MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Metodické usmernenie
Ministerstva investícií, regionálneho rozvoja a informatizácie
č. 024077/2023 z 2023
o kvalite zdrojových kódov a balíkov softvéru

Určené pre**:**	Sekcia informačných technológií verejnej správy, orgány riadenia podľa § 5 ods. 2 zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
Vydáva:	Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky, Sekcia informačných technológií verejnej správy
Záväznosť:	Tento dokument má odporúčací charakter
Počet príloh:	3
Dátum vydania:	05.12. 2023
Dátum účinnosti:	08.12. 2023
Schválil:	Ildikó Štúňová poverená vykonávaním funkcie generálneho riaditeľa sekcie Sekcia informačných technológií verejnej správy Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky

Obsah

Ministerstvo investícií, regionálneho rozvoja a informatizácie podľa § 15 ods. 2 písm. d) bod 1 zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a § 5 ods. 15, § 6 ods. 8 a 9 a § 14 ods. 15 vyhlášky Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. 401/2023 Z. z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy vydáva toto metodické usmernenie o kvalite zdrojových kódov a balíkov softvéru.

čl. 1

Predmet úpravy

(1) Predmetom tohto metodického usmernenia je obsah balíkov softvéru informačných systémov verejnej správy, procedúry ich kontroly a riadenia vydaní.

čl. 2

Cieľ

(1) Cieľom tohto metodického usmernenia je poskytnutie podkladov pre procedúry kontroly softvéru a riadenia vydaní tak, aby bolo možné efektívne vykonať ich kontrolu automatizovane, alebo s využitím ľudských zdrojov.

(2) Metodika zároveň ponúka podklady pre voľbu licenčného krytia vyvíjaného softvéru s dôrazom na zverejnenie zdrojových kódov informačných systémov verejnej správy tak, aby bolo možné zabezpečiť ich ďalší rozvoj a použitie v iných informačných systémoch verejnej správy.

čl. 3

Vymedzenie základných pojmov

(1) Na účely tohto metodického usmernenia sa rozumie

a) zdrojovým kódom softvéru kolekcia textu, s alebo bez komentárov, písaného použitím človekom čitateľného programovacieho jazyka
b) preexistentným zdrojovým kódom je zdrojový kód tej časti diela, ktorá je softvérovým produktom alebo službou tretej strany s jasne definovanými licenčnými pravidlami
c) balík softvéru kolekcia zdrojového kódu, skompilovaného kódu, inštalačného balíka alebo dokumentácie v prípade, že je distribuovaná samostatne
d) licenciou zmluvné dojednanie spôsobu použitia a distribúcie softvéru
e) programovacím jazykom systém notácií pre písanie počítačových programov,
f) vývojovým prostredím všetky prostriedky IKT, ktoré sú používané pre vývoj softvéru.

Všeobecné pravidlá

čl. 4

Použitý jazyk

Časti používateľského rozhrania, ktoré sú súčasťou zdrojového kódu, musia byť uvádzané v slovenskom jazyku. Ďalšie jazyky môžu byť podporované rozhraním lokalizácie použitého programovacieho jazyka.

čl. 5

Formát obsahu

Súbory balíka softvéru sú uložené spôsobom podľa vyhlášky Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy v znení vyhlášky Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. 546/2021 Z. z. (ďalej len „vyhláška o štandardoch pre ITVS“).

Metadáta

čl. 6

Metadáta názvu

(1) Názov balíka softvéru je zrozumiteľný, jedinečný a mal by vyjadrovať súvis so službou alebo funkciou, ktorú implementuje.

(2) Zmena pôvodného názvu softvérového komponentu je prípustná ak

a) došlo ku konfliktu mien v názvoch softvérových komponentov,
b) názov pôvodného komponentu obsahuje znaky mimo prenositeľnú znakovú[1)] sadu alebo
c) iného opodstatneného dôvodu.

(3) Zmena pôvodného názvu aj so zrozumiteľným zdôvodnením musí byť uvedená v dokumentácii, ktorá je súčasťou balíka softvéru.

čl. 7

Metadáta verzie

(1) Softvér musí mať jednoznačné sémantické pravidlá označenia verzií. Tieto pravidlá označenia verzií musí zohľadňovať dátová štruktúra repozitára alebo jeho stav popísaný metadátami tak, aby bolo možné jednoznačne určiť verziu softvéru pripravenú na ďalšie spracovanie.

(2) Pravidlá označenia verzií softvérového komponentu musia zohľadňovať požiadavku na priame strojové porovnávanie verzií bez nutnosti implementácie prídavných funkcionalít repozitára alebo nástrojov na ďalšie spracovanie zdrojových kódov.

(3) Označenie verzie musí zohľadňovať možnosť jednoduchého triedenia a zoraďovania reťazcov verzií nezávisle na nastaveniach prostredia, v ktorom sa porovnanie vykonáva.

(4) Označenie verzie softvérového komponentu musí byť zrozumiteľne, jedinečne zaznamenané a konzistentné vo všetkých častiach diela.

(5) Spôsob označenia verzií softvérového komponentu môže byť zaznamenaný vo forme informácie v dokumentácii zdrojového kódu a štruktúry súborového systému alebo metadát repozitára.

