TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Kristofer Säälik 233896IABB
Carmen Maar 230652IABB

MÄNGULINE PLATVORM KÜBERTURBERISKIDE JA ELUKUTSETE TUNDMAÕPPIMISEKS

Bakalaureusetöö

Juhendaja: Birgy Lorenz
PhD

Tallinn 2025

Autorideklaratsioon

Kinnitame, et oleme koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

Autor: Kristofer Säälik

Autor: Carmen Maar

20.05.2025

Annotatsioon

Lõputöö eesmärgiks on luua lahendus IT-s algajatele ja küberturvalisuse huvilistele (õpilased, tudengid, täiskasvanud), mis tõstaks teadlikkust küberturbe riskidest ja küberturvalisuse valdkonna ametitest. Lahenduse vastu on huvi üldhariduskoolidel, kutsekoolidel ja ka ülikoolidel, kes õpetavad küberturvalisuse teemat oma õppekavas, samamoodi saab keskkonda kasutada mängulise koolitusvahendina täiskasvanud õppijatega. Töö analüüsib erinevaid küberturvalisuse riske ja lahendusi. Töö metoodika põhineb ADDIE mudelil, mis koosneb analüüsi, kavandamise, väljatöötamise ja hindamise etappidest. Oluline osa tööst on platvormi loomine 12 erineva küberturvalisuse ameti vaatest (aluseks ENISA kübeturvalisuse oskuste raamistiku rolliprofiilid) ja testimine, et teada saada, millist lisandväärtust mänguline lähenemine toob. Platvormi testiti kokku 12 osalejaga erinevatest sihtrühmadest (tudengid, IT-huvilised, arendajad, täiskasvanud). Tulemused näitasid teadlikkuse tõusu küberturvalisuse riskide ja ametite osas.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 55 leheküljel, 7 peatükki, 13 joonist, 4 tabelit.

Abstract

A Playful Platform for Exploring Cybersecurity Risks and Related Careers

The aim of this thesis is to develop a solution for novice IT learners and cybersecurity enthusiasts including secondary-school pupils, university students, and adults that enhances their awareness of cybersecurity risks and the range of careers within the field. The study analyses a spectrum of cybersecurity threats along with corresponding countermeasures. Its methodological framework follows the ADDIE model, encompassing the phases of analysis, design, development, and evaluation. Central to the work is the creation and empirical testing of a gamified platform in order to determine the added value that a playful approach can deliver. The platform was evaluated with 12 participants representing different target groups (students, IT-enthusiasts, software developers, and adults). The findings indicate a measurable increase in participants understanding of cybersecurity risks and related professional roles.

The thesis is in estonian and contains 55 pages of text, 7 chapters, 13 figures, 4 tables.

Lühendite ja mõistete sõnastik

ADDIE	*Analysis, Design, Development, Implementation, Evaluation*, õppekavanduse etappide mudel
AI	*Artificial Intelligence* , tehisintellekt
APT	*Advanced Persistent Threat*, pikaajaline, sihitud küberrünne
CCDCOE	*Cooperative Cyber Defence Centre of Excellence,* NATO küberkaitse kompetentsikeskus (Tallinn)
CISA	*Cybersecurity & Infrastructure Security Agency,* USA riiklik küber- ja taristukaitse amet
CISO	*Chief Information Security Officer,* infoturbe juht
CI/CD	*Continuous Integration / Continuous Delivery,* järjestikune tarkvarakooste ja -paigaldus
CLI	*Command-Line Interface,* käsurealiides
CSS	*Cascading Style Sheets,* veebilehtede stiililehed
DDoS	*Distributed Denial of Service,* hajus teenusetõkestusrünne
DOM	*Document Object Model,* veebidokumentide objektmudel (nt React Virtual DOM)
DPI	*Dots per inch,* punkti tolli kohta (ekraani või trüki eraldusvõime)
DVWA	*Damn Vulnerable Web Application,* haavatavuste harjutusveeb
ECSF	*European Cybersecurity Skills Framework,* EL küberoskuste raamistik
ENISA	*European Union Agency for Cybersecurity,* Euroopa Liidu küberturbe agentuur
EU	*European Union,* Euroopa Liit
FBI	*Federal Bureau of Investigation,* USA Föderaalne juurdlusbüroo
FTC	*Federal Trade Commission,* USA Föderaalne kaubanduskomisjon
GDPR	*General Data Protection Regulation,* isikuandmete kaitse üldmäärus
HTML	*HyperText Markup Language,* veebilehtede märgistuskeel
HTTP	*HyperText Transfer Protocol,* veebiliikluse põhiprotokoll
IA	Arvutisüsteemide instituut, TalTechi Arvutisüsteemide instituut
IDE	*Integrated Development Environment,* tarkvaraarenduse integreeritud töökeskkond

