

Vytváření databází digitálních dat

Studijní text

Autor: Bc. Tomáš Černík

Konzultant: Mgr. Zdeněk Hruška

Ostrava 2019



VISK VEŘEJNÉ
INFORMAČNÍ SLUŽBY
KNIHOVEN



Odborná způsobilost	Vytváření databází digitálních dat
Profesní kvalifikace	Samostatný knihovník správce digitální knihovny (kód: 72-018-R)
Kvalifikační úroveň	6
Klíčová slova	Autentizace, autorizace, databáze, data, DBMS, metadata, indexy, popisná metadata, administrativní metadata, strukturální metadata, dlouhodobá ochrana digitálních dokumentů, ochrana bitů, logická ochrana, OAIS, digitalizace, hybridní technologie, Systém Kramerius, JPEG 2000, XML, CMS, Google Analytics
Anotace	Tento studijní text je určen pro zájemce o vytváření a zabezpečení digitálních dat. Provede čtenáře od návrhu struktury databáze až k zabezpečení dané databáze, dále její prezentaci v digitálních knihovnických systémech, jejich dlouhodobé ochrany a také k možnosti statistického sledování digitálních dat

Tvorba studijních textů je realizována za finanční podpory Ministerstva kultury České republiky v rámci projektu Veřejné informační služby knihoven (VISK 1).

Zkouška z odborné způsobilosti **Vytváření databází digitálních dat** má 5 částí, zkoušený musí splnit tato kritéria hodnocení:

Kritéria hodnocení	Způsob ověření
a Popsat způsoby zabezpečení přístupu k databázi (autentizace) a jeho význam	Ústní ověření
b Popsat obecně strukturu databáze digitálních dat	Písemné ověření
c Popsat základní funkce jednotlivých typů metadat	Ústní ověření
d Popsat způsoby dlouhodobé ochrany dat	Ústní ověření
e Orientovat se v současných provozovaných systémech pro uchovávání a zpřístupňování digitalizovaných a digitálních dokumentů	Ústní ověření
f Popsat práci s vybraným volným statistickým nástrojem na měření využívání elektronických informačních zdrojů a webových stránek	Ústní ověření

Tento text pro vás připravil Bc. Tomáš Černík, Moravskoslezská vědecká knihovna v Ostravě, cernik@svkos.cz

Text konzultoval Mgr. Zdeněk Hruška, Moravská zemská knihovna v Brně, zdenek.hruska@mzk.cz

OBSAH

RYCHLÝ NÁHLED STUDIJNÍHO TEXTU	5
1 ZABEZPEČENÍ PŘÍSTUPU K DATABÁZI	6
1.1 Základní terminologie.....	6
1.1.1 Základní metody autentizace uživatelů.....	6
1.2 Zabezpečení databáze.....	6
2 STRUKTURA DATABÁZE	8
2.1 Pojmy databáze a data	8
2.2 Struktura databáze – obecně	8
3 METADATA	9
3.1 Metadata v informační vědě a knihovnictví	9
3.2 Metadata v informační vědě a knihovnictví	9
3.2.1 Popisná metadata	9
3.2.2 Administrativní metadata.....	9
3.2.3 Strukturální metadata.....	10
4 ZPŮSOBY DLOUHODOBÉ OCHRANY DAT	11
4.1 Rozdělení ochrany digitálních dokumentů	12
5 SOUČASNÉ SYSTÉMY PRO DIGITALIZACI	13
5.1 Zpřístupňování digitálních dokumentů	13
6 MĚŘENÍ INFORMAČNÍCH ZDROJŮ A WWW STRÁNEK	14
6.1 Co je to Google Analytics	14
6.2 Analýza návštěvnosti	14
6.3 Způsob měření návštěvnosti	15

RYCHLÝ NÁHLED STUDIJNÍHO TEXTU

ÚVOD

Proces vytváření databáze digitálních dat není jednoduchá záležitost, a je spojen s mnoha dílčími kroky, které se tento studijní materiál snaží vysvětlit. K pochopení všech principů při návrhu, tvorbě, zabezpečení a analýze databází je ovšem třeba daleko hlubších znalostí – převážně z oboru informatiky.