[1)] POSIX.1-2017, kapitola 3.282 Portable Filename Character Set, https://pubs.opengroup.org/onlinepubs/9699919799

čl. 8
Licencia

(1) Zvolená licencia by mala umožniť zverejnenie a použitie softvérového balíka v požadovanom rozsahu.

(2) Zvolená licencia softvérového balíka je jednoznačným spôsobom uvedená vo forme

a) názvu zvolenej licencie uvedenom v referenčnom zozname[2)]
   a. v hlavičke súboru zdrojového kódu alebo
   b. v metadátach repozitára softvéru,
b) súboru s úplným názvom a znením licencie podľa požiadaviek uvedených v čl. 16.

(3) Typ licencie je volený z priorizovaného zoznamu licenčných modelov:

a) licencie verejnej domény,
b) copyleft licencie,
c) permissive licencie,
d) nekomerčné licencie,
e) proprietárne licencie alebo
f) licencie obchodného tajomstva.

(4) Voľba typu licencie z nižšej položky v zozname podľa odseku (3) musí byť zdôvodnená a zdokumentovaná.

(5) Ak existuje možnosť zvoliť z viacerých typov licencií, je vhodné zvoliť taký typ, ktorý poskytne najvyššiu mieru slobody pre opätovné použitie softvéru.

čl. 9
Doplňujúce informácie

(1) Súčasťou balíka softvéru sú aj kontaktné informácie o

a) správcovi zdrojového kódu,
b) tvorcovi distribuovaného balíka softvéru,
c) ostatných členov tímu vývojárov, ktorí sa podieľali na úprave zdrojového kódu, podľa uváženia.

(2) Kontaktné údaje musia byť uvedené minimálne v rozsahu e-mailovej adresy, a spôsobom, ktorý umožní ich automatizované spracovanie.

(3) Je vhodné uviesť aj ďalšie informácie, ktoré umožnia katalogizáciu a správu softvéru, a to:

a) kategória,
b) podporovaná architektúra,
c) typ balíka,
d) popis,
e) informácie o závislostiach,
f) ďalšie značky v rozsahu podľa požiadaviek distribúcie a správy repozitára a katalógu softvéru.

[2)] SPDX® License list, https://spdx.org/licenses/

čl. 10

Kontext pôvodného repozitára

(1) Zdrojový kód prevzatého softvéru, ktorý je priamo začlenený do zdrojového kódu vyvíjaného softvéru, musí byť v repozitári uložený tak, aby stav repozitára zohľadňoval metadáta pôvodného zdroja, a to najmä:

a) typ a veľkosť súboru,
b) časové pečiatky vytvorenia a poslednej úpravy súboru a
c) oprávnenia na prístup k zdrojovému kódu.

(2) Informácie o prevzatom softvéri sú zverejnené v rozsahu a spôsobom podľa čl. 23 ods. (1) a (2).

(3) Ak je zdrojový kód prevzatého softvéru priamo začlenený a upravený voči pôvodnému zdroju, musia byť kontaktné informácie podľa čl. 9 ods. (1) aktualizované. V takomto prípade musí byť informácia o pôvodnom zdroji a úpravách vhodne zahrnutá v metadátach repozitára a dokumentácii softvéru.

čl. 11

Menné konvencie

(1) Menné konvencie všetkých adresárových a sémantických štruktúr použité pri vývoji softvéru musia byť zrozumiteľné, jasné a súvisiace s predmetom alebo funkciou kódu a zároveň

a) nesmú obsahovať dvojzmyselné, hanlivé alebo inak nevhodné výrazy,
b) obsahujú výhradne prenositeľnú znakovú sadu[3)] s cieľom zabezpečiť vysokú úroveň prenositeľnosti kódu a
c) zohľadňujú obmedzenia všetkých podporovaných platforiem na pomenovanie štruktúr súborového systému.

(2) Adresárové štruktúry zdrojového kódu sú zrozumiteľné, jedinečne a jasne pomenované v súlade s očakávanou základnou štruktúrou zdrojových kódov podľa čl. 16 a v súlade s všeobecne platnými odporúčaniami použitého programovacieho jazyka, vývojového prostredia, či platformy.

(3) Sémantické štruktúry zdrojového kódu sú jasne pomenované v súvislosti s funkciou, ktorú vykonávajú, či predmetom alebo triedou, ktorú reprezentujú a sú v súlade s všeobecne platnými odporúčaniami použitého programovacieho jazyka, vývojového prostredia alebo platformy.

Zdrojový kód

čl. 12

Forma sprístupnenia zdrojového kódu

(1) Zdrojový kód má byť sprístupnený v plnom rozsahu diela prostredníctvom

a) požiadavky na aktualizáciu repozitára v systéme kontroly revízií alebo
b) archívneho súboru s obsahom
    1. exportu repozitára zo systému kontroly revízií alebo
    2. sady záplat.

[3)] POSIX.1-2017, kapitola 3.282 Portable Filename Character Set, https://pubs.opengroup.org/onlinepubs/9699919799

(2) Archívny súbor s obsahom zdrojového kódu musí byť sprístupnený spôsobom, ktorý poskytuje dostatočnú úroveň garancií dôveryhodnosti a integrity obsahu v súlade s odporúčaniami uvedenými v čl. 20.

