Dokumentace systémů ČRS

Informační rozcestník MoČRS, Sportovní portál ČRS, Fórum ČRS a společná knihovna účtů – celek, moduly, napojení na okolní systémy, bezpečnost a ochrana osobních údajů, rozsah díla.

Autor: **Tomáš Kočica** · Stav k: **14. 11. 2026** · verze č. 16 · vytvořeno 23. 11. 2026 03:18

OBSAH

Část A – Systémy ČRS a jejich vazby

- A1. Přehled systémů
- A2. Společné prvky a vazby
- A3. Společné technologie a provoz

Část B – Informační rozcestník MoČRS

- B1. Účel a rozsah systému
- B2. Architektura a technologie
- B3. Napojení na okolní systémy
- B4. Uživatelé, role a oprávnění
- B5. Moduly a agendy
- B6. Analytické nástroje
- B7. Datový model
- B8. Plánované úlohy a přepočty na pozadí
- B9. Bezpečnost a ochrana osobních údajů
- B10. Provoz, nasazení a údržba
- B11. Rozsah díla
- B12. Stav vývoje a otevřené body

Část C – Sportovní portál ČRS

- C1. Účel a rozsah portálu
- C2. Architektura a technologie
- C3. Napojení na okolní systémy
- C4. Funkční oblasti
- C5. Datový model
- C6. Bezpečnost a ochrana osobních údajů

C7. Provoz, nasazení a údržba
C8. Rozsah díla
C9. Stav vývoje a otevřené body

Část D – Fórum ČRS

D1. Účel a rozsah fóra
D2. Architektura a technologie
D3. Napojení na okolní systémy
D4. Funkční oblasti
D5. Datový model
D6. Bezpečnost
D7. Provoz a nasazení
D8. Rozsah díla

Část E – Společná knihovna účtů ČRS

E1. Účel a rozsah knihovny
E2. Přihlášení účtem RIS
E3. Struktura organizací, funkce a skupiny
E4. E-maily, upozornění a schránka
E5. Datový model
E6. Rozsah díla

Část F – Bezpečnost a ochrana osobních údajů

F1. Šifrovaný přenos a komunikace s okolím
F2. Přihlášení, hesla a relace
F3. Řízení přístupu
F4. Ochrana aplikací
F5. Osobní údaje v systémech
F6. Zásady ochrany osobních údajů
F7. Doporučení a otevřené body
F8. Bezpečnostní revize rozcestníku (listopad 2026)
F9. Penetrační testy a bezpečnostní nástroje (listopad 2026)

Část G – Rozsah díla celkem

G1. Souhrn všech systémů

Dokumentace popisuje tři webové aplikace Českého rybářského svazu, které vyvíjí a provozuje jeden autor a které sdílejí identifikaci osob, přihlašování účtem RIS a vzhled: **Informační rozcestník MoČRS**, **Sportovní portál ČRS** a **Fórum ČRS**, a jejich **společnou knihovnu účtů**. Část A popisuje vazby, části B–D jednotlivé systémy (celek i moduly), část E knihovnu účtů, část F bezpečnost a ochranu osobních údajů v celé rodině systémů a část G souhrnný rozsah díla. Všechny systémy běží na HTTPS. Rozsah kódu a počty tabulek se počítají při zobrazení stránky (stav k 14. 11. 2026).

Část A – Systémy ČRS a jejich vazby

A1. Přehled systémů

Systém	Účel	Uživatelé
Informační rozcestník MoČRS část B	Komunikace mezi Radou, územními svazy a místními organizacemi (aktuality, úkoly, formuláře, dokumenty, helpdesk), agendy (hájení revírů, objednávky, zpráva o činnosti, násady) a analytika nad daty svazu (prodeje z RIS, revíry a úlovky z E-Sumáře, rybářská stráž, členská základna, brigády).	Funkcionáři MO, ÚS a Rady; částečně veřejnost.
Sportovní portál ČRS část C	Prodej a evidence sportovní známky s online platbou Comgate a zápisem uhrazené známky do RIS, doklady, e-průkaz sportovce, veřejné seznamy sportovců, trenérů a rozhodčích a kalendář závodů převzaté z RIS.	Sportovci, rodiče, trenéři, veřejnost; správci sportovního oddělení.
Fórum ČRS část D	Diskuzní fórum podle oblastí (celosvazové, územní svaz, ÚS a Rada) s přístupem podle funkcí v RIS a e-mailovým sledováním.	Funkcionáři s platnou funkcí v RIS.

A2. Společné prvky a vazby

- **Rybářský informační systém (RIS)** je zdrojem osob, funkcí a organizací. Všechny tři systémy přihlašují účtem RIS a žádný si neukládá hesla RIS. Osoba se ve všech systémech identifikuje **eID** z RIS.
- **Společná knihovna účtů** (samostatný repozitář `ucty`, databáze `ucty_1`) – používají ji MoČRS a fórum: přihlášení účtem RIS a uložení uživatele (eID, platné funkce s organizacemi), číselník funkcí a jejich skupiny, log přihlášení po aplikacích, alternativní e-mail a nastavení upozornění, odesílání e-mailů a **společná schránka zpráv** – upozornění z fóra tak uživatel vidí i ve schránce rozcestníku. Sportovní portál ověřuje účet přímo v RIS (profil osoby) a knihovnu účtů zatím nepoužívá. Podrobně v části E.
- **Fórum je součástí rozcestníku** (složka `forum/`, adresa `…/main/forum`): používá jeho session, přihlášení, hlavičku a drobečkovou navigaci. Kdo je v rozcestníku přihlášen účtem RIS, je přihlášen i ve fóru; odhlášení v rozcestníku odhlásí i z fóra. Vlastní databázi fóra (témata, příspěvky) to nemění.
- **Společná relace přihlášení** (knihovna účtů, cookie `crs_ucet`) pro samostatné nástroje na stejném hostiteli (sport): kdo se přihlásí účtem RIS v rozcestníku, je přihlášen i v nich – bez dalšího zadávání hesla. Odhlášení v kterémkoli z nich odhlásí ze všech; relace platí 8 hodin od poslední aktivity a do zavření prohlížeče. Rozcestník relaci zakládá (přihlášení, ověření a připojení účtu RIS) a ruší (odhlášení, přihlášení e-mailem), sám se podle ní zatím nepřihlašuje ani neodhlašuje.
- **Struktura organizací** (Rada → územní svazy → místní organizace) se bere z číselníku organizací E-Sumáře (`keepers`, vazba na RIS přes `ris_sid`); rozcestník a fórum podle ní určují, co kdo vidí.
- **Data sportovního portálu v rozcestníku**: zpráva o činnosti (kap. B5.15) čte **jen ke čtení** databázi sportovního portálu (přístup z jeho `config.php`) a počítá z ní registrované sportovce, trenéry a rozhodčí po odvětvích a letech. Jiná vazba mezi databázemi není; sport do rozcestníku nic nezapisuje.
- **Comgate** – sportovní portál přes něj přijímá platby sportovní známky (identifikace podle IČO pro rozdělovník plateb ČRS), rozcestník importuje denní výpisy převodů plateb ze všech obchodů svazu a rozesílá je organizacím.

- **Společný vzhled** (logo, barvy, písmo, Bootstrap 5) a převzaté postupy – čištění HTML z editoru, editor Quill, tiskové styly.
- Každý systém má vlastní databázi a konfiguraci mimo repozitář; spojení mezi databázemi se neskládají SQL dotazem, ale v PHP.

A3. Společné technologie a provoz

- PHP 8 bez frameworku (stránka = skript, sdílená logika v knihovnách), MySQL / MariaDB s utf8mb4, serverově generované HTML, Bootstrap 5 a Bootstrap Icons, responzivní rozhraní a tiskové výstupy.
- Hostování na běžném PHP webhostingu, plánované úlohy přes cron (z příkazové řádky nebo přes URL s tokenem).
- Zdrojový kód v systému Git (GitHub), konfigurace a nahrané soubory mimo repozitář.

Část B – Informační rozcestník MoČRS

B1. Účel a rozsah systému

Informační rozcestník MoČRS je webová aplikace pro **organizační jednotky Českého rybářského svazu** – Radu ČRS, územní svazy (ÚS) a místní organizace (MO). Slouží jako společné místo pro komunikaci mezi úrovněmi svazu (aktuality, úkoly, formuláře, dokumenty, helpdesk), pro agendy, které v centrálních systémech chybějí (žádosti o hájení revírů, objednávky tiskopisů a zboží, zpráva o činnosti, produkce násad), a hlavně pro **analytiku nad daty svazu** – prodeje členských známek a povolenek z RIS, docházky a úlovky z E-Sumáře, rybářská stráž, členská základna, nastavení brigádnické povinnosti, redistribuce příjmů z celosvazových povolenek.

Rozcestník nevede vlastní registr osob ani organizací. Strom organizací, revíry a úlovková data čte z databáze **E-Sumáře**, osoby a funkce ověřuje přes **Rybářský informační systém (RIS)**, data o prodejích, členech, zarybnění či přestupcích přebírá z exportů sestav RIS (Oracle Analytics). Postupně přechází na **přímé čtení z rozhraní RIS** – už takto načítá kontroly a číselník rybářské stráže, funkcionáře, nastavení brigádnické povinnosti, konfiguraci členských příspěvků a žádosti o storna povolenek.

Uživatelé:

- **veřejnost bez přihlášení** – veřejné aktuality, manuál, veřejný přehled hájených revírů, publikovaná zpráva o činnosti a vybrané statistiky;
- **místní organizace** – plní úkoly a formuláře, rezervují termíny, podávají žádosti o hájení, objednávají, vidí analytiku a data jen za sebe;
- **územní svazy** – zadávají úkoly, formuláře a aktuality svým MO, vyřizují jejich žádosti a objednávky, vidí souhrny za sebe a své MO, importují prodeje;
- **Rada ČRS** – celosvazové zadávání a přehledy, správa celosvazových číselníků a nastavení;
- **správci (role admin)** – správa systému, importy dat, zadání pro AI, dlaždice, nápověda, práva.

B2. Architektura a technologie

Serverová část	PHP 8 bez frameworku – každá stránka je samostatný skript, sdílená logika v knihovnách (`*_lib.php`, `*_common.php`, soubory s podtržítkem v modulech `reviry/` a `zprava2/vypocty/`), PDO s parametrizovanými dotazy, u nových částí strict types. Rozšíření PHP: pdo_mysql, curl, mbstring, iconv, zip, zlib, gd.
Databáze	MySQL / MariaDB, dvě spojení: **lokální databáze** rozcestníku (`$pdo_local` – obsah, importy, předpočítané souhrny) a **databáze E-Sumáře** (`$pdo_ext` – organizace, uživatelé, revíry, povolenky a úlovky; jen čtení). Volitelně databáze historie starého E-Sumáře (`sumar_1`, sezóny 2020–2024) a společná databáze účtů ČRS (knihovna `ucty`). Kódování utf8mb4.
Schéma databáze	Tabulky lokální databáze zakládá kód sám při prvním použití modulu (`CREATE TABLE IF NOT EXISTS`, doplnění chybějících sloupců) – samostatné migrační skripty nejsou potřeba.
Uživatelské rozhraní	Serverově generované HTML, Bootstrap 5.3 a Bootstrap Icons (CDN), společná hlavička, drobečková navigace a nápověda ke stránce (`layout.php`, `crs.css`), responzivní, tiskové styly. Grafy Chart.js, export tabulek do Excelu knihovnou SheetJS (XLSX), editor aktualit Quill.

Knihovny třetích stran	PHPMailer (odesílání e-mailů přes SMTP), dompdf (PDF výstupy: přehledy prodejů a revírů, zpráva o činnosti, prezenční listiny, výpisy Comgate, uživatelská dokumentace). Načítání .xlsx vlastní implementací (ZipArchive + XML), bez externí knihovny.
Umělá inteligence	Google Gemini (REST, odpověď JSON podle schématu, záložní pořadí modelů) – texty hodnocení prodejů a revírů, návrhy textů zprávy o činnosti, AI asistent s voláním nástrojů. Čísla vždy počítá PHP, AI jen formuluje text.
Plánované úlohy	Cron: import výpisů Comgate a ranní rozesílka výpisů, přepočet souhrnů prodejů, přepočet souhrnů revírů, načtení kontrol rybářské stráže a žádostí o storna povolenek z RIS; všechny lze spustit z příkazové řádky i přes URL s tokenem (viz kap. B8).
Konfigurace	`db_config.php` (připojení k databázím) a soubory mimo repozitář podle vzorů `config_*.example.php`: `config_db.php` (přístupové údaje k databázím), `config_mail.php` (SMTP), `config_ucty.php` (přihlášení účtem RIS, záložní správci), `config_comgate.php` (API Comgate, token cronu, veřejná adresa), `config_ai.php` (klíč a modely Gemini), `config_prepocet.php` (token přepočtů), `config_import.php` (účet pro import SQL a historii), `config_straz.php` (technický účet rozhraní RIS a token cronů stráže a storen), `config_dokumentace.php` (cesty ke sportovnímu portálu a fóru pro rozsah v dokumentaci a výpočty zprávy).

Struktura adresářů: kořen obsahuje rozcestník, společné knihovny a většinu modulů; samostatné moduly mají vlastní složky `prodeje/`, `reviry/`, `brigady/`, `objednavky/`, `zprava2/` (zpráva o činnosti, násady a líhně) a `nastroje/`. Nahrané soubory jsou v `uploads/`, přímý přístup do podadresářů s citlivými soubory blokuje `.htaccess` a soubory se vydávají skripty po kontrole práv. Hostování je možné na běžném PHP webhostingu; dlouhé přepočty se spouštějí na pozadí nebo cronem.

B3. Napojení na okolní systémy

Systém	Rozhraní	K čemu slouží	Směr
E-Sumář	přímé spojení do databáze MySQL (jen čtení)	Strom organizací (`keepers` – ÚS, MO, Rada, vazba na RIS přes `ris_sid`), původní uživatelské účty, revíry a jejich části, hospodář revíru, povolenky, docházky a úlovky (`takes`, `take_districts`, `take_details`), kontroly rybářské stráže (`take_checks`).	E-Sumář → rozcestník (živě)
RIS – přihlášení	společná knihovna účtů ČRS (`../ucty`, sdílená s fórem; viz část A)	Ověření uživatelského jména a hesla RIS, eID osoby, platné funkce v organizacích, číselník funkcí; společná schránka zpráv z ostatních aplikací podle eID.	RIS → rozcestník (při přihlášení)
RIS – sestavy Oracle Analytics	soubory CSV / XLSX exportované ze sestav a nahrané správcem	Prodeje (transakce známek, povolenek a poplatků), souhrn členské základny, stav aktivace účtů rybářské stráže, nastavení brigádnické povinnosti a členských příspěvků, zarybňovací plány a vysazení, přestupky a kárná řízení, funkcionáři, vrácené povolenky.	RIS → rozcestník (import)

Systém	Rozhraní	K čemu slouží	Směr
RIS – rozhraní REST	REST rozhraní RIS (`/ma/a/p/features/_query`), HTTPS, HTTP Basic technickým účtem z `config_straz.php`, **jen čtení**	Kontroly rybářů (`ft_kontrolaRybare`), obchůzky (`ft_kontrolaObchuzka`), přestupky (`ft_prestupek`) a číselník stráže pro modul Kontroly rybářské stráže (kap. B6.16); přiřazené funkce pro funkcionáře zprávy o činnosti (kap. B5.15); nastavení brigádnické povinnosti (`ft_konfiguraceBrigadnickePovinnosti`, skupiny členů `ft_skupinaClenuCrs`) a konfigurace členských příspěvků (`ft_konfiguraceClenskyPrispevek`, kap. B6.11); povolenky ve stavu „Požádáno o storno“ a „Stornovaná“ (`ft_povolenka`, kap. B6.3); brigády MO a jejich účastníci (`ft_brigada`, `ft_ucastnikBrigady`) a osoby organizace se stavem člena (`ft_fyzickaOsoba`, záložně `ft_clenCrs`) pro sestavy rozcestníku Členové (kap. B6.7). Do RIS se nic nezapisuje.	RIS → rozcestník (cron, ručně)
Comgate	REST API (výpisy převodů ve ZIP/CSV, seznam převodů), HTTP Basic, údaje v konfiguraci	Denní import plateb plátců a převodů na účty organizací (párování podle IČO), výpisy pro organizace, ranní rozesílka.	Comgate → rozcestník (cron)
Starý E-Sumář (`sumar_1`)	databáze nahraná z SQL dumpu (nástroj Import SQL)	Historie docházek a úlovků 2020–2024 pro modul Revíry a dlouhodobé řady zprávy o činnosti.	jednorázový import
SMTP server	PHPMailer, STARTTLS, údaje v `config_mail.php`	Rozesílání aktualit, úkolů, formulářů, urgencí, upozornění na dokumenty, hájení, objednávky, výpisy Comgate.	rozcestník → uživatelé
Google Gemini	REST API, klíč v `config_ai.php`	Textová hodnocení a návrhy textů ze souhrnných čísel (bez osobních údajů), AI asistent.	obousměrně (na vyžádání)
Sportovní portál	přímé spojení do databáze portálu (jen čtení, přístup z jeho `config.php`; složka z `config_dokumentace.php`, jinak `../sport`)	Registrovaní sportovci (aktivní přihláška do soutěží v roce), trenéři a rozhodčí po odvětvích a letech pro zprávu o činnosti; rozsah kódu portálu pro tuto dokumentaci. Shodná identifikace osob podle eID, převzaté postupy (čištění HTML, vzhled). Popis v části C.	sport → rozcestník (při výpočtu)
Fórum	součást rozcestníku (složka `forum/`)	Sdílí knihovnu účtů (přihlášení RIS, eID, schránka zpráv). Popis v části D.	—

Exporty z RIS označují organizaci číslem `sid`, aplikace pracuje s `keepers.id` E-Sumáře – párování dělá společná funkce (`ris_keepers.php`): Moravský rybářský svaz a jednotky mimo ČRS se vynechávají, nejednoznačná `sid` se nepárují a import je vypíše. Územní svaz se určuje jako nejvyšší nadřízená jednotka přes všechny úrovně stromu.

B4. Uživatelé, role a oprávnění

B4.1 Rozsah dat podle organizace

Jediné místo, kde se ze session určuje, čí data uživatel smí vidět, je `crs_scope.php`; používají ho prodeje, AI asistent i další nové moduly, takže se pravidla nemohou rozejít:

Rada ČRS / admin	vše (Rada = organizace č. 331 v číselníku organizací)

Územní svaz	organizace bez nadřízené (`parent_id` prázdné) – sebe a své MO
Místní organizace	organizace s nadřízenou – jen sebe

U revírů je měřítkem hospodář revíru (vlastník v E-Sumáři), u povolenek výdejce povolenky, u prodejů prodávající organizace. Starší stránky (platby, migrace členů, analytika členské základny, regionální přehledy úlovků a stráže) si hierarchii určují obdobně samy podle číselníku organizací. Výběr MO z adresy (filtr `mo_id`) se u ÚS vždy ověřuje proti seznamu jeho MO – cizí MO se ignoruje a zobrazí se celý vlastní svaz.

Uživatel bez platné organizace (účet RIS bez funkce v organizaci, účet bez přiřazené jednotky nebo s neexistující jednotkou) nevidí žádná data: přehledy vrátí odmítnutí (403) a práva modulů i analytik mají úroveň „nevidí“ (`prava_mo_bez_organizace()` v `analytiky_lib.php`). Platí zásada *chybějící údaj = žádný přístup*, nikdy „bez omezení“.

B4.2 Způsoby přihlášení

- **Účet RIS** (cílový stav) – uživatelské jméno a heslo RIS ověří knihovna účtů. Uživatel vystupuje za některou z „voleb“ (přepínač v hlavičce): organizace, kde má platnou funkci, spárované původní účty (vidí jejich historii) a u správců navíc Rada.
- **E-Sumář** a **lokální účet** (původní způsob) – e-mail a heslo. Účet se při přihlášení jednorázově převede na RIS (ověření účtem RIS, spárování s eID) a e-mailem se pak už nepřihlásí; vyžadování lze nouzově vypnout v konfiguraci (např. při výpadku RIS).
- Role **čtenář** (lokální účty a uživatelé bez práva vyplňovat) – vidí, ale nic neukládá ani neodesílá.
- **Omezení pokusů**: po 10 neúspěšných pokusech na jeden účet (od jeho posledního úspěšného přihlášení) nebo po 30 z jedné IP adresy během 15 minut se přihlášení na 15 minut zablokuje a heslo se vůbec neověřuje. Platí pro přihlášení účtem RIS, e-mailem i pro ověření účtem RIS; počítá se z logu přihlášení (`prihlaseni_lib.php`).

B4.3 Správci a skupiny funkcí RIS

- **Správce** (role admin) se určuje podle eID (správa „Správci“), záložně funkcí či jménem v konfiguraci. Role admin platí, jen když správce vystupuje za Radu; za svou MO či ÚS je běžný uživatel.
- **Skupiny funkcí RIS** – Rada a každý ÚS si z číselníku funkcí RIS sestaví skupiny (např. „hospodáři“, „jednatelé“). Skupiny samy práva nenesou – slouží k určení adresátů a k výjimkám v právech místních organizací.
- Skupiny spravuje jen **správce nastavení** (funkce RIS č. 60 v Radě, č. 61 v ÚS). Obecné funkce (např. členství bez role) může admin označit jako **ignorované** – neurčují organizace ani skupiny.
- **Práva místních organizací** – na jednom místě ÚS určuje, co jeho MO smějí v modulech (Objednávky, Úkoly, Formuláře, Rezervace, Žádosti o hájení: *vidět a vyplňovat / jen vidět / nevidí*) a které analytické dlaždice (prodeje, revíry, výpis plateb) mají k dispozici. Výchozí stav je bez omezení, ÚS může jen zpřísnit a povolit výjimky vybraným skupinám funkcí RIS. Platí pro každého, kdo vystupuje za MO, bez ohledu na způsob přihlášení; ÚS, Radu ani admina neomezuje. Rozcestník nenabízí dlaždice, úkoly ani formuláře, které uživatel vidět nesmí (podrobně kap. B6.15).

B5. Moduly a agendy

Každý modul je popsán funkcemi, pravidly přístupu a hlavními soubory. Analytické nástroje jsou podrobně popsány v kapitole 6.