PO PROSTUDOVÁNÍ STUDIJNÍHO TEXTU BUDETE UMĚT

- vysvětlit pojmy autentizace, autorizace, zabezpečení přístupu k databázi a jeho význam,
- rozlišit typy zabezpečení databází,
- popsat obecně strukturu databáze digitálních dat,
- orientovat se ve způsobech dlouhodobé ochrany dat,
- orientovat se v současných provozovaných systémech pro uchovávání a zpřístupňování digitalizovaných a digitálních dokumentů,
- popsat práci s vybraným volným statistickým nástrojem na měření využívání elektronických informačních zdrojů a webových stránek.

KLÍČOVÁ SLOVA STUDIJNÍ OPORY

Autentizace, autorizace, databáze, data, DBMS, metadata, indexy, popisná metadata, administrativní metadata, strukturální metadata, dlouhodobá ochrana digitálních dokumentů, ochrana bitů, logická ochrana, OAIS, digitalizace, hybridní technologie, Systém Kramerius, JPEG 2000, XML, CMS, Google Analytics

1 ZABEZPEČENÍ PŘÍSTUPU K DATABÁZI

V této části se po definování základní terminologie seznámíme s nejběžnějšími metodami autentizace uživatelů. Poté navážeme popisem pokročilejších technik a nezbytných mechanismů pro jejich nasazení v praxi.

1.1 Základní terminologie

Autentizace uživatele je proces ověřování identity uživatele. Uživatel obvykle udá svoji identitu (např. přihlašovací jméno) a bezprostředně také nějakým způsobem (viz dále) umožní její ověření. Při autentizaci (neboli **ověřování**) se jedná o proces, při kterém subjekt předkládá tvrzení o své identitě (např. zadáním identifikátoru nebo vložením karty) a na základě takto udané identity se srovnávají aktuální biometrické charakteristiky s uloženými charakteristikami, které této identitě odpovídají podle záznamů autentizační databáze. Odpovídáme na otázku: „Je osoba opravdu tou, za kterou se sama vydává?“

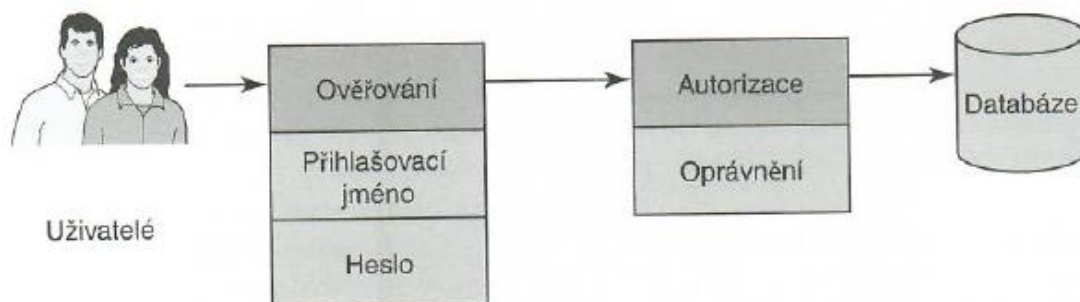
Autorizace uživatele je proces přiřazení oprávnění (na základě identity a bezpečnostní politiky) pro práci v systému a specifikuje, co daný uživatel může, příp. nemůže. Jedná se o proces, který obvykle následuje po autentizaci.

1.1.1 ZÁKLADNÍ METODY AUTENTIZACE UŽIVATELŮ

V principu existují tři základní metody autentizace uživatelů lišící se typem prostředků, které jsou pro autentizaci použity. Metody mohou být založeny buď na něčem, co **daný uživatel zná** (nějaká tajná informace, např. PIN, heslo či přístupová fráze), na něčem, co **daný uživatel má** (nějaký předmět/token jako např. čipová karta), nebo na něčem, čím **daný uživatel je** (nějaká biometrická informace, jako např. otisk prstu).