(3) Rozhranie pre sprístupnenie zdrojového kódu musí byť dostupné nepretržite a umožňovať priame stiahnutie zdrojového kódu vo forme archívneho súboru v súlade s § 25 vyhlášky o štandardoch pre ITVS a v súlade s podmienkami uvedenými v čl. 33.

čl. 13
Účel sprístupnenia zdrojového kódu

Účelom sprístupnenia zdrojového kódu je

a) zvýšenie kvality umožnením jeho priebežnej revízie,
b) zefektívnenie vývoja nových komponentov umožnením modifikácie a opätovného použitia kódu,
c) zvýšenie miery transparentnosti vývoja s možnosťou priebežnej revízie zmien,
d) ďalšie účely, ktoré nie sú v rozpore s distribučnou licenciou alebo zákonom.

čl. 14
Obsah zdrojového kódu

(1) Zdrojový kód musí obsahovať všetky komponenty, ktoré umožnia jeho preklad, spustenie alebo vytvorenie inštalačného balíka, a to najmä

a) zdrojový kód predmetnej aplikácie v súlade s týmto usmernením,
b) zdrojový kód závislostí, prípadne ich priame referencie v podporných súboroch,
c) podporné súbory vývojových nástrojov,
d) podporné súbory nástrojov balenia softvéru,
e) podporné súbory testovacích nástrojov a testovacie skripty,
f) metadáta pre jednoznačnú identifikáciu zdrojového kódu a jeho verzie.

(2) Zdrojový kód nesmie obsahovať citlivé a dôverné údaje, a to najmä

a) prihlasovacie údaje,
b) heslá,
c) kľúče,
d) IP alebo URI adresy,
e) iné bezpečnostné predmety a citlivé údaje.

čl. 15
Kvalita zdrojového kódu

(1) Zdrojový kód musí byť

a) človekom čitateľný a
b) komentovaný priamo v kóde tak, aby bola zjavná jeho štruktúra a funkcionalita čítaného kódu.

(2) Štýl zdrojového kódu by mal byť jednotný.

(3) Zdrojový kód nesmie byť modifikovaný spôsobom, ktorý zásadne obmedzuje jeho čitateľnosť, spracovanie alebo schopnosť porozumenia logike programu, a to najmä

a) strojovo modifikovaný,
b) šifrovaný,

c) minimalizovaný,
d) komprimovaný alebo
e) inak modifikovaný

čl. 16
Štruktúra zdrojového kódu

(1) Štruktúra zdrojového kódu by mala byť stála, aby bolo možné opakovane automatizovane zdrojový kód analyzovať a testovať.

(2) V koreňovom adresári repozitára zdrojového kódu sú uvedené súbory

a) **LICENSE** s plným znením textu zvolenej licencie zdrojového kódu predmetného softvéru a závislostí,
b) **README** so základnou dokumentáciou zdrojového kódu,
c) **INSTALL** s popisom postupu prípravy a inštalácie výsledného softvérového balíka,
d) **CONTRIBUTING** s popisom komunikácie a postupov otvorenej spolupráce na vývoji,
e) **SECURITY** so základnými informáciami o riadení bezpečnosti predmetného softvéru a popisom komunikácie hlásenia bezpečnostných zraniteľností,
f) **CODE_OF_CONDUCT** s popisom hodnôt a etických princípov pre zamestnancov verejného sektora, členov vývojového tímu a projektu pri vývoji softvéru,
g) **VERSIONING** s popisom pravidiel číslovania verzií,
h) **CHANGELOG** s popisom histórie verzií a vykonaných zmien.

(3) Adresárová štruktúra repozitára zdrojového kódu by mala zohľadňovať logické oddelenie

a) súborov vykonávacieho kódu,
b) podporných knižníc, modulov a závislostí,
c) dátových súborov,
d) konfiguračných súborov,
e) iných podporných súborov,
f) dokumentácie.

s prihliadnutím na požiadavky prípravy vydaní balíkov softvéru, ich ďalšie spracovanie alebo opätovné použitie.

(4) V koreňovom adresári repozitára zdrojového kódu môžu byť uvedené ďalšie štruktúry súborového systému podľa potrieb projektu tak, aby boli zrozumiteľné, neboli v rozpore s inými požiadavkami tejto metodiky alebo inými právnymi predpismi.

Balík softvéru

čl. 17
Forma sprístupnenia balíka softvéru

(1) Súbor balíka softvéru má byť sprístupnený v plnom rozsahu diela a formou

a) inštalačného balíka podporovanej platformy,
b) samostatne spustiteľného súboru alebo

c) archívneho súboru s obsahom skompilovaných softvérových komponentov a dokumentácie požiadaviek a postupu inštalácie.

(2) Rozhranie na sprístupnenie softvéru musí byť dostupné nepretržite a umožňovať priame stiahnutie balíka softvéru vo forme uspôsobenej na manuálnu alebo automatizovanú inštaláciu a v súlade s podmienkami uvedenými v čl. 33.

(3) Súčasťou balíka softvéru a jeho metadát musí byť jednoznačná informácia o názve a verzii softvéru.

