PRITAIKYTOJI IR STANDARTIZUOTOJI DUOMENŲ APSAUGA INFORMACINĖS SISTEMOS GYVAVIMO CIKLE

2020-12-11

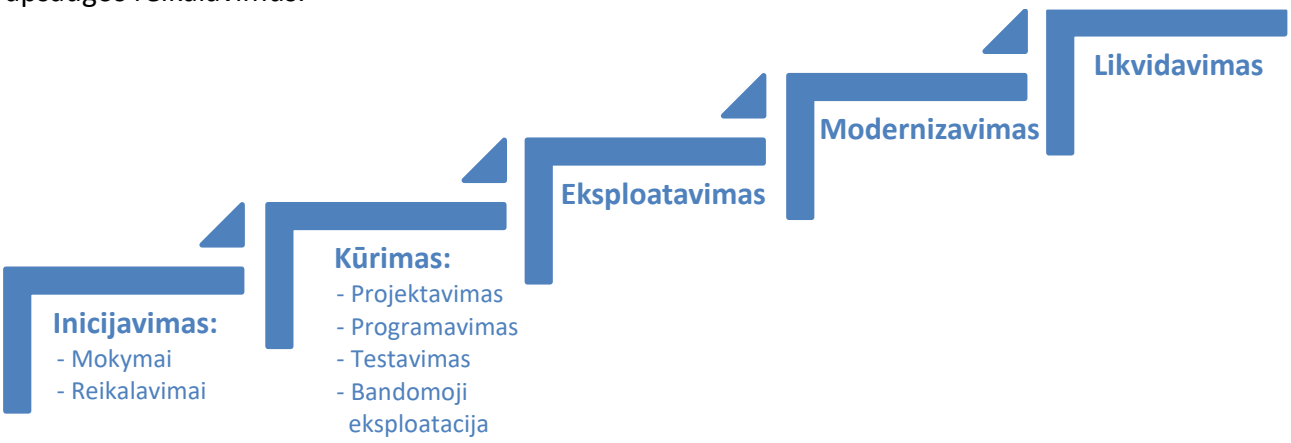
Valstybinė duomenų apsaugos inspekcija parengė šias gaires siekdama padėti duomenų valdytojams ir duomenų tvarkytojams suprasti ir laikytis Bendrojo duomenų apsaugos reglamento (toliau – BDAR) 25 straipsnyje numatytų pritaikytosios ir standartizuotosios duomenų apsaugos reikalavimų informacinės sistemos gyvavimo ciklo metu. Gairės dėl pritaikytosios ir standartizuotosios duomenų apsaugos reikalavimų informacinės sistemos gyvavimo cikle (toliau – Gairės) visų pirma skirtos informacinių sistemų ar atskiros programinės, techninės įrangos kūrėjams: informacinių technologijų (toliau – IT) projektų vadovams, IT architektams, programuotojams, testuotojams, duomenų apsaugos pareigūnams ir kitiems asmenims, kurie dalyvauja informacinių sistemų, kuriose tvarkomi asmens duomenys, kūrime. Informacinės sistemos gyvavimo ciklas apima visus sistemos būsenos pokyčius nuo jos steigimo pagrindo nustatymo iki veikimo pabaigos. Gairėse pateikta gyvavimo ciklo koncepcija taip pat taikytina atskiram programinės ar techninės įrangos vystymui.

Turinys

INFORMACINĖS SISTEMOS GYVAVIMO CIKLO ETAPAI....3
INFORMACINĖS SISTEMOS INICIJAVIMAS....4
Mokymai....4
Reikalavimai....4
INFORMACINĖS SISTEMOS KŪRIMAS....8
Projektavimas....8
Programavimas....10
Testavimas....11
Bandomoji eksploatacija....12
INFORMACINĖS SISTEMOS EKSPLOATAVIMAS....14
INFORMACINĖS SISTEMOS MODERNIZAVIMAS....15
INFORMACINĖS SISTEMOS LIKVIDAVIMAS....16

INFORMACINĖS SISTEMOS GYVAVIMO CIKLO ETAPAI

Gairėse pateikti gyvavimo ciklo etapai aprašyti atsižvelgiant į Lietuvos valstybės informacinių sistemų gyvavimo ciklo stadijas ir etapus, kombinuojant saugaus vystymo gyvavimo ciklo veiklas pagal „Microsoft“ praktiką[1] (toliau – SDL). Informacinių sistemų gyvavimo ciklas prasideda nuo idėjos sukurti produktą ir baigiasi šiam produktui nustojus veikti (1 pav.). Šiose gairėse duomenų apsaugos principai ir duomenų subjektų teisės pagal BDAR įtraukti į kiekvieną informacinės sistemos gyvavimo ciklo etapą pagal pritaikytosios ir standartizuotosios duomenų apsaugos reikalavimus.



1 pav. Gyvavimo ciklo etapai

[1] Microsoft Security Development Lifecycle – https://www.microsoft.com/en-us/securityengineering/sdl/practices.