1.2 Zabezpečení databáze

Zabezpečení databáze má zajistit, aby mohli autorizované operace s databází provádět jen autorizovaní uživatelé a to v autorizovaných částech. Tento cíl se obvykle dělí na dvě části: **ověřování** (autentizace), kdy se kontroluje, zda má uživatel vůbec právo používat systém, a **autorizaci**, která ověřenému uživateli přiřadí konkrétní práva neboli **oprávnění** provádět určité činnosti se systémem. Nejlépe je to patrné z obrázku č. 1.



Obrázek 1 – Zabezpečení databáze pomocí ověřování a autorizace

2 STRUKTURA DATABÁZE

Abychom mohli strukturu databáze pochopit, je třeba si nejprve vysvětlit, co to je databáze.

2.1 Pojmy databáze a data

Databáze je organizovaný soubor strukturovaných informací neboli dat, které se obvykle ukládají v elektronické podobě v počítačovém systému. Databáze je obvykle řízena systémem pro správu databáze (DBMS – database management system). Data a systém DBMS se společně s přidruženými aplikacemi označují jako databázový systém, často zkráceně jako databáze.

Data v nejběžnějších typech současných databází jsou obvykle modelována jako řada tabulek složených z řádků a sloupců, což umožňuje efektivní zpracování a vytváření dotazů. Je tak zajištěn snadný přístup k datům, správa, úpravy, aktualizace, řízení a organizace dat. Většina databází používá k zadávání dat a vytváření dotazů dotazovací jazyk SQL (structured query language).

2.2 Struktura databáze – obecně

Databáze se skládá z **uživatelských dat**. Ta tvoří největší část v databázi.

Data o struktuře databáze se označují jako **metadata**. K příkladům metadat patří názvy tabulek, názvy sloupců a tabulek, do kterých patří, vlastnosti tabulek a sloupců atd.

Jak jsme právě uvedli, databáze obsahuje uživatelská data a metadata. Kromě toho se v databázi nacházejí také **indexy** a jiné struktury, které umožňují zvýšit výkon databáze.

Některé databáze navíc zahrnují **aplikační metadata**. Jedná se o data, která popisují prvky aplikace, jako jsou formuláře a sestavy.

3 METADATA

Metadata jsou podle terminologického slovníku Národní knihovny: "Strukturovaná data, která nesou informace o primárních datech." Slovník dále uvádí, že "termín je používán především v souvislosti s elektronickými zdroji a vztahuje se k datům v nejširším smyslu slova (datové soubory, textové informace, obrazové informace, hudba aj.)". Autoři hesla připomínají, že "metadatové údaje se obvykle vkládají přímo do zdroje (umísťují se např. v záhlaví dokumentu HTML)."

3.1 Metadata v informační vědě a knihovnictví

Termín „metadata“ je spojován v informační vědě zejména s procesy popisování dat a informačních objektů (informačních zdrojů, informačních entit). Problematika metadat hovoří o dalších významných funkcích souvisejících s životním cyklem digitálních nebo digitalizovaných objektů. V souvislosti s těmito funkcemi jsou metadata definována také jako *"strukturované informace, které popisují, osvětlují, lokalizují a různými způsoby usnadňují vyhledávání a využívání informačního zdroje."*

3.2 Metadata v informační vědě a knihovnictví

Hovoří se o základních typech a podtypech metadat:

3.2.1 POPISNÁ METADATA

Popisná metadata reprezentují **vnitřní vlastnosti** informačních objektů (zdrojů) údaji o tvůrci, názvu, vydavateli, roku vydání zdroje, údaji k obsahu zdroje aj. Popisná metadata pomáhají identifikaci zdrojů, odlišují verzi zdroje, usnadňují vyhledávání a výběr. Jsou vytvářeny profesionály v bibliografických databázích, katalozích a při výstavbě digitálních fondů. Vytvářet je mohou i uživatelé při jejich vyhledávání a užívání (folksonomie). K významným metadatovým schémátům popisných metadat patří například schémata Dublin Core, MARCXML, MIX, ALTO, MODS, FOXML, hlavičky TEI, EAD aj.