IT	*Information Technology,* infotehnoloogia
JSON	*JavaScript Object Notation,* kergete andmestruktuuride tekstivorming
JS	*JavaScript* — veebiskriptide programmeerimiskeel
NIS	*Network and Information Security Directive,* Euroopa Liidu direktiiv kriitiliste teenuste küberkaitseks
NIST	*National Institute of Standards and Technology,* USA standardite ja tehnoloogia instituut
OWASP	*Open Web Application Security Project,* avatud veebirakenduste turbeprojekt
RIA	Riigi Infosüsteemi Amet, Eesti riigi infoturbekeskne amet
SQL	*Structured Query Language,* relatsioonandmebaaside päringukeel
TLS	*Transport Layer Security,* transpordikihi krüpteerimisprotokoll
UI	*User Interface,* kasutajaliides
UX	*User Experience,* kasutajakogemus
XSS	*Cross-Site Scripting,* skriptisisestuse rünne
WebGoat	WebGoat, OWASP-i harjutusveeb haavatavuste õppimiseks
Juice Shop	OWASP Juice Shop, haavatavustega mänguline õppeveebipood
RangeForce	RangeForce, Eesti päritolu küberturbe virtuaallaborite platvorm
Cybexer	Cybexer Technologies, Eesti küberõppe ja simulatsioonide platvorm
Kübertest	Kübertest, RIA juhendatud küberturvalisuse teadlikkuse test Eesti asutustele

Sisukord

1 Sissejuhatus 11
1.1 Probleem 12
1.2 Eesmärk 12
1.3 Töö ülesehitus 13
1.4 Sihtrühm 14
2 Probleemipüstitus ja rakenduse eesmärk 16
2.1 Ülemaailmsed riskid 16
2.2 Küberturvalisuse juhtumid 17
2.2.1 Eesti küberturvalisuse väljakutsed ja juhtumid 18
2.3 Olemasolevate turvaõppe platvormide analüüs 19
2.4 Hariduslikud õpimängud ja nende ülesehitus 22
2.4.1 Interaktiivsete ja mänguliste õppemeetodite rakendamine 22
2.4.2 Hariduslike õpimängude põhimõtete rakendamine küberturvalisuse valdkonnas antud bakalaureusetöö raames 23
2.5 Küberturvalisuse ametikohad ja vastutusvaldkonnad 25
3 Metoodika 28
3.1 Analüüs 29
3.1.1 Kavandamine 30
3.1.2 Väljatöötamine 30
3.1.3 Testimine 31
3.1.4 Eetilised kaalutlused ja piirangud 32
4 Lahendus 34
4.1 Tehnoloogia valik 34
4.2 Mängude ja disainide loomine 37
4.2.1 Funktsionaalsed nõuded 37
4.2.2 Mittefunktsionaalsed nõuded 38
4.2.3 Kasutuslood 38
4.2.4 Disaini loomine 41
4.2.5 Kasutaja teekond mängus 44
4.2.6 Mängude küsimuste loomine ja sisu kujundamine 45
4.2.7 Disainiotsused ja kasutajasõbralikkus 46
4.2.8 Iteratiivne kavandamine ja prototüüpimine 46

4.3 Lahenduse arendus 47
4.3.1 Eesrakenduse struktuur 47
4.3.2 Lahenduse näidised 52
5 Testimine 57
5.1 Testimise tulemused 57
5.2 Täiustamist vajavad aspektid 59
5.3 Kokkuvõte ja edasised soovitused 60
6 Arutelu 61
6.1 Autorite panus 63
7 Kokkuvõte 64

Jooniste loetelu

Joonis 1. Õppemängude disaini põhimõtted 23
Joonis 2. Küberturvalisuse õppeplatvormi arendus 29
Joonis 3. Karjääripööraja 39
Joonis 4. Tudeng 40
Joonis 5. Gümnaasiumiõpilane 41
Joonis 6. Infosüsteemi arhitektuur 42
Joonis 7. Canva algne disain 43
Joonis 8. Kasutaja liikumise skeem veebilehel 45
Joonis 9. src-kataloogi struktuur 47
Joonis 10. Ameti valik avalehel 53
Joonis 11. Ameti lehekülg ja sissejuhatus 54
Joonis 12. Mängu alustamine 55
Joonis 13. Mänguseeria lõpp 56

Tabelite loetelu

Tabel 1. Eesti küberturvalisuse kriitilised juhtumid (RIA 2020-2024) 18
Tabel 2. Olemasolevate turvaõppeplatvormide võrdlusanalüüs 20
Tabel 3. Eesrakenduse tehnoloogiate võrdlus 36
Tabel 4. Testimise tulemused 58

1 Sissejuhatus

Digitaalses ühiskonnas on küberturvalisus järjest olulisem teema, mis puudutab nii organisatsioone kui ka igapäevaseid tehnoloogiakasutajaid [17]. Kuna turvalisuse alaseid õppelahendusi on loodud eelkõige IT-spetsialistidele, puudub laialdaselt kättesaadav ja kasutajasõbralik lahendus, mis aitaks ka mittetehnilise taustaga inimestel mõista ja ennetada levinumaid küberturvalisuse riske [24]. Eestis on üldhariduse ja kutsekoolide õppekavas küberturvalisuse valikaine, ülikoolis õpetatakse küberturvalisust mitte IT eriala õppijatele näiteks Infotehnoloogia valikteema aines [51], IT-õppijatele, kes ei ole küberkaitse erialal, pakutakse näiteks Info- ja küberturbe alused ainet [50], kõikide nende ainete raames oleks hea kasutada mängustatud turvalisuse õppimise võimalust.