INFORMACINĖS SISTEMOS INICIJAVIMAS

Inicijavimo etapas prasideda nuo idėjos sukurti produktą, kuris padės supaprastinti ar pagerinti veiklos, proceso ar atskirų užduočių kokybę, nustatant pagrindinius tikslus ir uždavinius. Šis etapas yra labai svarbus, nes jame ***identifikuojamos asmens duomenų tvarkymo operacijos, asmens duomenų ir duomenų subjektų kategorijos, duomenų teikėjai ir duomenų gavėjai***. Be kita ko, identifikuojamas poreikis įgyti papildomas žinias ar kompetencijas. Taip pat nustatomi ***pagrindiniai reikalavimai sistemos vientisumui, konfidencialumui ir prieinamumui užtikrinti***.

Mokymai

Mokymai yra viena pagrindinių organizacinių asmens duomenų saugumo priemonių, padedanti užtikrinti bet kokios organizacijos atitiktį BDAR 24, 25, 28, 32 straipsnių ir 39 straipsnio 1 dalies b punkto reikalavimams.

Pagal SDL programinės įrangos kūrėjai turi turėti pagrindines duomenų saugos žinias ir gebėti įdiegti (integruoti) duomenų saugą į kuriamą produktą. Atsižvelgiant į BDAR numatytą pritaikytąją ir standartizuotąją asmens duomenų apsaugą, tiek programinės įrangos kūrėjai, tiek kuriamo produkto naudotojai taip pat turėtų įgyti ir papildomas asmens duomenų apsaugos kompetencijas, žinoti kokių tvarkų ir metodikų reikia laikytis. Organizacija turi nuspręsti, kas yra aktualu konkrečiu atveju ir kokio tipo mokymai ir (ar) kompetencijos bei tai patvirtinantys sertifikatai reikalingi atskiriems darbuotojams ir kuriamo projekto komandai, ir parengti mokymų planą.

Mokymai ir kompetencijos pagal profesines grupes turi apimti bent šias temas:

- Su asmens duomenų tvarkymu susiję principai, asmens duomenų teisėto tvarkymo sąlygos, specialiųjų kategorijų asmens duomenų, asmens duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymas (BDAR 5–10 straipsniai);
- Duomenų subjekto teisės (BDAR 12–23 straipsniai);
- Duomenų valdytojai ir duomenų tvarkytojai, jų atsakomybės, asmens duomenų saugumo principai (BDAR 24–43);
- Informacijos saugumo valdymo sistemų pagrindai (pvz., *ISO 27001, ISF Standard of Good Practice for Information Security*);
- Programinės įrangos kūrimo standartai (pvz., *ISO 27034, SDL*);
- Saugumo testavimas (pvz., *OWASP Testing Guide, OWASP ASVS, OWASP Top 10*);
- Kibernetinių grėsmių rizikos vertinimas (pvz., *STRIDE, DREAD*);
- Vidinės organizacijos privatumo, saugos procedūros ir dokumentacija.

Reikalavimai

Šiame etape nustatomi pagrindiniai reikalavimai galutiniam produktui dėl asmens duomenų apsaugos ir duomenų saugumo. Siekiant nustatyti tinkamus reikalavimus, svarbu žinoti, kokios asmens duomenų kategorijos bus tvarkomos programinėje įrangoje, kas bus duomenų

valdytojai ir duomenų tvarkytojai, asmens duomenų teikėjai ir gavėjai. Tai būtina norint nustatyti, kokie teisės aktai, taisyklės, gairės ir elgesio kodeksai taikytini kuriamam produktui.

BDAR 35 straipsnis numato, kad tais atvejais, kai dėl duomenų tvarkymo rūšies, visų pirma, kai naudojamos naujos technologijos, ir atsižvelgiant į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, fizinių asmenų teisėms bei laisvėms gali kilti didelis pavojus, duomenų valdytojas, prieš pradėdamas tvarkyti duomenis, atlieka numatytų duomenų tvarkymo operacijų poveikio asmens duomenų apsaugai vertinimą (toliau – PDAV). Nustatant pagrindinius reikalavimus galutiniam produktui turi būti atsižvelgta į:

- Valstybinės duomenų apsaugos inspekcijos skelbiamą duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašą[2];
- 29 straipsnio duomenų apsaugos darbo grupės poveikio duomenų apsaugai vertinimo gaires[3].

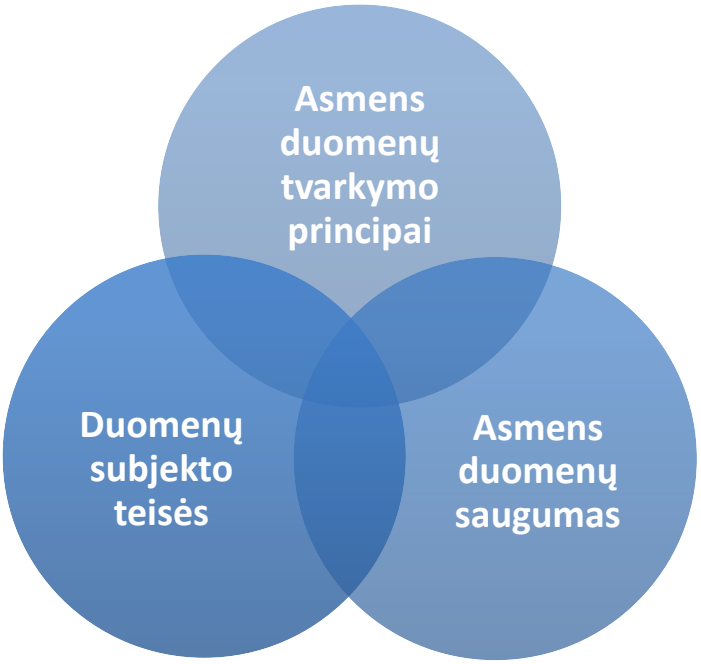
Pagrindinės BDAR nuostatos dėl pritaikytosios ir standartizuotosios duomenų apsaugos, turinčios įtaką kuriamo produkto pamatinėms architektūros ir funkcionalumų technologiniams sprendimams, yra šios (2 pav.):