3.2.2 ADMINISTRATIVNÍ METADATA

Administrativní metadata slouží zejména profesionálům k řízení a správě digitálních objektů v rámci digitálních fondů. Někdy jsou mezi administrativní metadata zařazována také metadata archivační/ochranná, technická a právní. Administrativní metadata pomáhají lokalizovat informační objekty, poskytují časové informace o vzniku a úpravách digitálního objektu, specifikují okolnosti digitalizace. Poskytují informace o vstupu objektu do repozitáře, o elektronickém podpisu, o právních aspektech přístupu k objektu aj.

- **Archivační/ochranná metadata** (angl. Preservation metadata) – podporují procesy ošetřující dlouhodobou archivaci a ochranu digitálních informačních zdrojů. Měla by zajistit trvalou integritu a kontext dokumentu. Obsahují informace o původu a historii objektu, upřesňují jeho vztah k dalším informačním objektům, poskytují údaje o nutném zobrazovacím hardwaru a softwaru. Archivační/ochranná metadata jsou požadována také mezinárodní normou ISO – Referenčním modelem OAIS. Příkladem archivačních/ochranných metadat je například známý standard PREMIS.
- **Technická metadata** – reprezentují technické charakteristiky digitálních (počítačových) souborů (údaj o datovém formátu zdroje, velikosti souboru, komunikačním protokolu, kompresním poměru, kontrolním součtu aj.). Jsou důležitá pro dlouhodobou archivaci a ochranu digitálních objektů. Známým schématem technických metadat je metadatové schéma MIX pro statické digitální obrazy, hlavičky TEI pro textové zdroje aj.
- **Právní metadata a metadata o přístupu** (angl. Rights metadata and Access metadata) – poskytují informace o omezeních vyplývajících z duševního vlastnictví (autorské právo, patentové právo aj.) a případných právních dohodách (licencích), které umožňují uživatelům přístup k informačním objektům (např. oprávnění kopírovat, reprodukovat nebo šířit informační objekt).

3.2.3 STRUKTURÁLNÍ METADATA

Strukturální metadata poskytují **informace o vnitřní organizaci či struktuře digitálního objektu**. Vyjadřují strukturu a také vztahy dílčích digitálních objektů tvořících komplexní digitální informační objekt (např. jednotlivé stránky čísel časopisů daného ročníku). Při zpřístupnění objektu koncovým uživatelům jsou tato metadata nezbytná pro správné zobrazení a navigaci digitálního objektu. Významná jsou i pro dlouhodobou archivaci. Pro strukturální metadata je vhodné využít dílčí část (<structMap>) metadatového standardu METS.

4 ZPŮSOBY DLOUHODOBÉ OCHRANY DAT

Dlouhodobá ochrana digitálních dokumentů (DODD; anglicky *digital preservation*) zahrnuje širokou škálu definic lišících se úhlem pohledu na danou problematiku. Jedna z definic vytvořená H. M. Gladneym říká, že DODD je: „*organizované opatření k zajištění dlouhodobé použitelnosti digitálních objektů; zásadní je, že digitální objekty nebudou nikdy ztraceny nebo poškozeny, jsou důvěryhodné, je možné je vždy najít, rozumět jim, a to i přes problémy zastarávání technologií*”.

Cílem dlouhodobé ochrany digitálních dokumentů neboli dlouhodobé archivace je zajištění trvalé udržitelnosti digitálních dat. Tím se rozumí především trvalý přístup k informacím nezávislý na degradaci nosičů dat a technologických změnách, a udržení jejich srozumitelnosti a využitelnosti. Digitální objekty by měly být chráněny před zničením a ztrátou důvěryhodnosti a to v dlouhodobém horizontu.

Dlouhodobou ochranu je možné rozdělit na tzv. **ochranu bitů** (bit-stream preservation) a **logickou ochranu** (content preservation), která spočívá v uchování informačního obsahu. Digitální objekty jsou uchovávány na nosičích, které podléhají degradaci. Samotná dlouhodobá ochrana tak musí začínat u bitové ochrany, která se nejčastěji realizuje redundantním uložením a řízeným kopírováním na nové nosiče. Součástí logické ochrany jsou procesy, které mají zajistit ochranu obsahu tak, aby význam informací zůstal zachován. Je nutné se vypořádat se zastaráváním softwarových aplikací, které jsou využívány pro zpřístupnění obsahu. Toto je řešeno formátovou migrací či emulací. Opatření digitálních objektů vhodnými metadaty vede k zajištění autenticity a důvěryhodnosti obsahu. Metadata mají popsat obsah, strukturu a kontext informačního objektu.