B5.1 Rozcestník a dlaždice

`index.php`, `tiles_admin.php`, `admin_notes.php`, `layout.php`

- Úvodní stránka: hlavní aktualita, přehled dalších aktualit, dlaždice ve třech skupinách – **Rychlý rozcestník** (odkazy do jiných systémů), **Další nástroje** (moduly rozcestníku) a **Analytické nástroje**.
- Dlaždice spravuje admin: název, ikona, adresa, pořadí, viditelnost (všem / jen admin / konkrétní organizace), štítky „V testu“ a „Nové“. Dlaždice do modulu, který územní svaz místní organizaci nezpřístupnil, se skryje.
- Boxy **Úkoly pro MO/ÚS** (otevřené formuláře, úkoly a rezervační kalendáře seřazené podle termínu) a pro ÚS a Radu **Úkoly pro podřízené MO**; dále vyplněné formuláře, počty otevřených dotazů helpdesku, dlaždice hájení s počtem žádostí čekajících na uživatele.
- Admin může zobrazení přefiltrovat podle územního svazu (vidí rozcestník jako daný ÚS); má soukromé poznámky a box **Urgovaných žádostí o storno** s počtem nevyřízených žádostí, jejichž schválení urgoval územní svaz (proklik na seznam, kap. B6.3).
- Přehled dalších aktualit na úvodní stránce se stránkuje po 10 položkách.
- Horní lišta úvodní stránky má odkaz **Notifikace** (zvoneček) na nastavení Moje notifikace (kap. B5.4); na mobilu je ve vysouvacím panelu Účet.
- Nabídka **Správa** obsahuje podle oprávnění aktuality, termíny a formuláře, správu účtů, skupiny RIS, **práva MO** (správci nastavení ÚS a Rady, admin), ignorované funkce, přehled přihlášení, správce, blokované osoby, dlaždice a poznámky (admin).
- Společná šablona (`layout.php`): hlavička s přepínačem organizace, schránkou a odhlášením, drobečková navigace podle mapy stránek (přesunuté stránky se přesměrují), u každé stránky volitelná nápověda, kterou admin upravuje přímo z hlavičky.

B5.2 Přihlášení a správa účtů

`login.php`, `ucty_prihlaseni.php`, `overeni_ris.php`, `pripojit_ucet.php`, `ris_organizace.php`, `uzivatele_admin.php`, `spravci.php`, `blokovane.php`, `ris_skupiny.php`, `analytiky_pristup.php`, `ris_ignorovane.php`, `prihlaseni_lib.php`, `cookies.php`

- Rozcestí přihlášení: účet RIS, nebo e-mail (E-Sumář / lokální účet). Po přihlášení návrat na stránku, ze které uživatel přišel.
- **Sjednocení účtů**: původní účty se párují s eID (tabulka `ucty_parovani`) – uživatel sám při přihlášení e-mailem (ověření účtem RIS), dodatečně „Připojit původní účet“, nebo admin ve správě účtů. Jeden člověk může mít víc spárovaných účtů.
- **Správa účtů**: přehled účtů organizace (admin všech), stav párování na RIS; nové lokální účty už nelze zakládat.
- Každý pokus o přihlášení se zapisuje do logu, aktivita přihlášených se průběžně posouvá – vyhodnocení viz kap. B6.12. Opakované úspěšné přihlášení téže osoby ze stejné IP do 2 minut (typicky správce hesel s automatickým přihlášením) se sloučí do jednoho záznamu s počtem opakování; už přihlášeného přihlašovací stránka rovnou přesměruje dál.

- **Blokované osoby** (admin, tabulka `ris_blokovane`): osoba blokovaná podle eID se nepřihlásí účtem RIS (kontrola po ověření v RIS, i při ověření e-mailového účtu) a přihlášenou systém do minuty odhlásí, i ze společné relace nástrojů ČRS. Odhlášeného blokovaného systém pošle na rozcestí přihlášení bez formuláře s hláškou o blokaci – automatické přihlášení ze správce hesel se tak nezacyklí. Kontrola běží jen na stránkách se zapisovatelnou relací (stránky, které relaci hned uzavírají, odhlášení neuloží). Blokace trvalá nebo do zadaného dne, s interním důvodem; správce zablokovat nelze. Nespárované účty E-Sumáře a lokální účty eID nemají – blokace se jich netýká.
- Správa správců podle eID, skupin funkcí RIS, práv místních organizací a ignorovaných funkcí (viz kap. B4.3 a B6.15).
- Veřejná stránka **Cookies a soukromí** (odkaz v patičce rozcestníku a na přihlášení) – viz kap. B9.

B5.3 Aktuality

`admin.php`, `edit_news.php`, `detail.php`, `news_stats.php`, `upload.php`, `upload_file.php`, `html_sanitize.php`

- Zakládá Rada, ÚS a admin: nadpis, obsah ve WYSIWYG editoru (obrázky, video YouTube / Vimeo), hlavní zpráva, období zobrazení, cílová skupina (všichni / oblast ÚS a jeho MO), veřejná nebo jen pro přihlášené.
- Volitelné rozeslání e-mailem a **potvrzení přečtení** organizacemi; statistika přečtení ukazuje, kdo potvrdil a kdo ne. Rozesílka se připraví v okně s předvyplněným předmětem a textem (nadpis, perex a odkaz na `https://mocrs.cz/main/detail.php?id=…`), který lze před odesláním upravit. Název a perex se do okna předávají přes atributy `data-*` a do textu se vkládají escapované – apostrof ani zalomení řádku v perexu tlačítko nerozbije.
- Detail aktuality ukazuje bublinu **„Zveřejnil“** podle uložené cílové oblasti (`target_area_id`: prázdná = Rada ČRS, jinak název ÚS) se stejnou barvou jako na úvodní stránce – už se neodvozuje z autora, jehož ID mezi zdroji účtů nejsou jednoznačná.
- HTML z editoru se čistí při uložení i při zobrazení (povolené značky a atributy, bez skriptů, obsluh událostí a cizích iframe).
- Přílohy vložené do textu (složka `uploads/aktuality`) jsou dostupné každému, kdo zná odkaz – slouží pro dokumenty určené k rozeslání; výpis obsahu složky je zakázaný. Aktualitu maže admin libovolnou, ÚS jen svou, a to jen tlačítkem s ověřením (ne odkazem).

B5.4 E-mailové notifikace a schránka

`mailer_helper.php`, `notifikace_prehled.php`, `notifikace_zarazeni.php`, `schranka.php`, `schranka_lib.php`, `moje_notifikace.php`, `notif_odber_lib.php`

- Centrální odesílání přes SMTP (PHPMailer) v dávkách po 50 adresách, s přílohami z paměti. Testovací režim (přepínač admina sdílený moduly) hromadné rozesílky fyzicky neodesílá, jen ukáže, na kolik adres by e-mail šel.
- Každé rozeslání se loguje (modul, zdrojový záznam, dávka, odesílatel a jeho organizace). **Přehled odeslaných notifikací** ukazuje rozeslání vlastní organizační jednotky, admin vše; historické záznamy bez jednotky admin ručně zařadí podle vodítek.
- Logují se i **automatické e-maily** (potvrzení rezervace, notifikace objednávky, denní výpis ComGate, upozornění na žádosti o storno povolenek) s příznakem `is_auto`; v přehledu jsou označené „Automaticky“ a lze je filtrovat (Typ: rozeslané uživatelem / automatické). Patří organizaci, které se týkají (potvrzení rezervace rezervující MO, výpis ComGate organizaci výpisu).

- **Schránka**: kopie všech e-mailů, které rozcestník poslal na e-mail účtu (aktuality, úkoly, formuláře, dokumenty, hájení, objednávky …), s počtem nepřečtených v hlavičce. U účtu RIS za všechny jeho e-maily a navíc zprávy z ostatních aplikací (např. fórum) ze společné schránky podle eID.
- **Moje notifikace** (odkaz „Notifikace“ v horní liště, každý přihlášený): uživatel si po oblastech zapíná a vypíná e-mailová upozornění. Nabízejí se jen oblasti, které mají pro úroveň jeho organizace smysl:

Oblast	Komu	Výchozí	Jak působí
Žádosti o storna povolenek	Rada, ÚS	vypnuto	přihlášení k odběru – souhrnný e-mail o nových žádostech (kap. B6.3)
Denní výpisy plateb ComGate	Rada, ÚS, MO	vypnuto	přidá / pozastaví e-mail účtu v seznamu adres organizace pro výpisy (stejný seznam jako stránka Zasílání denních výpisů)
Žádosti o hájení revíru	Rada, ÚS, MO	zapnuto	odhlášení – modul dál posílá všem uživatelům organizace, jen vyřadí adresy, které si oblast vypnuly
Potvrzení rezervace termínu	ÚS, MO	zapnuto	
Nové objednávky do skladu	Rada, ÚS	zapnuto	
Aktuality	Rada, ÚS, MO	zapnuto	

  Přihlášení k odběru patří účtu (zdroj + ID) a organizaci, za kterou uživatel vystupuje (Rada a admin za Radu); odhlášení platí pro e-mail účtu bez ohledu na organizaci. Rozesílky úkolů, formulářů, termínovníků (pozvánky) a dokumentů jsou povinné a vypnout nejdou. Odběr bez e-mailu v účtu nelze zapnout.

- **E-mail osoby z knihovny účtů** (`ucty_prihlaseni.php`: `mocrs_ris_email`, `mocrs_emaily_uctu`): kdo má eID, tomu rozcestník posílá vždy na e-mail podle knihovny účtů (`ucty_email_adresa`) – e-mail z RIS, nebo ověřený alternativní při volbě „alt“; čte se živě, změna platí hned. Volitelná upozornění (Moje notifikace) respektují i volbu „nikam“, povinné rozesílky chodí vždy. Rozesílky organizacím (aktuality, úkoly, formuláře, termínovníky, dokumenty, hájení, rezervace, objednávky) berou účty E-Sumáře a lokální účty jednotek; **spárovaný původní účet dostane poštu na e-mail své osoby**, ne na starou adresu účtu. Stejný e-mail osoby ukazuje Moje notifikace a používá Schránka, ať uživatel vystupuje za kteroukoli organizaci.

B5.5 Úkoly s termínem

`tasks_admin.php`, `tasks_edit.php`, `tasks_results.php`, `task_detail.php`, `task_soubor.php`

- Rada, ÚS a admin zadávají úkoly pro MO nebo ÚS (případně jen pro oblast jednoho ÚS) s termínem, popisem a volitelně s povinnou přílohou.
- Organizace úkol splní na detailu (potvrzení, poznámka, nahraný soubor s jednotným názvem); po termínu se úkol ze seznamu k vyřízení ztrácí.
- Plnění úkolu: kdo splnil a kdo ne, stažení příloh, urgence e-mailem neplnícím organizacím.
- Odevzdané soubory vydává `task_soubor.php` jen adminovi, organizaci, která soubor odevzdala, a jejímu ÚS; přímý přístup do `uploads/tasks` je zakázaný.

B5.6 Formuláře

`forms_admin.php`, `forms_edit.php`, `form.php`, `forms_results.php`, `forms_results_public.php`, `moje_formulare.php`

- Editor formulářů: krátký a dlouhý text, výběr jedné / více možností, datum; cílová entita MO nebo ÚS, oblast, období zveřejnění, zamčení.
- Režim vyplnění: jednou za organizaci bez změn, jednou s přepsáním předchozí odpovědi, nebo neomezeně. ÚS může vyplnit za svou MO.
- Výsledky po organizacích s přehledem nevyplněných, urgence e-mailem, export do CSV; volitelně veřejné souhrnné výsledky pro MO.
- „Moje vyplněné formuláře“ – historie odeslaných odpovědí organizace s možností úpravy, dokud to formulář dovoluje.
- Formulář upravuje jen admin, jeho autor nebo ÚS, kterému je určen – oprávnění se ověřuje před zobrazením editoru i před uložením (hlavička, heslo i otázky).

B5.7 Rezervační kalendáře

`reservations_admin.php`, `reservations_edit.php`, `reservation.php`, `reservations_results.php`

- Rada / ÚS založí rezervační téma (např. školení, převzetí tiskopisů) s dny a časovými sloty a kapacitou; zveřejnění od–do, zamčení, oblast.
- MO si zarezervuje termín, dostane potvrzení e-mailem (na všechny účty organizace); zadavatel vidí obsazenost, může rezervaci zrušit či přesunout a urgovat MO bez rezervace.

B5.8 Správce dokumentů

`dokumenty.php`, `dokumenty_api.php`, `dokumenty_lib.php`, `dokumenty_stahnout.php`, `dokumenty_kos.php`

- Strom složek, souborů a odkazů po organizačních jednotkách (Rada, ÚS); nahrávání více souborů přetažením, kopírování odkazu do e-mailu či aktuality, naposledy přidané soubory.
- **Viditelnost** kombinací příznaků: všichni přihlášení, Rada, podřízené jednotky, jen ÚS, vybrané jednotky; platnost od–do. Položku musí povolit ona i všechny nadřazené složky. Vlastník, Rada a admin vidí vše.
- Soubory leží pod náhodnými názvy mimo přímý přístup z webu, stahují se jen přes kontrolu práv a platnosti.
- Upozornění organizací e-mailem na nový dokument; **koš** s obnovením, trvalým smazáním a automatickým vysypáním po 30 dnech.

B5.9 Žádosti o hájení revíru

`hajeni.php`, `hajeni_edit.php`, `hajeni_detail.php`, `hajeni_duvody.php`, `hajeni_verejne.php`, `hajeni_soubor.php`, `hajeni_lib.php`

- **MO se svěřeným revírem** podává žádost za svůj revír (případně vybrané části revíru): období hájení, důvod z číselníku ÚS, zdůvodnění, příloha. Ve stavu Požádáno / Vráceno ji smí upravit nebo stáhnout, k zadané žádosti podat žádost o úpravu.
- **ÚS** vyřizuje žádosti svých MO: Zadáno do RISu / Odmítnuto / Vráceno k doplnění s poznámkou; může žádost zadat za MO nebo opravit, spravuje vlastní číselník důvodů (důvody se nemažou, jen vyřazují), smí žádost smazat (po potvrzení).
- Rada a admin vidí vše jen ke čtení; admin má náhled „za MO“, při kterém se nic neukládá ani neodesílá.
- Každá změna stavu se zapisuje do historie a posílá e-mail druhé straně. Revír a jeho části se ukládají i s číslem a názvem, aby žádost zůstala čitelná po změně číselníku.
- **Veřejný přehled** zadaných hájení bez přihlášení (revír, období, důvod, zveřejněná příloha; bez zdůvodnění a autorů), filtr podle roku, ÚS a textu; bez hlavičky, aby šel vložit do jiného webu.

B5.10 Helpdesk a uživatelská podpora

`helpdesk.php`, `helpdesk_create.php`, `helpdesk_answer.php`, `helpdesk_down.php`, `helpdesk_soubor.php`, `support.php`, `support_admin.php`

- Dotazy mezi úrovněmi svazu (MO → ÚS → Rada) s vláknem odpovědí a přílohami, stav otevřeno / uzavřeno; Rada může dotaz MO předat na příslušný ÚS. Rozcestník ukazuje počet nezodpovězených vlastních dotazů a dotazů položených uživateli.
- Přílohy dotazů vydává `helpdesk_soubor.php` jen adminovi, autorovi a aktuálnímu řešiteli dotazu; přímý přístup do `uploads/helpdesk` je zakázaný.
- **Výzva organizační jednotce** – Rada pošle výzvu nebo dotaz konkrétní organizaci.
- **Návrhy na úpravu mocrs.cz** (složka `rozvoj/`: `navrhy.php`, `navrhy_novy.php`, `navrhy_detail.php`, `navrhy_soubor.php`, `navrhy_lib.php`) – každý přihlášený podá návrh přes tlačítko na rozcestníku nad úkoly: oblast z číselníku podle modulů systému (a „Jiné“), stručný název, formátovaný popis (editor Quill, HTML se čistí) a 1–3 přílohy do 10 MB. Admin vidí všechny návrhy s filtrem podle stavu a oblasti, mění stav (nový, posuzuje se, přijato k realizaci, realizováno, zamítnuto), komentuje a může návrh smazat; autor vidí jen své návrhy a v komentářích s adminem komunikuje. O reakci admina dostane autor e-mail. Tlačítko na rozcestníku ukazuje adminovi počet návrhů čekajících na reakci, autorovi počet odpovědí. Přílohy vydává jen autorovi a adminovi `rozvoj/navrhy_soubor.php`, přímý přístup do `uploads/navrhy` je zakázaný.
- **Uživatelská podpora** – kontakty podpory RIS a E-Sumáře po oblastech s filtrem, správa kontaktů adminem.

B5.11 Nápověda, manuál a metodika

`napoveda.php`, `napoveda_edit.php`, `napoveda_pdf.php`, `napoveda_lib.php`, `napoveda_seed_data.php`, `napoveda_aktualizace.php`, `manual.php`, `dokumentace.php`, `metodika.php`, `metodika_soubor.php`, `sys_dokumentace.php`, `helps_admin.php`

- **Uživatelská dokumentace**: kapitoly a témata se screenshoty, přepínání pohledu ÚS / MO, vyhledávání, export do PDF; výchozí obsah se naplní automaticky, dál se upravuje v editoru. Nové a změněné články k novým funkcím se dodávají jako číslované aktualizace (`napoveda_aktualizace.php`), které se na serveru provedou jednou při otevření nápovědy: chybějící moduly a články se doplní, existující článek se přepíše jen tehdy, když ho admin dosud ručně neupravoval (tabulka `manual_aktualizace`).
- **Manuál** (jedna upravitelná stránka), **Návody a dokumentace RIS** (sekce s odkazy, soubory a videi YouTube), **Metodika a předpisy** (centrální směrnice Rady a metodické pokyny vlastního ÚS), **Systémová dokumentace** (pro admina a Radu – seznam systémových popisů s odkazy na aktualizaci).
- **Metodika – oprávnění**: územní svaz spravuje jen své sekce (úpravy, mazání, položky), celostátní sekce zakládá a upravuje jen admin; odkazy jen http(s), video jen z YouTube / Vimeo; soubory vydává `metodika_soubor.php` tomu, kdo sekci vidí.
- **Nápověda ke stránce** – krátký text nad obsahem libovolné stránky, upravuje admin tlačítkem v hlavičce.
- Tato **dokumentace systému** – technický popis rozcestníku, sportovního portálu a fóra (veřejná). PDF se vyrábí na serveru (dompdf: titulní strana s obsahem, záhlaví, čísla stran), takže nezávisí na nastavení tisku v prohlížeči. Admin ji upravuje ve WYSIWYG editoru (TinyMCE) s historií verzí; výchozí znění je v souboru `dokumentace_systemu_obsah.html`, živé údaje (rozsah kódu, počty tabulek) se vkládají značkami a počítají při zobrazení.

B5.12 AI asistent

`asistent.php`, `asistent_lib.php`

- Chat nad daty rozcestníku. AI nikdy nepíše SQL ani neurčuje, kdo je uživatel – smí jen volat nástroje: hledání a čtení v uživatelské dokumentaci, vyhledání organizace, přehled prodejů, přehled revírů, údaje o vlastní organizaci.
- Každý nástroj si rozsah oprávnění spočítá ze session; parametry od AI bere jen jako přání. Ven nejdou osobní údaje. Čísla prodejů a revírů bere ze stejných výpočtů jako AI vyhodnocení a PDF přehledy (kap. B6.4, 6.6).
- Každá otázka se loguje (kdo, co, které nástroje), uživatel může odpověď ohodnotit.

B5.13 Objednávky (e-shop a sklad)

`objednavky/index.php`, `objednat.php`, `dosle.php`, `sklad.php`, `export.php`, `obrazky_lib.php`, `obrazek.php`

- Dodavatelem je nadřízená organizace (pro MO její ÚS, pro ÚS Rada): katalog zboží a tiskopisů podle kategorií, objednávka s dodacími údaji, přehled vlastních dřívějších objednávek.
- **Sklad** dodavatele: položky, ceny, kategorie, zásoby (skladem, rezervováno, vydáno), aktivní / skryté, 0–3 obrázky (přeuloží se, zmenší, srovná otočení z mobilu, vznikne miniatura; vydávají se jen přihlášeným).
- **Došlé objednávky**: stavy nová – zpracovává se – vyřízeno – zrušeno, úprava obsahu se zápisem změn, dodací list k tisku, e-mailová upozornění; **sdružené objednávky** – export souhrnu položek za období.
- Když ÚS svým MO nastaví modul jen ke čtení (práva MO, kap. B6.15), je pro ně modul jen ke čtení (odeslaný formulář se zahodí).

B5.14 Platby Comgate a denní výpisy

`comgate_lib.php`, `cron_comgate.php`, `cron_comgate_reports.php`, `payments.php`, `comgate_vypis.php`, `comgate_vypisy.php`, `comgate_vypis_pdf.php`

- Noční úloha stáhne z Comgate výpisy převodů za den (ZIP s CSV – jeden soubor = jeden převod na účet organizace), uloží platby plátců se všemi sloupci a převody, doplní čísla účtů; organizace se určí podle IČO. Import je opakovatelný – existující záznamy přepíše. Chybějící den lze dotáhnout spuštěním úlohy s datem.
- **Výpis plateb** pro organizaci, **sloučený výpis** za všechny organizace (jen Rada a admin), výpis převodu v PDF a Excelu.
- **Zasílání denních výpisů**: organizace si zadá 1–n e-mailů; ranní úloha jí pošle výpis jen za den, kdy jí Comgate poslal peníze – shrnutí, Excel v příloze a odkaz na PDF s omezenou platností. Opakované spuštění odeslané výpisy znovu nepošle.
- E-mail plátce se ve výpisech nezobrazuje ani neexportuje.

B5.15 Zpráva o činnosti, násady a líhně

`zprava2/` (43 výpočtů v `zprava2/vypocty/`)

- Celosvazová výroční zpráva za rok, členěná do stromu kapitol. Admin spravuje strukturu (řazení přetažením, kopie z předchozího roku, převzetí z tabulek původní verze), přiřazuje **řešitele** kapitol, otevírá a uzavírá kapitoly a zprávu publikuje – publikovaná zpráva je uzamčená. Řešitele přiřazuje podle eID osoby (jméno se dohledá ve funkcionářích, v účtech, které se už přihlásily, nebo přímo v RIS); kapitolu řešitel upravuje po přihlášení účtem RIS, předem se přihlašovat nemusí.
- Kapitola se skládá z bloků: text, obrázek, odkaz, tabulka, vložená stránka, **výpočet** a tabulka od ÚS. Výpočet je samostatný soubor, který vrací tabulky a graf (sloupcový, pyramida, protichůdný) – členská základna a věková struktura, migrace a toky mezi ÚS, vyúčtování členských příspěvků a ceny známek, prodej povolenek po druzích, bezplatné povolenky, úlovky (celkem, po ÚS, revíry Rady, TOP 30, úhoř,

skupiny ryb), výměry revírů, zarybnění a plnění plánů, produkce násad a její vývoj od roku 1998, produkce líhní, rybářská stráž, přestupky, funkcionáři, sportovní výsledky a medaile.