čl. 18
Účel sprístupnenia balíka softvéru

(1) Účelom zverejnenia balíka softvéru sa považuje

a) umožnenie inštalácie softvéru v prostrediach produkčného nasadenia pre verzie, ktoré prešli procesom odsúhlasenia vydaní podľa čl. 32,
b) umožnenie inštalácie softvéru v prostrediach vývojového cyklu pre zabezpečenie naplnenia požiadaviek jednotlivých fáz vývojového cyklu,
c) zvýšenie kvality umožnením priebežnej revízie jeho obsahu,
d) umožnenie validácie integrity súboru voči pôvodnému zdroju,
e) prípadné ďalšie účely, ktoré nie sú v rozpore s distribučnou licenciou alebo zákonom.

čl. 19
Obsah balíka softvéru

(1) Balík softvéru musí obsahovať všetky komponenty, ktoré umožnia jeho inštaláciu, a to najmä

a) spustiteľný kód predmetnej aplikácie,
b) podporné súbory inštalácie pre zabezpečenie základnej kontroly
    1. požiadaviek inštalácie
    2. dostupnosti závislostí
c) metadáta pre jednoznačnú identifikáciu inštalovaného softvéru a jeho verzie.

(2) Balík softvéru nesmie obsahovať citlivé a dôverné údaje uvedené v čl. 14 ods. (2).

čl. 20
Kvalita balíka softvéru

(1) Dôveryhodnosť balíka softvéru je garantovaná

a) informáciami o názve softvéru, verzii a dátume vydania, a prípadných ďalších metadátach, ktoré sú uložené v interných štruktúrach súboru tak, že ich nie je možné zmeniť bez narušenia integrity súboru,
b) elektronickým podpisom súboru kľúčom, ktorého dôveryhodnosť pre toto použitie je možné kedykoľvek overiť vo verejne dostupnom zdroji.

(2) Integrita balíka softvéru je garantovaná

a) hešovacím kontrolným súčtom inštalačného súboru alebo
b) elektronickým podpisom súboru kľúčom, ktorého dôveryhodnosť pre toto použitie je možné kedykoľvek overiť v dostupnom zdroji.

(3) Integrita obsahu balíka softvéru je garantovaná zoznamom mien súborov, ktoré sú predmetom inštalácie, s ich hešovacím kontrolným súčtom a integrita týchto súborov je v priebehu inštalačného procesu skontrolovaná.

(4) Úrovne garancií dôveryhodnosti, konzistencie a integrity balíka softvéru musia byť kedykoľvek overiteľné štandardnými nástrojmi pre správu inštalačných súborov operačného systému alebo aplikačného rozhrania operačného systému.

(5) Pri redistribúcii súboru je nutné zachovať mieru garancií na požadovanej úrovni. Súčasťou redistribúcie musia byť všetky časti, ktoré umožnia kontrolu dôveryhodnosti a integrity balíka softvéru. Zároveň by mala byť zverejnená informácia o zdrojovom repozitári pre umožnenie spätnej kontroly súboru a súladu verzií.

Závislosti softvéru

čl. 21
Závislosť softvéru

(1) Závislosťou softvéru sa rozumie

a) iný softvérový komponent,
b) dátová štruktúra,
c) rozhranie aplikačného programovania (API),
d) alebo binárne aplikačné rozhranie (ABI),

(2) Závislosti podľa odseku (1) písm. a) a b) sú spravidla priamym predpokladom pre preklad, spustenie alebo správnu funkčnosť softvéru.

(3) Závislosťou softvéru nie je

a) štandardné API rozhranie operačného systému alebo
b) štandardná dátová štruktúra poskytovaná operačným systémom alebo jeho komponentom.

čl. 22
Priame a nepriame závislosti

(1) Priama závislosť softvéru je explicitne definovaná a priamo používaná softvérovým komponentom.

(2) Nepriama závislosť softvéru predstavuje závislosť priamej a každej ďalšej nepriamej závislosti softvérového komponentu.

(3) Priame aj nepriame závislosti softvéru sú v kontexte zabezpečenia dodávateľského reťazca podľa Príloha č.1 predmetom kontroly kvality softvéru.

čl. 23
Správa závislostí softvéru

(1) Úplný zoznam priamych závislostí musí byť uvedený v dokumentácii zdrojového kódu. Tento zoznam tvorí jeden súvislý text, a pre každú závislosť obsahuje všetky informácie potrebné pre jej jednoznačnú identifikáciu

a) názov,
b) označenie verzie,

c) zdroj informácií, prípadne iné kontaktné informácie na poskytovateľa predmetnej závislosti,
d) licencia pre použitie v projekte vo forme jednoznačného identifikátora, [4)]
e) popis závislosti s informáciami o
    1. spôsobe a rozsahu použitia v projekte,
    2. prípadných obmedzeniach funkčnosti,
    3. alebo iných skutočnostiach ovplyvňujúcich funkčnosť alebo očakávané správanie softvéru.

(2) Zoznam závislostí pre balík softvéru môže byť uvedený vo forme metadát v minimálnom rozsahu názvu a verzie podľa ods. (1) písm. a) a b).

(3) Podmienky použitia závislosti musia zohľadňovať princípy predchádzania „vendor lock-in“ v súlade s metodickým usmernením MIRRI SR č. 009417/2021/oSBAA-1 k aplikácii základných princípov pri realizácii projektov IT financovaných z verejných zdrojov a zdrojov EÚ.

(4) Závislosť by mala byť široko používaná, informácie o pôvode a dokumentácia o nej verejne dostupné a poskytnuté vo forme, stave a spôsobom, ktorý zabezpečí požadovanú mieru dôveryhodnosti, umožní overenie integrity poskytovaných súborov a zhodnotenie jej kvality.