Paljud tudengid, kontoritöötajad ja teised tavakasutajad ei pruugi teadlikult märgata igapäevaseid turvavigu, mis võivad ohustada nende andmeid, seadmeid ja kontosid. Samas võib ka algajal IT-huvilisel olla keeruline leida struktureeritud ja mängulist õppimisviisi, mille kaudu tutvuda küberturvalisuse põhitõdede ja tööelus ettetulevate turvariskidega [74]. Kuigi olemas on mitmeid õppimisplatvorme, näiteks WebGoat [73], Juice Shop [71], DVWA [21] ja Cybexer [6] on need peamiselt suunatud tehnilise taustaga kasutajatele. Samuti pakub Eesti riik Kübertesti [58] mille eesmärk on tõsta üldist turvateadlikkust, kuid sellele ligipääs on piiratud ehk seda saavad kasutada ainult organisatsioonid, kes selle omale on tellinud, mistõttu ei pruugi see kõnetada laiemat sihtrühma. Samuti ei ole tegemist mängustatud lahendusega, vaid Moodle testiga [58]. Lisaks ei mõista enamus inimesed, vahel ka IT-taustaga, milliseid tegevusi ja erinevaid rolle täidetakse küberturvalisuse valdkonnas. On tekkinud väärarusaam, et kõik küberturvalisusega tegelejad on intsidentide haldurid või turvatestijad ehk rahvakeeli häkkerid [31] Seetõttu eksisteerib vajadus uue lahenduse järele, mis muudaks küberturvalisuse õppimise lihtsamaks, kaasahaaravamaks ja praktilisemaks just väheste eelnevate teadmistega kasutajatele ja tõstaks ka teadlikkust valdkonnas eksisteerivate rollide ja ametite kohta [25].

1.1 Probleem

Olemasolevad küberturvalisuse õppelahendused on valdavalt orienteeritud tehnilisele kasutajale ning eeldavad varasemaid teadmisi, mis takistab laiemal kasutajaskonnal turvateadlikkuse tõusu läbi praktiliste või mänguliste kogemuste nagu näiteks küberturvalisuse lipuvõistlused (CTF) või simulatsioonid [45], [105]. Samas näitavad nii rahvusvahelised kui ka kohalikud raportid OWASP Top 10 [72] NIST Cybersecurity Framework [101], ENISA [20], RIA aastaraamatud [85] – [91], et suur osa turvariskidest tuleneb inimfaktoritest ja lihtsatest eksimustest, mida oleks võimalik ennetada praktilise õppimise abil.

Lõputöös püstitati hüpotees, et interaktiivne ja mänguline õppelahendus, mis võimaldab kasutajatel realistlikke küberturberiske kogeda ja neid mõtestada, suurendab kasutajate turvateadlikkust ning aitab vähendada levinud turvavigade esinemist ja aitab saada teadlikumaks erinevatest ametitest küberturvalisuse valdkonnas.

Hüpoteesi tõestamist aitavad töös uuritavad küsimused:

- Millised on kõige olulisemad ja sagedasemad küberturberiskid ja ametid Eestis ja rahvusvahelisel tasandil, mida tuleks platvormil kajastada?
- Millised on olemasolevate küberturbeõppe lahenduste tugevused ja piirangud?
- Milliseid tehnoloogiaid ja mängustatud disainipõhimõtteid tuleks kasutada, et platvorm oleks tõhus ja kasutajasõbralik?
- Kuidas hinnatakse loodud platvormi kasutatavust ja õppemõju sihtrühma (kasutajate) poolt?

1.2 Eesmärk

Käesoleva lõputöö eesmärk on arendada interaktiivne ja mängustatud veebipõhine õppeplatvorm, mis võimaldab kasutajatel praktiliselt tutvuda küberturvalisuse ametites esinevate riskistsenaariumidega ning õppida nende ennetamise viise. Platvormi sisu tugineb reaalsetel juhtumitel ning rahvusvahelistel küberturvalisuse standarditel ja suunistel nagu OWASP Top 10 [72], NIST Cybersecurity Framework [101] ja ENISA raportid [30] – [32]. Samuti võetakse arvesse Eesti küberturvalisuse olukorda, kasutades allikaid nagu RIA aastaraamatud [85] – [91] ja Cybersecurity Skills Needs Analysis

Report: Estonia raport [17]. Platvorm põhineb Euroopa küberturvalisuse oskuste raamistiku rolliprofiilidel [31].

Platvormi arendamiseks on kavandatud mitmeastmeline tegevusplaan:

- Esmalt kaardistatakse Eesti ja rahvusvahelise statistika alusel olulisemad küberturbeprobleemid, keskendudes just sagedasematele ja kriitilisematele riskidele. Seejärel analüüsitakse olemasolevaid õppelahendusi, hinnates nende tugevusi ja piiranguid, et mõista, millised aspektid vajavad täiustamist või uutmoodi lähenemist (vt peatükk 1, 2);
- Edasi määratletakse platvormi arendamiseks sobivaimad tehnoloogiad ning koostatakse nõuete analüüs, mis loob aluse platvormi funktsionaalsuse ja kasutuskogemuse kujundamiseks. Arendusetapis luuakse esmane prototüüp, mis sisaldab vähemalt neljakümne kaheksat ametitel põhinevat interaktiivset ülesannet või stsenaariumi, mis on jaotatud 12 küberturvalisuse rolli vahel (vt peatükk 4);
- Lõpetuseks viiakse läbi kasutajate testimine, mille käigus kogutakse tagasisidet platvormi kasutusmugavuse ja tõhususe kohta. Testimisetulemuste põhjal hinnatakse, kuivõrd platvorm aitab kasutajatel mõista küberturvalisuse aluseid ja suurendab nende turvateadlikkust igapäevastes digikeskkondades (vt peatükk 5);

Töö lõpptulemusena valmib veebipõhine õpperakendus, mis aitab laiendada küberturvalisuse alast teadlikkust just tavakasutajate seas ning pakub uudset viisi turvapädevuste omandamiseks läbi praktiliste stsenaariumide.