- **Rybářská stráž z mobilní aplikace** (data kontrol a obchůzek z RIS, kap. B6.16): po ÚS aktivní strážní, obchůzky, hodiny (z toho noční 22–4 h), kontrolní dny, kontroly, pochybení a jejich podíl, zadržené povolenky a udice, lov bez povolenky a přestupky; souhrn ČRS proti předchozímu roku jen při úplných datech. Přestupky podle druhu kárného provinění s podílem, meziroční změnou a rozdělením po ÚS. ÚS se určuje podle hospodáře revíru, činnost mimo revíry a na nenapojených revírech podle MO strážného; revíry Moravského rybářského svazu se vynechávají.
- **Registrovaní sportovci ze sportovního portálu** (část C, databáze portálu jen ke čtení): registrovaný = aktivní přihláška do soutěží v roce; sportovci po věkových kategoriích jako u členské základny (děti do 15, mládež 16–18, dospělí 19+), trenéři, rozhodčí a přihlášky podle odvětví s meziroční změnou a vývoj po letech od začátku registru s grafem.
- Od roku 2025 se počty berou z prodejů v RIS, dřívější roky z historických řad; zdroje se v jednom roce nemíchají.
- **Revize údajů územními svazy**: tabulky zprávy s rozpadem na ÚS (počty členů a vyúčtování, muži a ženy, organizace, migrace, prodej povolenek CS a ÚS, bezplatné povolenky, přestupky, rybářská stráž, výměry revírů) stojí na datových sadách, které ÚS za svůj řádek prověří, případně opraví, a potvrdí. Revize má ve zprávě přednost před vypočtenou hodnotou a je označená značkou R s poznámkou; součty ČRS se upraví o rozdíl revizí, změny a podíly se přepočítají, meziroční změna bere revidované údaje i za předchozí rok. Když se vypočtená data po potvrzení změní, jsou znovu k prověření. Admin vidí stav všech ÚS, reviduje řádek Rady, ruší potvrzení a uzavírá tabulky pro revize jednotlivě i hromadně.
- **Tabulky vyplňované ÚS**: admin navrhne tabulku (obecná nebo s předvyplněnými řádky), ÚS a Rada ji za sebe vyplní a odevzdají; stavy příprava / otevřeno / uzavřeno, vrácení odevzdané tabulky. **Korekce zarybnění** pro ÚS, které nezadávají do RIS.
- Podpůrné stránky: **funkcionáři z RIS** (Rada, RDR, jednatelé Rady a ÚS i s historií; dotaz na přiřazené funkce technickým účtem RIS, územní svaz podle funkce v ÚS, jinak podle členství v MO; u jednatele v Republikové radě se územní svaz neuvádí), importy (zarybnění, přestupky), párování druhů úlovků s druhy zarybnění pro výlovek, přepočet statistik úlovků z E-Sumáře, sport (závody, výsledky, číselníky disciplín a kategorií, vložení z Excelu). Ceny známek bere zpráva z ceníku členských známek v prodejích; rozdělení tržby MO / ÚS / Rada (50 / 37 / 13 %) je pevné.
- **AI návrh textu** k výpočtu – do AI jdou jen souhrnná čísla; návrh se vloží do editoru k úpravě, každý se loguje, řešitel má denní limit.
- Zobrazení celé zprávy na webu a export do PDF stejnou vykreslovací funkcí; veřejnost vidí jen publikované zprávy, Rada a řešitelé náhled.
- **Násady a líhně**: ÚS vyplní výkaz produkce násad (kusy a kg po kategoriích z číselníku admina) a odevzdá ho, Rada ho může vrátit k opravě; ÚS a MO evidují své líhně a jejich roční produkci po druzích a věkových kategoriích. Přehled (veřejný) zobrazuje stejné výpočty jako zpráva. Záložně **import funkcionářů z CSV**. Původní složka `zprava/` je zrušená; adresy jejích stránek ve starších kapitolách se převádějí na nové.

B5.16 Nástroje

`nastroje/schuze.php`, `import_sql.php`

- **Generátor prezenčních listin** pro členské schůze MO: z XLSX členské základny z RIS vznikne PDF pro každou místní skupinu (více skupin v ZIP). Nic se neukládá na server – zpracování probíhá v paměti.

- **Import SQL dumpu** (admin nebo příkazová řádka): proudové nahrání velkých dumpů (.sql / .sql.gz) do zvolené databáze, úprava odkazů na databázi a DEFINER, pokračování přerušeného importu; lokální databázi aplikace a E-Sumář jako cíl odmítne.

B6. Analytické nástroje

Analytická část tvoří největší část díla (145 souborů). U každého nástroje je uvedeno, kdo k němu má přístup, z jakých dat čte, co přesně zobrazuje a jak se čísla počítají.

B6.1 Společné principy

- **Rozsah podle role** – Rada a admin vidí celý svaz a mohou se prokliknout do ÚS a MO, ÚS vidí sebe a své MO, MO jen sebe (kap. B4.1). Parametry v adrese (organizace, ÚS) jsou jen přání – mimo rozsah se nic nezobrazí.
- **Omezení územním svazem** – ÚS může v právech MO jednotlivé dlaždice prodejů, revírů a výpisu plateb svým MO zakázat (s výjimkami pro skupiny funkcí RIS). Zakázaná dlaždice má v přehledu zámek a stránka i všechny její podstránky a detaily místo dat ukážou hlášku, kdo a kdy zákaz zadal (kap. B6.15).
- **Předpočítané souhrny** – přehledy přes celé svazy by z milionů transakcí a záznamů počítaly dlouho, proto se čtou z lokálních souhrnných tabulek, které po importu nebo změně dat přepočítává úloha na pozadí (kap. B8). Detail (dny, transakce, jednotlivá povolenka) se čte živě. Na stránkách je vidět stav dat (do kdy jsou platby, kdy proběhl přepočet).
- **Meziroční srovnání ke stejnému dni** – během sezóny se letošek porovnává s loňskem do stejného data, aby čísla nebyla zkreslená nedokončenou sezónou.
- **Storna** se odečítají podle typu transakce (příchozí × odchozí) – „čistý počet“ a „reálně uhrazeno“ jsou po stornech.
- **Osoba = eID** z RIS (sjednocené napříč zdroji); Moravský rybářský svaz a jednotky mimo ČRS se nezapočítávají.
- Tabulky lze řadit kliknutím na záhlaví a exportovat do Excelu; vybrané přehledy mají export do PDF.

B6.2 Prodeje – import a přepočet

`sales_import.php`, `sales_agg.php`, `prodeje/prepocet.php`, `prodeje/cron_prepocet.php`, `prodeje/prepocet_stav.php`, `prodeje/kontrola_dnu.php`

> Import: ÚS a Rada (MO ne). Ruční spuštění přepočtu: admin.

- Vstupem je export transakcí z RIS (.xlsx) – každý řádek je jedna položka transakce: číslo a datum transakce, prodávající organizace, položka (členská známka, povolenka, brigáda, zápisné, poplatky …), cena, slevy Rady / ÚS / MO, uhrazeno, eID a ročník kupujícího, u povolenek druh, časová platnost, revír a číslo povolenky, důvod slevy či poplatku.
- Import čte soubor ve dvou průchodech; transakce, které už v databázi jsou, se znovu nevkládají (lze nahrávat překrývající se období), jen se jim doplní chybějící důvod platby. Organizace se párují podle názvu. Každé nahrání je dávka s obdobím, souborem a autorem.
- Zasažené úseky *rok* × *organizace* se zařadí do **fronty přepočtu**. Úloha je zpracovává po jednom ve vlastní transakci (smazat a znovu spočítat, takže opakování nevadí), souběžně běží jen jeden přepočet. Po vyprázdnění fronty se po krocích dopočítá členství a migrace, zápisné, brigády po osobách a děti zdarma. Průběh je vidět na stránce importu.

- **Kontrola importů – dny bez prodeje**: pro každý ÚS se sjednotí období všech nahraných dávek a vypíšou se dny, kdy žádná organizace ÚS neměla žádnou platbu, a mezery mezi nahranými obdobími – odhalí zapomenutý nebo neúplný import.
- Souhrnné tabulky: denní součty (organizace × den × položka × cena × typ × druh povolenky × věková kategorie), souhrn povolenek po kódech, podezřelé platby známek, členství po osobách a přechody mezi roky (viz kap. B7).

B6.3 Prodeje – přehledy

`prodeje/` – rozcestník `index.php` ukazuje poslední aktualizaci dat (první a poslední platba po ÚS) a dlaždice přehledů.

> Všechny přehledy: Rada (celý svaz, rozpad po ÚS a organizacích), ÚS (sebe a své MO), MO (sebe, rozpad po měsících). Výběr sezóny a u většiny i období od–do. Proklik z organizace (u MO z měsíce) vede na detail po dnech a na jednotlivé transakce. Každou dlaždici může ÚS svým MO zakázat (kap. B6.15).

Celkové prodeje celkove.php	Reálně uhrazeno celkem a čistý počet transakcí za sezónu (s datem, do kdy jsou data), sloupcový graf uhrazených částek podle oblastí letos proti loňsku ke stejnému dni (klik na sloupec otevře oblast) a karty oblastí (známky, povolenky, brigády, zápisné, mimořádné známky, kárná řízení, další platby, SHR, FRR, navýšené ceny, ostatní) s čistým počtem, uhrazenou částkou a meziroční změnou.
Prodeje známek znamky.php, znamky_detail.php, ceny_znamek.php	Čistý počet členských známek podle kategorií podle zaplacené ceny (dospělí, mládež, děti – ceny sezóny z ceníku) s meziroční změnou a tržbou; rozpad po organizacích / měsících. **Ceník členských známek** (admin) – ceny po letech od 1991, jediné místo pro prodeje, AI vyhodnocení i zprávu o činnosti; chybí-li cena pro sezónu, přehledy použijí cenu z předchozího roku a upozorní. Po uložení se přepočtou podezřelé platby. **Podezřelé platby** – známky, jejichž cena neodpovídá kategorii podle ročníku kupujícího (dospělí 19+, mládež 16–18, děti do 15 let), s organizací, datem, číslem transakce a eID. Detail: prodeje po dnech a jmenný seznam plateb podle kategorie.
Prodeje povolenek povolenky.php	Shrnutí sezóny a koláčové grafy podle věkové kategorie, druhu a revíru. Tři tabulky – celosvazové + celorepublikové, územní, revírní a ostatní: řádek je kód povolenky (druh, časová platnost, revír, věková kategorie) s počtem, trendem proti loňsku (párování podle prvních 5 číslic kódu), nominální hodnotou, slevami Rady / ÚS / MO a reálně uhrazenou částkou. Kód se rozbalí na územní svazy a ty na organizace (organizace se dočítají až při rozbalení). ÚS a MO vidí v územních a revírních tabulkách jen kódy, které prodával jejich ÚS. Hledání konkrétní povolenky podle čísla (všechny transakce k ní). Export řádků tak, jak jsou rozbalené.
Migrace členů migrace.php, migrace_osoby.php	Porovnání plateb členských známek letos a loni po osobách. Ukazatele: členů loni a letos, bilance, **skutečná obnova** (loňští členové, kteří letos platí ve stejné organizaci / ÚS / svazu), **obnova ve svazu** (včetně odchodů jinam), odchody. Podle věkových kategorií: zůstali, noví, navrátilci (po pauze), příchody, přechody do vyšší kategorie, odešli jinam, neobnovili. Pro ÚS výměna s ostatními ÚS (odešlo, přišlo, saldo) a přesuny mezi vlastními MO, pro Radu matice toků mezi ÚS. **Seznam osob** pro každý typ přechodu (eID, ročník, kategorie, odkud, kam, datum platby) s exportem. Hostování (známka ve více organizacích) se rozlišuje.
Prodeje brigád brigady.php, brigady_detail.php	Finanční náhrada za brigádu: čistý počet, mělo být uhrazeno, individuální sleva MO, reálně uhrazeno. **Průměrná cena podle věku** (svaz, ÚS, organizace – včetně osvobozených za 0 Kč) a **průměrná tržba na člena** (uhrazeno za brigády ÷ počet prodaných členských známek ve věkové kategorii). U Západočeského ÚS navíc známka SHR a součet brigáda + SHR. Detail: dny a transakce s eID, ročníkem, věkem, pásmem a důvodem slevy.

Zápisné zapisne.php, zapisne_sekce.php	Souhrn, průměrná cena podle věku a rozpad jako u fondů. Navíc **kdo a proč platil**: osoby se zápisným rozdělené podle členských známek v celém svazu – noví, propadlé členství (měli známku loni a letos ji nezaplatili do 30. 4.), návrat po pauze, nelze určit; ukazatele propadlí z loňských, medián dní po 30. 4., udržení nováčků. **K prověření**: zápisné u platného člena, nový člen bez zápisného, zápisné bez známky.
Fond SHR, Fond FRR, Mimořádné známky fond_shr.php, fond_frr.php, mimoradne_znamky.php	Společná šablona fondů: souhrn podle druhu (prodáno, zrušeno, čistý počet, tržba) s meziroční změnou, průměrná cena podle věku, rozpad po organizacích. Počítají se jen placené položky (cena nad 0 Kč). Mimořádné známky sčítají známky Rady, ÚS a MO.
Další platby dalsi_platby.php, jine_platby_*.php	Položka „Jiná platba“ podle volného textu důvodu: přehled **podle kategorie** (organizací, plateb, tržba, podíl) a podle důvodu. Kategorie zakládá admin a důvody do nich řadí ručně nebo pravidly se vzorem („*brig*“ = obsahuje „brig“); porovnává se sjednocený text bez diakritiky a čísel. Kategorie má závažnost (např. „k prověření“) a kontext pro AI. Změna platí hned, bez přepočtu.
Navýšené ceny povolenek navysene_ceny.php, navyseni_detail.php	Navýšení ceny za nevrácenou povolenku. Sezóna se počítá podle data platby (7. 12. – 6. 12.), ne podle roku povolenky. Rozdělení podle typu povolenky (CS/CR, územní, revírní) s meziročním srovnáním, rozpad po organizacích; detail s číslem povolenky, typem a platností.
Kárná řízení karna_rizeni.php	Poplatky za náklady kárného řízení za kalendářní rok platby, rozpad po ÚS, seznam transakcí. U každé platby je MO, kde je plátce členem (kde naposledy před platbou zaplatil členskou známku) – MO tak vidí platby svých členů bez ohledu na to, který ÚS je vybral.
Povolenky pro děti zdarma deti_zdarma.php	Jen Rada a ÚS. Děti, které v předchozí sezóně dostaly povolenku se slevou ÚS, a kolik z nich si v hodnocené sezóně zaplatilo členskou známku – kdekoli ve svazu a z toho ve stejném ÚS. Rada vidí rozpad po ÚS s proklikem na organizace, ÚS po organizacích, které povolenku vydaly.
Orientační rozdělení příjmů rozdeleni_prijmu.php	Jen Rada. Kolik procent reálně uhrazených příjmů sezóny připadne Radě, ÚS a MO (bez absolutních částek) podle pravidel: členské známky 13 / 37 / 50 %, zápisné, brigády a další platby MO, SHR, FRR, kárná řízení a navýšené ceny ÚS, z každé povolenky 50 Kč MO, zbytek územních povolenek ÚS a celosvazových podle redistribuce.
Transakce po dnech transakce_dny.php	Počet transakcí po dnech roku pro dva roky vedle sebe se společným měřítkem, zvýrazněné víkendy, nejsilnější den; stažení dat v CSV.

Žádosti o storna povolenek storna_povolenek.php, storna_data.php, test_povolenka.php	Povolenky ve stavu **Požádáno o storno** a **Stornovaná** načtené přímo z RIS (`ft_povolenka`, jen čtení) za předchozí, aktuální a následující rok povolenky. Rozsah podle organizace prodejce (Rada vše, ÚS sebe a své MO, MO jen sebe), výběr roku a stavu, řazení kliknutím na záhlaví, na mobilu karty místo tabulky. U každé povolenky číslo, eID (a držitel a typ, pokud je RIS vrátí – jinak se prázdné sloupce skryjí), prodejce, platnost, datum vydání, stav, datum a důvod storna a **průběh stavů**, jak je zachytila synchronizace. Žádost, která z RIS zmizí bez storna, se označí jako **zamítnutá**. **Urgence**: ÚS může u celosvazové povolenky (číslo začíná 8) ve stavu „Požádáno o storno“ urgovat schválení storna Radou (nejvýš jednou denně za organizaci); Rada vidí počet urgencí a seznam urgovaných žádostí, admin i na úvodní stránce. Synchronizace běží cronem jednou denně (kap. B8), admin ji může spustit ručně a vidí výsledek posledního běhu. **E-mailové upozornění**: o nových žádostech (od druhé synchronizace dál) dostanou souhrnný e-mail odběratelé oblasti „Žádosti o storna povolenek“ (kap. B5.4) v organizaci, která storno v RIS schvaluje – u celosvazové povolenky Rada, jinak územní svaz prodejce. E-mail se uloží i do schránky a přehledu notifikací (modul „Storno povolenky“), testovací režim rozesílek se na něj nevztahuje. Pro admina je k dispozici diagnostická stránka pro dohledání jedné povolenky v RIS podle čísla (všechny atributy, i z příkazové řádky).

B6.4 Prodeje – AI vyhodnocení a přehled do PDF

`prodeje/ai_vyhodnoceni.php`, `ai_common.php`, `ai_helper.php`, `ai_zadani_admin.php`, `pdf_prehled.php`, `pdf_data.php`

> AI vyhodnocení a PDF: Rada (celý svaz nebo libovolná jednotka), ÚS (sebe a své MO), MO (sebe). Zadání pro AI: admin.

- **AI vyhodnocení** – pro každou z 11 oblastí (známky, migrace, povolenky, brigády, navýšené ceny, kárná řízení, SHR, FRR, mimořádné známky, zápisné, další platby) krátký text: hodnocení a body „k prověření“.
- Postup: PHP spočítá **fakta** (vlastní čísla, meziroční srovnání ke stejnému dni, srovnání s ostatními jednotkami podle oprávnění – mediány a nejlepší / nejhorší, zjištěné nesrovnalosti) a **semafor** podle prahů v zadání – např. meziroční pokles, podíl storen, podezřelé platby na 1 000 známek, známky mimo ceník, nízká obnova členů, hromadné přesuny. AI z faktů jen napíše text; do pole „k prověření“ smí dát jen nesrovnalosti, které PHP opravdu zjistilo.
- Fakta pro MO neobsahují názvy jiných organizací, fakta pro ÚS názvy MO z jiných ÚS; osobní údaje se nepředávají.
- Hotové hodnocení se ukládá; nové se generuje tlačítkem, jen když se změnila data nebo zadání. Limit 20 generování denně na uživatele (admin bez omezení). Uživatelé mohou text ohodnotit; admin vidí podklady předané AI.
- **Zadání pro AI** (admin) je verzované v databázi: text zadání, prahy semaforu (JSON), vzorová odpověď; testovací běh pro libovolnou organizaci bez uložení (i jen podklady bez AI), obnovení starší verze, přehled zpětné vazby.
- **Přehled do PDF** – uživatel zvolí jednotku, sezónu a datum „k“. Obsah: příjmy podle oblastí (tržba, podíl, semafor), tabulka příjmů po ÚS (Rada) nebo po MO (ÚS), migrace členů (obnova po věkových kategoriích, ÚS podle obnovy / MO s nejnižší obnovou), prodané povolenky podle kódu, grafy a u každé oblasti AI hodnocení. Generuje se na pozadí jako úloha, stránka sleduje průběh; hotová PDF se stahují jen po kontrole oprávnění.
- **Sezóna a předprodej**: sezóna = rok, na který je platba určena (sloupec `rok` z exportu RIS), ne rok platby. Sezóna nemá spodní hranici data – předprodej (např. známka na 2027 prodaná v prosinci 2026) do ní patří. Datum „k“ proto může ležet i v roce před sezónou; meziroční srovnání je vždy „sezóna R do d. m. Y“ proti

„sezóna R−1 do stejného dne o rok dříve“. Navýšené ceny se řadí podle data platby od 7. 12. předchozího roku. Sezóna, jejíž rok ještě nezačal, se v AI i PDF bere jako probíhající (`ai_sezona_probiha()`), takže se neporovnává s celým loňským rokem.

- **Graf po měsících**: platby z doby před 1. 1. roku sezóny (předprodej, navýšení z prosince) mají vlastní první sloupec „pro 'RR“ (prosinec předchozího roku), u loňska obdobně; sloupec se kreslí jen tehdy, když v něm v jednom z obou let něco je. Je-li datum „k“ ještě před 1. 1. sezóny, letošní hodnoty jsou jen v tomto sloupci.

B6.5 Revíry – data a přepočet

`reviry/index.php`, `_lib.php`, `_data.php`, `_prodej.php`, `_rybari.php`, `_ceny.php`, `_historie.php`, `historie.php`, `cron_prepocet.php`, `prepocet_stav.php`

> Admin a Rada: vše. ÚS: své revíry a revíry svých MO, povolenky vydané jeho organizacemi. MO: své revíry a své povolenky. Revír patří hospodáři (vlastníkovi) podle E-Sumáře. Každou dlaždici může ÚS svým MO zakázat (kap. B6.15).

- Data jsou z E-Sumáře (povolenky, sumáře, denní záznamy, kontroly rybářské stráže) a z prodejů v RIS. Rok = rok povolenky.
- Předpočítávají se po celých letech: docházky a úlovky po revírech, úsecích a výdejcích povolenek (ks a kg celkem i po 25 druzích), rybáři s docházkou, dny (docházky, úlovek, kontroly), kontroly po odznacích strážců, zpracování sumářů po měsících, prodané × zpracované povolenky, chování rybářů (členství × povolenky) a ceny povolenek.
- Úloha přepočítá jen roky, ve kterých se E-Sumář změnil (podle poslední změny povolenek); admin může přepočet spustit z rozcestníku (změněné roky / vše) a sleduje průběh. Rozcestník ukazuje po letech zdroj, čas přepočtu, poslední změnu v E-Sumáři a trvání.
- **Kontroly RS** = záznamy kontrol na povolenkách (odznaky strážců), všude v modulu stejně. Počet kontrol zapsaný v sumáři je jen doplňkový údaj.
- **Prodané povolenky** se berou z prodejů v RIS (E-Sumář obsahuje i neprodané tiskopisy); se sumářem se párují podle čísla povolenky bez mezer.
- **Historie 2020–2024** ze starého systému (admin): párování revírů podle čísla, import docházek a úlovků po sezónách, protokol (součty ze zdroje, importováno, zahozeno). Pro historické roky se nezobrazují dny, kontroly ani výdejci.

B6.6 Revíry – stránky

Přehled prehled.php	Tři úrovně: svaz (územní svazy), ÚS (revíry ÚS a jeho MO + souhrn po organizacích), MO (revíry organizace). Ukazatele za sezónu proti loňsku: revírů, docházky, úlovek kg, kg na docházku, kontroly RS. Tabulka revírů (číslo, název, vlastník, povolenek, docházky, kg, výměra, kg/ha, podíl na úlovku), vývoj v letech, úlovek po druzích (ks, kg, změny, průměrná váha, podíl).
Detail revíru revir.php	Sezóna na jednom revíru: ukazatele, průběh sezóny po dnech (docházky a kontroly), dny v týdnu, měsíce, vývoj v letech, úlovek po druzích (průměrná váha kusu), největší úlovky, odkud rybáři jsou (výdejci povolenek), úseky revíru, rybářská stráž na revíru (odznak, kontrol, podíl, poslední kontrola, organizace strážce a stav jeho účtu v RIS).
Rybářská stráž straz.php, strazce.php	Kontroly, strážci, docházky, **kontrol na 100 docházek**, pokrytí revírů kontrolami; kdy se loví a kdy se kontroluje (dny v týdnu); strážci s počtem revírů, hlavním revírem, poslední kontrolou a stavem účtu v RIS; revíry s docházkou bez kontroly. Detail strážce: kontroly po revírech s podílem na kontrolách revíru, měsíce, dny v týdnu, vývoj v letech, kontroly po dnech.