(5) Zdrojový kód závislosti, ktorý je priamou súčasťou zdrojového kódu projektu, musí byť v štruktúre repozitára jednoznačne oddelený a uložený v pôvodnej forme zdroja tak, aby bolo možné validovať jeho integritu.

(6) Zmeny implementované v zdrojovom kóde závislosti podľa odseku (5) nad rámec pôvodnej verzie, musia byť v štruktúre zdrojového kódu uložené oddelene vo forme záplaty a zdokumentované. Ak je táto závislosť distribuovaná ako samostatný softvérový balík, je potrebné úpravy zohľadniť v označení verzie.

(7) Označenie verzie softvérovej závislosti je potrebné uviesť v zozname závislostí a môže byť upravená do formy, ktorá je v súlade s čl. 7.

Kontrola softvéru

čl. 24

Základné ustanovenia o kontrole softvéru

(1) Kontrolou softvéru sa rozumie kontrola naplnenia požiadaviek na

a) kvalitu,
b) funkčnosť,
c) bezpečnosť,
d) súlad s legislatívnymi predpismi a licenciami.

(2) Výstupom kontroly je protokol, ktorý obsahuje informácie o

a) predmete kontroly,
b) rozsahu kontroly,
c) zodpovednej osobe za vykonanie kontroly,
d) identifikovaných nedostatkoch,
e) výsledku kontroly,

[4)] SPDX® License list, https://spdx.org/licenses/

f) iných podstatných skutočnostiach v rozsahu, ktorý umožní naplnenie požiadaviek pre riadenie vývoja.

(3) Pre naplnenie požiadaviek a vykonanie kontroly je odporúčané využitie automatizovaných testovacích nástrojov pre statické a dynamické testovanie softvéru.

(4) Všetky postupy kontroly a testovania softvéru musia byť zdokumentované a vykonané spôsobom, ktorý umožní postupy kedykoľvek zopakovať a výsledky vzájomne porovnať. Možnosť porovnania výsledkov je kľúčová na potvrdenie odstránenia výhrad voči očakávanej kvalite alebo potenciálnej zmene.

čl. 25

Postup kontroly softvéru

(1) Priebežná kontrola softvéru musí byť zahrnutá v procese riadenia vývoja tak, aby mohli byť prípadné výhrady voči očakávanej kvalite alebo potenciálnym zmenám včas odhalené a odstránené.

(2) Pri preberaní vydania softvéru sa vykonáva

a) statická kontrola kvality a bezpečnosti
b) dynamická kontrola kvality a bezpečnosti.

(3) Výstupy kontrol predstavujú protokoly s rozsahom podľa čl. 24 ods. (2).

čl. 26

Statická kontrola kvality softvéru

Statická kontrola balíka softvéru je zameraná na kontrolu

a) obsahu a štruktúry,
b) kvality,
c) závislostí,
d) súladu licencií softvéru a jeho závislostí,
e) rozsahu a kvality dokumentácie,
f) úrovne integrity a dôveryhodnosti,
g) úrovne výhrad voči očakávanej kvalite alebo potenciálnym zmenám.

čl. 27

Statická kontrola bezpečnosti softvéru

(1) Statická kontrola bezpečnosti musí pokrývať kontrolu softvéru na výskyt

a) chýb programovania vedúcim k bezpečnostným zraniteľnostiam,
b) iných chýb alebo nedostatkov s ohľadom na bezpečnosť softvéru,
c) bezpečnostných predmetov a iného citlivého obsahu, ako napríklad privátnych kľúčov, hesiel, privátnych URI a podobne,
d) použitia priamych a nepriamych závislostí so známymi zraniteľnosťami,
e) nesúladu nastavení vývojového prostredia, kompilátora, prípadne ďalších súčastí s všeobecne uznávanými bezpečnostnými štandardami a odporúčaniami.

(2) Statická kontrola bezpečnosti môže byť vykonaná

a) automatizovane nástrojom na statickú analýzu softvéru s podporou detekcie bezpečnostných zraniteľností,

b) manuálne so zameraním na kontrolu kritickej súčasti alebo funkcionality, vopred identifikovanou vykonaním modelovania a analýzy rizík, prípadne revíziu zraniteľností v závislostiach softvéru.

čl. 28

Dynamická kontrola kvality softvéru

Dynamická kontrola a testovanie kvality softvéru pokrýva kontrolu

a) úplnosti, správnosti a funkčnosti postupov inštalácie, odinštalácie a aktualizácie,
b) funkčnosti softvéru v súlade s požiadavkami a všeobecnými odporúčaniami,
c) integrity a dôveryhodnosti inštalačných balíkov,
d) dynamickým aplikačným bezpečnostným testovaním.

čl. 29

Dynamická kontrola bezpečnosti softvéru

(1) Dynamická kontrola bezpečnosti softvéru pozostáva z

a) odhaľovania výhrad voči očakávanej kvalite počas spustenia softvéru,
b) kontroly úrovne zabezpečenia prostredia spustenia softvéru,
c) automatizovaného testovania prítomnosti zraniteľností,
d) penetračného testovania v obmedzenom rozsahu v testovacom prostredí vývojového cyklu.