- Su asmens duomenų tvarkymu susiję principai (BDAR 5 straipsnis):
  - duomenų subjekto atžvilgiu asmens duomenys tvarkomi teisėtu, sąžiningu ir skaidriu būdu ***(teisėtumo, sąžiningumo ir skaidrumo principas)***;
  - asmens duomenys renkami nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau netvarkomi su tais tikslais nesuderinamu būdu ***(tikslo apribojimo principas)***;
  - asmens duomenys turi būti adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi ***(duomenų kiekio mažinimo principas)***;
  - asmens duomenys turi būti tikslūs ir prireikus atnaujinami; turi būti imamasi visų pagrįstų priemonių užtikrinti, kad asmens duomenys, kurie nėra tikslūs, atsižvelgiant į jų tvarkymo tikslus, būtų nedelsiant ištrinami arba ištaisomi ***(tikslumo principas)***;
  - asmens duomenys turi būti laikomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, negu tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi ***(saugojimo trukmės apribojimo principas)***;
  - asmens duomenys turi būti tvarkomi tokiu būdu, kad taikant atitinkamas technines ar organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo ***(vientisumo ir konfidencialumo principas)***.

[2] Valstybinės duomenų apsaugos inspekcijos direktoriaus 2019 m. kovo 14 d. įsakymas Nr. 1T-35 (1.12.E) „Dėl duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašo patvirtinimo“ – https://www.e-tar.lt/portal/lt/legalAct/abb01940465511e9a221b04854b985af.

[3] Poveikio duomenų apsaugai vertinimo (PDAV) gairės, kuriomis BDAR taikymo tikslais nurodoma, kaip nustatyti, ar duomenų tvarkymo operacijos gali sukelti didelį pavojų – https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

- Duomenų subjekto teisės (BDAR 12–22 straipsniai):
  - teisė gauti informaciją apie duomenų tvarkymą;
  - teisė susipažinti su duomenimis;
  - teisė reikalauti ištaisyti duomenis;
  - teisė reikalauti ištrinti duomenis („teisė būti pamirštam“);
  - teisė apriboti duomenų tvarkymą;
  - teisė į duomenų perkeliamumą;
  - teisė nesutikti su duomenų tvarkymu;
  - teisė reikalauti, kad nebūtų taikomas tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamas sprendimas.
- Asmens duomenų saugumas (BDAR 24, 25, 32–34 straipsniai).



2 pav. Kuriamo produkto pritaikytosios ir standartizuotosios duomenų apsaugos nuostatos

Asmens duomenų saugumo reikalavimų nustatymas:

- Įvertinti fizinių asmenų pagrindinėms teisėms ir laisvėms kylantį poveikį dėl galimo asmens duomenų saugumo pažeidimo;
- Atlikti rizikos vertinimą:
  - nustatyti priimtinos rizikos lygius duomenų apsaugai bent pagal šias kategorijas:
    - duomenų subjektas privalo kontroliuoti savo asmens duomenis;
    - negali būti nepagrįstai apribotos duomenų subjekto teisės ar laisvės;
    - duomenų subjektas negali būti profiliuojamas arba diskriminuojamas;
    - negali būti pavogta duomenų subjekto tapatybė;
    - duomenų subjektas neturi patirti finansinių nuostolių;
    - negali būti paveikta duomenų subjekto reputacija;
    - pseudonimų suteikimo atvejais neturi būti įmanoma atsekti tikrosios tapatybės;

        - neturi įvykti asmens duomenų saugumo pažeidimai.
    - nustatyti priimtinos rizikos lygius duomenų saugumui bent pagal šias kategorijas:
        - asmens duomenys negali būti netyčia ar neteisėtai pakeisti, prarasti ar sunaikinti;
        - asmens duomenys negali būti neteisėtai atskleisti;
        - asmens duomenys turi būti apsaugoti atsižvelgiant į programinės įrangos konfidencialumą, vientisumą, prieinamumą ir atsparumą;
        - asmens duomenys turi būti pseudonimizuoti ir (ar) užšifruoti;
        - įvykus fiziniam ar techniniam incidentui, turi būti įmanoma laiku atkurti galimybę tvarkyti asmens duomenis;
        - turi būti užtikrintas reguliarus duomenų tvarkymo saugumo priemonių veiksmingumo vertinimas.
- Pagal rizikos vertinimo rezultatus numatyti tinkamas organizacines ir technines saugumo priemones.