Povolenky povolenky.php, povolenka.php	Pohled výdejce: vydáno, zpracováno (vrácený a zpracovaný sumář), s docházkou, docházky a úlovek, podíl na vlastních revírech; průběh zpracování sumářů po měsících; podle druhu povolenky prodáno × nezpracováno; kde rybáři s povolenkami rozsahu loví. Na úrovni ÚS a MO **seznam povolenek** s filtry (stav sumáře – zpracované, bez docházky, nezpracované prodané bez sumáře; platnost; revír) – číslo, prodejce, datum prodeje, eID kupujícího, zpracoval, docházky. Detail povolenky: revíry, úlovek po druzích, denní záznamy a kontroly RS (výdejce vidí celou, vlastník revíru jen záznamy ze svých revírů).
Kde lovili moji členové clenove.php	Docházky a úlovky na povolenky vydané jednotkou rozdělené podle vlastníka revíru: vlastní organizace / téhož ÚS / jiné ÚS, po územních svazech, po revírech a po druzích, proti předchozí sezóně.
Rybáři rybari.php	Z prodejů v RIS: kolik členů nemá povolenku, kolik má jen pstruhovou / jen mimopstruhovou / obě, podle věkových kategorií; kde členové povolenku koupili (doma / jen jinde, z toho v jiné MO téhož ÚS); matice členové ÚS × ÚS nákupu; kupující povolenek bez členské známky. Rozsah celý svaz nebo ÚS (MO vidí svůj ÚS).
Extrémní úlovky a docházky extremy.php	Top 10 povolenek podle úlovku (kg) a podle docházek a top 10 největších ryb každého druhu (hmotnost kusu = kg ÷ ks záznamu); dva pohledy – na revírech rozsahu, nebo u povolenek vydaných rozsahem. Podezřelé hodnoty (např. víc docházek, než je reálné) se označí k ověření zápisu.
Ceny povolenek, kalkulace ceny.php, kalkulace.php	Roční územní, celosvazové a celorepublikové povolenky: u každého druhu (oblast × MP/P × věková kategorie) prodáno, držitelů se sumářem, cena podle ceníku i průměrně zaplacená, průměrné docházky a kg a jejich hodnota podle hodnot z redistribuce (hodnota docházky, cena kg podle skupin ryb), poměr cena / hodnota a rozdělení držitelů do pásem. Kalkulace je simulace s vlastními hodnotami. Přístup: Rada vše, ÚS celosvazové a své územní.
Celkový přehled do PDF prehled_pdf.php, _prehled.php, ai_zadani.php	Šest oblastí – revíry a úlovky, rybářská stráž, povolenky a sumáře, rybáři a ceny povolenek, kde lovili členové, extrémy – s ukazateli, grafy, srovnáním s předchozí sezónou, AI hodnocením a **semaforem podle pevných pravidel**: docházky klesly o 5 % (žlutá) / 15 % (červená); intenzita kontrol pod 80 % / 50 % svazu, víc než 30 % revírů bez kontroly, připravenost RS pod 50 %; vrácenost sumářů pod 80 % / 60 %; růst podílu členů bez povolenky o 3 / 6 p. b.; podezřelé záznamy. Generuje se na pozadí. Libovolnou stránku modulu lze také exportovat do PDF.

B6.7 Členové – rozcestník sestav a analytika členské základny

`clenove/index.php`, `clenove_lib.php`, `demografie.php`, `ucast_brigady.php`, `ucast_brigady_lib.php`, `ucast_brigady_vysledek.php`, `ucast_brigady_pdf.php`, `prezencni_listina.php`, `prezencni_listina_lib.php`, `prezencni_listina_pdf.php`, `podezrele.php`, `podezrele_lib.php` (vše ve složce `clenove/`); `members_import.php`, `members_souhrn.php`, `migration.php`

Rozcestník **Členové** (`clenove/index.php`) sdružuje sestavy o členech pro potřeby MO. Má čtyři dlaždice: Vyhodnocení účasti na brigádách, Demografické údaje, Prezenční listina členské schůze a Podezřelé členské záznamy. Nepřihlášeného pošle na přihlášení a po něm zpět na stránku ve složce (`clen_require_login`). Sestavy kromě demografie čtou data **živě z rozhraní REST RIS** (technický účet stejný jako u konfigurací příspěvků), nic neukládají a organizaci hledají v RIS podle `keepers.ris_sid` – organizace bez jednoznačného `ris_sid` nelze načíst.

> Sestavy z RIS (brigády, prezenční listina, podezřelé záznamy): MO jen sebe, ÚS výběr ze svých MO, Rada a admin všechny organizace (+ surová data z RIS pro kontrolu). Rozsah přes `crs_scope.php`, cizí organizace → 403.

Vyhodnocení účasti na brigádách

- Za organizaci a rok seznam brigád (`ft_brigada`; filtr `at_akce_rf_mistniOrganizace`, rok podle `at_brigada_rokVykonaniBrigady`, jinak z termínu akce) a ke každé účastníci (`ft_ucastnikBrigady`) s plánovanými a odpracovanými hodinami; **souhrn hodin po osobách**.
- Účastníci se načítají **pro každou brigádu samostatným dotazem** – RIS z více dotazů v jednom požadavku `_query` vyřídí jen první. Atribut vazby (`rf_brigada` / `rf_akce`) se určí podle první brigády s účastníky; celkový limit 150 s.
- Stránka se zobrazí hned s **lištou průběhu**; sestava se dotáhne AJAXem (`?fragment=1`, výsledek v `ucast_brigady_vysledek.php`). Průběh (seznam brigád, účastníci brigáda i z n) se zapisuje do dočasného souboru pod náhodným tokenem a lišta ho čte přes `?prubeh=`; session se během načítání uvolní.
- **Export do PDF** (`ucast_brigady_pdf.php`, Dompdf): souhrnné karty, přehled brigád, souhrn po osobách s pruhy odpracovaných hodin a detail každé brigády s účastníky. Sestava byla dříve ve složce `brigady/` (tam zůstává jen kontrola nastavení, kap. B6.11).
- Data z RIS se převádějí z milisekund vždy (dřívější odhad sekundy / milisekundy dával nesmyslná data narození u osob narozených 1966–1973); datum bez časové zóny se čte v pražském čase.

Prezenční listina členské schůze

- Za MO a den schůze osoby z `ft_fyzickaOsoba` se stavem člena „člen“ (`at_fyzickaOsoba_cl_stavClenaCrs`, záložně z `ft_clenCrs`) v **kategorii dospělí** – v kalendářním roce schůze dosáhnou aspoň 19 let (rok schůze − rok narození ≥ 19, den narození nerozhoduje).
- Seznam s eID, datem narození, věkem v roce schůze, ke dni schůze a podle RIS; volba zobrazit i osoby, které na listinu nepatří. **Export do CSV** (středník, UTF-8 s BOM) pro porovnání s RIS podle eID. Pod seznamem diagnostika (kolik osob RIS vrátil, použité atributy, rozložení stavů člena), pro Radu surový první záznam.
- **Záznamový arch do PDF** (`prezencni_listina_pdf.php`): záhlaví s datem a místem konání, počet členů s právem účasti, nadpoloviční většina, prázdná pole pro počet přítomných a kvorum, seznam podle příjmení s místem na podpis a ověření listiny na konci. Seznam se skládá po stranách ze samostatných tabulek a logo je PNG, takže PDF zvládne i velké MO (3 000 osob cca 10 s a 290 MB paměti; limit 1 GB, při fatální chybě čitelná hláška).
- Na rozdíl od generátoru prezenčních listin v Nástrojích (kap. B5.16) nepotřebuje ruční export členské základny; generátor zůstává pro listiny rozdělené po místních skupinách.

Podezřelé členské záznamy

- Na tlačítko **Spustit kontrolu** se načtou všechny osoby organizace z RIS (stejně jako pro prezenční listinu, bez filtru na členy) a vyhodnotí se kritéria z `podezrele_lib.php`. Zjištění mají dvě úrovně: **podezřelé** (k opravě, červeně) a **k prověření** (může být v pořádku, oranžově); podezřelé se řadí první. Souhrnné karty: zkontrolováno osob, podezřelých, jen k prověření a počet nálezů podle kritérií.
- Kritéria: **datum narození** – chybí, je v budoucnosti, věk pod 5 nebo nad 95 let; **přehozené jméno a příjmení** – jiná osoba se stejným datem narození a navzájem přehozeným jménem a příjmením (bez diakritiky a velikosti písmen); **tituly a zvláštní znaky** – titul (Ing., Bc., Mgr., MUDr., Ph.D. … jako celé slovo) nebo jiné znaky než písmena, mezera a pomlčka; apostrof a dvojitá mezera jen k prověření; **možná duplicita** – jiná osoba s jiným eID, stejným jménem a příjmením (i přehozeným) a stejným nebo velmi podobným datem narození (jedna jiná číslice, prohozené sousední číslice, prohozený den a měsíc).

- U nálezu odkaz **upravit osobu v RIS** (správa členské základny, fulltext podle eID). Nové kritérium = nový záznam v `podez_kriteria()` s funkcí, která dostane osobu, datum a kontext se všemi načtenými osobami.

Demografické údaje (analytika členské základny)

> Admin: celý svaz s filtrem ÚS a MO. ÚS: sebe s filtrem na své MO. MO: sebe. Import členské základny: admin. Původní adresa `analytics.php` přesměrovává na `clenove/demografie.php`; nápověda stránky se převede na novou adresu.

- Filtr: rok, ÚS, MO. Ukazatele: **věkový průměr a trend** proti předchozímu roku a celosvazový průměr, **věková struktura**, **členské kategorie** (děti, mládež, dospělí), **poměr žen a mužů** a **aktivace účtů RIS**. U každé části je uvedeno, z jakého zdroje a k jakému datu je.
- Věk, struktura, kategorie a počet členů se počítají z prodejů (osoby se zaplacenou členskou známkou, storna odečtena) – na úrovni ÚS a svazu se člen platící ve více organizacích počítá jednou. Roky bez prodejních dat se berou z dřívější evidence členů po osobách.
- Pohlaví a aktivace účtů RIS jsou jen v **souhrnu členské základny z RIS** (organizace × pohlaví × aktivace → počet, bez osobních údajů). Import: nahrání CSV a roku → náhled párování organizací → potvrzení nahradí data roku. Členem je v RIS i ten, kdo má schválenou přihlášku a ještě nezaplatil – počty se proto mohou lišit od počtů z prodejů.
- Starší stránka `migration.php` ukazuje migraci podle dřívější evidence po osobách; aktuální migrace je v prodejích (kap. B6.3).

B6.8 Kontrola platnosti povolenek

`ulovky_problemy.php` (organizace), `ulovky_pytlaci.php` (celá ČR), `ulovky_kontrola.php` (kontrola dat)

> ÚS: chyby na svých revírech, na revírech svých MO a u povolenek, které vydal on nebo jeho MO. MO: jen záznamy, kde je výdejcem povolenky, nebo hospodaří na dotčeném revíru. Celostátní pohled a kontrola dat: přihlášený admin, Rada a ÚS (MO ne). ÚS v celostátním pohledu vidí jen nálezy, kde povolenku vydal on nebo jeho MO, nebo kde se lovilo na revíru jeho či jeho MO; kontrolu dat má jen za sebe.

- Prochází zápisy úlovků v E-Sumáři (povolenka × revír) za sezónu a hledá dva typy chyb: **chybná územní platnost** – územní povolenka, se kterou se lovilo na revíru jiného ÚS, než pro který platí; **chybný režim** – mimopstruhová povolenka na pstruhovém revíru nebo naopak.
- U každého nálezu: povolenka (číslo, druh, územní platnost), výdejce a kdo zápis provedl, revír, kdo na revíru hospodaří, zapsané úlovky, druh chyby. Filtr podle typu chyby; celostátní verze navíc podle ÚS výdejce a ÚS revíru.
- Výsledek slouží k dohledání chybně zapsaných sumářů i skutečného lovu bez platné povolenky.
- **Kontrola dat** (Rada a admin po výběru ÚS, ÚS za sebe): extrémní počet docházek na jednom revíru (typicky přepsané číslo revíru do pole docházek) a anomálie hmotnosti úlovků – příliš nízká či vysoká průměrná váha kusu, v ročních součtech i v denních záznamech.

B6.9 Návratnost povolenek

`ztracene_povolenky.php` (organizace), `analytika_povolenek.php` (admin)

> Rada a admin: vše; import čísel vrácených povolenek jen admin. ÚS: povolenky vydané jeho organizacemi. MO: povolenky, které vydala.

- Admin nahraje z RIS CSV s čísly **odevzdaných povolenek** (rybář povolenku vrátil). Ukazatele: celkem importováno, zpracováno MO (v pořádku), nepotvrzeno (k analýze).

- Kontrola porovná nevyřešená čísla s E-Sumářem: povolenka, která už má zpracovaný sumář, se automaticky označí jako vyřešená a z přehledu zmizí; zbývající jsou odevzdané povolenky, které organizace do E-Sumáře nezadala.
- Filtr podle druhu (celosvazové a celorepublikové, územní, revírní a ostatní). Přehled podle ÚS (ztraceno a procento chyb) a podle MO se **seznamem čísel** nezpracovaných povolenek – organizace tak ihned vidí, které vrácené povolenky zapomněla zadat.

B6.10 Aktivace účtů rybářské stráže

`rs_aktivace.php`, `rs_import.php`, `rs_lib.php`

> Rada a admin: přehled všech ÚS a detail kteréhokoli ÚS. ÚS: svůj svaz. MO přístup nemají. Import stavu: admin.

- Zdroj: export z RIS – řádek = průkaz rybářské stráže (organizace, eID, číslo průkazu, stav aktivace účtu RIS). Import: náhled párování, potvrzení nahradí stav; uchovává se poslední stav a historie importů. Počítá se po osobách (kdo má víc průkazů, je jeden strážce).
- **Aktivované účty**: podíl strážců ÚS (včetně MO) s aktivovaným účtem RIS, pořadí mezi ÚS, graf srovnání ÚS, rozpad po organizacích (strážců, aktivovaných, bez aktivace, %) a seznam strážců bez aktivace (organizace, eID, průkaz, stav, počet kontrol) – podklad pro oslovení.
- **Připravenost RS na využívání aplikace**: kontroly zapsané v E-Sumáři se párují na průkazy podle čísla odznaku a dělí na kontroly strážců s aktivovaným účtem a bez něj – za všechny roky nebo vybraný rok, po ÚS podle revíru. Pro Radu srovnání připravenosti ÚS a rozpětí mezi ÚS.

B6.11 Brigádnická povinnost a členské příspěvky MO

`brigady/index.php`, `detail.php`, `import.php`, `brigady_lib.php`, `brigady_ris.php`, `kontrola_lib.php`, `prispevky_lib.php`, `prispevky_ris.php`

> Rada a admin: všechny organizace s filtrem ÚS a kritéria. ÚS: své MO. MO: rovnou detail své organizace. Import: Rada a admin.

- **Nastavení brigádnické povinnosti** se načítá **přímo z rozhraní RIS** (`brigady_ris.php`, `ft_konfiguraceBrigadnickePovinnosti` – rok, MO, věková kategorie, hodiny, sazba; skupina osob `ft_skupinaClenuCrs` – věk, pohlaví, příznaky student / ZTP / ZTP/P, brigády splněny, „funkce definovány v RIS“). Skupiny se drží v trvalé lokální kopii (`brig_ris_skupiny`); při každém načtení se z RIS jedním dotazem vezmou jen skupiny změněné od minulého načtení (s překryvem 30 minut) a chybějící. Když RIS filtr podle data změny nepřijme, kopie zůstane a stránka varuje; admin může kopii načíst celou znovu. Podmínění rolí se bere jen jako ano / ne (skupinu zužují funkce).
- **Postup importu**: náhled z RIS s porovnáním proti uloženým datům (počet spárovaných a nespárovaných organizací, rozdíly i se surovými daty) → tlačítko **Uložit do databáze** s potvrzením. Uložení stáhne data znovu, projde stejnou kontrolou, páruje na MO a nahradí data roku; uložit nelze při neúplně načtených skupinách, chybných záznamech nebo bez spárovaných MO. Dlouhé čekání na RIS je ošetřené – po komunikaci s RIS se ověří a případně obnoví spojení s databázemi; místo prázdné chyby 500 se vypíše fatální chyba. CSV export „analytika brigád“ z Oracle Analytics a diagnostika zůstávají jako záložní cesta ve sbalených sekcích.
- **Konfigurace členských příspěvků** (mimořádný příspěvek, zápisné, snížené zápisné pro děti, mládež/ZTP a dospělé) se načítá z RIS (`prispevky_ris.php`, `ft_konfiguraceClenskyPrispevek`) stejným postupem náhled → uložení; ruční import CSV pro příspěvky byl zrušen. Technický účet RIS je v `config_straz.php` (vlastní účet

`PRISP_RIS_*`, jinak účet stráže).

- **Kontrolní kritéria** (každé zjištění má závažnost, údaj, kterého se týká, popis a doporučené řešení v RIS):
  1. chybí nastavení pro dospělé nebo mládež (problém),
  2. pohlaví „Neurčeno“ – skupina nezahrne muže ani ženy (problém),
  3. vyplněné „Brigády splněny“ – zúží skupinu jen na ty, kdo brigádu (ne)splnili (problém),
  4. souběh příznaků student / ZTP / ZTP/P – podmínky se kombinují jako „a zároveň“ (problém),
  5. skupina bez omezujících podmínek – platí pro všechny osoby organizace (problém),
  6. věk od / do – stejné hodnoty (problém), podezřelá spodní hranice (varování),
  7. chybí konfigurace členských příspěvků na sezónu (problém),
  8. extrémní hodnoty – sazba nad 1 500 Kč/h, víc než 25 hodin, zápisné nad 3 000 Kč (varování).
- Přehled organizací s celkovým hodnocením (zelená / oranžová / červená), počty problémů a varování a řádků nastavení; filtr podle kritéria. Detail organizace: připravenost na sezónu (členské příspěvky), nastavení brigád s obarvenými buňkami a zjištění s doporučeným řešením.

B6.12 Přehled přihlášení

`prihlaseni_prehled.php`, `prihlaseni_lib.php`

> Jen admin.

- Každý pokus o přihlášení (i neúspěšný) se zapisuje se způsobem přihlášení (účet RIS, E-Sumář, lokální účet), účtem, eID, jménem, rolí, organizací a IP. U přihlášeného se průběžně posouvá čas poslední aktivity.
- **Právě aktivní** – uživatelé s aktivitou za posledních 15 minut (uživatel, organizace, kdy se přihlásil, naposledy aktivní).
- **Uživatelé podle způsobu přihlášení** za zvolené období (7, 30, 90, 365 dní): počet přihlášení a unikátních uživatelů – uživatel se počítá jednou za způsob přihlášení, u účtu RIS podle eID; ukazuje postup převodu účtů na RIS.
- **Podle územních svazů a Rady** – sloupcový graf unikátních uživatelů za celou uchovávanou historii podle organizace, pod kterou se přihlásili (MO se přičítají ke svému ÚS), sloupce rozdělené podle způsobu přihlášení; pod sloupcem počet přihlášení.
- Vývoj po dnech (přihlášení a uživatelé), poslední přihlášení s výsledkem a označením převedených účtů, počet neúspěšných pokusů za 7 dní, upozornění, když je vyžadování převodu na RIS vypnuté.

B6.13 Redistribuce CS/CR povolenek

`redistribuce_rozcestnik.php`, `redistribuce.php`, `redistribuce_predikce.php`, `redistribuce_nastaveni.php`, `redistribuce_prijmy.php`, `redistribuce_prijmy_prehled.php`, `redistribuce_pristup.php`, `import_predikce.php`

> Přehledy: ÚS a Rada. Nastavení, ceníky a import predikce: Rada a admin. Typ organizace se určuje z číselníku organizací.

- Rozdělení příjmů z celosvazových a celorepublikových povolenek mezi územní svazy ve třech složkách: **za výměru** revírů, **za docházky** cizích rybářů na revírech ÚS (matice docházek ÚS revíru × ÚS vydavatele a jejich finanční vyjádření) a **za úlovky** podle cenových skupin ryb (matice po skupinách).
- **Nastavení roku**: základní parametry, skupiny ryb a ceny za kilogram, zařazení druhů do skupin, dopočet výměr revírů (bez MRS); **ceníky a prodeje** CS/CR a územních povolenek (příjmová část) a jejich přehled pro ÚS.

- **Předběžná analytika**: odhad rozdělení fondu během sezóny podle predikční křivky prodejů (import křivky adminem).
- Hodnoty z nastavení používají i ceny povolenek v modulu Revíry a orientační rozdělení příjmů v prodejích.

B6.14 Starší přehledy z E-Sumáře

`dashboard.php`, `takes*.php`, `take_*.php`, `rangers*.php`, `reports*.php`, `report_district.php`, `statistika_*.php`

- Původní přehledy, které běží souběžně s modulem Revíry a čtou z E-Sumáře živě: dashboard zpracovaných a nevyplněných povolenek, přehled a detail povolenek (i za podřízené MO), denní docházky, aktivita rybářské stráže (i regionálně), statistické reporty a detail revíru, statistiky úlovků po druzích a revírech s meziročním srovnáním a dlouhodobým průměrem.
- Funkčně je pokrývá modul Revíry (kap. B6.5–B6.6); po ověření je lze vyřadit.

B6.15 Práva místních organizací (řízení územním svazem)

`analytiky_pristup.php`, `analytiky_lib.php`, `ucty_prihlaseni.php`

> Nastavuje správce nastavení ÚS (funkce RIS č. 61; u původního přihlášení účet ÚS), každý jen za svůj ÚS; admin (vystupující za Radu) může upravovat nastavení kteréhokoli ÚS, ostatní v Radě ho jen prohlížejí. Omezení se týká jen místních organizací – admina, Radu ani ÚS neomezuje.