Aktivita v oblasti dlouhodobé ochrany dat popisuje referenční model **OAIS** (Open Archival Information System), schválený jako mezinárodní norma ISO 14721:2003, resp. v aktualizaci ISO 14721:2012. Podle tohoto modelu by digitální informace udržované v rámci dlouhodobé archivace měly být spravovány tak, aby bylo možné se vypořádat s měnícími se technologiemi a změnami očekávání uživatelské komunity. Jejich správu zajišťuje digitální archiv, ve kterém jsou uloženy. Norma OAIS definuje tento archiv jako organizaci lidí a systémů se závazkem ochraňovat a zpřístupňovat digitální data pro určitou skupinu uživatelů.

4.1 Rozdělení ochrany digitálních dokumentů

Ochrana digitálních dokumentů je možné rozdělit na:

- ochranu dat nyní i v budoucnu neboli **ochranu bit-streamu**,
- ochranu použitelnosti dat v budoucnu, tzv. **ochranu logickou**, která je podstatou dlouhodobé ochrany.

Logická ochrana zahrnuje procesy, které digitálním objektům dávají do budoucna záruku:

- snadné vyhledatelnosti,
- zpřístupnění,
- opakované využitelnosti,
- smysluplnosti,
- autentičnosti.

5 SOUČASNÉ SYSTÉMY PRO DIGITALIZACI

Digitalizace knižních dokumentů může sloužit pro vytváření kopií dokumentů, které nejsou bezprostředně ohroženy degradací papíru, ale které je třeba nahradit v přímých službách uživatelům, nebo v těch případech, kdy není možné dokument v původní podobě bezpečně zpřístupnit (např. v případě map). Spojením mikrofilmu a digitálního záznamu se vytváří tzv. **hybridní technologie** využívající předností obou formátů. Mikrofilm zajišťuje trvalé dochování obsahu dokumentu, digitální záznam jeho snadné zpřístupnění uživatelům. Hybridní technologie je vhodná pro reformátování dokumentů ohrožených degradací s limitovanou životností.

5.1 Zpřístupňování digitálních dokumentů

Nejpoužívanější digitální knihovnou u nás je **Systém Kramerius**. Existuje už řadu let, v současnosti je aktuální verze 5. Přehled všech instalací Krameria nalezneme na <https://registr.digitalniknihovna.cz>. Pro zpřístupňování dokumentů slouží Systém Kramerius obsahující kopie všech obrazových souborů ve formátu JPEG 2000, který má výhodnější kompresní parametry a jehož plug-in je podporováním operačním systémem Windows a metadata ve struktuře založené na XML. Pomocí systému lze provádět jednoduché operace s dokumenty jako spojování, nahrazování, mazání a replikace. Součástí systému jsou i externí moduly pro tvorbu metadat v XML a pro řízenou konverzi jak obrazových souborů, tak metadat.

Systém Kramerius představuje specifický typ CMS (Content Management System), jehož primárním účelem je zpřístupnění archivních a cenných dokumentů široké veřejnosti v souladu s autorským zákonem. V systému sestávajícího z více provázaných aplikací, které tvoří tzv. "výrobní linku" v digitalizaci dokumentů.

Asi největší rozcestník u nás provozovaných digitálních knihoven Kramerius nalezneme na stránce <http://digitalniknihovna.cz/mzk>. Na stránce je možnost přepínat se do ostatních digitálních knihoven u nás.

6 MĚŘENÍ INFORMAČNÍCH ZDROJŮ A WWW STRÁNEK

Jeden z mnoha nejznámějších volně dostupných statistických nástrojů pro měření využívání informačních zdrojů a webových stránek je Google Analytics. V následující kapitole si o něm povíme podrobněji.