Asmens duomenų tvarkymo organizacinių ir techninių saugumo priemonių parinkimas gali būti atliekamas pasitelkus šiuos dokumentus:

- Valstybinės duomenų apsaugos inspekcijos metodinis dokumentas dėl duomenų saugumo priemonių ir rizikos įvertinimo[4];
- OWASP programinės įrangos saugos užtikrinimo standartas[5] (angl. *OWASP Application Security Verification Standard 4.0.1*).

[4] Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams – https://vdai.lrv.lt/uploads/vdai/documents/files/VDAI_saugumo_priemoniu_gaires-2020-06-18.pdf.

[5] OWASP ASVS 4.0.1 – https://owasp.org/www-pdf-archive/OWASP_Application_Security_Verification_Standard_4.0-en.pdf.

INFORMACINĖS SISTEMOS KŪRIMAS

Projektavimas

Šiame etape privalo būti specifikuoti pagrindiniai kuriamo produkto privatumo ir saugumo reikalavimai. Atsižvelgiant į Europos Sąjungos kibernetinio saugumo agentūros (*ENISA*) rekomendaciją, siūloma projektavimo reikalavimus asmens duomenų apsaugos kontekste suskirstyti į ***8 strategijas – 4 duomenų projektavimo ir 4 procesų projektavimo***.

Duomenų projektavimo strategijos:

1 strategija – MINIMIZAVIMO

Surinktų ir toliau tvarkomų asmens duomenų kiekis turėtų būti ribojamas duomenų tvarkymo tikslų atsižvelgiant į tai, kas tikrai būtina.

Pavyzdžiai:

- apriboti asmens duomenų pateikimą ir atvaizdavimą per vartotojo sąsają, apsvarstyti pseudonimizavimo sprendimus tiesiogiai asmenį identifikuojančios informacijos tvarkymui taikomojoje programinėje įrangoje;
- apriboti apdorojamos informacijos kiekį pažeidžiamiausiose kuriamo produkto vietose atsižvelgiant į PDAV ir (ar) rizikos vertinimą;
- vengti jautrios informacijos rinkimo.

2 strategija – NUSLĖPIMO

Asmens duomenys negali būti apdorojami, atvaizduojami ir perduodami atviruoju tekstu ar atviraisiais formatais.

Pavyzdžiai:

- atlikti atakos paviršiaus mažinimo analizę (angl. *Attack Surface Analysis*);
- minimizuoti išorinių kompiuterinių tinklų, aplikacijų programavimo sąsajų (*API*) naudojimą ir šifruoti bet kokį duomenų perdavimą išoriniu tinklu.

3 strategija – ATSKYRIMO

Asmens duomenys, kai tai įmanoma, turi būti atskirti nuo kitų duomenų. Duomenys kiekvienam tikslui ir procesui turėtų būti saugomi atskirose duomenų bazėse, duomenų rinkiniuose ar reliacinėse lentelėse. Atskyrus skirtingus tą patį asmenį identifikuojančių požymių apdorojimą ir saugojimą, sumažėja tikimybė profiliuoti konkretų asmenį. Atskyrimas taip pat yra veiksminga priemonė siekiant išvengti skirtingų duomenų rinkinių susiejimo. Reliacinėse lentelėse ar duomenų rinkiniuose, kuriuose yra asmens duomenys, turėtų būti trumpesnis saugojimo laikas ir automatinio ištrynimo terminas.

Pavyzdžiai:

- atskirti asmens duomenis pagal jų jautrumą duomenų bazėse;
- nustatyti prieigos prie reliacinių lentelių kontrolę atsižvelgiant į darbo funkcijas;
- reliacinėse lentelėse esančių eilučių susiejimas tarpusavyje turėtų būti apsunkintas, pašalinant bet kokius identifikatorius arba naudojant specifinius pseudonimus.

4 strategija – AGREGAVIMO

Pagal šią strategiją duomenų rinkiniai turėtų būti sudaromi tokiu būdu, kad konkretų asmenį apibūdinančių požymių kiekis būtų minimizuotas, stengiamasi naudoti kuo bendresnius požymius kuo didesnei asmenų grupei.

Pavyzdžiai:

- pakeisti laiko matus, naudoti savaites vietoje dienų ar valandų;
- pakeisti tikslius adresus į miestus ar regionus;
- naudoti asmenų grupes pagal panašumus, o ne atskirų asmenų sąrašus;
- naudoti anonimizavimo metodus, kur tik tai įmanoma.

Procesų projektavimo strategijos:

5 strategija – INFORMAVIMO

Kuriamas produktas turi būti suprojektuotas ir sukonfigūruotas taip, kad duomenų subjektas būtų pakankamai informuotas apie tai, kaip programinė įranga veikia ir kaip joje tvarkomi asmens duomenys. Duomenų subjektas turi turėti galimybę susipažinti su produkto asmens duomenų tvarkymu prieš pradedant naudoti šį produktą.

Pavyzdžiai:

- turi būti paruoštos formos gauti informaciją apie asmens duomenų tvarkymą;
- turi būti pateikta informacija apie produkto saugumą, priežiūrą, duomenų tvarkytojus ir pan.;
- informacija turi būti pasiekiama bent keliais būdais ar kanalais. Pagal galimybę, informacija pateikiama skirtingomis kalbomis.