1.3 Töö ülesehitus

Töö koosneb kahest põhiosast. Teoreetiline osa käsitleb küberturvalisuse peamisi ohte, olemasolevaid õppelahendusi ja tehnoloogilisi valikuid. Praktiline osa kirjeldab interaktiivse õppeplatvormi arendusprotsessi, kasutatud tehnoloogiaid, testimismetoodikat ja tulemusi. Töö sisuliseks osaks on ka metoodika, analüüsi, sissejuhatuse ja kokkuvõtte peatükid.

1.4 Sihtrühm

Käesoleva töö raames loodud interaktiivse ja mängustatud küberturvalisuse õppeplatvormi sihtrühm on lai ja mitmekesine, hõlmates erinevaid kasutajaprofiile ja teadmiste tasemeid.

Esmaseks sihtrühmaks on gümnaasiumiealised noored, kellel puuduvad varasemad teadmised küberturvalisusest. Selle sihtrühma puhul on platvormi eesmärk pakkuda esmast tutvustust küberturvalisuse teemadesse ning tõsta teadlikkust igapäevastest riskidest, mis võivad mõjutada nende digitaalseid tegevusi ja turvalisust. Gümnaasiumis õppivale noorele on oluline mõista ka erinevaid küberturvalisuse ameteid ja rolle, sest peale gümnaasiumi lõppu hakatakse valima eriala, mida minna õppima. Kui õppija näeb mängus erinevaid rolle ja ameteid, siis mõistab ta enam, et küberturvalisuse valdkond võiks sobida ka talle, sest seal on palju erinevaid võimalusi teha tulevikus tööd. Sarnane sihtrühm on ka kutsekoolis õppivad noored, kelle programmis õpitakse küberturvalisuse aluseid ning ka ülikoolis õppivad mitte IT-eriala üliõpilased.

Platvorm on mõeldud ka karjääripöörajatele, kes kaaluvad küberturvalisuse erialal edasiõppimist oma järgmise karjäärisammuna ning soovivad mõista, milliseid erinevaid ameteid ja tööülesandeid küberturvalisuse valdkonnas leidub. Sellisel juhul täidab platvorm ka karjäärinõustamise funktsiooni, andes ülevaate ametitest ja aidates mängijal teha teadlikumaid valikuid oma tuleviku osas.

Lisaks sobib platvorm kasutamiseks esimese kursuse IT-tudengitele, kes ei ole valinud erialaks küberkaitse süvaõpet, aga kelle küberturvalisuse teema õppejõud või miks mitte ka programmijuht, võiks seda kasutada sissejuhatava materjalina küberturvalisuse põhitõdede ja valdkonnas olevate ametite tutvustamiseks. See võimaldab esmakursuslastel interaktiivselt tutvuda teemaga ja luua parem alus otsustamiseks, kas küberturvalisuse valdkonda spetsialiseerumine oleks edasiseks õppimiseks huvitav ka neile.

Samuti on sihtrühmaks laiem üldsus, kes soovib teada, mis toimub küberturvalisuse valdkonnas, soovitakse parandada oma teadlikkust digiturvalisuses riskidest ja ametitest. Selle kasutajagrupi puhul keskendub platvorm turvalisuse aluste selgitamisele praktiliste ülesannete kaudu, mis on kergesti mõistetavad ka ilma tehnilise taustata kasutajatele ning

ametite tutvustamisele. Mäng sobib seega kasutada ka küberturvalisuse teema algkoolitusel tavakasutajatele.

Seega on loodud platvorm disainitud nii, et see vastaks erinevate kasutajagruppide vajadustele, pakkudes praktilist ja ligipääsetavat õpikeskkonda, kus saab tõsta teadlikkust ning omandada esmaseid küberturvalisuse oskusi ja teadmisi.

2 Probleemipüstitus ja rakenduse eesmärk

Digitaalses maailmas on veebipõhised lahendused ja teenused muutunud igapäevaelu lahutamatuks osaks. Pangatehingud, e-poed, hariduskeskkonnad, sotsiaalmeedia ja e-riigi teenused on vaid mõned näited sellest, kuidas meie elu sõltub üha rohkem veebipõhistest rakendustest. Selle suurenenud sõltuvusega kaasnevad ka suuremad turvariskid, kuna järjest rohkem andmeid ja äriprotsesse on veebikeskkonnas kättesaadavad [19].

2.1 Ülemaailmsed riskid

Eestis on küberturvalisus oluline riiklik prioriteet. Riigi Infosüsteemi Ameti (RIA) aastaraamatute kohaselt [80]-[87] esineb Eestis igal aastal mitmeid küberturbeintsidente, mis mõjutavad nii ettevõtteid kui ka eraisikuid. Sageli on nendeks lunavararünnakud, mille tagajärjel ettevõtted kaotavad ligipääsu olulistele andmetele. Samuti esineb andmelekked ja identiteedivargused, mis võivad tavakasutajatele põhjustada suuri isiklikke ja rahalisi probleeme. Eestis rõhutatakse vajadust tõsta elanike küberturvalisuse alast teadlikkust, et ennetada taolisi intsidente. Avaliku sektori infoturvet reguleerib Eesti infoturbestandard (E-ITS), mis sätestab riskipõhised turvameetmed ning tugineb rahvusvahelisele standardile ISO/IEC 27001 [69].