- Jedno místo pro všechno, co ÚS svým MO povoluje (dříve dvě oddělená nastavení – práva skupin RIS v modulech a zákazy analytik). Stránka „Práva místních organizací“ (dlaždice „Práva MO“ v nabídce Správa).
- **Moduly** Objednávky, Úkoly, Formuláře, Rezervace a Žádosti o hájení: úroveň *vidět a vyplňovat* (výchozí), *jen vidět* nebo *nevidí*.
- **Analytické dlaždice** po skupinách: **Prodeje** (celkové prodeje, AI vyhodnocení, přehled do PDF, povolenky, známky, migrace, brigády, navýšené ceny, kárná řízení, fondy SHR a FRR, mimořádné známky, zápisné, další platby), **Revíry** (přehled a detail revíru, rybářská stráž, povolenky, kde lovili moji členové, extrémy, rybáři a povolenky, celkový přehled do PDF) a **Platby** (výpis plateb). Úroveň *přístupná* (výchozí) nebo *nepřístupná*.
- U každé položky ÚS nastaví **výchozí úroveň pro všechny MO svého ÚS** a může přidat **výjimky – skupiny funkcí RIS** (skupiny Rady i ÚS, kap. B4.3) s vlastní úrovní (např. MO modul jen vidí, hospodáři ho smějí vyplňovat; revíry nepřístupné, hospodářům přístupné). Z výchozí úrovně a výjimek všech skupin uživatele platí nejvyšší. Ukládají se jen změněné položky a u nich kdo a kdy změnu zadal.
- Nastavení platí pro každého, kdo vystupuje za MO, bez ohledu na způsob přihlášení (účet RIS, E-Sumář, lokální účet). Výjimka se posuzuje podle skupin, do kterých uživatel patří v organizaci, za kterou právě vystupuje.
- Kontrola je zapojená do každé stránky dlaždice včetně podstránek a detailů (po dnech, transakce, seznamy osob, detail revíru, povolenky, strážce, PDF), takže zákaz nejde obejít přímou adresou. Uživatel dostane hlášku „Váš územní svaz rozhodl…“ se jménem toho, kdo zákaz zadal, a datem; na rozcestnících prodejů a revírů má zakázaná dlaždice zámek. V modulech se nepřístupný modul skryje z rozcestníku i úkolů a u „jen vidět“ se odeslaný formulář zahodí.
- Tabulka `mo_prava` (ÚS × položka: úroveň, výjimky pro skupiny, kdo a kdy). Dřívější zákazy analytik (`analytiky_zakazy`) se do ní převedly automaticky; dřívější práva skupin v modulech se nepřevádějí (měla opačný smysl – ÚS je nastaví znovu).

B6.16 Kontroly rybářské stráže z RIS

`straz/index.php`, `reviry.php`, `revir.php`, `strazni.php`, `prestupky.php`, `mapa.php`, `vykaz.php`, `prehrat.php`, `odznaky.php`, `strazni_mo.php`, `sync.php`, `_lib.php`, `_data.php`, `_dim.php`, `_mapa.php`; `cron_straz.php`, `config_straz.php` (mimo repozitář)

> Admin a Rada: vše. ÚS: kontroly a obchůzky na svých revírech a na revírech svých MO. MO: jen na svých revírech. O příslušnosti rozhoduje **hospodář revíru** podle E-Sumáře (`districts.keeper_id`), ne organizace stráže. Přístup MO řídí ÚS přes dlaždici „Rybářská stráž“ (kap. B6.15). Synchronizace, odznaky a diagnostika: jen admin. Domovskou MO stráže (výchozí podle RIS) může změnit Rada (všem) a ÚS (strážím s MO podle RIS v ÚS nebo s činností na jeho revírech, jen na MO svého ÚS); ruční přiřazení má přednost před RIS a používá se ve filtru „Domovská MO“.

- **Zdroj**: kontroly, obchůzky a přestupky zapsané strážemi v mobilní aplikaci RIS. Rozcestník je načítá rozhraním RIS **pouze ke čtení** (dotaz `_query` s filtrem na datum, dávky do 5 000 záznamů) a ukládá do vlastních tabulek; stránky pak pracují jen s lokální kopií. Data se načítají od 1. 8. 2026.
- **Synchronizace**: denně cronem (`cron_straz.php`, klouzavé okno posledních N dní, výchozí 7) a ručně adminem (`straz/sync.php` – průběh po krocích, chyba jednoho kroku nezastaví ostatní). Záznamy se ukládají podle stabilního identifikátoru RIS (`sid`), opakované stažení je přepíše, nic se nezdvojí. Přestupky se dotahují **inkrementálně** jen u kontrol s výsledkem „zjištěno pochybení“, které ještě nebyly zpracované; každý vrácený přestupek se ověří, že opravdu patří k dané kontrole (cizí záznamy se zahodí). Každý běh se zapisuje do logu synchronizace.
- **Napojení na revír**: identifikátor vodní oblasti z RIS se páruje na revír nebo část revíru v E-Sumáři (`ris_sid`), záložně podle čísla revíru v názvu. Kontrola bez napojeného revíru nemá hospodáře, a proto ji vidí jen admin a Rada.
- **Strážní a odznaky**: stráž se identifikuje identifikátorem RIS. Číslo odznaku se bere v pořadí: číselník stráže z RIS (`straz_straznici.odznak`) → ruční doplnění adminem → E-Sumář (`badge_numbers`) jako pojistka; společné funkce `straz_odznaky_zdroje()` a `straz_odznak()` používá přehled odznaků i výkaz. Přehled odznaků ukazuje i stav v RIS, datum ukončení a MO; ruční doplnění jen u strážích bez odznaku z RIS.
- **Typ stráže a domovská MO**: všechny přehledy (index, revíry, detail revíru, strážní, přestupky, mapa, výkaz, přehrání dne) mají filtr typu stráže (zařazení z RIS, parametr `rs_typ`) a domovské MO (`rs_mo`), včetně volby „bez údaje“; filtruje se přes číselník `straz_straznici`. Nabídka obsahuje jen hodnoty strážích v rozsahu práv uživatele (s počty) a filtr se přenáší v odkazech mezi přehledy. Bez staženého číselníku se pole nezobrazí. Domovská MO je efektivní: ruční přiřazení (`straz_mo_rucni`) má přednost před MO z RIS; MO z RIS se páruje přes `mo_ris_sid` na `keepers.ris_sid` a názvy se sjednocují podle E-Sumáře.
- **Činnosti mimo revír**: technický revír v RIS číslo **8999999** („Činnosti mimo revír“), na který stráž vykazuje obchůzky mimo revíry (přejezdy apod.). V E-Sumáři nemá hospodáře, rozpoznává se podle čísla v názvu (`straz_tech_sql()`) a ve výkazu má pseudo-revír 0. Ve výkazu ho uživatel vidí u strážích, které měly za poslední rok kontrolu nebo obchůzku na jeho revírech (`straz_filtr_s_tech()`); Rada a admin vždy. Započítává se normálně do součtů, ve výstupu po revírech je u každé stráže první se žlutým podkresem (i v PDF). V přehledu revírů a strážních se zatím nezobrazuje.

Přehled index.php	Souhrn za období (kontroly, v pořádku, pochybení, zadržené povolenky a udice, lov bez povolenky, počet strážích), graf po dnech a rozcestník dlaždic. Graf kontrol po územních svazech vidí všichni (jen počty za ÚS, bez detailu), vlastní ÚS je zvýrazněný.
Po revírech, detail revíru reviry.php, revir.php	Kontroly, pochybení a povolenky po revírech s filtrem období a stráže; detail revíru se souhrnem, mapou, strážemi, přestupky podle druhu, vývojem po dnech a výpisem kontrol (odkaz do RIS).

Po strážných strazni.php	Činnost jednotlivých stráží, proklik na jejich kontroly po revírech.
Číselník přestupků prestupky.php	Druhy kárných provinění z RIS s četností; číselník se drží v databázi a doplňuje se z nově stažených přestupků. Proklik na mapu a výpis kontrol s daným přestupkem.
Mapa kontrol mapa.php	Kontroly na mapovém podkladu OpenStreetMap (Leaflet), barvy podle výsledku, seskupování bodů, filtr období, stráže, revíru a výsledku.
Výkaz o činnosti RS vykaz.php	Podklad pro výkaz: výběr stráží a revírů (všechny / jen vybrané / všechny kromě), výstup souhrnně nebo po revírech – obchůzky, hodiny, kontrolní dny, kontroly, výsledky, zadržené povolenky a udice, přestupky; export CSV a PDF. Zahrnuje „Činnosti mimo revír“ (8999999, žlutě, vždy první); filtr typu stráže a domovské MO se ukazuje štítky v hlavičce.
Domovská MO stráže strazni_mo.php	Seznam stráží s MO podle RIS a efektivní domovskou MO, změna MO nebo návrat „podle RIS“, kdo a kdy změnil, historie změn (`straz_mo_historie`). Admin a Rada: všem strážím na libovolnou MO (mimo MRS a jednotky mimo ČRS); ÚS: strážím s MO podle RIS (či ruční MO) v ÚS a strážím s činností na revírech ÚS, jen na MO svého ÚS; MO bez přístupu. Synchronizace ruční přiřazení nepřepisuje.
Přehrání dne prehrat.php	Časosběr vybraného dne na mapě: kontroly přibývají podle času, kontroly téže stráže propojuje čára se šipkami, deník zahájení a ukončení obchůzek.

> **Bezpečnost modulu.** Rozsah viditelných revírů se počítá na serveru z přihlášení (Rada / ÚS / MO podle organizace, za kterou uživatel z RIS vystupuje) a promítá se do každého dotazu jako seznam povolených revírů; výběry v adrese (revír, stráž, druh přestupku) ho jen dál zužují. Detail revíru mimo rozsah vrátí „nemáte oprávnění“. Účet RIS pro synchronizaci zadává admin při ručním běhu (neukládá se), pro cron je v `config_straz.php` mimo repozitář; cron přes web vyžaduje token. Rozhraní RIS se volá jen ke čtení přes HTTPS. Formuláře měnící data (ruční odznaky, domovská MO, synchronizace) jsou chráněné CSRF tokenem.

B7. Datový model

Lokální databáze rozcestníku – hlavní skupiny tabulek (aplikace sama zakládá 160 tabulek, další – starší – byly založeny ručně):

Tabulky	Obsah	Zdroj
`local_users`, `ucty_parovani`, `ris_spravci`, `ris_blokovane`, `ris_skupiny*`, `ris_funkce_ignorovane`, `mo_prava`, `prihlaseni_log`	Lokální účty, párování účtů s eID, správci, blokované osoby, skupiny funkcí RIS, práva místních organizací nastavená ÚS, log přihlášení	rozcestník
`news`, `news_confirmations`, `tiles`, `page_helps`, `admin_notes`	Aktuality a potvrzení přečtení, dlaždice, nápovědy ke stránkám	správa
`tasks`, `task_completions`, `forms`, `form_fields`, `form_responses`, `form_answers`, `reservation_topics`, `reservation_days`, `reservation_slots`, `reservation_bookings`	Úkoly a jejich plnění, formuláře a odpovědi, rezervační kalendáře	rozcestník
`mail_logs`, `mail_inbox_*`	Log rozeslaných e-mailů, schránka	rozcestník
`notif_odber`	Nastavení e-mailových notifikací (Moje notifikace): účet, organizace, oblast, zapnuto / vypnuto, e-mail a jméno v době změny	uživatel

Tabulky	Obsah	Zdroj
doc_nodes, doc_node_keepers, doc_categories, doc_items, metodika_*, manual_*, crs_sys_docs, dokumentace_verze	Správce dokumentů, návody, metodika, uživatelská a systémová dokumentace, verze této dokumentace	správa
hajeni_zadosti, hajeni_zadosti_casti, hajeni_zadosti_historie, hajeni_duvody	Žádosti o hájení, části revíru, historie stavů, číselník důvodů	MO, ÚS
helpdesk_tickets, helpdesk_messages, helpdesk_attachments, support_*	Dotazy helpdesku, kontakty podpory	rozcestník
navrhy, navrhy_prilohy, navrhy_komentare	Návrhy na úpravu mocrs.cz, jejich přílohy a komentáře	rozcestník
shop_items, shop_item_images, shop_categories, shop_orders, shop_order_items, shop_order_changes, shop_org_details	Sklad, objednávky, změny objednávek, dodací údaje	rozcestník
sales_transactions, sales_import_batches, sales_agg_*, sales_znamky_podezrele, sales_clenove, sales_prechody*, sales_zapisne*, sales_brig_*, sales_deti_zdarma*, sales_org_us, jp_*, prepocet_fronta, prepocet_stav, pdf_ulohy	Transakce z RIS a dávky importu, denní a souhrnné součty, podezřelé platby, členství a přechody po osobách, zápisné, brigády, děti zdarma, kategorie jiných plateb, fronta přepočtu, úlohy PDF	RIS (import)
ai_zadani, ai_vyhodnoceni, ai_zpetna_vazba, ai_chat_log, zp2_ai_log	Verzovaná zadání pro AI, uložená hodnocení, zpětná vazba, logy asistenta a návrhů textů	rozcestník
rv_*	Předpočítané souhrny revírů (docházky, dny, odznaky, výdejci, zpracování), prodané × zpracované povolenky, chování rybářů, ceny povolenek, cache extrémů, historie, úlohy PDF	E-Sumář, RIS (přepočet)
stats_*, district_areas, returned_permits	Statistiky úlovků po revírech a druzích, výměry revírů, ceníky a parametry redistribuce, predikce prodejů, vrácené povolenky	E-Sumář, RIS, správa
members_*, rs_stav*, brig_*, contacts_officials, offenses, fish_stocking_plans, fish_catch_mapping, znamky_cenik	Členská základna, stav rybářské stráže, brigády a příspěvky (včetně trvalé kopie skupin členů z RIS brig_ris_skupiny), funkcionáři, přestupky, zarybnění, ceník členských známek	RIS (import, čtení API), správa
pov_storna, pov_storna_historie, pov_storna_urgence, pov_storna_sync_log	Žádosti o storna povolenek: aktuální stav povolenky (číslo, prodejce, eID a jméno držitele, typ, platnost, datum a důvod storna), přechody mezi stavy, urgence ÚS, log synchronizací	RIS (čtení API)
straz_kontroly, straz_obchuzky, straz_prestupky, straz_cis_provineni, straz_odznaky_rucni, straz_sync_log, straz_straznici, straz_mo_rucni, straz_mo_historie	Kontroly rybářské stráže (datum, výsledek, příznaky, GPS, revír, stráž, obchůzka, číslo povolenky; bez údajů o kontrolované osobě), obchůzky (začátek, konec, revír, stráž), přestupky ke kontrolám, číselník druhů kárných provinění, ručně doplněná čísla odznaků, ručně přiřazená domovská MO stráže a historie jejích změn, log synchronizací; straz_straznici = číselník stráže z RIS (odznak, typ / zařazení, domovská MO; stahuje se po jednotlivých strážích, RIS dotaz bez filtru nepodporuje)	RIS (čtení API)

Tabulky	Obsah	Zdroj
`fish_seed_*`, `crs_hatcheries`, `crs_hatchery_production`	Produkce rybích násad, číselník kategorií, líhně a jejich produkce	ÚS
`comgate_payments`, `comgate_transfers`, `comgate_report_*`, `mo_ico_map`	Platby a převody Comgate, příjemci a log rozesílky výpisů, IČO organizací	Comgate
`zp2_*`; `report_chapter*`, `custom_report*`, `sport_*`	Zpráva o činnosti: kapitoly, bloky, řešitelé, tabulky ÚS, sport; tabulky původní verze slouží jako zdroj pro převzetí	rozcestník

Databáze E-Sumáře se jen čte: `keepers` (organizace a hierarchie), `users` (původní účty), `districts`, `district_parts` (revíry a jejich části), `takes`, `take_districts`, `take_details`, `take_checks` (povolenky, docházky, úlovky, kontroly). Spojení mezi databázemi nejde dělat SQL JOINem – vazby se skládají v PHP. Osoba se napříč zdroji identifikuje **eID** z RIS.

B8. Plánované úlohy a přepočty na pozadí

Úloha	Co dělá	Doporučený běh
`cron_comgate.php`	Import výpisů převodů a plateb z Comgate (bez parametru za včerejšek, jinak za zadané datum)	v noci, denně
`cron_comgate_reports.php`	Rozesílka denních výpisů organizacím (volitelně za zadané datum)	ráno po importu
`prodeje/cron_prepocet.php`	Fronta přepočtu prodejů, kroky migrace, úlohy PDF přehledů prodejů	každých 5 minut
`reviry/cron_prepocet.php`	Přepočet souhrnů revírů za roky se změnami v E-Sumáři (volba „vše“), úlohy PDF přehledů revírů	každé 2 hodiny
`cron_straz.php`	Načtení kontrol, obchůzek a přestupků rybářské stráže z RIS (jen čtení) za posledních N dní (`STRAZ_SYNC_DNI`)	v noci, denně
`cron_storna_povolenek.php`	Načtení povolenek ve stavu „Požádáno o storno“ a „Stornovaná“ z RIS (jen čtení) za předchozí, aktuální a následující rok, zápis přechodů mezi stavy a zamítnutých žádostí, e-mail odběratelům o nových žádostech; token a účet RIS v `config_straz.php`, adresa aplikace pro odkazy v e-mailu volitelně `MOCRS_PUBLIC_URL` v `config_mail.php` (výchozí `https://mocrs.cz/main/`)	1× denně

Úlohy se spouštějí z příkazové řádky, nebo přes URL s tokenem z konfigurace. Když není co dělat, skončí okamžitě; když už běží jiný přepočet, také (zámek v databázi). PDF přehledy a dlouhé přepočty spouští i stránka sama na pozadí (odpověď se odešle, PHP pokračuje) a sleduje průběh dotazy na stav; cron je záložní cesta, když server spuštění na pozadí nedovolí.

B9. Bezpečnost a ochrana osobních údajů

- Přihlášení účtem RIS – hesla RIS se v rozcestníku neukládají, ověřuje je knihovna účtů. Původní účty mají hesla jako hash (`password_verify`) a po převodu na RIS se e-mailem už nepřihlásí.
- Rozsah dat podle organizace se počítá na serveru ze session (`crs_scope.php`), parametry z adresy jsou jen přání – MO vidí vždy jen sebe, filtr ÚS smí jen admin, výběr MO se ověřuje proti MO vlastního ÚS a uživatel

bez platné organizace nevidí nic. Práva MO nastavená územním svazem se vynucují i při odeslání formuláře a na každé podstránce analytik (bez práva se POST zahodí).

- Dotazy do databáze parametrizované, výstupy escapované, **všechny formuláře chráněné CSRF tokenem** (starší moduly vlastním, ostatní společným `csrf.php`; akce měnící data jen přes POST), obnova ID relace po každém přihlášení, při odhlášení se maže i cookie relace, návrat po přihlášení jen na stránky aplikace.
- Omezení pokusů o přihlášení: 10 neúspěšných na účet nebo 30 z jedné IP adresy za 15 minut → blokace na 15 minut (kap. B4.2).
- HTML z editorů se čistí (aktuality, zpráva o činnosti, export stránek do PDF – jen povolené značky, žádné skripty ani vzdálené zdroje).
- Nahrávané soubory: povolené jen běžné dokumenty, obrázky a archivy (kontroluje se i „vnitřní“ přípona), obrázky se přeukládají přes GD; citlivé soubory (dokumenty, hájení, přílohy helpdesku, úkolů a metodiky, obrázky zprávy a obchodu) leží mimo přímý přístup (`.htaccess`) a vydávají se skriptem po kontrole práv (`soubor_lib.php` hlídá i cestu k souboru); výpis obsahu veřejných složek (přílohy aktualit, obrázky) je zakázaný.
- AI dostává jen souhrnná čísla bez osobních údajů a názvů cizích organizací; asistent smí jen předem dané nástroje s oprávněním ze session; vše se loguje.
- Minimalizace údajů: analytiky pracují s eID místo jmen, e-mail plátce se ve výpisech Comgate nezobrazuje, veřejný přehled hájení bez zdůvodnění a autorů, souhrn členské základny bez osobních údajů, odkazy na PDF výpisy s omezenou platností.
- Přístupové údaje (databáze, SMTP, Comgate, AI, tokeny cronů, knihovna účtů) jsou v konfiguračních souborech mimo repozitář.
- Logy: přihlášení, rozesílky e-mailů, AI, importy dávek, rozesílka výpisů – pro dohledání incidentů. Logy přihlášení a e-mailů se uchovávají 1 rok.
- **Kontroly rybářské stráže z RIS** (kap. B6.16): rozhraní RIS se volá jen ke čtení, účet pro synchronizaci se neukládá (ruční běh) nebo je v konfiguraci mimo repozitář (cron, přístup přes web jen s tokenem). Viditelnost se odvozuje od hospodáře revíru a vynucuje se v každém dotazu. Modul **nezpracovává osobní údaje kontrolovaných rybářů** – jméno, adresa, datum narození, číslo rybářského lístku ani identifikátor kontrolované osoby se z RIS neukládají ani nezobrazují. Ukládá se jen průběh služby: kdo z rybářské stráže (jméno a číslo odznaku jako údaj o výkonu funkce), kdy, kde (revír, souřadnice) a s jakým výsledkem; u kontroly je navíc uloženo číslo kontrolované povolenky, které se nikde nezobrazuje. Mapové podklady načítá prohlížeč ze serverů OpenStreetMap, knihovnu mapy z CDN unpkg.
- Celý web na HTTPS s hlavičkou HSTS; požadavek přes HTTP aplikace sama přesměruje na HTTPS (`prihlaseni_lib.php`); cookie relace s příznaky Secure, HttpOnly a SameSite, přísný režim relace (`session.use_strict_mode`, jen cookies) a vypnutý výpis chyb na obrazovku (`.user.ini`).
- **Bezpečnostní hlavičky** (`prihlaseni_lib.php`): zákaz vkládání do cizích rámů (X-Frame-Options, frame-ancestors – výjimkou je veřejný přehled hájení, který se do webů vkládá), nosniff, Referrer-Policy, Permissions-Policy a Content-Security-Policy zatím v režimu „Report-Only“ (nic neblokuje, jen hlásí).
- **Knihovny z CDN** (jsDelivr, unpkg) se načítají s kontrolou integrity (SRI, sha384) a pevnou verzí – podvržený soubor na CDN prohlížeč nespustí.
- **Ochrana souborů na serveru**: kořenový `.htaccess` zakazuje skryté soubory a vnitřní soubory gitu, pomocné skripty s podtržítkem, dokumentaci, data a zálohy (`sql`, `md`, `json`, `ini`, `bak` …) a vzory konfigurace;

adresáře `vendor/`, `dompdf/`, `forum/lib/`, `forum/sql/`, `security/` a `zprava2/vypocty/` mají vlastní zákaz. Používají se jen konstrukce, které hosting v `.htaccess` povoluje (bez `<If>`, `Header` a přepisů – jinak celý web vrací chybu 500). Knihovny a fragmenty stránek při přímém volání vrací 404.