6 strategija – KONTROLĖS

Duomenų subjektas turi teisę kontroliuoti savo asmens duomenis: peržiūrėti, atnaujinti ir (arba) ištrinti. Produktas turi būti sukurtas taip, kad duomenų subjektas galėtų kuo lengviau naudotis šiomis teisėmis.

Pavyzdžiai:

- produktas turi maksimaliai apsaugoti privatumą pagal numatytuosius nustatymus, kurie gali būti keičiami tik duomenų subjekto aktyviais veiksmais;
- galimybė prižiūrėti ir tvarkyti duomenų subjekto duotus sutikimus. Atšaukus sutikimą, turėtų būti automatiškai nutrauktas toks duomenų tvarkymas, dėl kurio šis sutikimas buvo duotas;
- suteikti duomenų subjektui prieigą prie asmens duomenų taisymo, blokavimo ar ištrynimo;
- numatyti informacijos eksportą ir patogų atvaizdavimą (spausdinimą);
- įdiegti, pašalinti, įgalinti ar išjungti taikomuosius programinius komponentus ar paslaugas;
- galimybė pateikti klausimus ar skundą, susijusius su duomenų apsauga ir saugumu.

7 strategija – VYKDYMO

Programinė įranga turi būti suprojektuota taip, kad ji atitiktų organizacijos privatumo politiką ar kitą privatumo ir BDAR atitikties dokumentą, apimantį, jei naudojama, dirbtinį intelektą, profiliavimą ir automatizuotą tvarkymą.

Pavyzdžiai:

- pagal numatytuosius nustatymus programinė įranga turi taikyti aukščiausius privatumo nustatymus, o pakeitimas į mažiau privatumui palankius nustatymus turi vykti aktyviais duomenų subjekto veiksmais atskirame meniu;

- jeigu duomenų tvarkymas grindžiamas sutikimu arba sutartimi, turi būti įdiegtas duomenų perkeliamumo funkcionalumas, t. y. duomenų subjektas turi turėti galimybę perkelti savo pateiktus asmens duomenis kitam paslaugų teikėjui standartizuotu ir daugkartinio naudojimo formatu;
- jeigu produktas skirtas nepilnamečiams, prieš suteikiant prieigą, turi būti funkcionalumas, užtikrinantis tėvų ar kitų teisėtų vaiko atstovų sutikimo gavimą (kai vaikui tiesiogiai siūlomos informacinės visuomenės paslaugos, vaiko asmens duomenų tvarkymas yra teisėtas, jei sutikimą pagal BDAR 6 straipsnio 1 dalies a punktą duoda ne jaunesnis negu 14 metų vaikas.);
- duomenų subjektas turi turėti prieigą prie savo atliktų veiksmų žurnalų įrašų (logų).

8 strategija – ATITIKTIES

Duomenų valdytojas turi gebėti dokumentais patvirtinti duomenų tvarkymo saugumą ir atitiktį BDAR.

Pavyzdžiai:

- dokumentai, įrodantys, kad programinė įranga buvo sukurta naudojant tam tikrą metodiką, pvz., SDL;
- saugos auditų ataskaitos;
- pažeidžiamumo vertinimai, saugumo, įskverbties testai ir pan.;
- vidinės saugumo politikos;
- atitiktis saugiam informacijos valdymui organizacijoje, pvz., ISO sertifikatai ar pan.

Programavimas

Programuojant privaloma laikytis saugaus programavimo gerųjų praktikų, pvz., OWASP Saugaus programavimo gairių[6].

Turi būti apibrėžtas ir dokumentais patvirtintas leidžiamų programinės įrangos kūrimo ir diegimo įrankių, programinės įrangos karkasų (angl. *Software framework*) ir bibliotekų sąrašas:

- turi būti aišku, kam skirtingos priemonės gali būti naudojamos, turi būti aprašytos ir patvirtintos su įrankių naudojimu susijusios saugos funkcijos ir procedūros;
- sąraše turi būti nurodyta, kuriuos trečiųjų šalių įrankius ar komponentus galima naudoti programuojant numatomą įrangą;
- priemonės ir pagalbiniai komponentai turėtų būti įvertinti ir išanalizuoti dėl pažeidžiamumo;
- sąrašas turi būti suderintas ir patvirtintas saugos įgaliotinio;
- sąrašas turi būti reguliariai naujinamas;
- bet koks sąrašo elementas gali būti įtrauktas arba pakeistas tik suderinus su atsakingu už saugą asmeniu ar padaliniu;
- turi būti naudojamos naujausios patvirtintų įrankių versijos, kad būtų galima pasinaudoti naujų saugumo funkcijų teikiamomis galimybėmis;
- sąraše gali būti patvirtinta šifravimo technologija ir kriptografinio rakto ilgis.

[6] OWASP SCP Quick Reference Guide v2 – https://owasp.org/www-pdf-archive/OWASP_SCP_Quick_Reference_Guide_v2.pdf.

Turi būti privaloma statinio kodo analizė[7] (angl. *Static code analysis*), programinis kodas turi būti išnagrinėtas peržvelgimo, verifikavimo ir automatiniu būdu prieš paleidžiant programą.