(2) Penetračné testovanie sa odporúča vykonať pri každej zmene kódu, ktorá môže viesť k zavedeniu novej zraniteľnosti kritickej súčasti identifikovanej v procese modelovania rizík.

Vydanie softvéru

čl. 30

Životný cyklus vydania

(1) Každé právoplatné vydanie musí mať definovaný životný cyklus vydania.

(2) Životný cyklus vydania definuje fázy cyklu so stanovením termínov a podmienok ich počiatku a ukončenia. Naplnenie podmienok pre inicializáciu fázy vydania je vyhodnocované na základe výstupov z fázy testovania.

(3) Životný cyklus vydania pozostáva z fáz

a) **plánovania a špecifikácie**, počas ktorej sú dokumentované požiadavky na nové vydanie,
b) **vývoja**, počas ktorej sú vyvíjané požiadavky,
c) **implementácie a spustenia**, počas ktorej sú kompilované a spustené zdrojové kódy,
d) **testovania**, počas ktorej sú vykonávané postupy testovania a kontroly softvéru,
e) **vydania**, počas ktorej sú sprístupnené výstupy vývoja,
f) **nasadenia**, počas ktorej sú softvérové komponenty nasadené do produkčného prostredia,
g) **prevádzky**, počas ktorej sú softvérové komponenty prevádzkované,
h) **monitorovania**, počas ktorej sú zbierané údaje z prevádzky pre zhodnotenie ďalšieho rozvoja.

(4) Vo fázach vývojového cyklu, konkrétne fázach implementácie a spustenia a testovania sú používané balíky softvéru, ktoré nenapĺňajú požiadavky právoplatného vydania definované v čl. 31.

čl. 31

Formy vydania softvéru

(1) Právoplatným vydaním sa rozumie balík softvéru pripravený na sprístupnenie a nasadenie, ktorý bol odsúhlasený s rôznym stupňom výhrad voči očakávanej kvalite alebo potenciálnym zmenám.

(2) Právoplatným vydaním sa nerozumie balík softvéru sprístupnený pre komunitu vývojárov pre ďalší vývoj alebo na testovacie účely. Takéto vydanie nepodlieha riadeniu vydaní a musí byť jednoznačne odlíšené od vydaní pripravených pre vyhlásenie za právoplatné.

(3) Predmetom vydania sú

a) zdrojové kódy,
b) skompilované spustiteľné súbory,
c) inštalačné balíky,
d) dokumentácia.

(4) Predmety vydania musia byť sprístupnené spôsobom, ktorý umožní vykonanie kontroly softvéru podľa čl. 25 v požadovanom rozsahu.

(5) Výstup kontroly predmetov vydania musí potvrdiť, že neobsahujú

a) žiadnu kritickú chybu, a to najmä
    1. spôsobenie nefunkčnosti nesúvisiaceho softvéru,
    2. spôsobenie vážnej straty alebo poškodenia dát,
    3. zavedenie bezpečnostnej zraniteľnosti na cieľovom systéme úrovne Kritická alebo Vysoká podľa škály hodnotenia zraniteľností[5)],
b) žiadnu vážnu chybu, a to najmä
    1. spôsobenie nefunkčnosti softvéru,
    2. spôsobenie straty alebo poškodenia dát,
    3. zavedenie bezpečnostnej zraniteľnosti na cieľovom systéme úrovne Stredná podľa škály hodnotenia zraniteľností,
c) iné prekážky k vydaniu zohľadňujúce požiadavky projektu, ktoré nemožno ignorovať.

(6) Rôzne verzie vydania musia byť ľahko a jednoznačne od seba odlíšiteľné. Spôsob odlíšenia verzií musí byť zdokumentovaný v zdrojovom kóde podľa čl. 16 ods. (2) písm. g).

(7) Balík softvéru musí byť pred vydaním novej verzie sprístupnený v dostatočnom časovom predstihu podľa ustanovení čl. 12 a čl. 17 spôsobom, aby bolo možné vykonať kontrolu kvality a bezpečnosti.

[5)] FIRST, Common Vulnerability Scoring System SIG, https://www.first.org/cvss/.

čl. 32
Odsúhlasenie vydania

(1) Vydanie konkrétnej verzie balíka softvéru musí byť pred sprístupnením odsúhlasené spôsobom, ktorý garantuje dôveryhodnosť a integritu schvaľovaného balíka softvéru spôsobom, ktorý je overiteľný štandardnými prostriedkami.

(2) Odsúhlasením vydania oprávnenou osobou je

a) elektronický podpis balíka softvéru dôveryhodným osobným kľúčom oprávnenej osoby,
b) dôveryhodne zaznamenané potvrdenie v nástroji pre riadenie vydaní vykonané osobným účtom oprávnenej osoby,
c) iný spôsob odsúhlasenia, ktorý preukazuje integritu a dôveryhodnosť odsúhlasovaného vydania s dostupnou možnosťou overenia úrovne garancií, a je autorizovaný vhodným autorizačným prostriedkom oprávnenej osoby.

(3) Oprávnená osoba a jej autorizačné prostriedky musia byť uvedené v štruktúre zdrojového kódu podľa čl. 16 ods. (2) písm. d) alebo transparentne evidované v nástroji pre správu vydaní.