- Přihlášení e-mailem u neexistujícího účtu ověřuje heslo proti fiktivnímu otisku – podle doby odpovědi nelze zjistit, zda e-mail existuje. Tokeny cronů nesmějí být prázdné ani výchozí hodnotou ze vzoru.
- **Žádosti o storna povolenek** (kap. B6.3) ukládají z RIS i eID a jméno držitele povolenky, pokud je RIS vrátí; vidí je jen organizace v rozsahu podle prodejce. Rozhraní RIS se volá jen ke čtení technickým účtem z konfigurace.
- **Moje notifikace** ukládají k nastavení e-mail a jméno uživatele (aby šlo upozornění doručit i z cronu); změnu smí udělat jen přihlášený uživatel sám za sebe (formulář s CSRF tokenem), oblast se ověřuje proti úrovni jeho organizace.
- Pravidelné bezpečnostní testy podle metodiky v `security/` (kap. F9).
- **Cookies**: rozcestník používá jen nezbytné cookies přihlášení (vlastní relace a společná relace nástrojů `crs_ucet`) a v prohlížeči si pamatuje skrytí nápovědy (localStorage) a průběh rozhovoru s AI asistentem (sessionStorage). Měření návštěvnosti, reklamu ani sledovací nástroje nepoužívá, proto nevyžaduje souhlas s cookies. Veřejná stránka `cookies.php` to uživatelům popisuje včetně obsahu třetích stran (videa YouTube v Metodice a Dokumentaci, knihovny vzhledu z CDN jsDelivr) a doby uchování logů.

B10. Provoz, nasazení a údržba

- Instalace: nahrání souborů a konfiguračních souborů podle vzorů `config_*.example.php` (mj. `config_db.php` s přístupy k databázím – bez něj web nenaběhne), knihovna účtů ve vedlejším adresáři `../ucty`, šest plánovaných úloh (kap. B8). Tabulky lokální databáze vzniknou samy.
- Aktualizace: nahrání změněných souborů; nové tabulky a sloupce doplní kód při prvním použití. Styly se verzují podle data úpravy, prohlížeč tak po změně nepoužije starou kopii.
- Pravidelné importy dat z RIS provádějí ÚS (prodeje) a správci (členská základna, stav RS, zarybnění, přestupky, vrácené povolenky) – každý import má náhled párování a hlášení vynechaných organizací. Brigády a členské příspěvky správce načítá přímo z RIS (náhled → uložení), kontroly stráže a žádosti o storna se načítají cronem, funkcionáři zprávy přímo z RIS.
- Před nasazením spustit bezpečnostní testy ochranných funkcí a statický audit (`security/README.md`); po nasazení ověřit ochranu souborů dynamickým testem D03/D12.
- Nasazení přes FTP: soubory, na které se jiné odkazují (např. `csrf.php`, `soubor_lib.php`, `config_db.php`), nahrát dřív nebo současně se stránkami; nevynechat soubory `.htaccess` a `index.html` v adresářích s nahranými soubory.
- Nouzové režimy: vypnutí vyžadování přihlášení RIS (výpadek RIS), testovací režim e-mailů.
- Zdrojový kód je veden v systému Git s historií změn; konfigurace, nahrané soubory a vygenerovaná PDF jsou vyřazeny z repozitáře. Záložní kopie skriptů (`*_orig` apod.) ani diagnostické soubory na server nepatří – server by je vydal jako čitelný text, případně by obcházely opravy.

B11. Rozsah díla

Vlastní kód aplikace podle oblastí (PHP, JS, CSS; bez knihoven třetích stran, nahraných souborů a záložních kopií). Počty se počítají ze skutečných souborů při zobrazení stránky.

Oblast	Souborů	Řádků kódu
Jádro: rozcestník, šablona, přihlášení, účty a práva	34	6 060
Aktuality, e-mailové notifikace a schránka	13	3 597
Úkoly s termínem	5	1 105
Formuláře	6	1 756
Rezervační kalendáře	4	1 689
Správce dokumentů	5	1 928
Žádosti o hájení revíru	7	2 611
Helpdesk, uživatelská podpora a návrhy na úpravu	12	2 689
Nápověda, manuál, metodika, AI asistent, dokumentace systému	21	7 154
Objednávky (e-shop a sklad)	13	3 225
Platby Comgate a denní výpisy	6	1 755
Zpráva o činnosti	90	15 608
Nástroje (prezenční listiny, import SQL dumpu)	2	1 101
Analytika: přístup MO k analytikám	2	526
Analytika: prodeje z RIS (import, přepočty, přehledy, storna, AI, PDF)	57	18 271
Analytika: revíry, docházky, úlovky, stráž, povolenky	27	7 322
Analytika: kontroly rybářské stráže z RIS	19	4 910
Analytika: výpis plateb	1	327
Členové (sestavy z RIS, demografie) a aktivace účtů RS	23	5 725
Analytika: kontroly úlovků a návratnost povolenek	5	2 367
Analytika: brigádnická povinnost a příspěvky MO	10	3 655
Analytika: přehled přihlášení	1	325
Analytika: redistribuce CS/CR povolenek	8	4 097
Analytika: starší přehledy z E-Sumáře	15	9 302
Bezpečnostní testy (nástroje penetračních testů)	3	1 021
Ostatní a servisní skripty (diagnostika)	45	6 174
Celkem	**434**	**114 300**

Souhrn: 2 databázová spojení (lokální, E-Sumář) a databáze historie, napojení na RIS (přihlášení přes knihovnu účtů, importy exportů sestav Oracle Analytics, čtení rozhraní REST RIS), čtení databáze sportovního portálu, Comgate, SMTP a Google Gemini; 160 tabulek zakládaných aplikací; 6 plánovaných úloh; 16 modulů agend a 15 analytických nástrojů pro veřejnost, MO, ÚS, Radu a správce; 43 výpočtů zprávy o činnosti; exporty do Excelu, CSV a PDF (přehledy prodejů a revírů, zpráva o činnosti, prezenční listiny, výpisy, dokumentace).

B12. Stav vývoje a otevřené body

- **Sjednocení přihlášení na účet RIS** probíhá: původní účty se převádějí při přihlášení, nové lokální účty už nelze zakládat. Práva místních organizací (kap. B6.15) zatím řídí pět modulů (Objednávky, Úkoly, Formuláře,

Rezervace, Hájení) a analytické dlaždice.

- **Souběh starých a nových částí**: modul Revíry nahrazuje starší přehledy z E-Sumáře, migrace členů z prodejů nahrazuje původní evidenci. Původní zpráva o činnosti je zrušená – násady, líhně a párování druhů úlovků jsou součástí nové zprávy (kap. B5.15).
- Starší stránky si oprávnění a hierarchii určují samy (kontroly doplněny při bezpečnostní revizi, kap. F8) – výhledově sjednotit na `crs_scope.php`. Kontrola platnosti povolenek má sezónu pevně v kódu – doplnit výběr sezóny.
- **Bezpečnostní revize a penetrační testy 11/2026** (kap. F8 a F9) odstranily nalezené úniky dat a slabiny konfigurace; zbývá přepnout Content-Security-Policy z režimu „Report-Only“ na vynucující, na serveru nastavit vlastní tokeny cronů a po zprovoznění odstranit diagnostické stránky (stráž, dohledání povolenky v RIS, diagnostika brigád).
- **Přechod z exportů sestav na rozhraní RIS** probíhá: kontroly a číselník stráže, funkcionáři, brigády, členské příspěvky storna povolenek a sestavy rozcestníku Členové (účast na brigádách, prezenční listina, podezřelé záznamy) se už čtou přímo z RIS; prodeje, členská základna, stav RS, zarybnění, přestupky a vrácené povolenky dál přicházejí exporty, které je třeba ručně nahrávat.

Část C – Sportovní portál ČRS

C1. Účel a rozsah portálu

Sportovní portál ČRS je samostatná webová aplikace pro sportovní agendu Českého rybářského svazu. Jejím hlavním účelem je **prodej a evidence sportovní známky** registrovaných sportovců, včetně online platby, zápisu uhrazené známky zpět do RIS, vydání dokladu o úhradě a elektronického průkazu sportovce. Dále zveřejňuje **kalendář závodů** převzatý z RIS.

Portál nevede vlastní registr osob – sportovce, trenéry, rozhodčí, jejich přihlášky do soutěží, místní organizace a závody přebírá z **Rybářského informačního systému (RIS)**. Přihlašování uživatelů probíhá rovněž účtem RIS, portál tedy nespravuje vlastní hesla.

Uživatelé portálu:

- **veřejnost a sportovci bez přihlášení** – titulní stránka, statistiky, veřejné seznamy, kalendář závodů, e-průkaz, doklad, platba za jiného sportovce;
- **přihlášení uživatelé (účet RIS)** – navíc platba za sebe, Moje platby, Můj průkaz;
- **správci** (platná funkce RIS č. 98) – správa plateb, sezón, obsahu, exporty, závěrka, synchronizace a provozní logy.

C2. Architektura a technologie

Serverová část	PHP 8.1+ bez frameworku (vlastní lehká struktura: stránky + knihovny v `lib/`), PDO, strict types. Rozšíření PHP: pdo_mysql, curl, mbstring, iconv, zip (export .xlsx).
Databáze	MySQL / MariaDB, kódování utf8mb4, české řazení (utf8mb4_czech_ci), InnoDB s transakcemi.
Uživatelské rozhraní	Serverově generované HTML, Bootstrap 5.3 a Bootstrap Icons (CDN), vlastní styly podle vizuálu rybsvaz.cz, písmo Roboto (lokálně). Responzivní – mobil, tablet, počítač; tiskové styly.
Knihovny třetích stran	qrcode-generator 1.4.4 (MIT) pro QR kód průkazu, editor Quill (CDN) pro aktuality, čištění HTML převzaté z portálu mocrs. Export do Excelu vlastní implementací bez externí knihovny.
Plánované úlohy	Cron: denní synchronizace sportovců a přihlášek z RIS, denní synchronizace závodů z RIS, pravidelné ověřování plateb v Comgate s opakováním zápisu známek do RIS (lze spouštět z příkazové řádky i přes URL s tokenem).
Konfigurace	`config.php` (mimo repozitář): přístup k DB, RIS (včetně zapnutí zápisu známek), Comgate, roky synchronizace, parametry synchronizace závodů, záložní správci, token pro cron. Vzor v `config.example.php`.

Struktura je záměrně jednoduchá: každá stránka je jeden PHP skript, sdílená logika je v knihovnách (`lib/ris.php`, `lib/ris_znamka.php`, `lib/zavody.php`, `lib/platby.php`, `lib/comgate.php` …). Identifikátory z RIS (`id`, `sid`) se ukládají a porovnávají jako text – část z nich je delší než největší celé číslo v PHP. Hostování je možné na běžném PHP webhostingu bez dalších služeb.

C3. Napojení na okolní systémy

Systém	Rozhraní	K čemu slouží	Směr
RIS – přihlášky do soutěží	REST/JSON, `features/by-path`, HTTP Basic (technický účet)	Načtení přihlášek do soutěží daného roku včetně osob (sportovec, role, rodné číslo, eID), místních organizací a sportovních odvětví.	RIS → portál (denně)
RIS – profil osoby	REST/JSON, `…/ft_fyzickaOsoba/action/nactiProfilOsoby`, HTTP Basic (účet uživatele)	Ověření jména a hesla při přihlášení; jméno, příjmení, eID, datum narození, platné přidělené funkce (z nich role správce).	RIS → portál (při přihlášení)
RIS – registrační známka	REST/JSON, `PUT …/features/business/ft_registracniZnamka`, HTTP Basic (technický účet s právem zápisu)	Zápis uhrazené sportovní známky do RIS: sportovec, rok, cena známky (bez poplatku), datum zakoupení. Zapíná se v konfiguraci.	portál → RIS (po úhradě, cron)
RIS – závody	REST/JSON, `features/_query` (`ft_zavod`), HTTP Basic (technický účet)	Závody se zahájením od 1. 1. předchozího roku: název, stav, odvětví, termíny, místo, startovné, pořadatel, odbor, ředitel, garant, hlavní rozhodčí, ligová soutěž, propozice.	RIS → portál (denně)
Comgate	REST API v2.0, HTTP Basic (merchant + secret), notifikace na URL portálu	Založení platby, přesměrování plátce na bránu, ověření stavu, storno; identifikace pro rozdělovník plateb ČRS podle IČO (refId `S-IČO-datum-pořadí`), eID plátce v produktu.	obousměrně (online + cron)
mocrs	rozcestník čte databázi portálu (jen čtení)	Zpráva o činnosti počítá z registru portálu registrované sportovce, trenéry a rozhodčí (kap. B5.15). Shodná identifikace osob (eID), převzaté postupy (aktuality, čištění HTML) a vzhled; společná relace přihlášení `crs_ucet` (kap. A2).	portál → mocrs

Testovací a produkční prostředí RIS se přepíná jedinou adresou v konfiguraci (adresa profilu se z ní odvozuje). Comgate má samostatný testovací režim (platby bez stržení peněz).

C4. Funkční oblasti

C4.1 Přihlášení účtem RIS a role

- Přihlášení jménem a heslem do RIS. Portál je neukládá – předá je RIS (akce `nactiProfilOsoby`); odpověď 401/403 znamená špatné údaje, jiná chyba hlášku „RIS nedostupný“.
- Z profilu se do relace uloží jméno, příjmení, **eID** a platné přidělené funkce (funkce, organizační jednotka). V hlavičce se zobrazuje jméno a příjmení, menu účtu nabízí Moje platby a Můj průkaz.
- **Správce** = osoba s platnou funkcí RIS č. 98; záložně seznam účtů v konfiguraci.

- Každý pokus o přihlášení (i neúspěšný) se zapisuje do logu: čas, účet, osoba a eID, výsledek, IP, prohlížeč. Správa v logu hledá podle účtu, eID nebo IP a vidí počet plateb zadaných z účtu. Log se uchovává 1 rok – starší záznamy se průběžně mažou při zápisu nových přihlášení.
- Ochrana relace: HttpOnly a SameSite cookie, obnova ID relace po přihlášení, CSRF token ve formulářích, návrat po přihlášení jen na stránky portálu.

C4.2 Synchronizace registru z RIS

- Denní úloha načte z RIS všechny přihlášky do soutěží pro zvolené roky (pevný seznam nebo všechny roky od zadaného roku do aktuálního; od 1. 11. i příští rok).
- Osoby se párují podle **eID** (nové se vloží, existující aktualizují), přihlášky podle identifikátoru RIS (`sid` jako text – dřívější převod na číslo slil dlouhé identifikátory do jedné hodnoty a přihlášky se přepisovaly; opraveno migrací, která poškozené hodnoty uklidila). Přihlášky, které v RIS zmizely, se jen označí jako neaktivní – nemažou se, protože na ně mohou vázat platby.
- Přenáší se: jméno, tituly, datum a rok narození, rodné číslo, číslo sportovce, role (sportovec, trenér, funkcionář, rozhodčí, technicko-organizační pracovník), cizinec, příznak „aktivní“ (známka placená přes RIS), místní organizace a sportovní odvětví (plavaná, muška, feeder …).
- **Pojistka proti výpadku RIS:** přijde-li výrazně méně přihlášek než je v databázi (výchozí méně než 50 %), synchronizace se nepovede a data zůstanou beze změny. Zápis probíhá v jedné transakci.
- Každý běh se zapisuje do historie (počty nových a změněných záznamů, chyby); správce může synchronizaci spustit ručně.

C4.3 Veřejné seznamy a statistiky

- **Seznamy sportovců, trenérů a rozhodčích** s přihláškou v dané sezóně: číslo sportovce, jméno, rok narození, odvětví, role; u sportovců stav známky (zeleně uhrazeno). Hledání podle jména a čísla sportovce, filtr podle odvětví a stavu známky, řazení kliknutím na záhlaví, stránkování.
- Veřejně se zobrazuje jen **rok narození**; místní organizaci a eID vidí jen správa.
- Správa navíc: ruční zápis úhrady známky (hotově, převodem, jinak) s vystavením dokladu, export do Excelu podle filtru.
- **Výpis pro NSA** (jen správa): sportovci s rodným číslem a datem narození, export do Excelu.
- **Statistiky na titulní stránce** pro zvolenou sezónu: počet sportovců, přihlášek celkem a podle odvětví, trenérů a rozhodčích.

C4.4 Platba sportovní známky

- Platit lze jen v **období prodeje sezóny** (nastavuje správa: cena známky, servisní poplatek, od–do). Prodává-li se víc sezón současně, plátce si vybere.
- **Platím za sebe** – vyžaduje přihlášení účtem RIS. Sportovec se dohledá podle eID, zobrazí se rekapitulace (jméno, rok narození, číslo sportovce, místní organizace, cena) a vyplňuje se jen e-mail.
- **Platím za někoho jiného** (rodič, trenér, organizace) – i bez přihlášení. Sportovec se hledá podle jména, příjmení a čísla sportovce. Přihlášenému se jméno plátce převezme z účtu RIS bez možnosti úpravy.
- Kontroly: sportovec musí být v registru a mít aktivní přihlášku na rok známky; uhrazenou známku (přes portál nebo přes RIS) nelze zaplatit znovu; nejasná shoda se odmítne s odkazem na sportovní oddělení.

- Založením vznikne platba s jedinečným kódem a rekapitulací; předchozí nezaplacená platba téhož sportovce a roku se zruší (i na bráně), aby existovala vždy nejvýš jedna rozpracovaná.
- K platbě se ukládá účet RIS a eID přihlášeného plátce, IP adresa a čas.

C4.5 Platební brána Comgate

- Z rekapitulace „Zaplatit online“: portál založí platbu na bráně (částka v haléřích, návratové adresy) a přesměruje plátce; rozpracovanou transakci použije znovu. Platební karta, bankovní převod, rychlé platby.
- Identifikace pro rozdělovník plateb ČRS podle IČO, stejně jako u ostatních obchodů svazu: `refId = S-{IČO}-{RRRRMMDD}-{pořadí}`, produkt `Plátce: eID = …`, volitelně identifikátor účtu.
- **Obsahu návratu ani notifikace se nevěří** – stav se vždy ověří dotazem na API Comgate. Při zaplacení se zkontroluje částka, měna a refId; teprve pak se platba označí jako zaplacená a dostane číslo dokladu. Nesouhlasí-li částka, platba se neoznačí, další placení se zablokuje a správě se zobrazí varování.
- Storno: zrušená platba se stornuje i na bráně. Byla-li mezitím zaplacena, zobrazí se varování k vrácení peněz.
- Pojistná úloha (cron, každých 15–30 minut) dověří nedokončené platby, dostornuje zrušené a zopakuje nezdařené zápisy známek do RIS.
- Celá komunikace s bránou se loguje (bez tajného klíče); správa má přehled stavu napojení, test spojení a log.

C4.6 Doklady o úhradě a účetní závěrka

- **Doklad o úhradě** (A4, tisk / PDF z prohlížeče) ke každé zaplacené platbě: plátce, sportovec, sezóna, částka a poplatek, způsob úhrady, příjemce podle fakturačních údajů v nastavení.
- Číslování `SZ2026-00001` – samostatná řada pro každý kalendářní rok úhrady, číslo se přiděluje až při úhradě (další číslo v řadě, chráněno unikátním klíčem).
- Doklad lze dohledat veřejně, otevřít z rekapitulace platby, z Mých plateb i z přehledu plateb ve správě.
- **Účetní závěrka** (správa): uhrazené platby za měsíc, sezónu nebo libovolné období – souhrn, rozpis podle způsobu úhrady, sezóny a měsíce, rozsah čísel dokladů, seznam dokladů. Tisk / PDF a export do Excelu.

C4.7 Zápis známky do RIS

`lib/ris_znamka.php`, `admin_platby.php`, `cron_comgate.php`

- Po úhradě – ať přes platební bránu, nebo ručním zápisem úhrady ve správě – portál zapíše známku do RIS jako registrační známku (`ft_registracniZnamka`): sportovec (identifikátory z registru), rok, cena známky bez servisního poplatku, čas úhrady. RIS tak eviduje známky placené přes portál stejně jako známky placené přímo v RIS.
- Selhání zápisu úhradu nevrací: chyba se uloží k platbě, v přehledu plateb je u ní „není v RIS“ s počtem pokusů a důvodem v nápovědě a tlačítko pro ruční zápis. Pojistná úloha zápis opakuje automaticky (nejvýš 10×, platby za posledních 60 dní).
- Úspěšný zápis se u platby označí časem a identifikátorem záznamu v RIS („v RIS“).
- Zápis se zapíná v konfiguraci (`ris.zapis_znamek`, výchozí vypnuto); technický účet RIS musí mít právo zápisu.

C4.8 E-průkaz sportovce

- Kartička pro mobil i tisk v rozměru platební karty: jméno, rok narození, číslo sportovce, stav známky, odvětví s přihláškou a QR kód.
- Průkaz se otevírá přes náhodný neuhodnutelný kód; QR kód vede na stejnou stránku, takže ověření vždy ukazuje aktuální stav (např. pro rozhodčího u závodu).
- Výchozí je aktuální sezóna; přepínač nad kartičkou ukáže sezóny, kdy měl sportovec přihlášku.
- Dohledání: veřejně podle jména, příjmení a čísla sportovce, přihlášený uživatel přímo přes „Můj průkaz“, ze seznamu sportovců proklikem.

C4.9 Moje platby a Můj průkaz

- **Moje platby** – platby, kde je přihlášený plátcem nebo sportovcem (párování podle eID): sezóna, sportovec, plátce, částka, stav, doklad, případně dokončení rozpracované platby. Je-li v prodeji sezóna s neuhrazenou vlastní známkou, nabídne se rovnou její zaplacení.
- **Můj průkaz** – přesměruje na e-průkaz přihlášeného sportovce.

C4.10 Titulní stránka, upozornění a aktuality

- Titulní stránka: upravitelný úvodní text, informace o probíhajícím prodeji, rozcestník dlaždic, aktuality, statistiky.
- **Upozornění** v liště pod hlavičkou ve třech úrovních (informace, výstraha, důležité), zapínání a vypínání.
- **Aktuality**: nadpis, perex, obsah ve WYSIWYG editoru (HTML se čistí proti škodlivému kódu), datum vydání, volitelné období zobrazení, hlavní (zvýrazněná) zpráva, zveřejnění; detail na samostatné stránce.

C4.11 Závody z RIS

`zavody.php`, `lib/zavody.php`, `cron_sync_zavody.php`, `admin_sync.php`

- Denní úloha načte z RIS závody se zahájením od 1. 1. předchozího roku (počet let zpět v konfiguraci) a uloží je podle identifikátoru RIS: nové vloží, změněné aktualizuje, závody, které v RIS v daném období zmizely, jen označí jako neaktivní.
- Stejné pojistky jako u registru: přijde-li výrazně méně závodů než je v databázi, synchronizace se neprovede; strop počtu závodů v jednom dotazu; zápis v jedné transakci; každý běh v historii (přijato, nových, změněných, zrušených, přeskočených).
- **Veřejný výpis** (dlaždice Závody): filtr roku a odvětví, hledání, volba „jen nadcházející“; detail závodu s termíny (prezentace, začátek a konec), místem, startovným, pořadatelem a odborem, ředitelem, garantem a hlavním rozhodčím, ligovou soutěží a texty propozic (přihláška, harmonogram, pravidla, vyjádření, poznámka). Texty z RIS s HTML se čistí proti škodlivému kódu.
- Závody ve vybraných stavech (např. neschválené) se veřejně nezobrazují, správa je vidí.
- Správa: ruční spuštění synchronizace závodů a její historie vedle synchronizace registru. Tabulky závodů se založí samy při prvním spuštění. Diagnostická stránka pro test importu bez zápisu (jen správce nebo příkazová řádka).