Automatinio statinio kodo analizės įrankio pasirinkimo kriterijai:

- ar palaiko taikomą ar taikomas programavimo kalbas;
- ar palaiko naudojamas bibliotekas ir programinės įrangos karkasus;
- aptinkamų pažeidžiamumų rūšys, kurias jis gali apimti (bet kuriuo atveju ne mažiau, negu *OWASP Top 10*[8]);
- ar įrankis palaiko ir supranta visus komponentus, reikalingus programos sukonstravimui (angl. *Build*);
- įrankio patikimumas, pvz., rezultato tikslumo, jautrumo įverčiai;
- ar gali būti integruotas į integruotąją kūrimo aplinką (angl. *IDE*);
- naudojimosi patogumas ir sudėtingumas;
- įrankio licencijavimo ypatumai.

Testavimas

Testavimo tikslas – įsitikinti, ar kuriamam produktui keliami reikalavimai buvo įgyvendinti, ir jei taip, ar įgyvendinti tinkamai. Svarbu atminti, kad ***BDAR taikomas sistemos kūrimo ir testavimo aplinkoms***, o testavimui turi būti vengiama naudoti tikrus asmens duomenis. Tais atvejais, ***kai naudoti testinių duomenų neįmanoma, turi būti nustatytos specialios testavimo metu naudojamų asmens duomenų apsaugos procedūros***.

Kuriamo produkto pritaikytosios ir standartizuotosios asmens duomenų apsaugos nustatymų testavimas turėtų apimti bent šias veiklas:

- Patikrinti, ar suprojektuoti ir specifikuoti reikalavimai atitinka įgyvendintus duomenų apsaugos reikalavimus. Sukurti standartinius testavimo scenarijus pagal nustatytus funkcionalumus:
  - dėl numatytųjų maksimalių duomenų subjekto privatumo nustatymų;
  - dėl duomenų subjekto duomenų eksporto ir importo (duomenų perkeliamumo);
  - dėl duomenų saugojimo vietos tinkamumo;
  - dėl renkamų duomenų atitikties nustatytiems funkcionalumams;
  - dėl duomenų subjekto sutikimo davimo ir atšaukimo;
  - dėl programų, paslaugų, techninių komponentų ar pan. įjungimo ir išjungimo, diegimo ir pašalinimo duomenų subjekto iniciatyva;
  - dėl prieigos kontrolės;
  - dėl duomenų subjekto prieigų prie savo asmens duomenų;
  - dėl duomenų subjekto galimybių ištaisyti, užblokuoti ar ištrinti asmens duomenis;

[7] Automatinių statinio kodo analizės įrankių sąrašas – https://owasp.org/www-community/Source_Code_Analysis_Tools.
[8] OWASP Top 10 – https://owasp.org/www-project-top-ten.

- dėl užklausų ir skundų, susijusių su duomenų apsauga ir saugumu, pateikimo;
- dėl duomenų subjekto profiliavimo užkardymo mechanizmų;
- dėl duomenų subjekto tinkamo informavimo apie automatizuotų spendimų priėmimą, duomenų rinkimą, saugojimą, apdorojimą, tvarkymo skaidrumą ir pan.

– Patikrinti ar pranešimo apie asmens duomenų saugumo pažeidimą ir (ar) kitų pranešimų priežiūros ir kitoms institucijoms ir duomenų subjektams funkcionalumai ir procedūros tinkamai veikia, ar paruošti tipinių tekstų projektai;
– Atlikti saugumo patikrinimus:
  - programinės įrangos pažeidžiamumams nustatyti naudoti tiek statinius, tiek dinaminius saugos patikrinimus pagal juodosios dėžės (angl. *Black box*), pilkosios dėžės (angl. *Grey box*), baltosios dėžės (angl. *White box*) testus ir (ar) jų derinius:
    - įsilaužimo testai (angl. *Penetration Testing*) – galimų įsilaužimo scenarijų įgyvendinimas ir produkto atsako stebėsena;
    - pažeidžiamumų skenavimai (angl. *Vulnerability Scan*) – ištestuoti pagal iš anksto žinomus, galimai nesaugius sistemos komponentus ir konfigūracijas, vykdant iš anksto nustatytus atakos modelius;
    - Atsitiktinių duomenų testai (angl. *Fuzz Testing, Fuzzing*) – atsitiktinių įvesties duomenų, kuriems apdoroti nenumatyta sukurta sistema, generavimas ir įvedimas, siekiant kompromituoti sistemos vientisumą.

Produkto saugumo patikrinimui patariama naudoti OWASP taikomosios interneto programinės įrangos saugumo testavimo vadovą[9] (angl. *OWASP Web Security Testing Guide*).

Testavimo rezultatų išvados apie buvusius neatitikimus veiklos ir realizavimo reikalavimams, pašalintus trūkumus ir paliekamus dalinius neatitikimus su priimtina rizika patikslintam programiniam kodui, diegimo paketui, patikslintai techninei dokumentacijai ***turi būti dokumentuojamos***.

Bandomoji eksploatacija

Bandomosios eksploatacijos tikslas – patvirtinti, kad sukurtas produktas yra tinkamas eksploatuoti.