6.1 Co je to Google Analytics

Google Analytics (zkráceně GA) je dalším zástupcem rozsáhlé rodiny webových aplikací Google. Jeho prostřednictvím je možné měřit návštěvnost webových stránek a zejména zkoumat trendy v chování návštěvníků na sledovaných webových stránkách. Výsledky těchto výzkumů jsou zajímavé zejména pro provozovatele webových stránek, pro webmastery a pro marketingové pracovníky.

Nezbytnou součástí GA je služba, která zaznamenává a archivuje údaje o přístupech návštěvníků k jednotlivým webovým stránkám. Kvalita a spolehlivost měření se několikaletou praxí osvědčila natolik, že se GA zařadila mezi uznávané nástroje v oblasti měření návštěvnosti.

Google Analytics je bezplatná služba s velkým potenciálem, kterou Google neustále rozvíjí. GA najdeme na <http://www.google.com/analytics/>.

6.2 Analýza návštěvnosti

Cílem analýzy návštěvnosti je získat odpovědi. Analýza návštěvnosti prostřednictvím Google Analytics nám může odpovědět pouze na otázky spjaté se souhrnným chováním návštěvníků našich webových stránek, neumožňuje monitorovat chování konkrétních návštěvníků. Příklad relevantních otázek:

- Kolik návštěvníků navštívilo naše webové stránky minulý týden?
- Jaký je trend v návštěvnosti za poslední měsíc?
- Ve kterém týdnu v roce jsme zobrazili nejvíce stránek?
- Které hypertextové odkazy uživatelé na dané stránce nejčastěji využívají?
- Jaký webový prohlížeč používají naši návštěvníci? Jakou verzi?
- Jaké jsou nejčtenější webové stránky posledního měsíce?
- Kolik návštěvníků se minulý týden zaregistrovalo?
- Na které stránce tráví návštěvníci nejvíce času?
- Kolik % návštěvníků se na naše stránky pravidelně vrací?
- Přes která klíčová slova použitá ve vyhledávači se dostal návštěvník na naši stránku?

GA umožňuje sledovat různé ukazatele související s návštěvníky, s webovými stránkami, s klíčovými slovy apod. Tyto ukazatele postupně v tomto článku představíme.

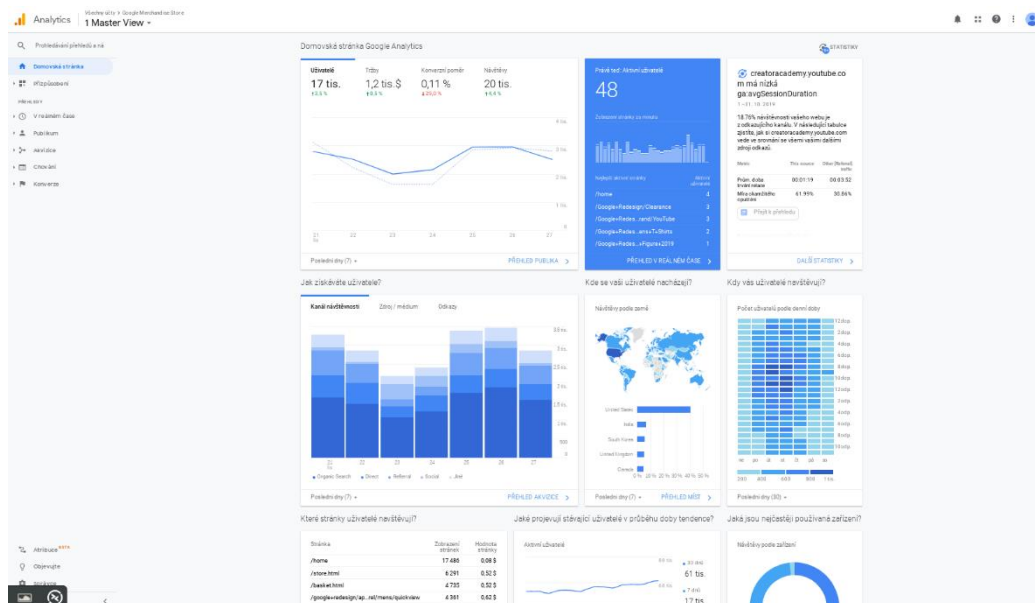
6.3 Způsob měření návštěvnosti

Pokud chcete využívat možnosti, které GA přináší, je potřeba si nechat pro svůj web vygenerovat unikátní měřicí kód a umístit jej do patičky všech stránek, které chcete monitorovat. Po uplynutí několika hodin budete mít k dispozici ve svém účtu první údaje o návštěvnosti.