Euroopa tasandil reguleerivad küberturvalisust mitmed standardid ja direktiivid, näiteks Euroopa Liidu võrgu- ja infoturbe direktiiv (NIS direktiiv) [60]. Selle eesmärk on tagada ühtlane kõrge turvatase kogu Euroopa Liidus ning kaitsta olulisi teenuseid, nagu pangandus, energia ja transport. Euroopa standardid rõhutavad ka isikuandmete kaitset, mille eest seisab andmekaitse üldmäärus (GDPR) [38] tagades, et ettevõtted ja asutused kaitsevad kasutajate andmeid ning reageerivad turvaintsidentidele kiiresti ja tõhusalt. Ka USA Riiklik Standardite ja Tehnoloogia Instituut (NIST) [36] defineerib küberturvalisust kui „tehnoloogiate, protsesside ja praktikate kogumit, mille eesmärgiks on kaitsta võrke, seadmeid, programme ja andmeid küberrünnakute, kahjustuste või volitamata juurdepääsu eest”. USA näited näitavad selgelt, kuidas küberturvalisus puudutab otseselt tavakasutajaid. Näiteks 2021. aasta Colonial Pipeline lunavararünnak [100] tõi kaasa ulatuslikud kütusetarneprobleemid, mõjutades miljonite inimeste igapäevaelu.

2.2 Küberturvalisuse juhtumid

Digitaalsete süsteemide kasvav keerukus ja üha enam virtualiseeruv elukeskkond on suurendanud vajadust küberturvalisuse alaste teadmiste ja oskuste järele. Hariduslikes kontekstides on oluline pakkuda õppijatele praktilisi tööriistu ja kogemusi, mis tuginevad reaalsetele juhtumitele ja rahvusvahelistele standarditele [72], [84].

Rahvusvahelises kontekstis on OWASP Top 10 [72] raportis välja toodud kriitilised veebirakenduste turvariskid, nagu süstimisrünnakud ja ebaturvalised ligipääsukontrollid, mille mõju võib ulatuda andmelekete ja suurte finantskahjudeni [84] Samuti rõhutab Euroopa Küberturvalisuse Agentuur (ENISA), et transpordisektor on muutunud üha haavatavamaks lunavararünnakutele ja tarneahela nõrkustele, mis võivad halvata olulise infrastruktuuri [30], [94].

Veebirakendused on praegu kõige sagedasemad küberrünnakute sihtmärgid. OWASP Top 10 raporti [72] andmetel on veebirakenduste vastu suunatud rünnakute arv ja keerukus märkimisväärselt tõusnud. Küberrünnakutel on tõsised tagajärjed nii ettevõtetele kui ka üksikisikutele. Ettevõtted võivad kogeda mainekahju, rahalisi kaotusi, kliendiandmete kadu ja teenusekatkestusi. Üksikisikutele võib küberintsident tähendada privaatsuse kaotust, identiteedivargust või finantsilisi kahjusid. Näiteks Eestis on Riigi Infosüsteemi Ameti (RIA) aastaraamatute [85] – [92] kohaselt olnud mitmeid juhtumeid, kus ettevõtete süsteemid on sattunud lunavararünnakute alla, mille tagajärjel kaotati juurdepääs kriitilistele andmetele [16].

USA Riikliku Standardite ja Tehnoloogia Instituudi (NIST) küberturvalisuse raamistik toob välja vajaduse süsteemseks turvameetmete rakendamiseks läbi viieastmelise protsessi: tuvastamine, kaitsmine, avastamine, reageerimine ja taastamine. NIST rõhutab eriti sotsiaalmanipulatsiooni ja lunavararünnakute ohtusid, mille mõju tõestasid selgelt SolarWindsi ja Colonial Pipeline'i juhtumid [36], [63], [100], [107].

Paljud küberturbeintsidendid leiavad aset tavakasutajate ebapiisava teadlikkuse tõttu. Enamik kasutajaid ei mõista turvariskide tõsidust ega oska rakendada esmaseid ennetusmeetmeid nagu tugevate paroolide kasutamine või kahefaktoriline autentimine [12].

- Näiteks 2018. aastal lekkis Facebookist sadade miljonite kasutajate andmeid, mis hõlmas ka paljude tavakasutajate isiklikku informatsiooni. Viimaste aastate jooksul on toimunud mitmeid suuri turvaintsidente, mille mõju on ulatunud tavakasutajateni [66].
- Näiteks LinkedIni 2012. aasta paroolilekkes sattusid avalikuks miljonite kasutajate andmed ning 2021. aasta Colonial Pipeline lunavararünnak tõi kaasa suuremahulised kütusetarneprobleemid USA-s, mõjutades otseselt tavakodanikke [65], [100], [107].