C4.12 Správa portálu

Platby	Přehled plateb s filtrem (sezóna, stav) a hledáním (jméno, číslo sportovce, e-mail, účet RIS, eID, kód platby, číslo dokladu); ruční označení zaplaceno / zrušeno; varování z platební brány; stav zápisu známky do RIS a ruční opakování zápisu (C4.7).
Účetní závěrka	Viz C4.6.
Sportovci, výpis pro NSA	Viz C4.3 – zápis úhrad, exporty.
Synchronizace RIS	Historie běhů a ruční spuštění – zvlášť registr sportovců a závody (C4.11).
Přihlášení	Log přihlášení účtem RIS (uchování 1 rok).
Comgate	Stav napojení, adresy k nastavení v portálu Comgate, test spojení, log komunikace.
Titulní stránka, aktuality	Viz C4.10.
Nastavení	Sezóny (cena známky, servisní poplatek, období prodeje) a fakturační údaje příjemce plateb.

C5. Datový model

Tabulka	Obsah	Zdroj
`sportovci`	Osoby s přihláškou: eID, číslo sportovce, jméno, narození, rodné číslo, role, MO, kód průkazu	RIS
`prihlasky`	Přihlášky do soutěží (osoba × rok × odvětví), příznak aktivní	RIS
`organizace`, `odvetvi`	Místní organizace, číselník sportovních odvětví	RIS
`sezony`	Cena známky, servisní poplatek, období prodeje	správa
`platby`	Platby známek: částky, plátce, stav, způsob úhrady, číslo dokladu, údaje Comgate, účet a eID plátce, stav zápisu známky do RIS (čas, identifikátor záznamu, chyba, počet pokusů)	portál
`zavody`	Závody: identifikátor RIS, název, stav, odvětví, termíny, místo, startovné, pořadatel, odbor, ředitel, garant, hlavní rozhodčí, ligová soutěž, akce, propozice, příznak aktivní	RIS
`nastaveni`	Fakturační údaje, úvodní text titulky	správa
`upozorneni`, `aktuality`	Obsah titulní stránky	správa
`prihlaseni`, `sync_log`, `zavody_sync_log`, `comgate_log`	Provozní logy: přihlášení (1 rok), synchronizace registru a závodů, komunikace s bránou	portál

Celkem 14 tabulek; změny struktury se dodávají jako číslované migrace (11 souborů v `sql/migrace/`; tabulky závodů zakládá kód sám při prvním spuštění). Identifikátory RIS (`id`, `sid`) jsou textové sloupce.

C6. Bezpečnost a ochrana osobních údajů

- Hesla se v portálu neukládají – ověřuje je RIS. Role správce se odvozuje z funkce v RIS.
- Technický účet RIS (synchronizace, závody, zápis známek) je jen v `config.php` mimo repozitář; pro zápis známek potřebuje právo zápisu, proto se zápis zapíná výslovně v konfiguraci. Do RIS se zapisují jen údaje o uhrazené známce.

- Plánované úlohy přes web jen s tokenem z konfigurace; diagnostické stránky jen pro správce nebo z příkazové řádky.
- Texty závodů převzaté z RIS (propozice) se před zobrazením čistí stejně jako aktuality.
- Všechny formuláře chráněny CSRF tokenem, výstupy escapovány, dotazy do databáze parametrizované.
- Stav platby se nikdy nepřebírá z prohlížeče ani z notifikace, ale ověřuje se přímo u Comgate včetně částky.
- Minimalizace údajů na veřejných stránkách: jen jméno, rok narození, číslo sportovce, odvětví a stav známky. Rodné číslo, datum narození, místní organizace a eID jen ve správě; průkaz jen přes neuhodnutelný kód.
- HTML z editoru aktualit se čistí (povolené značky a atributy).
- Logování přihlášení a komunikace s bránou pro dohledání incidentů; tajné klíče se do logů nezapisují.
- Chyby se zapisují do logu serveru; uživatel vidí srozumitelnou hlášku bez technických detailů.

C7. Provoz, nasazení a údržba

- Instalace: databáze ze `sql/schema.sql`, konfigurace `config.php`, tři plánované úlohy (cron): synchronizace sportovců, synchronizace závodů (denně, např. 3:30) a ověřování plateb Comgate (každých 15–30 minut).
- Aktualizace: nahrání souborů a spuštění nových migrací ze `sql/migrace/` v pořadí čísel.
- Přechod test → produkce: změna adresy RIS v konfiguraci (adresy profilu, závodů a zápisu známek se z ní odvozují, lze je přepsat), technický účet s právem zápisu známek a zapnutí zápisu, údaje produkčního obchodu Comgate a vypnutí testovacího režimu.
- Zdrojový kód je veden v systému Git s historií změn.

C8. Rozsah díla

Vlastní kód portálu podle oblastí (PHP, SQL, CSS; bez knihoven třetích stran a písem). Počty se počítají ze skutečných souborů při zobrazení stránky.

Oblast	Souborů	Řádků kódu
Přihlášení účtem RIS a role	4	323
Synchronizace registru z RIS	4	637
Závody z RIS (synchronizace, veřejný výpis)	3	579
Seznamy osob, statistiky, exporty	6	563
Platba sportovní známky, Moje platby, zápis známky do RIS	4	811
Platební brána Comgate	6	565
Doklady o úhradě a účetní závěrka	2	479
E-průkaz sportovce	2	254
Titulní stránka, upozornění, aktuality	8	827
Správa plateb, sezón a fakturačních údajů	3	492
Společný základ (vzhled, DB, konfigurace, dokumentace)	17	1 492
Celkem	**59**	**7 022**

Souhrn: 2 externí integrace (RIS – 4 rozhraní včetně zápisu známek, Comgate), 14 databázových tabulek, 3 plánované úlohy, veřejná část (včetně kalendáře závodů), část pro přihlášené uživatele a správa s 10 sekcemi, exporty do Excelu, tiskové výstupy (doklad, průkaz, závěrka, tato dokumentace).

C9. Stav vývoje a otevřené body

- Portál je ve fázi testování: napojen na **testovací prostředí RIS**, platební brána v testovacím režimu.
- Ověřit na testovacím RIS přihlašování běžných účtů a role správce (funkce č. 98).
- Příznak „známka placena přes RIS“ nemá v RIS vazbu na rok – u starších sezón průkazu proto může být nepřesný.
- Postupné omezování data narození na rok narození (vyhledání dokladu dosud používá datum narození).
- Zápis známek do RIS je připravený, ale ve výchozím stavu vypnutý – zapnout po ověření na testovacím RIS a přidělení práva zápisu technickému účtu.
- Závody z RIS: doplnit výsledky a vazbu na přihlášky sportovců; ověřit, které stavy závodu skrýt veřejnosti.
- Bezpečnost: doplnit ochranu souborů mimo PHP (`.htaccess`), bezpečnostní hlavičky a odmítnutí výchozího tokenu cronu, odstranit přístupové údaje testovacího RIS ze vzoru konfigurace (kap. F9).
- Před ostrým provozem: produkční údaje RIS a Comgate, nastavení rozdělovníku v Comgate, odstranění diagnostických skriptů.

Část D – Fórum ČRS

D1. Účel a rozsah fóra

Fórum ČRS je diskuzní fórum pro funkcionáře svazu. Diskuze jsou rozdělené do oblastí podle organizační struktury a do témat, která vidí jen držitelé vybraných funkcí v RIS. Fórum je **součástí rozcestníku MoČRS** (složka `forum/`): přihlašuje se v rozcestníku účtem RIS, fórum nemá vlastní přihlášení, registraci ani hesla. Přihlášený e-mailem (bez eID) do fóra nesmí.

- **přihlášení uživatelé** – vidí a píší do témat, kam je pustí jejich funkce; sledují vlákna a témata e-mailem;
- **správci fóra** (podle funkcí, které si vybrala Rada a každý ÚS) – zakládají, upravují a mažou témata ve své oblasti;
- **admin fóra** (admin rozcestníku, platná funkce z konfigurace, záložně vyjmenované účty) – vidí vše, moderuje vlákna a příspěvky, spravuje číselník a skupiny funkcí, simuluje roli. Přihlášení eviduje přehled přihlášení rozcestníku.

D2. Architektura a technologie

Serverová část	PHP 8, strict types, stránky ve složce `forum/` rozcestníku a knihovny v `forum/lib/` (`app.php` – společný začátek stránky, napojení na session, přihlášení a hlavičku rozcestníku, CSRF, zachycení chyb; `forum.php` – oblasti, témata, přístup, správci; `upozorneni.php`; `html_sanitize.php`; `editor.php`; `layout.php`; `db.php`).
Databáze	Vlastní databáze fóra (témata, vlákna, příspěvky, sledování, nastavení, správci) a společná databáze knihovny účtů `ucty_1` (uživatelé, funkce, skupiny, log přihlášení, e-maily). Každá databáze má vlastní účet; vazby se skládají v PHP.
Rozhraní	Serverově generované HTML, Bootstrap 5, hlavička a drobečková navigace rozcestníku (`layout.php`, `crs.css`), pod ní pruh správy fóra; editor příspěvků Quill.
Konfigurace	`forum/config.php` (mimo repozitář, vzor `config.example.php`): databáze fóra, veřejná adresa pro odkazy v e-mailech, funkce a účty adminů. Knihovnu účtů bere z `config_ucty.php` rozcestníku.
Chyby	Nezachycená chyba se zapíše do logu serveru a zobrazí se srozumitelná stránka; admin vidí text chyby, u chybějící tabulky nebo sloupce i radu k nahrání schématu.

D3. Napojení na okolní systémy

- **Rozcestník MoČRS** – session a přihlášení účtem RIS (eID ze session), návrat po přihlášení na stránku fóra, hlavička, schránka.
- **Knihovna účtů** – uživatel s funkcemi a organizacemi (snímek z přihlášení v rozcestníku, `ucty_uzivatel`), číselník a skupiny funkcí, organizace a ÚS, odesílání e-mailů a ukládání upozornění do společné schránky (vidí je i rozcestník MoČRS), alternativní e-mail.
- **RIS** – přes knihovnu účtů (adresa RIS a SMTP jsou v její konfiguraci).
- **Struktura organizací** – přes knihovnu účtů z číselníku organizací E-Sumáře (názvy ÚS, příslušnost MO k ÚS).

D4. Funkční oblasti

D4.1 Přihlášení a můj účet

`lib/app.php`, `login.php`, `logout.php`, `muj_ucet.php`, `overit_email.php`

- Přihlášení a odhlášení je rozcestníku: nepřihlášeného fórum pošle na jeho přihlašovací stránku a po přihlášení účtem RIS zpět na stránku fóra (`login_redirect`); `login.php` a `logout.php` fóra jen přesměrují (staré odkazy). Uživatele fóra (funkce, kontakty) načte knihovna účtů podle eID ze session a drží ho v session; po odhlášení nebo přihlášení jiného účtu se zahodí i se simulací role.
- Správcem fóra je i admin rozcestníku (role admin – vystupuje za Radu), přepočítává se při každém zobrazení.
- **Můj účet ve fóru** (tlačítko v hlavičce): funkce z RIS s organizací (Rada / ÚS / MO), skupiny, do kterých uživatel patří, kontakty.
- **E-maily a upozornění**: alternativní e-mail s ověřením odkazem (funguje i bez přihlášení), kam posílat upozornění (e-mail z RIS / alternativní / neposílat), automatické sledování vláken, do kterých uživatel napíše, seznam sledovaných vláken a témat.

D4.2 Funkce, skupiny funkcí a správci fóra

`admin_funkce.php`, `admin_skupiny.php`, `admin_spravci.php`, `admin_presun_do_uctu.php`

- **Číselník funkcí** (admin): import ze souboru CSV / TXT nebo vloženého textu (ID a název; středník, tabulátor nebo čárka; UTF-8 i Windows-1250 z Excelu, záhlaví se přeskočí). Import funkce nemaže, názvy přepíše jen na požádání.
- **Skupiny funkcí** (admin): funkcí je v RIS hodně, proto se slučují do pojmenovaných skupin (název, popis, výběr funkcí s filtrem, „jen vybrané“, „jen bez jiné skupiny“, hromadné vybrání). Jedna funkce může být ve více skupinách. Uživatel patří do každé skupiny, která obsahuje aspoň jednu jeho platnou funkci; počítá se při každém zobrazení, změna platí hned.
- **Správci fóra**: Rada a každý ÚS si vedou seznam funkcí, které smí spravovat témata. Funkce ze seznamu Rady, kterou má uživatel v Radě, dává práva ve všech oblastech; funkce ze seznamu ÚS, kterou má v tomto ÚS, dává práva v oblasti tohoto ÚS. Funkce v MO práva nedává. Seznam Rady a všech ÚS upravuje admin a správce Rady, seznam ÚS jeho správce.
- Jednorázový přesun dřívějších uživatelů, číselníku, skupin a logu z databáze fóra do knihovny účtů (opakované spuštění nic nezdvojí).

D4.3 Oblasti, témata a přístup

`index.php`, `admin_temata.php`, `lib/forum.php`

Oblast	Kdo do ní patří
Celosvazové fórum	Rada, územní svazy i všechny místní organizace
Územní svaz (jedna pro každý ÚS)	daný ÚS a jeho MO (Rada ne)
Územní svazy a Rada	Rada a všechny ÚS (MO ne)

- Správci zakládají témata s názvem, popisem a pořadím a vybírají skupiny funkcí, které téma vidí. Téma v oblasti ÚS lze založit hromadně pro více nebo všechny ÚS (vznikne samostatné téma pro každý svaz). Téma bez skupin vidí jen admin.

- **Přístup (přísně)**: téma vidí a smí v něm psát, kdo má platnou funkci, která je *zároveň* ve vybrané skupině *a* v organizaci patřící do oblasti – funkce a organizace se posuzují jako dvojice. Admin vidí vše.
- Úvodní stránka: viditelná témata po oblastech (oblast ÚS po svazech), počet vláken, poslední aktivita.

D4.4 Vlákna a příspěvky

`tema.php`, `vlakno.php`, `lib/editor.php`, `lib/html_sanitize.php`

- Téma: vlákna (připnutá nahoře, pak podle poslední aktivity, 30 na stránku), založení vlákna s prvním příspěvkem.
- Vlákno: příspěvky (20 na stránku), odpověď v editoru Quill, úprava vlastního příspěvku. HTML z editoru se čistí (povolené značky, odkazy, obrázky, video YouTube / Vimeo; bez skriptů a obsluh událostí).
- U příspěvku a vlákna se zobrazuje jméno autora a jedna organizace – ta s nejvyšší úrovní z jeho platných funkcí (Rada, jinak ÚS, jinak MO); ukládá se v okamžiku psaní.
- **Moderace** (admin): připnout, zamknout, smazat vlákno či příspěvek – mazání je skryté, místo obsahu se zobrazí „smazán správcem“.

D4.5 Sledování a upozornění e-mailem

`lib/upozorneni.php`

- Sledování vlákna (e-mail o každé nové odpovědi) a tématu (e-mail o každém novém vláknu) tlačítky Sledovat / Nesledovat; vlákno, do kterého uživatel napíše, začne sledovat automaticky (lze vypnout).
- Upozornění dostane jen ten, kdo do tématu stále smí (podle funkcí z posledního přihlášení), nikdy autor sám; každý příjemce jednou.
- Rozesílá se až po odeslání stránky autorovi, aby nečekal na SMTP; každé upozornění se uloží do společné schránky v knihovně účtů a podle nastavení příjemce pošle e-mailem. Odkazy vedou na veřejnou adresu fóra z konfigurace.

D5. Datový model

Tabulka	Obsah
`temata`, `temata_skupiny`	Témata (oblast, ÚS, název, popis, pořadí) a skupiny funkcí, které je vidí
`vlakna`	Vlákna: autor (eID a jméno), poslední příspěvek, počet příspěvků, připnuto / zamčeno / smazáno
`prispevky`	Příspěvky: autor (eID, jméno, organizace), HTML obsah, úprava, smazáno
`sledovani`, `nastaveni_uzivatele`	Sledovaná vlákna a témata, nastavení uživatele (automatické sledování)
`spravci_funkce`	Funkce s právem spravovat témata – seznam Rady a jednotlivých ÚS

Celkem 13 tabulek ve schématu (`sql/schema.sql`, nahrání vytvoří jen chybějící tabulky) a číslované migrace v `sql/migrace/`. Uživatelé, funkce, skupiny, log přihlášení a e-maily jsou v databázi knihovny účtů. Autor se ukládá eID a jménem v době psaní, protože databáze účtů je jiná a nedá se s ní spojit dotazem.

D6. Bezpečnost

- Hesla se neukládají – ověřuje je RIS přes knihovnu účtů. Práva se odvozují z platných funkcí v RIS při každém zobrazení.
- Přístup k tématu se kontroluje u každé stránky i akce (dvojice funkce × organizace), e-maily jen oprávněným příjemcům.
- CSRF token ve formulářích, session rozcestníku (HttpOnly, SameSite, Secure), parametrizované dotazy, escapované výstupy, čištění HTML příspěvků.
- Mazání příspěvků je skryté (zůstává pro dohledání), chyby se logují bez zobrazení technických detailů běžným uživatelům.

D7. Provoz a nasazení

- Instalace: fórum se nahrává s rozcestníkem (složka `forum/`); vytvořit databázi fóra a nahrát `forum/sql/schema.sql`, u existující databáze chybějící migrace v pořadí čísel; `forum/config.php` podle vzoru. Knihovna účtů je společná s rozcestníkem.
- Fórum nemá plánované úlohy; e-maily se odesílají po odpovědi na požadavek.

D8. Rozsah díla

Oblast	Souborů	Řádků kódu
Napojení na přihlášení rozcestníku, můj účet, e-maily	6	594
Funkce, skupiny funkcí a správci fóra	4	647
Oblasti, témata, vlákna a příspěvky	7	1 649
Upozornění e-mailem a sledování	1	149
Přílohy, reakce a obrázky v příspěvcích	4	327
Převod ze starého fóra MyBB	4	960
Společný základ (vzhled, DB, konfigurace, schéma)	13	562
Celkem	**39**	**4 888**

Souhrn: 1 integrace (knihovna účtů – RIS, e-maily, schránka), 13 tabulek, 3 typy oblastí, přístup podle funkcí a skupin, správci podle funkcí Rady a ÚS, sledování a e-mailová upozornění, správa číselníku a skupin funkcí.

Část E – Společná knihovna účtů ČRS

E1. Účel a rozsah knihovny

Knihovna účtů (repozitář `ucty`) je společný základ přihlašování pro nástroje ČRS – dnes ji používají rozcestník MoČRS a fórum. Každý nástroj přihlašuje účtem RIS stejným kódem a zapisuje do jedné databáze `ucty_1`, takže jeden člověk je ve všech nástrojích jeden záznam podle eID. Knihovna nemá vlastní stránky: nepracuje se session ani nevypisuje HTML – to dělá nástroj, který ji připojí jedním řádkem (`require_once …/ucty/ucty.php`). Všechny funkce mají předponu `ucty_`, aby nekolidovaly s nástroji.

Co poskytuje	Přihlášení účtem RIS, uživatele s platnými funkcemi a organizacemi, číselník funkcí a jejich skupiny, log přihlášení ze všech nástrojů, e-mail z RIS a alternativní e-mail, nastavení upozornění, odesílání e-mailů a schránku zpráv podle eID.
Co neřeší	Práva v jednotlivých nástrojích (co smí skupina, kdo je správce) – to si určuje každý nástroj sám; session, formuláře a vzhled.
Konfigurace	Jeden `config.php` pro všechny nástroje (mimo repozitář, vzor `config.example.php`): databáze účtů, databáze E-Sumáře jen pro čtení (struktura organizací), adresa profilu RIS (produkce / test), SMTP, cesta k PHPMaileru, adresa stránky pro ověřovací odkazy.

E2. Přihlášení účtem RIS

`lib/ris.php`, `lib/uzivatele.php`

- Uživatelské jméno a heslo se pošlou přes HTTPS do RIS (akce `nactiProfilOsoby`, HTTP Basic, časový limit 20 s); heslo se nikde neukládá ani neloguje. Odpověď 401 / 403 znamená špatné údaje, nedostupnost RIS nebo nečitelná odpověď srozumitelnou chybu.
- Z profilu se převezme jméno, příjmení, **eID**, e-mail a telefon z RIS a **platné** přidělené funkce s organizační jednotkou (neplatné funkce se zahodí). Účet bez eID se nepřihlásí.
- Uživatel se uloží podle eID (účet RIS, jméno, kontakty, první a poslední přihlášení, poslední nástroj) a jeho funkce se nahradí aktuálním stavem – v databázi je vždy snímek z posledního přihlášení v kterémkoli nástroji. Funkce chybějící v číselníku se doplní. Pokud účet RIS dříve patřil jiné osobě, uvolní se.
- Každý pokus (úspěch, špatné heslo, bez eID, chyba) se zapíše do logu se jménem nástroje, účtem, eID, jménem, příznakem správce, IP adresou a prohlížečem. Chyba logu přihlášení neblokuje.
- Nástroj předá funkci, která rozhodne, zda je uživatel jeho správcem (např. podle funkce v RIS); výsledek se zapíše do logu.
- **Společná relace** (`lib/relace.php`): po přihlášení nástroj založí relaci (`ucty_relace_zaloz`) – náhodný token v cookie `crs_ucet` (path /, HttpOnly, SameSite=Lax, Secure, do zavření prohlížeče), v databázi jen jeho otisk SHA-256 s eID, nástrojem, IP a prohlížečem. Ostatní nástroje podle ní uživatele přihlásí se snímkem funkcí z posledního přihlášení (`ucty_relace_eid`), odhlášení (`ucty_relace_zrus`) platí všude. Platnost 8 hodin od poslední aktivity v kterémkoli nástroji (nastavitelné).

E3. Struktura organizací, funkce a skupiny

`lib/organizace.php`, `lib/funkce.php`

- Organizační jednotka každé funkce se páruje podle `sid` z RIS na číselník organizací E-Sumáře (`keepers.ris_sid`) a určí se typ (Rada / ÚS / MO) a územní svaz. Výpadek databáze E-Sumáře přihlášení neblokuje – organizace pak zůstanou neurčené.
- **Číselník funkcí** RIS a pojmenované **skupiny funkcí** jsou společné pro všechny nástroje; import číselníku z textu (CSV / TXT, různé oddělovače a kódování). Uživatel patří do každé skupiny, která obsahuje některou jeho platnou funkci.