Měření návštěvnosti je realizováno pomocí kódu Javascriptu využívajícího cookies. Ke korektní inicializaci měřicího kódu GA a zaslání reportu GA serverům ke zpracování je zapotřebí, aby návštěvníci měli v prohlížeči povolen Javascript a cookies.

Jestliže některý z těchto elementů není povolen nebo nefunguje správně, nebude daný návštěvník v GA reportech zaznamenán. Další situací, která způsobuje nepřesnost v GA reportech, je mazání cookies, ať již uživatelem nebo automaticky po vypnutí prohlížeče. V tomto případě bude návštěvník při každé návštěvě stránky identifikován jako nový unikátní návštěvník, a tudíž příslušné reporty nebudou plně relevantní.

Tyto nepřesnosti nikterak nesnižují sílu tohoto nástroje. Znalost, že návštěvnost dané stránky vzrostla o 40 % po spuštění internetové kampaně je podstatnější než informace o tom, že danou stránku navštívilo přesně 120 uživatelů.



Obrázek 3 – Grafické rozhraní Google Analytics

LITERATURA

MATYÁŠ, Vašek; KRHOVJÁK, Jan a kolektiv. *Autorizace elektronických transakcí a autentizace dat i uživatelů* Brno: Masarykova Univerzita, 2008. ISBN 978-80-210-4556-9

KROENKE, M, David; AUER, J, David. *Databáze*. Vyd. 6. Computer Press. ISBN 978-80-251-4352-0

Dvojklik. *5 tipů jak zabezpečit databázi* [online]. [cit. 2019-10-15]. Dostupné z: <https://www.dvojklik.cz/5-tipu-jak-zabezpecit-databazi/>

Computerworld. *Jsou vaše databáze připraveny na aktuální hrozby?* [online]. [cit. 2019-10-15]. Dostupné z: <https://computerworld.cz/securityworld/jsou-vase-databaze-pripraveny-na-aktualni-hrozby-1-52166>

Oracle. *What is databse* [online]. [cit. 2019-10-15]. Dostupné z: <https://www.oracle.com/cz/database/what-is-database.html>

Wikisofia. *Dlouhodobá ochrana digitálních dokumentů* [online]. [cit. 2019-10-15]. Dostupné z: https://wikisofia.cz/wiki/Dlouhodobá_ochrana_digitálních_dokumentů

Wikisofia. *Digitalizace a knihovnictví* [online]. [cit. 2019-10-15]. Dostupné z: https://wikisofia.cz/wiki/Digitalizace_a_knihovnictví/old

Národní knihovna ČR. *Digitalizace a digitální zpřístupnění dokumentů* [online]. [cit. 2019-10-15]. Dostupné z: https://www.nkp.cz/o-knihovne/odborne-cinnosti/sprava-a-ochrana-fondu/zzz_osof/digitalizace

Wikipedia. *Google Analytics* [online]. [cit. 2019-10-15]. Dostupné z: https://cs.wikipedia.org/wiki/Google_Analytics

ÚVT MU zpravodaj. *Nástroje Google* [online]. [cit. 2019-10-15]. Dostupné z: <http://webserver.ics.muni.cz/bulletin/articles/632.html>

Wikisofia. *Metadata* [online]. [cit. 2019-10-15]. Dostupné z: https://wikisofia.cz/wiki/Metadata#cite_note-bratkova2012-7

KVAŠOVÁ Zuzana, SVOBODA Tomáš. *Dlouhodobá ochrana elektronických publikací*, [online]. [cit. 2019-10-15]. Dostupné z: <http://www.phil.muni.cz/journals/index.php/proinflaw/article/view/2013-2-10/908>

Název: Vytváření databází digitálních dat

Autor: Bc. Tomáš Černík

Počet stran: 16