информационни активи, изложени на киберрискове, а освен това самият процес на дигитализация въвежда зависимости по веригата на доставки.*

Дигитализацията на културното наследство следва да се проектира и управлява като „сигурна цифрова верига на съхранение и достоверност" – от първичната дигитална фиксация (сканиране/снимка/3D модел) до дългосрочното архивно съхранение и публичното предоставяне.

Научната и практическата значимост на статията е в това, че предлага операционализиран мост между културно-наследствената дигитализация и киберсигурността, където дигиталните колекции се третират като критични активи, а киберконтролите се подбират не абстрактно, а спрямо жизнения цикъл на дигиталния обект и нормативните ограничения.

Изводът който се формулира е, че институциите следва да преминат към „дигитализация като непрекъсваем, сигурен и правно съобразен процес", където доказаната автентичност и устойчивата наличност са равностойни на публичния достъп.

Ключови думи: *Дигитализация; културно наследство; киберсигурност; отворени данни; цифрово съхранение.*

DIGITISATION OF CULTURAL HERITAGE AS PART OF THE CYBERSECURITY SYSTEM

Prof. D.Sc. Maria Neykova, PhD [*]

Abstract: *The digitisation of cultural heritage has traditionally been viewed as a technological and cultural-policy process involving the selection of objects, photographing/scanning, description through metadata, storage, and the provision of access. In today's environment, however, digitisation is also becoming an element of the cybersecurity and cyber-resilience system of institutions that manage cultural assets (museums, libraries, archives, research units, and administrative bodies).*

[*] Проф. д.н. Мария Нейкова, Бургаски свободен университет.
[*] Prof. D.Sc. Maria Neykova, PhD, Burgas Free University

The reason is twofold: digital copies and their associated metadata are high-value information assets exposed to cyber risks, and, in addition, the digitisation process itself introduces dependencies along the supply chain.
The digitisation of cultural heritage should be designed and managed as a „secure digital chain of custody and trustworthiness" – from the initial digital capture (scan/photograph/3D model) to long-term archival preservation and public access.
The scientific and practical significance of the article lies in the fact that it offers an operationalised bridge between cultural-heritage digitisation and cybersecurity, where digital collections are treated as critical assets and cybersecurity controls are selected not abstractly, but in accordance with the lifecycle of the digital object and the applicable regulatory constraints.
The conclusion is that institutions should move toward „digitisation as a continuous, secure, and legally compliant process", in which proven authenticity and resilient availability are on a par with public access.

Key words: *Digitisation; cultural heritage; cybersecurity; open data; digital preservation.*

Дигитализацията на културното наследство се ускорява под натиска на фактори като обществена потребност от достъп, научни и образователни нужди, и европейски политики за мащабно цифрово представяне. Европейската комисия, със своя Препоръка (ЕС) 2021/1970 очертава рамка към общо европейско пространство за данни за културното наследство, а инициативи като „Twin it!" конкретизират амбиции за 3D дигитализация на обекти „в риск" и значима част от най-посещаваните обекти до 2030 г.

Едновременно с това киберзаплахите срещу публични институции и хранилища на данни нарастват, а регулаторният натиск в ЕС се усилва, във връзка с което е необходимо да се установи обща рамка за високо ниво на киберсигурност, която да задължава организациите в определени сектори да въвеждат мерки за управление на риска и докладване на инциденти.

В България, приложимостта на сега действащия Закон за киберсигурност и подзаконови нормативни актове свързани с прилагането му, въвеждат нормативна рамка за минимални изисквания към мрежовата и информационна сигурност, приложими за административни органи и други субекти. Това поражда основен въпрос, с научно-приложен характер, а именно: как да се проектира дигитализацията на културното наследство така, че едновременно да гарантира автентичност, дългосрочна съхранимост и законен достъп, при измеримо управление на киберриска?

В условията на дигитална трансформация, културното наследство следва да се разглежда не само като материален/нематериален обект на опазване, но и като информационен актив, т.е. ресурс, който носи измерима стойност, подлежи на управление, има жизнен цикъл, рисков профил и изисква прилагане на контролни механизми. Това се основава на две утвърдени линии на научна обосновка. Първата е свързана с управлението на риска и информационната сигурност, а втората поставя акцент върху цифровото съхранение.