Šiame žingsnyje kuriamas produktas parengiamas darbui, todėl svarbu ***suplanuoti***, kaip ***efektyviai valdyti duomenų saugumo incidentus***, kurie gali kilti pradėjus eksploataciją, taip pat ***sukurto produkto techninės ir programinės įrangos atnaujinimo procedūras (pokyčių valdymą)***. Prieš paleidžiant techninę ir programinė įrangą, reikia atlikti išsamią ir ***galutinę saugumo analizę***.

Organizacija turi parengti su sukurto produkto programine ir technine įranga susijusių ***incidentų ir pokyčių valdymo planus***.

[9] OWASP Web Security Testing Guide – https://owasp.org/www-project-web-security-testing-guide/stable/.

Incidentų valdymo (veiklos tęstinumo) planas turi apimti bent šiuos aspektus:

- turi būti apibrėžti atsakingų asmenų (įskaitant pagalbos centrą) incidentų valdymo veiksmai ir įgaliojimai, kontaktai, reikalingi ištekliai veiklos tęstinumui užtikrinti;
- turi būti nurodyta kontaktinė informacija dėl eskalavimo (darbuotojų hierarchija pagal atsakomybes), įskaitant organizacijos duomenų apsaugos pareigūno kontaktinę informaciją;
- veiksmų, kurie būtų atliekami įvykus saugos incidentui, vykdymo eiliškumas ir atsakingi vykdytojai pagal kiekvieną veiklą;
- plane turi būti aprašytos incidentų valdymo procedūros dėl trečiųjų šalių komponentų, kodo ar pan.;
- turi būti apibrėžtas sukurto produkto darbo atstatymo laikas, atsižvelgiant į programinės ir techninės įrangos komponentų svarbą ir teisės aktų reikalavimus;
- turi būti nustatytos pranešimų atsakingoms institucijoms formos ir tvarkos;
- turi būti nustatyti saugūs komunikacijos kanalai incidentui valdyti.

Pokyčių valdymo planas turi apimti bent šiuos aspektus:

- pokyčių identifikavimą;
- suskirstymą į kategorijas pagal pokyčio tipą (administracinis, organizacinis ar techninis);
- įtakos vertinimą ir pokyčių prioritetų nustatymą;
- pokyčių inicijavimo procesus.

Visi pokyčiai, galintys sutrikdyti ar sustabdyti sukurto produkto darbą, turi būti suderinti su atsakingu asmeniu ir vykdomi tik gavus jo raštišką pritarimą. Pokyčiai, galintys daryti neigiamą įtaką elektroninės informacijos konfidencialumui, vientisumui ar prieinamumui, turi būti patikrinti bandomojoje aplinkoje (kurioje nėra konfidencialių duomenų ir asmens duomenų) ir kuri atskirta nuo eksploatuojamo produkto.

Turi būti atlikta galutinė saugumo analizė, įvertinant visus galimus nukrypimus nuo reikalavimų pagal šiuos aspektus:

- duomenų apsaugos reikalavimai;
- duomenų saugumo reikalavimai;
- poveikio duomenų apsaugai vertinimas;
- rizikos vertinimas, priimtini rizikos lygiai;
- produkto specifikacija;
- atakos paviršiaus analizė;
- programinio kodo analizė;
- trečiųjų šalių komponentai;
- dinaminė įrangos analizė, įskverbties ir pažeidžiamumų testavimai.

Bandomosios eksploatacijos eiga, užfiksuoti trūkumai ir jų šalinimo rezultatai turi būti dokumentuojami.

INFORMACINĖS SISTEMOS EKSPLOATAVIMAS

Pasibaigus bandomajai eksploatacijai produkto tinkamumas eksploatuoti turi būti patvirtintas atsakingų asmenų. Eksploatuojant sistemą privaloma nustatyti vaidmenis ir atsakomybes bei įgaliojimus, užtikrinti jų laikymąsi.

Visi svarbūs viso kūrimo proceso duomenys turi būti archyvuojami, įskaitant visas specifikacijas, programinį kodą, poveikio duomenų apsaugai vertinimą, rizikos vertinimą, veiklos tęstinumo planus, licencijas, trečiųjų šalių programinės įrangos paslaugų teikimo sąlygas ir kitus dokumentus.

Taip pat privaloma nustatyti sistemos komponentus, kurie gali tapti atakų taikiniais (programos, serveriai, tinklai) ir ***nuolatos vertinti techninių ir organizacinių saugumo priemonių veiksmingumą:***

- pažeidžiamumo analizė ir skverbimosi testai;
- nuolatiniai automatiniai programinės įrangos, infrastruktūros ir tinklo būklės patikrinimai;
- serverio ir kliento programinės įrangos bei trečiųjų šalių komponentų taisymas;
- našumo patobulinimai, laiku atliekami įrangos atnaujinimai, pvz., operacinių sistemų, programinės įrangos bibliotekų, šifravimo algoritmų ir jų raktų atnaujinimai ir pan.;
- sistemos įvykių ir vartotojų veiklos registravimas, periodiškos žurnalų peržiūros siekiant nustatyti saugumo pažeidimus;
- reguliarūs mokymai, instruktažai ir pan.;
- asmens duomenų apsaugos kultūros laikymasis (pvz., apklausos, testai ir pan.);
- incidentų valdymo plano reguliarus atnaujinimas;
- vidaus ir išorės auditai ar kitokios formos atitikimų taisyklėms (teisės aktams, elgesio kodeksams, vidaus taisyklėms, saugos politikai ir pan.) dokumentavimas;
- periodiniai duomenų tvarkytojų ir trečiųjų šalių patikrinimai dėl susitarimų laikymosi.