2.2.1 Eesti küberturvalisuse väljakutsed ja juhtumid

Eesti küberturvalisuse maastikku analüüsides on Riigi Infosüsteemi Ameti (RIA) aastaraamatud [85] – [92] osutunud võtmeallikaks, tuues esile olulisemad juhtumid ja trendid perioodil 2020–2024. Juhtumite põhjal võib välja tuua neli kriitilist teemat (vt Tabel 1):

Tabel 1. Eesti küberturvalisuse kriitilised juhtumid (RIA 2020-2024)

Aasta	**Juhtum**	**Mõjuvaldkond**	**Vastutavad osapooled**
2020	Andmepüük ja sotsiaalmanipulatsioon	Avalik ja erasektor	RIA, infoturbeametnikud
2022	APT-sihtrünnakud	Avalik sektor, riigikaitse	RIA, Kaitseväe küberväejuhatus
2023	Kriitiliste teenuste katkestused	Side-, makseteenused	RIA, sideettevõtted, Tehnilise Järelevalve Amet
2024	Tehisintellekti abil toime pandud pettused (deepfake)	Avalik sektor, meedia	RIA, andmekaitseinspektsioon

Eestis on eriti sagedased andmepüügi olukorrad, mille korral kasutatakse üha nutikamaid sotsiaalmanipulatsiooni meetodeid [85]. Samuti on kasvanud riiklikult suunatud ja pikaajalise planeerimisega APT-rünnakud, mis ohustavad nii strateegilisi infosüsteeme kui ka infrastruktuuri [89]. Lisaks on kriitiliste teenuste katkestused, eriti side- ja makseteenustes, olulised riskid ühiskonna toimimisele [90]. Viimastel aastatel on lisandunud AI-põhised pettused, mille levik võib mõjutada olulisi ühiskondlikke protsesse, sealhulgas valimisi ja meediamaastikku [91].

2.3 Olemasolevate turvaõppe platvormide analüüs

Paljud küberturbeintsidendid leiavad aset tavakasutajate ebapiisava teadlikkuse tõttu. Enamik kasutajaid ei mõista turvariskide tõsidust ega oska rakendada esmaseid ennetusmeetmeid, nagu tugevate paroolide kasutamine või multifaktoriline autentimine.

Käesolevas peatükis analüüsitakse olemasolevaid turvaõppe platvorme, mis on keskendunud veebirakenduste ja küberjulgeoleku teemade õpetamisele. Platvormide valikul lähtuti järgmistest kriteeriumitest: rahvusvaheline tuntus ja tunnustatud organisatsioonide soovitused (näiteks OWASP), ligipääsetavus ja populaarsus hariduslikus või professionaalses kontekstis ja eelistatud platvormid, mida kasutatakse laialdaselt Eesti ja ka rahvusvahelistes haridusasutustes kui ka ettevõtetes.

Platvormide võrdlemisel keskendume järgmistele aspektidele: Sihtgrupi sobivus (tehnilised või mittetehnilised kasutajad), õppesisu praktilisus (reaalne rakendatavus, interaktiivsus), kasutusmugavus (kasutajaliides, juhendamise tase, tehniliste teadmiste vajadus) ning ligipääsetavus ja hind (tasuta või kommertsplatvorm, üldine kättesaadavus). Tabel 2 annab kokkuvõtliku ülevaate võrreldud platvormidest koos nende peamiste tugevuste ja nõrkustega.

Tabel 2. Olemasolevate turvaõppeplatvormide võrdlusanalüüs

Platvorm	**Tootja ja link**	**Sihtgrupp**	**Plussid**	**Miinused**
WebGoat	OWASP (https://owasp.org/www-project-webgoat/)	Tehnilised kasutajad, IT-õppijad	Interaktiivsed praktilised ülesanded, tasuta kasutus	Vajab tehnilisi üldteadmisi, keeruline mittetehnilistele kasutajatele
Juice Shop	OWASP (https://owasp.org/www-project-juice-shop/)	Tehnilised kasutajad, IT-õppijad	Mängustatud ja realistlik simulatsioon, atraktiivne kasutajaliides	Vajab spetsiifilisi tööriistu ja tehnilisi eelteadmisi
DVWA	DVWA projekt (https://dvwa.co.uk/)	Tehnilised kasutajad, IT-õppijad	Lihtne kasutada, reguleeritav raskusaste, tasuta	Ebapiisav realism, tehniliste teadmiste vajadus
RangeForce	Rangeforce (https://www.rangeforce.com)	IT-professionaalid, küberturvalisuse spetsialistid	Realistlikud stsenaariumid, virtuaalsed laborid, praktiline õpe	Kommertsplatvorm, kõrge keerukus, piiratud ligipääs
Cybexer	Cybexer Technologies (https://cybexer.com)	Ettevõtted, riigiasutused, IT-spetsialistid	Realistlikud ja keerulised stsenaariumid, professionaalse taseme simulatsioonid	Kõrge hind, mittesobiv algajatele ja mittetehnilistele kasutajatele
Kübertest	Riigi Infosüsteemi Amet (https://www.ria.ee)	Tavakasutajad, Eesti elanikud	Lihtne kasutada, tasuta, üldhariv	Vähene praktiline kogemus, pinnapealne lähenemine

Alljärgnevalt on toodud põhjalikumad kirjeldused iga platvormi kohta, tuues välja nende omadused ja sobivuse mittetehnilistele kasutajatele:

- **WebGoat** on OWASP-i loodud veebipõhine õppekeskkond, mis võimaldab praktiliselt läbi teha tüüpilisi veebirakenduste turvaauke, näiteks SQL-süstimist ja Cross-Site Scriptingut (XSS). Platvorm on interaktiivne, pakkudes selgeid ülesandeid ja tagasisidet lahenduste kohta. Samas eeldab WebGoat kasutajatelt tehniliste mõistete ja tööriistade tundmist, mis võib mittetehnilistele kasutajatele osutuda raskeks; [73]