При гарантиране на информационна сигурност и при управление на риска, активите (вкл. информацията) се управляват чрез риск-базиран подход, като по този начин се цели да се запазят ключовите свойства на информацията (поверителност, цялостност, наличност) в рамките на система за управление на сигурността.

При цифрово съхранение (дигитална консервация), дългосрочното запазване изисква институционална отговорност, контролирани процеси и гарантиране на смисловата интерпретация на цифровите обекти за определена общност потребители.

Към класическите свойства на сигурността, при културното наследство се добавят две „наследствени“ характеристики с критична важност, а именно:

1) автентичност/достоверност (възможност да се докаже, че цифровият обект е „това, което твърди“, и че промените са контролирани); и
2) произход и контекст (кой, кога, как и защо е създал/модифицирал цифровия обект и метаданните).

Когато културното наследство се третира като информационен актив, заплахите се формулират по активи и свойства. Те могат да се изразят в:

а) Заплахи за наличността, включват саботаж или разрушаване на хранилища.
б) Заплахи за цялостта и автентичността подмяна на файлове, манипулация на метаданни, неоторизирани редакции.
в) Заплахи по веригата на доставки – уязвим софтуер за колекции, външни изпълнители по дигитализация, облачни услуги.
г) Риск от неправомерно разкриване на информация – лични данни в архиви, чувствителни локации/описания, вътрешни данни за сигурност на обекти.

Когато културното наследство се третира като информационен актив, заплахите се описват не като абстрактни „информационни рискове“, а като конкретни въздействия върху определени видове активи и върху техните ключови свойства. Този подход променя начина на анализ по същество. Вместо да се говори общо за „киберзаплахи срещу институцията“, се формулира какво точно трябва да бъде защитено и какво би означавало нарушаване на неговата стойност. В среда на дигитализация културното наследство не е един единствен „файл“, а сложна система от взаимно зависими информационни компоненти, които заедно създават научната и обществената му значимост. Дигиталният обект е само видимата част; към него принадлежат описателните, техническите, административните и правните метаданни, които определят смисъла, контекста и режима на използване; принадлежат и доказателствените следи за произход и история на измененията, чрез които се гарантира достоверността; принадлежат и платформите, в които тези данни се съхраняват, обработват и предоставят; принадлежат и идентичностите, ролите и процесите, чрез които хора и системи създават, редактират и публикуват съдържанието. Поради тази многослойност, една атака може да не унищожи никакви файлове и въпреки това да компрометира културната стойност на колекцията, ако подмени контекста, произхода или правния статус на материалите.

Свойствата, които определят сигурността на културното наследство като информационен актив, надхвърлят класическото разбиране за опазване на поверителност, цялост и наличност. За културното наследство особено важно значение имат още автентичността и доказуемостта. Това на практика включва възможността да се установи, че даден дигитален обект и неговите метаданни са именно „официалната“ версия, съответстваща на институционалния запис и на методиката на дигитализацията, както и възможността да се докаже как се е стигнало до конкретната форма на цифровото представяне. Не по-малко важна е интерпретируемостта във времето. Дигиталният обект трябва да остане четим и разбираем в дългосрочен план, което изисква контрол върху формати, технически параметри и придружаваща информация за представяне. В този смисъл заплаха за културното наследство може да бъде както злонамерена ата-

ка, така и процесна или технологична деградация, която прави обекта неизползваем или подвеждащ за научна работа, реставрационни решения или публично представяне.

Формулирането на заплахи по активи и свойства позволява ясно разграничаване между различни типове сценарии и техния реален ефект. При дигиталните обекти с най-висока стойност, като архивните „мастер“ изображения, триизмерните модели или суровите записи, най-тежките сценарии включват загуба на наличност поради криптиране или унищожение на хранилища, което може да прекъсне работата на институцията и да постави под въпрос възможността за възстановяване на данните. Но също толкова критичен е сценарият на „тиха“ подмяна или незабележима модификация, при която файловете остават налични, но съдържанието им вече не отразява оригиналното заснемане или е променено така, че да влияе върху интерпретацията на обекта. При културното наследство подобна компрометация не е просто технически инцидент, а посегателство върху доказателствената стойност: научни анализи, атрибуции, експертни становища и публични наративи могат да стъпят на данни, които изглеждат „истински“, но вече не са надеждни. Отделно от това, ако процесът на обработка и конвертиране не е строго контролиран, може да настъпи качествена загуба чрез неправилна компресия, промяна на цветови профили или некоректни трансформации на триизмерна геометрия, която да намали измервателната и изследователската стойност на резултата. Тук рискът е специфичен – не става дума само за това дали има ли файл, а за това „дали има файл с достатъчна точност и доказуем произход“.