čl. 33
Sprístupnenie vydania

(1) Právoplatné vydanie musí byť sprístupnené spôsobom, ktorý zabezpečí jeho dôveryhodnosť a integritu digitálnym podpisom dôveryhodným kľúčom alebo aspoň kontrolným súčtom balíkov softvéru, ktoré sú súčasťou vydania.

(2) Dostupnosť právoplatného vydania je vhodné zabezpečiť v repozitári softvéru, ktorý v akceptovateľnej miere spĺňa požiadavky dôveryhodnosti, integrity a dostupnosti.

(3) Právoplatné vydanie môže byť sprístupnené aj alternatívnym spôsobom ak je v súlade s licenčnými podmienkami a sú splnené požiadavky podľa odseku (2) v očakávanej miere.

(4) Verzia, ktorá nie je právoplatným vydaním, môže byť sprístupnená aj mimo komunity vývojového tímu. Táto verzia musí byť jednoznačne odlíšiteľná od právoplatného vydania sprístupnením v oddelenej štruktúre repozitára. Súčasťou zverejnenia musí byť informácia s poukázaním na nižšiu úroveň garancií kvality softvéru.

Príloha č.1
Kontrola zabezpečenia dodávateľského reťazca

Dodávateľský reťazec predstavuje úplný zoznam závislostí a procesov, ktoré sú využívané v procesoch vývoja softvéru a prípravy balíkov softvéru.

Kontrola zabezpečenia dodávateľského reťazca zahŕňa tri oblasti kontrol (v kontexte vyhlášky MIRRI SR č.401/2023 Z. z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy):

Oblasť	popis	fázy riadenia projektov
Dodávateľské zdroje	predstavuje všetky formy externých závislostí a zmluvných garancií ich dodania	prípravná, iniciačná, realizačná R1, R2 agilné E, R
Vývoj produktu a testovanie	IKT prostriedky, ľudské zdroje a prostredie použité pri vývoji	realizačná R3 agilná R
Doručenie produktu	distribúcia balíkov a údržba	realizačná R4, dokončovacia agilné R, D

Využívanie externých zdrojov, prípadne závislosti na softvéri, ktorý je vyvíjaný mimo riadeného vývojového prostredia, predstavuje riziko zanesenia zraniteľností, chýb, prípadne škodlivého kódu. Tieto riziká je potrebné v dostatočnej miere zmierniť využitím technologických možností prostredia a procesov kontroly.

Zabezpečenie dodávateľského reťazca softvéru zahŕňa najmä oblasti:

- zabezpečenie zdrojového kódu,
- zabezpečenie materiálov tretích strán,
- zabezpečenie spracovania vydania,
- zabezpečenie artefaktov,

Oblasť	Položka	Pokrytie
Zdrojové kódy	Požadované podpisovanie commitov	
	Automatizované skenovanie na predídenie nahratia bezpečnostných predmetov	
	Definované pravidlá úrovne pre neakceptovateľné riziko pre zraniteľnosti	
	Automatizované skenovanie na detekciu zraniteľností v súlade s pravidlami z predchádzajúceho bodu	
	Jednoznačné dokumentované a overiteľné role prispievateľov	
	Vynútenie revízie a schválenia požiadavky na zlúčenie kódu	
	Riadenie prístupov k jednotlivým vývojovým vetvám	
	Autentifikácia použitím MFA a SSH kľúčov s implementáciou ich rotovania	
	Riadenie prístupov automatizačných agentov s implementovaním princípov najnižšie práva a len v čase	
Materiály tretích strán	Kontrola závislostí na naplnenie požiadaviek kvality a spoľahlivosti	
	Automatické skenovanie závislostí na prítomnosť zraniteľností a súladu licencií	
	Automatická analýza nepriamych závislostí	
	Monitorovanie aktualizácií a zraniteľností v závislostiach	
	Inštalácia predkompilovaných závislostí z verejných repozitárov	
	Je dostupný kompletný zoznam priamych závislostí	
Spracovanie vydania	Použitie minimalizovaných a zabezpečených balíkov	
	Správa spracovania vydaní prístupom “Infrastructure-as-Code”	
	Automatizované kroky spracovania vydaní okrem revízií zlučovaného kódu a odsúhlasenia vydania	
	Podpisovanie výstupov jednotlivých krokov spracovania vydania pre garanciu overiteľnosti pôvodu	
	Validácia podpisov a odtlačkov všetkých závislostí pred ich zapojením do spracovania vydania	
	Využitie samostatných komponentov pre každý krok spracovania vydania	
	Dostatočná sieťová izolácia komponentov spracovania vydania	
	Produkované overiteľné a opakovateľné vydania	
Artefakty a nasadenie	Každý artefakt vydania je podpísaný	
	Metadáta artefaktov sú distribuované tak, že ich môže konzument pri použití verifikovať	
	Konzument môže artefakt validovať ešte pred jeho použitím	

Príloha č.2
Základná sada kontrol softvéru

Nižšie sú uvedené kontroly softvéru a jeho testovania s primárnym zameraním na bezpečnosť podľa Guidelines on Minimum Standards for Developer Verification of Software, NIST. [6)]

Rozsah testovania je vhodné priebežne prehodnocovať a evidovať zoznam všetkých aktuálnych testovacích scenárov.