INFORMACINĖS SISTEMOS MODERNIZAVIMAS

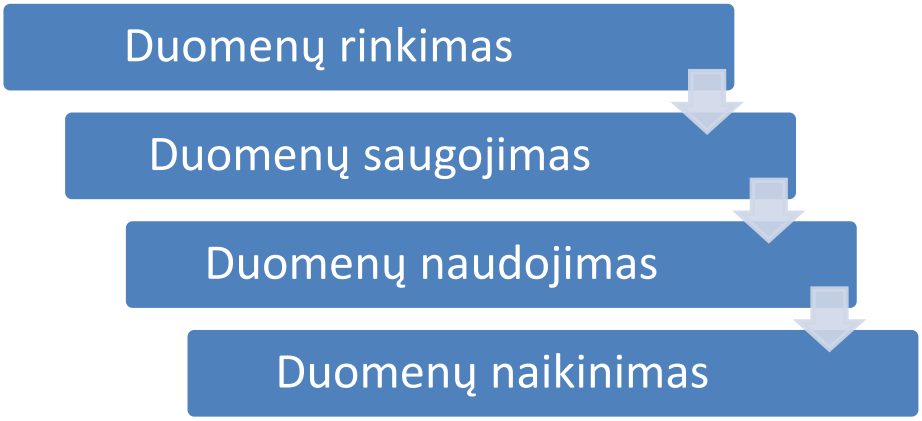
Informacinės sistemos modernizavimu siekiama papildyti ir (arba) pakeisti informacinės sistemos funkcijas, informacijos apdorojimo procesus, funkcinę ir techninę struktūras, asmens duomenų tvarkymo operacijas, todėl privaloma atlikti šiuos veiksmus:

- įvertinti informacinės sistemos modernizavimo apimtį;
- įvertinti, ar modernizavimo sprendimo priėmimo etapo metu vykdomos veiklos atitinka veiklas, numatytas sistemos inicijavimo stadijos metu;
- išanalizuoti aktualių teisės aktų pakeitimus;
- identifikuoti poreikį keisti asmens duomenų struktūras ir jų apdorojimo procesus;
- peržiūrėti ir atnaujinti poveikio asmens duomenų apsaugai vertinimą;
- peržiūrėti ir atnaujinti rizikos vertinimą;
- specifikuoti naujus ir patikslinti esamus sistemos reikalavimus;
- parengti modernizavimo planą.

Modernizuojant informacinę sistemą vykdyti inicijavimo ir kūrimo etapo veiklas, atsižvelgiant į modernizavimo apimtis.

INFORMACINĖS SISTEMOS LIKVIDAVIMAS

Informacinės sistemos gyvavimo ciklo pabaigoje privaloma įvertinti sistemoje tvarkytų asmens duomenų struktūras atsižvelgiant į likvidavimo ir asmens duomenų tvarkymo tikslus bei šių duomenų gyvavimo ciklą (*3* pav.). ***Turi būti parengtas informacinės sistemos likvidavimo planas*** su detaliais likvidavimo darbais ir numatytais atsakingais vykdytojais.



3 pav. Asmens duomenų gyvavimo ciklo etapai

Likviduojant sistemą asmens duomenys gali būti ***perduodami kitoms informacinėms sistemoms, archyvuojami (perduodami archyvui), anonimizuojami arba sunaikinami***, todėl ***būtina apibrėžti tokio duomenų tvarkymo tikslus ir uždavinius,*** atsižvelgiant į šias galimas veiklas:

- duomenys perduodami kitoms sistemoms išlaikant sistemos inicijavimo metu nustatytus asmens duomenų tvarkymo tikslus;
- duomenys perduodami kitoms sistemoms keičiant sistemos inicijavimo metu nustatytus asmens duomenų tvarkymo tikslus;
- duomenys toliau tvarkomi archyvavimo tikslais (keičiasi sistemos inicijavimo metu nustatyti asmens duomenų tvarkymo tikslai);
- duomenys anonimizuojami arba sunaikinami.

Bet kuriai iš išvardintų veiklų turi būti nustatytos atitinkamos procedūros, įvertintos ir dokumentuotos techninės ir organizacinės saugumo priemonės. Asmens duomenų naikinimas turėtų būti atliekamas tik įvertinus asmenų, kurių duomenys buvo tvarkyti, pagrindines duomenų subjektų teises ir kitus BDAR teisėto tvarkymo aspektus. Asmens duomenų naikinimas turi būti negrįžtamas, be teorinės ir praktinės galimybės juos pakartotinai nuskaityti ar atstatyti. Jeigu to padaryti neįmanoma pasitelkus programinę įrangą, turi būti įvykdytas fizinis duomenų laikmenos sunaikinimas be galimybės atstatyti.