Метаданните са особено чувствителен обект на заплахи, защото те са носителят на смисъл, контекст и управленски решения. Подмяната на авторство, датировка, място на произход, материал или културна принадлежност може да промени научната интерпретация и да създаде дезинформация с висока степен на правдоподобност. Подмяната на правни метаданни, например обозначаване на произведение като свободно за повторна употреба, когато то не е, създава пряк правен риск и може да доведе до нарушения и санкции, докато обратната подмяна може неоправдано да ограничи публичния достъп и да блокира научна и образователна употреба. Понякога метаданните съдържат и чувствителна информация, която не е предназначена за публичност, като вътрешни бележки, координати на уязвими археологически локации, данни за дарители или сведения, които могат да идентифицират физически лица. В тези случаи заплахата за поверителност се превръща в заплаха и за физическата сигурност на обекти и места, както и за репутацията на институцията и правното ѝ съответствие. Особено проблематични са масовите промени в метаданни чрез компрометиран профил на служител или външен изпълнител, защото резултатът може да изглежда като „легитимна редакция“, ако липсват надеждни следи за проверка, одобрение и връщане към предходни версии.

Критичен слой, който често остава подценен, е слоят на произхода и доказателствените записи за историята на измененията. Ако една атака успее да изтрие или подмени журналите на действията, историята на версиите или фиксираните отпечатъци за цялост, институцията може да загуби способността да установи какво е оригиналното състояние на цифровия обект и кога е настъпила промяна. Това е съществено, защото при културното наследство доверието в цифровия обект се гради не само на текущото му съдържание, а и на възможността то да бъде проследено до конкретна процедура, оператор, устройство и момент на дигитализация. Без този доказателствен механизъм цифровото наследство става уязвимо към оспорване и към невидима манипулация, която може да бъде открита твърде късно или изобщо да не бъде открита. Дори когато файловете са налични, разрушаването на доказателствената рамка обезсмисля част от научната им употреба, защото се губи гаранцията за достоверност.

Платформите и услугите за съхранение и достъп добавят още една група рискове, които имат директно отражение върху общественото доверие. Компрометирането на публичен портал може да доведе до подмяна на страници, разпространение на фалшиво съдържание или злоупотреба с функционалности за извличане на данни, а прекъсването на услугата може да блокира достъпа в ключови моменти, когато институцията има висока видимост. Особено опасно е, когато публичната платформа и архивното хранилище не са ясно разделени, защото пробив през публичния интерфейс може да прерасне в достъп до архивното ядро. При културното наследство това означава, че рискът не е само „да падне сайтът“, а да се достигне до мастър колекциите и да се наруши тяхната цялост или да се ексфилтрира непубликувано съдържание. С нарастването на интеграциите чрез програмни интерфейси и автоматизирани потоци на данни се увеличава и възможността за злоупотреби, ако няма строг контрол на удостоверяването, разрешенията и мониторинга на необичайни заявки.

Идентичностите, ролите и процесите свързват всички слоеве, поради което заплахите към тях са „множител на риска“. Когато бъде компрометиран администраторски или кураторски профил чрез фишинг, повторно използване на пароли или неправилно управление на достъпа, атакуващият получава възможност да извършва действия, които изглеждат напълно легитимни. В резултат могат да настъпят едновременно загуба на наличност чрез изтриване или криптиране, загуба на цялост чрез редакция на файлове и метаданни, загуба на автентичност чрез подмяна на официални версии, както и загуба на доказуемост чрез изтриване на журнални следи. Допълнителен фактор е зависимостта от външни изпълнители, доставчици на софтуер и облачни услуги, които разширяват границите на доверие и въвеждат риск по веригата на доставки. В този контекст заплахите трябва да се оценяват не само през „какво може да направи външен нападател“, но и през „какво може да се случи при грешка, пропуск или компрометиране на партньор“, защото културните институции често имат ограничени ресурси и силно разчитат на външна експертиза.