	metodika	fázy riadenia projektov	Pokrytie
Zabezpečenie dodávateľského reťazca			
kontrola licenčného krytia	čl. 8	iniciačná experimentálna	
kontrola závislostí	čl. 10 čl. 23	iniciačná realizačná (R1) experimentálna	
kontrola ostatných metadát	čl. 6 čl. 7 čl. 9	realizačná (R1)	
Modelovanie útokov			
príprava možných scenárov zneužitia	-	iniciačná realizačná (R1)	
Automatizované testovanie			
Statické testovanie bezpečnosti (Static Application Security Testing - SAST)			
automatizovaná analýza kódu	čl. 11 čl. 14(1) čl. 26 čl. 27	realizačná (R3)	
prítomnosť bezpečnostných predmetov	čl. 14(2)	realizačná (R3)	
použitie dostupných kontrol a ochrán	čl. 14(1)c)d)e) čl. 27(1)e)	realizačná (R3)	
Dynamické testovanie bezpečnosti (Dynamic Application Security Testing - DAST)			
black-box testovanie	čl. 28a)b)c) čl. 29(1)a)b)	realizačná (R3)	
code-based testovanie	čl. 28a)b)c) čl. 29(1)a)b)	realizačná (R3)	
regresné testovanie	čl. 28a)b)c) čl. 29(1)a)b)	realizačná (R3)	
Fuzznig	čl. 28a)b)c) čl. 29(1)a)b)	realizačná (R3)	
skenovanie zraniteľností	čl. 29(1)c)	realizačná (R3-R4)	
Akceptačné testy			
záťažové a výkonnostné	-	realizačná (R3)	
systémové a integračné	-	realizačná (R3)	
používateľské a funkčné	čl. 28a)b)c) čl. 29(1)a)b)	realizačná (R3) dokončovacia	
smoke testovanie	čl. 28a)b)c) čl. 29(1)a)b)	realizačná (R3-R4) dokončovacia	
Penetračné testovanie			
testovanie možných scenárov zneužitia	čl. 29(1)d),(2)	realizačná (R3-R4)	
analýza kódu	čl. 27(2)b)	realizačná (R3-R4)	

[6)] Guidelines on Minimum Standards for Developer Verification of Software, NIST, https://doi.org/10.6028/NIST.IR.8397

Zabezpečenie dodávateľského reťazca a modelovanie útokov sa vykonávajú v prvotných fázach projektu.

Následné automatizované testovanie prebieha kontinuálne počas realizačnej fázy projektu implementácie a testovania, prípadne nasadenia.

Black-box testovanie predstavuje sadu testov na základe analýzy funkcionalít a ich možných vzájomných dopadov.

Code-based testovanie predstavuje sadu testov na základe analýzy zdrojových kódov a vytipovania častí, ktoré vyžadujú testovanie (citlivé oblasti bezpečnostných komponentov, spracovania citlivých údajov a podobne).

Regresné testovanie predstavuje sadu testov, ktoré boli vytvorené na základe opráv kódu implementovaných k výhradám vo funkčnosti alebo bezpečnosti. Sada týchto testov sa vykonáva ako prevencia opätovného zavedenia chyby.

Fuzzing predstavuje použitie špecializovaných nástrojov na testovanie reakcií aplikácie na rôzne sady vstupov. Takéto testovanie má za úlohu odhaliť neočakávané reakcie aplikácie na niektoré neočakávané vstupy.

Smoke testovanie predstavuje obmedzenú sadu funkčných a používateľských testov a pokrýva najmä vytipované kritické funkcie softvéru s ohľadom na konkrétne produkčné nasadenie.

Skenovanie zraniteľností za využíva nástroje pre simuláciu známych scenárov zneužitia zraniteľností.

Penetračné testovanie môže zahŕňať časti automatizovaných testov, testovanie scenárov z modelovania útokov, pričom ich môže rozšíriť o menej predpokladané scenáre na základe dodatočnej analýzy testovaného prostredia a zdrojových kódov. Rozsah a zameranie penetračných testov je predmetom dohody s vykonávateľom testov.

Príloha č.3
Zdroje metodického usmernenia

Apache Software Foundation. (1. Január 2023). *Release Policy*. Dostupné na Internete: Apache Software Foundation: https://www.apache.org/legal/release-policy.html

Central Digital & Data Office, His Majesty's Government. (1. Január 2023). *Open Source Guidance*. Dostupné na Internete: His Majesty's Government: https://www.gov.uk/government/publications/open-source-guidance

Debian Project. (1. 1 2023). *Debian Policy Manual v. 4.6.2.0*. Dostupné na Internete: Debian: https://www.debian.org/doc/debian-policy/

FEDORA Project. (1. Január 2023). *Fedora Packaging Guidelines*. Dostupné na Internete: Fedora Documentation: https://docs.fedoraproject.org/en-US/packaging-guidelines

Government of Canada. (1. Január 2023). *Open Source Software*. Dostupné na Internete: Canada.ca: https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/open-source-software.html

National Institute of Standards and Technology, U.S. Department of Commerce. (2021). *Guidelines on Minimum Standards for Developer Verification of Software.*

OWASP. (2017). *OWASP Code Review guide 2.0.*

SAFECode. (2009). *The Software Supply Chain Integrity Framework.*

U.S Department of Homeland Security. (1. Január 2023). *DHS Source Code Inventory Process*. Dostupné na Internete: U.S Department of Homeland Security: https://www.dhs.gov/scip