- **Juice Shop** on OWASP-i realistlik simulatsioon veebipoest, mille kaudu saab õppida veebirakenduste turvariske lahendama mängustatud keskkonnas. Selle platvormi suurim tugevus on interaktiivne ja atraktiivne kasutajakogemus. Juice Shop vajab siiski tehniliste tööriistade (näiteks Burp Suite, Postman) oskuslikku kasutamist, mis piirab selle sobivust algajatele või tehnilise taustata õppijatele; [71]
- **DVWA (Damn Vulnerable Web Application)** pakub lihtsat ligipääsetavat keskkonda veebirakenduste turvalisuse harjutamiseks. Platvormi eelised hõlmavad kiiret seadistamist ja reguleeritavat raskustaset. Siiski puudub DVWA-l piisav realism ja juhendamine mittetehnilistele kasutajatele, kuna kasutamine nõuab teadmisi HTTP-päringutest ja SQL-ist; [21]
- **RangeForce** pakub sügavat praktilist õppimiskogemust realistlikes virtuaallaborites. Platvorm sobib hästi küberturbe professionaalidele, kellel on juba tugev tehniline baas. RangeForce'i kasutamine on piiratud kommertsplatvormina, mille kõrge keerukus muudab selle mittetehnilistele kasutajatele kättesaamatuks; [79]
- **Cybexer platvorm** keskendub kõrgema taseme simulatsioonidele ettevõtetele ja riigiasutustele, pakkudes realistlikke stsenaariume ja keerulisi ülesandeid. Platvormi keerukus ja hind teevad selle tavakasutajale ja algajale mittesobivaks; [18]
- **Kübertest** on mõeldud tavakasutajate küberturvalisuse teadlikkuse hindamiseks. Platvorm on tasuta ja lihtne kasutada, kuid ei paku piisavat praktilist kogemust ega sügavaid teadmisi turvalisuse rakendamisest. Samamoodi on väljakutseks, et keskkonnale saab ligi ainult organisatsioon, mis on endale selle teenuse käivitanud. Lahendus jookseb Moodlel ja teenust pakub RIA. [58]

Kuigi olemasolevad turvateemalised õppelahendused pakuvad head praktilist kogemust IT-spetsialistidele, ei ole need sageli sobivad tavakasutajatele, kuna eeldavad tehnilisi eelteadmisi. Seetõttu on tekkinud vajadus interaktiivsete, lihtsasti ligipääsetavate ja mittetehnilisele kasutajale arusaadavate turvateadlikkuse lahenduste järele.

2.4 Hariduslikud õpimängud ja nende ülesehitus

Digitaaltehnoloogia areng ja muutused õppimiskäsitustes on toonud kaasa mänguliste ja interaktiivsete õpimeetodite laialdase leviku. Käesolevas peatükis analüüsitakse hariduslike õpimängude olemust, struktuuri ja kujunduspõhimõtteid ning tuuakse välja juhised, millele peab vastama antud töös loodav õpimäng.

2.4.1 Interaktiivsete ja mänguliste õppemeetodite rakendamine

Interaktiivsed ja mängulised õppemeetodid aitavad parandada õppijate motivatsiooni, teadmiste sügavust ja oskuste praktilist rakendatavust [43], [93]. Mängustamine (gamification) loob kaasahaaravaid õpikogemusi, mis vastavad õppijate psühholoogilistele põhivajadustele: autonoomia, kompetentsus ja sotsiaalne seotus [90][108]. Sellised meetodid toetavad eksperimentaalset õppimist, mis võimaldab õppijatel katsetada, teha vigu ning õppida praktiliste kogemuste kaudu [94].

Mängustatud õpikeskkonnad aitavad luua vooseisundi (*flow*), kus õppija oskused ja ülesande raskusaste on tasakaalus, mis suurendab keskendumist ja õppimise efektiivsust [54], [61]. Lisaks pakuvad interaktiivsed meetodid võimalusi personaliseeritud õpiradade loomiseks, mis võimaldavad õppijatel valida ülesandeid oma võimete ja huvide alusel, suurendades nii motivatsiooni kui ka õpitulemuste kvaliteeti [43], [75].

Mängustamise kontseptsioon

Mängustamine (*gamification*) tähendab mänguliste elementide, mehaanika ja esteetika rakendamist mitte-mängulises kontekstis [93]. Hariduslikes õpimängudes võib see väljenduda punktide, saavutuste, avatari loomise, lugude, tasemete ja reaalajas tagasiside kujul. Need elemendid aitavad kujundada kasutajakogemust, mis suurendab õppija aktiivsust ja järjepidevust õpitegevustes [43].