E4. E-maily, upozornění a schránka

`lib/email.php`

- Uživatel má e-mail z RIS (přepisuje se při každém přihlášení) a může mít jeden **alternativní** e-mail, který se použije až po ověření odkazem s omezenou platností. V databázi se ukládá jen otisk (SHA-256) náhodného tokenu, ne token sám.
- Kam posílat upozornění: e-mail z RIS / alternativní / nikam. Volitelná upozornění respektují i „nikam“, **služební** zprávy chodí vždy. Neověřený nebo smazaný alternativní e-mail → posílá se na e-mail z RIS.
- Odesílá se přes SMTP se šifrováním (STARTTLS / SSL), HTML i textová verze; každý e-mail se zapíše do logu (nástroj, eID, adresa, předmět, výsledek).
- **Schránka**: každá zpráva poslaná uživateli se uloží k jeho eID (předmět, obsah, odkaz, kam a s jakým výsledkem šel e-mail) – i při volbě „nikam“. Nástroje ji čtou společnými funkcemi; rozcestník MoČRS ukazuje zprávy z fóra v záložce „Fórum a další aplikace“.

E5. Datový model

Tabulka	Obsah
`uzivatele`	Uživatel podle eID: účet RIS, jméno, e-mail a telefon z RIS, alternativní e-mail a jeho ověření, kam posílat upozornění
`uzivatele_funkce`	Platné funkce uživatele s organizační jednotkou a organizací z číselníku organizací
`funkce`, `skupiny`, `skupiny_funkce`	Číselník funkcí RIS, pojmenované skupiny a jejich funkce
`prihlaseni`	Log přihlášení ze všech nástrojů
`relace`	Společná relace přihlášení nástrojů: otisk tokenu z cookie `crs_ucet`, eID, nástroj, poslední aktivita, IP, prohlížeč
`email_overeni`, `tokeny`	Otisky ověřovacích odkazů a jednorázových tokenů (připraveno pro centrální přihlašovací stránku)
`email_log`, `zpravy`	Odeslané e-maily, schránka zpráv podle eID

Celkem 12 tabulek (`sql/schema.sql` a číslované migrace). Databáze má vlastního uživatele; nástroje se k ní připojují přes knihovnu, ne přímo svými účty.

E6. Rozsah díla

Oblast	Souborů	Řádků kódu
Přihlášení účtem RIS a uživatelé	2	260

Oblast	Souborů	Řádků kódu
Struktura organizací	1	88
Číselník a skupiny funkcí	1	185
E-maily, alternativní e-mail a schránka zpráv	1	204
Základ (připojení, konfigurace, schéma)	7	370
Celkem	**12**	**1 107**

Část F – Bezpečnost a ochrana osobních údajů

Tato část shrnuje zabezpečení a nakládání s osobními údaji v celé rodině systémů. Podrobnosti k jednotlivým systémům jsou v kapitolách B9 (MoČRS), C6 (sport) a D6 (fórum).

F1. Šifrovaný přenos a komunikace s okolím

- Všechny tři systémy běží výhradně na **HTTPS** – přihlašovací údaje, osobní údaje i cookies relace putují mezi prohlížečem a serverem šifrovaně. Rozcestník navíc posílá hlavičku **HSTS** (1 rok) – prohlížeč ho pak otevírá jen přes HTTPS, i když uživatel zadá adresu bez https. Požadavek, který na rozcestník přesto přijde přes HTTP, aplikace přesměruje na HTTPS (301, u odeslaných formulářů 303).
- Šifrovaná je i komunikace serveru s okolními systémy: RIS (HTTPS, HTTP Basic jen přes šifrované spojení), Comgate (HTTPS API, údaje obchodu v konfiguraci), Google Gemini (HTTPS), odesílání e-mailů (SMTP se STARTTLS / SSL).
- Rozhraní RIS používají technické účty z konfigurace mimo repozitář. Rozcestník RIS jen čte (stráž, funkcionáři, brigády, příspěvky, storna povolenek); **jediný zápis do RIS** v celé rodině systémů je zápis uhrazené sportovní známky sportovním portálem, který se zapíná výslovně v konfiguraci.
- Odkazy v e-mailech (ověření e-mailu, PDF výpisy Comgate, upozornění z fóra) vedou na HTTPS adresy z konfigurace.

F2. Přihlášení, hesla a relace

- **Hesla RIS se nikde neukládají** – ověřuje je RIS a systémy si drží jen výsledek (eID, funkce). Původní účty rozcestníku (E-Sumář, lokální) mají hesla jen jako hash a po převodu na účet RIS se jimi už nelze přihlásit.
- Oprávnění se odvozují z **platných funkcí v RIS** při každém přihlášení – kdo funkci v RIS ztratí, přijde o práva při příštím přihlášení, bez ruční správy účtů. Správci se určují podle eID nebo funkce, ne podle sdílených účtů.
- Relace: cookies s příznaky HttpOnly (nepřečte je JavaScript), SameSite (neposílají se s požadavky z cizích webů) a Secure (jen přes HTTPS) ve všech systémech, obnova ID relace po přihlášení, návrat po přihlášení jen na stránky téže aplikace.
- Společná relace nástrojů (`crs_ucet`): v databázi jen otisk tokenu, vyprší po 8 hodinách nečinnosti; odhlášení v jednom nástroji odhlásí ze všech, přihlášení e-mailem v rozcestníku ji zruší.
- Každý pokus o přihlášení (i neúspěšný) se loguje s IP adresou – rozcestník ve vlastním logu s přehledem pro admina, fórum v logu knihovny účtů, sport ve vlastním logu.
- **Omezení pokusů** (rozcestník): po 10 neúspěšných pokusech na účet nebo 30 z jedné IP adresy během 15 minut je přihlášení na 15 minut zablokované a heslo se neověřuje ani správné – zkoušení hesel tak nejde automatizovat.
- **Doba uchování**: logy přihlášení a e-mailů se uchovávají **1 rok** – starší záznamy se průběžně mažou automaticky (rozcestník: přihlášení, rozeslané notifikace, rozesílka výpisů Comgate; knihovna účtů: přihlášení a e-maily všech nástrojů; sport: přihlášení). Schránka zpráv uživatele je obsah, ne log, a nemaže se.

F3. Řízení přístupu

- Rozsah dat se počítá na serveru ze session, nikdy z parametrů prohlížeče: v rozcestníku Rada / ÚS / MO (MO vidí jen sebe), ve fóru dvojice funkce × organizace, ve sportu správa jen pro funkci správce.
- Jemnější práva: v rozcestníku územní svaz na jednom místě nastaví svým MO moduly (nevidí / vidět / vyplňovat) a analytické dlaždice, s výjimkami pro skupiny funkcí RIS; ve fóru vidí témata jen vybrané skupiny funkcí. Kontrola je na každé stránce i akci, ne jen v menu.
- Soubory s osobními údaji (dokumenty, přílohy, PDF výpisy a přehledy) leží mimo přímý přístup z webu a vydávají se skriptem po kontrole práv; veřejné odkazy jsou neuhodnutelné, odkazy na výpisy v e-mailech mají omezenou platnost. V rozcestníku platí i pro přílohy helpdesku, úkolů a metodiky.
- Výběr organizace v adrese (např. MO ve filtru) se vždy ověřuje proti rozsahu uživatele; chybějící nebo neznámá organizace znamená **žádný přístup**, nikdy celou ČR. Úpravy záznamů (formuláře, metodika, aktuality) se ověřují na serveru podle vlastníka záznamu, ne podle toho, co stránka nabízí.

F4. Ochrana aplikací

- Parametrizované dotazy do databáze (ochrana proti SQL injection), escapované výstupy, čištění HTML z editorů podle seznamu povolených značek (aktuality, příspěvky fóra, zpráva o činnosti, tato dokumentace, propozice závodů z RIS ve sportu), CSRF tokeny ve všech formulářích; akce měnící data jen přes POST.
- Rozcestník: bezpečnostní hlavičky (zákaz vkládání do cizích rámů, nosniff, Referrer-Policy, Permissions-Policy, CSP v režimu Report-Only), kontrola integrity (SRI) u všech knihoven z CDN, přísný režim relace, vypnutý výpis chyb, zákaz přístupu k souborům mimo PHP a k vnitřním knihovnám přes `.htaccess`; přihlášení neprozradí existenci e-mailu dobou odpovědi. Sportovní portál tato opatření zatím nemá (kap. F9).
- Nahrávané soubory: povolené typy, kontrola i skryté přípony, přeuložení obrázků, zákaz spouštění skriptů v adresářích s nahranými soubory, zákaz výpisu jejich obsahu.
- Na serveru ani v repozitáři nejsou záložní kopie skriptů a diagnostické soubory (odstraněny při revizi 11/2026, vzory přípon v `.gitignore`).
- Tokeny v odkazech se ukládají jen jako otisk (SHA-256); stav plateb se vždy ověřuje přímo u Comgate včetně částky, nikdy se nepřebírá z prohlížeče.
- Přístupové údaje (databáze, SMTP, Comgate, AI, tokeny cronů) jsou v konfiguračních souborech mimo repozitář; každý systém se ke své databázi připojuje vlastním účtem, E-Sumář se jen čte.
- Chyby se zapisují do logu serveru, běžný uživatel vidí srozumitelnou hlášku bez technických detailů.

F5. Osobní údaje v systémech

Systém	Osobní údaje	Zdroj a účel
Knihovna účtů	eID, účet RIS, jméno, e-mail a telefon z RIS, alternativní e-mail, funkce a organizace, log přihlášení (IP, prohlížeč), log e-mailů, schránka zpráv	RIS při přihlášení; přihlášení, oprávnění, upozornění

Systém	Osobní údaje	Zdroj a účel
MoČRS	Účty a jejich e-maily, log přihlášení s IP, blokované osoby (eID, důvod); v analytikách eID a ročník (bez jmen) u transakcí, členství, migrace a strážců; čísla povolenek a průkazů; u žádostí o storna povolenek eID a jméno držitele, pokud je RIS vrátí; platby Comgate (eID a e-mail plátce – e-mail se nezobrazuje); autoři žádostí, dotazů, odpovědí a návrhů na úpravu; u kontrol rybářské stráže z RIS jméno a číslo odznaku strážce (výkon funkce) a číslo kontrolované povolenky (nezobrazuje se) – **žádné údaje o kontrolovaných osobách**	RIS a E-Sumář (importy, čtení), Comgate; správa svazu, analytika, agendy
Sportovní portál	Sportovci, trenéři, rozhodčí: jméno, datum narození a rodné číslo, číslo sportovce, MO, eID; platby (plátce, e-mail, účet RIS, IP), doklady; u závodů jména ředitele, garanta a hlavního rozhodčího (veřejně, jako v propozicích); do RIS se zapisuje uhrazená známka sportovce	RIS (synchronizace), plátci; prodej známky, doklady, průkaz, výpis pro NSA, kalendář závodů
Fórum	Jméno, organizace a eID autora u příspěvků, sledování vláken a témat, nastavení upozornění	Knihovna účtů; diskuze funkcionářů

F6. Zásady ochrany osobních údajů

- **Minimalizace**: systémy převzaté údaje nerozšiřují – registr osob vede RIS. Analytiky pracují s eID místo jmen a se souhrny; souhrn členské základny z RIS je bez osobních údajů. Veřejně se zobrazuje jen nezbytné (sport: jméno, rok narození, číslo sportovce, odvětví, stav známky; veřejný přehled hájení bez zdůvodnění a autorů).
- **Pseudonymizace a oddělení**: databáze jednotlivých systémů jsou oddělené, propojení probíhá jen přes eID v aplikaci; citlivé údaje (rodné číslo, datum narození, e-mail plátce) vidí jen správa.
- **Umělá inteligence**: do Google Gemini jdou jen souhrnná čísla bez osobních údajů a bez názvů cizích organizací; AI nemá přístup k databázím (AI asistent smí volat jen předem dané nástroje s oprávněním přihlášeného). Každé volání se loguje.
- **Účelové omezení**: údaje se používají jen pro agendy svazu, ke kterým byly převzaty; e-maily jen pro upozornění, která si uživatel nevypnul (služební zprávy vždy).
- **Dohledatelnost**: logy přihlášení, e-mailů, importů, plateb a AI umožňují zjistit, kdo co a kdy udělal; mazání v diskuzích a dokumentech je skryté nebo přes koš.
- **Cookies**: rozcestník používá jen technicky nezbytné cookies přihlášení (vlastní relace a společná relace nástrojů `crs_ucet`) a místní úložiště prohlížeče pro nastavení zobrazení; žádné měření návštěvnosti, reklamu ani sledování, proto nevyžaduje souhlas. Popisuje to na veřejné stránce „Cookies a soukromí“ (`cookies.php`) včetně obsahu třetích stran a doby uchování logů.

F7. Doporučení a otevřené body

- Stanovit dobu uchování ostatních záznamů – logů AI, komunikace s platební bránou, synchronizace a importovaných transakcí (logy přihlášení a e-mailů už mají 1 rok).
- Sjednotit starší stránky rozcestníku na společnou kontrolu přístupu (`crs_scope.php`) (CSRF, kontroly rozsahu a vypnutí výpisu chyb už doplněny).
- Rozcestník: přepnout Content-Security-Policy z režimu „Report-Only“ na vynucující, na serveru nastavit `ServerTokens Prod`, `ServerSignature Off`, `TraceEnable Off`; dotestovat fórum a přihlášení účtem RIS na

testovací kopii serveru; po zprovoznění odstranit diagnostické stránky (stráž, dohledání povolenky v RIS).

- Sportovní portál: doplnit opatření z kap. F9 (ochrana souborů, hlavičky, tokeny cronů, SRI, limit pokusů o přihlášení), změnit heslo účtu testovacího RIS uvedeného ve vzoru konfigurace a před ostrým provozem odstranit složku `diagnostika/`.
- Pravidelně měnit přístupová hesla k databázím a poště, každé jiné; přístup k databázi E-Sumáře povolit jen z adresy webového serveru.
- Před každým nasazením zkontrolovat, že na server nejdou záložní ani diagnostické soubory.
- Promítnout zpracování do záznamů o činnostech zpracování ČRS (správce, účely, kategorie údajů, zpracovatelé – hosting, Comgate, Google) a ověřit smluvní zajištění zpracovatelů.
- Pravidelně obnovovat knihovny třetích stran (PHPMailer, dompdf, editory z CDN) a při změně verze přepočítat otisky SRI.
- Cookies a třetí strany: videa YouTube načítat až po kliknutí (nebo přes youtube-nocookie.com), knihovny vzhledu hostovat na vlastním serveru místo CDN; na stránku Cookies doplnit správce údajů a kontakt na pověřence; ověřit, zda informační stránky mají i sport a fórum.
- HSTS rozšířit o `includeSubDomains` (případně preload) až po ověření, že všechny subdomény běží na HTTPS; přesměrování HTTP → HTTPS nastavit i v konfiguraci serveru a cron úlohy volat přes https.

F8. Bezpečnostní revize rozcestníku (listopad 2026)

Revize kódu rozcestníku zaměřená na **úniky dat a přístup k datům mimo přidělenou roli** (Rada / ÚS / MO). Nalezené problémy jsou opravené; přehled slouží jako záznam o provedených opatřeních a jako vodítko pro další vývoj.

Oblast	Zjištění	Opatření
Výběr MO v přehledech ÚS	ÚS mohl úpravou adresy zobrazit data MO jiného svazu (platby včetně eID plátců, migrace, analytika členů, regionální přehledy úlovků a stráže).	Výběr MO se ověřuje proti MO vlastního ÚS, cizí MO se ignoruje.
Uživatel bez organizace	Prázdný rozsah organizací se na několika stránkách vyhodnotil jako „bez omezení“ = celá ČR.	Odmítnutí přístupu (403); práva modulů a analytik „nevidí“.
Formuláře	Otázky a heslo cizího formuláře šlo změnit nebo smazat.	Oprávnění (admin, autor, ÚS formuláře) se ověřuje před zobrazením editoru i uložením.
Přílohy helpdesku, úkolů a metodiky	Soubory byly dostupné přímým odkazem i bez přihlášení.	Přímý přístup zakázán, soubory vydávají skripty po kontrole práv; přílohy vyřazeny z repozitáře.
Metodika	ÚS mohl upravit či smazat cizí i celostátní sekce a založit celostátní sekci; odkaz položky nebyl kontrolován.	Kontrola vlastníka sekce, celostátní sekce jen admin, odkazy jen http(s), video jen z povolených serverů.
Záložní a diagnostické soubory	Staré kopie skriptů obcházely novější opravy, zálohy server vydával jako čitelný text.	Odstraněny ze serveru i repozitáře; vzory přípon v `.gitignore`.

Přístupové údaje	Přístupy k databázím byly přímo v kódu.	Přesunuty do `config_db.php` mimo repozitář (vzor `config_db.example.php`).
Přihlášení	Neomezený počet pokusů o heslo; po přihlášení e-mailem se neobnovovalo ID relace.	Limit 10 pokusů na účet a 30 na IP adresu za 15 minut, blokace 15 minut; obnova ID relace, při odhlášení smazání cookie.
Podvržené požadavky (CSRF)	Přibližně 60 starších stránek přijímalo formuláře bez tokenu; aktuality se mazaly odkazem.	Token ve všech formulářích (`csrf.php`, 94 formulářů, 7 volání z JavaScriptu); mazání aktualit přes POST.
Výpis adresářů	Při zapnutém výpisu adresářů na serveru by šel zobrazit seznam příloh aktualit a obrázků.	Prázdný `index.html` ve veřejných složkách s nahranými soubory.
Výsledky formulářů a úkolů	Prověřeno: zobrazení i export jsou omezené na organizace v rozsahu uživatele.	Bez změny.

Zásady pro další vývoj (aby se úniky neopakovaly):

- Rozsah dat vždy ze session přes `crs_scope()` / `crs_scope_allows()`; parametr z adresy (organizace, záznam) je jen přání a musí se ověřit proti rozsahu uživatele.
- Chybějící nebo neznámý údaj o organizaci či roli znamená **žádný přístup** – nikdy prázdný filtr.
- Úprava a mazání záznamu: nejdřív načíst záznam a ověřit vlastníka, teprve potom měnit – a to pro všechny navazující údaje (otázky, položky, soubory).
- Soubory s daty ukládat do adresáře se zákazem přímého přístupu a vydávat je skriptem s kontrolou práv (`soubor_lib.php`).
- Každý formulář s `method="POST"` obsahuje `csrf_pole()` a stránka volá `csrf_over()`; akce měnící data nikdy přes odkaz (GET).
- Hesla a tokeny jen v `config_*.php` mimo repozitář; na server nenahrávat zálohy ani diagnostické skripty.

F9. Penetrační testy a bezpečnostní nástroje (listopad 2026)

Na revizi kódu (kap. F8) navázaly penetrační testy podle metodiky v adresáři `security/` (OWASP WSTG 4.2, ASVS 4.0.3 úroveň 2, hodnocení CVSS 3.1). Adresář obsahuje metodiku, nástroje a protokoly; z webu je zakázaný a nástroje běží jen z příkazové řádky. Protokoly popisují slabiny systému – **nesdílet veřejně**.

Nástroj	K čemu slouží
`test_ochran.php`	Testy ochranných funkcí bez databáze – čištění HTML, bezpečné adresy, kontrola nahrávaných souborů (123 testů). Spouštět před každým nasazením.
`staticky_audit.php`	Automatická revize kódu (kontroly S01–S12): stránky bez kontroly přihlášení, formuláře bez CSRF, SQL s vloženou proměnnou, výpis chyb, diagnostické skripty, knihovny z CDN bez SRI …; výsledkem jsou kandidáti k ruční kontrole.

`dynamicky_test.php`	Test běžící instance (D01–D16): hlavičky, citlivé soubory, přístup bez přihlášení, XSS, přesměrování, crony, CSRF, eskalace práv, přístup k datům cizí organizace (IDOR). Výchozí sada je nedestruktivní.

Kolo	Rozsah	Výsledek
Kolo 1 (6. 11. 2026)	Revize kódu rozcestníku a automatizované nástroje.	13 nálezů (N-01 až N-13), nejvýš střední závažnosti: výchozí token cronu Comgate, chybějící kořenový `.htaccess`, bezpečnostní hlavičky, výpis chyb v 85 skriptech, diagnostika stráže bez CSRF, testovací účty v přihlášení, nastavení relace, přímo volatelné fragmenty, knihovny z CDN bez SRI a drobnosti. Opraveno kromě N-05 (diagnostika stráže – po ladění smazat) a N-11 (přihlašovací formulář bez CSRF – akceptováno).
Kolo 2 (6. 11. 2026)	Opakování + dynamické testy lokální instance (Apache 2.4, PHP-FPM, HTTPS, MariaDB) s účty všech rolí, přes 2 000 požadavků.	Opravy z kola 1 ověřeny. Řízení přístupu obstálo – nepřihlášený, MO ani ÚS se k datům cizí organizace nedostali. 4 nové nálezy, opravené: N-14 zjištění existence e-mailu podle doby odpovědi, N-15 název cizí organizace v detailu prodejů, N-16 přímo volatelné knihovny fóra a výpočty zprávy, N-17 slepé místo skeneru. Neotestováno: fórum a přihlášení účtem RIS (vyžadují knihovnu účtů a RIS).
Doplněk (10. 11. 2026)	Revize kódu změn od kola 2 v rozcestníku (storna povolenek, brigády a příspěvky z RIS, blokace osob, návrhy na úpravu, výpočty zprávy ze sportu) a první revize sportovního portálu.	Rozcestník: nové části mají kontrolu přihlášení, rozsahu a CSRF, RIS jen čtou; nová diagnostická stránka dohledání povolenky (jen admin) – po zprovoznění storen odstranit. Sportovní portál: řízení přístupu a CSRF v pořádku, chybí ale ochrana konfigurace serveru zavedená v rozcestníku – soubory mimo PHP (`README.md`, `sql/`) nejsou chráněné `.htaccess`, chybí bezpečnostní hlavičky a SRI, crony přijmou prázdný či výchozí token, chybí limit pokusů o přihlášení, ve vzoru konfigurace jsou přístupové údaje testovacího RIS a diagnostický skript RIS je dostupný bez přihlášení. Podrobně v protokolu `security/protokoly/2026-11-10_doplnek_protokol.md`.

Souhrnný bezpečnostní audit MoČRS ve výsledné podobě je v `security/audit/bezpecnostni_audit.html` (PDF v `security/protokoly/`). Nové kolo testů se řídí postupem v `security/README.md`; protokol se zakládá podle šablony v metodice.

Část G – Rozsah díla celkem

G1. Souhrn všech systémů

Vlastní kód všech systémů včetně společné knihovny účtů (PHP, JS, CSS, SQL; bez knihoven třetích stran, písem a nahraných souborů). Počet tabulek u MoČRS zahrnuje tabulky, které zakládá aplikace sama, u ostatních tabulky ve schématu a migracích.

Systém	Tabulek DB	Souborů	Řádků kódu
Informační rozcestník MoČRS	160	434	114 300
Sportovní portál ČRS	14	59	7 022
Fórum ČRS	13	39	4 888
Společná knihovna účtů ČRS	12	12	1 107
Celkem	**199**	**544**	**127 317**