Най-съществения извод от формулирането на заплахите по активи и свойства е, че мерките за защита трябва да бъдат съобразени с това, което прави културното наследство уникално като информационен актив – ценността му се намира в достоверното съдържание, в контекста и в доказуемия произход, а не само в техническата наличност на някакъв цифров файл. Поради това, „успешна“ защита не означава единствено да се предотврати неоторизиран достъп или да се възстанови услуга след прекъсване, а да се гарантира, че цифровите представяния остават проверими, неизменени без надлежно документирана причина, интерпретируеми в дългосрочен план и предоставяни в съответствие с правните ограничения. Именно тази прецизна връзка между актив, свойство и сценарий прави управлението на риска приложимо и научно валидно в сферата на дигиталното културно наследство, защото превежда киберсигурността от обща техническа тема в дейност, която защитава научната, обществената и правната стойност на културните данни.

Библиография:

1. Nguyen, C. D. Digital preservation and cybersecurity: could digital preservation practices help mitigate cyberattacks? // Insights. 2024, т. 37, статия 7. DOI: 10.1629/uksg.650.
2. Vuković, M.; Štefanac, D. Digital Cultural Heritage, Cybersecurity, and the Human Factor. // Preservation, Digital Technology & Culture. 2023, т. 52, бр. 4, с. 129–141. DOI: 10.1515/pdtc-2023-0040.

3. Bolatov, B.; Aitymbetov, N.; Ospanova, R.; Shakimova, G. Cybersecurity of digital museum applications. // Procedia Computer Science. 2024, т. 241, с. 482–487. DOI: 10.1016/j.procs.2024.08.068.
4. Deliversky, Jordan., Rule of Law mechanism and fight against corruption; in Knowledge Society and 21st Century Humanism, The 20th International Scientific Conference Sofia, 1st November 2022, „Za bukvite – o-pismeneh“, Sofia, 2022, pp. 389–402. ISSN 2683-0094.
5. Todorov, T.; Lutfiu, S. Cyber Risk Assessment Principles for Modern Digital Museums. // Digital Presentation and Preservation of Cultural and Scientific Heritage. 2022, т. 12, с. 235–242. DOI: 10.55630/dipp.2022.12.20.
6. Simeonova, N.; Belovski, I.; Torlakov, G. Preservation and Protection of Cultural Heritage through Digital Security System. // Digital Presentation and Preservation of Cultural and Scientific Heritage. 2019, т. 9, с. 353–358. DOI: 10.55630/ dipp.2019.9.38.
7. Pennock, M. Disentangling Digital Preservation Risk: A Risk-driven Approach to Digital Preservation. Дисертация (PhD). University of Cambridge, 2024.
8. National Institute of Standards and Technology. Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53, Revision 5. Gaithersburg, MD: NIST, 2020
9. International Organization for Standardization; International electrotechnical commission. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls. Geneva: ISO, 2022.
10. International Organization for Standardization; International electrotechnical commission. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection – Guidance on managing information security risks. Geneva: ISO, 2022.
11. Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 година относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (Директива МИС 2, *ОВ L 333, 27.12.2022 г., стр. 80–152*
12. Деливерски, Й., Държавната политика при финансирането на културните институции, „Информационни технологии в образователния процес“, За буквите – О писменехь, 2025, София, с. 137-141, ISBN: 978-619-185-754-8
13. Деливерски, Й., Информационните технологии в помощ на борбата с корупцията – потенциал и предизвикателства, Юридически сборник – 2016, том XX III, стр. 374 – 378, ISSN: 1311-3771
14. Манева, К., Нормативна уредба за действия при бедствия, извънредни ситуации и кризи на регистрирани в република България чуждестранни юридически лица, Сборник с доклади от Научна конференция „Научна конференция „Право, сигурност и културно-историческо наследство“, организирана от БСУ, 28-30 август 2023 г. в Бургас, с. 173-182, ISSN: 1311-3771
15. Манева, К., Човешкият фактор в политиката за сигурност – организационно-културен подход, Сборник от МНК „Съвременни изследвания и технологии за отбраната“, ARTDef 2023. Институт по отбрана „Професор Цветан Лазаров“. София, 2023, с. III-191-III-201. ISSN 2185-2581.