Motivatsioon ja vooseisund

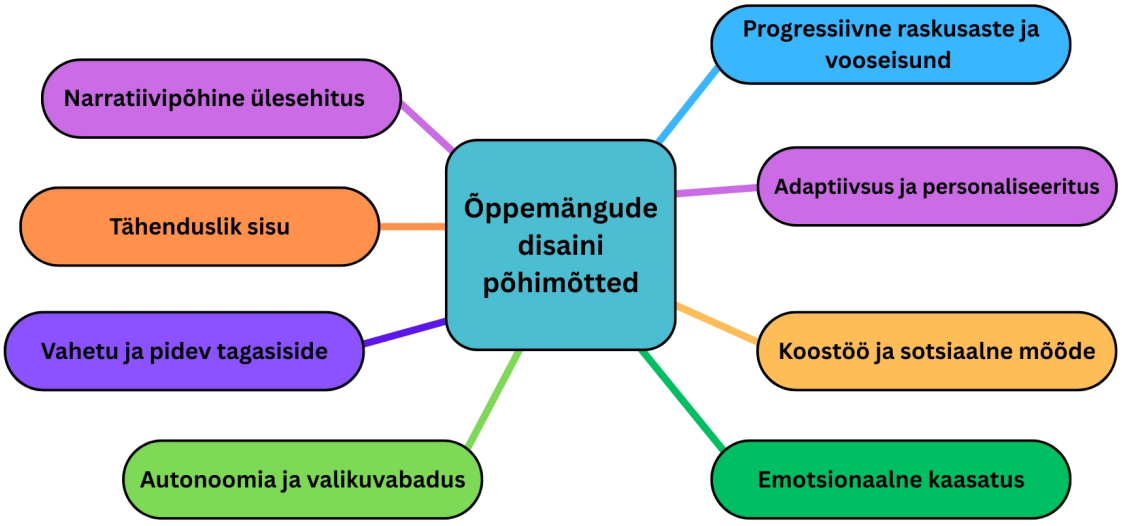
Enesemääratlusteooria (*Self-Determination Theory*) [59], [64] kohaselt peab hea õppemäng toetama autonoomiat, kompetentsust ja seotust – psühholoogilisi aluseid, mis aitavad kaasa sisemisele motivatsioonile. Kui õppija saab valida tegevuse suuna, kogeb eduelamust ning tunneb kuuluvustunnet, kasvab tema pühendumus. Vooseisund [54],

[61] lisab õppemängudele veel ühe mõõtme: tegevuse ja oskuste optimaalne tasakaal hoiab õppijat „mängus“ ning soodustab keskendumist ja järjepidevat pingutust.

Kognitiivne ja sotsiaalne areng

Mängud toetavad kognitiivset arengut, kuna pakuvad õppijale võimalust katsetada, vigu teha ja õppida nendest kogemustest [94]. Digitaalsed mängud, eriti need, mis põhinevad konstruktiivsel ja uurimuslikul õppimisel, aitavad arendada probleemilahendust ja loogilist mõtlemist. Lisaks pakuvad hariduslikud õpimängud võimalusi sotsiaalseks interaktsiooniks – koostöö, võistlus ja suhtlemine mitmikmängudes loovad õpikeskkonna, kus teadmised kinnistuvad praktilise tegevuse kaudu [75]

Alljärgnevalt on kokku võetud peamised disainipõhimõtted, millele käesolevas bakalaureusetöös loodav õpimäng peab vastama (vt joonis 1):



Joonis 1. Õppemängude disaini põhimõtted

Järgmises peatükis vaatame lähemalt erinevaid põhimõtteid.

2.4.2 Hariduslike õpimängude põhimõtete rakendamine küberturvalisuse valdkonnas antud bakalaureusetöö raames

Käesoleva bakalaureusetöö eesmärk on arendada mängustatud ja interaktiivne õppeplatvorm, mis tutvustab küberturvalisuse valdkonna kriitilisi riske ja ennetusmeetmeid laiemale kasutajaskonnale – sealhulgas ka neile, kel puudub varasem tehniline taust. Õpimäng tugineb eelpool kirjeldatud hariduslike mängude

kujunduspõhimõtetele, et saavutada maksimaalne kaasatus, mõtestatud õppimine ja praktiline rakendatavus.

Alljärgnevalt on kirjeldatud, kuidas iga peamine haridusliku mängu komponent realiseeritakse arendatavas platvormis nüüd või tulevikus:

Narratiivipõhine ülesehitus

Mängu keskkond on üles ehitatud juhtumipõhistele stsenaariumitele, kus kasutaja astub eri küberturbeametnike rollidesse (nt küberturbe audiitor, nõrkustestija, infoturbe juht). Iga episood keskendub ühele reaalelulisele olukorrale, näiteks andmeleke, *phishing*-rünnak või sotsiaalne manipulatsioon. Selline lähenemine toetab loo kasutamist õppimise ankurdamiseks (seostatud õppimine) ja seob uue info õppija olemasoleva kogemusmaailmaga ja mängu juhistega [108].

Autonoomia ja valikuvabadus

Õppijale antakse valikuvabadus, milliseid rolle või missioone ta soovib lahendada ning millises järjestuses. See toetab õppija autonoomiat ning võimaldab individuaalset tempo ja huvide järgimist [23].

Progressiivne raskusaste

Mäng jaguneb tasemeteks, mis muutuvad järjest keerulisemaks: alguses tutvustatakse lihtsamaid kontseptsioone (nt turvaline parool), hiljem keerulisemaid (nt XSS või SQL süst). Väljakutsete raskusaste on kohandatud nii, et see ei vii algajaid pingeseisundisse ega muutu igavaks edasijõudnutele – see toetab vooseisundi saavutamist [54], [61].

Vahetu ja pidev tagasiside

Kasutajale antakse iga tegevuse järel reaalajas tagasisidet – kas tema otsus oli turvameetmete seisukohalt õige, millised oleksid alternatiivid, ning millised oleksid potentsiaalsed riskid. Samuti saab kasutaja lühikese ülevaate, kuidas selliseid juhtumeid reguleerivad näiteks NIST või OWASP Top 10 raamistikud [64], [65], [101].

Koostöö ja sotsiaalne mõõde (tulevik)

Platvormi tulevases laienduses on ette nähtud grupitöövõimalused, kus kasutajad saavad jagada oma lahendusi, arutada stsenaariume ja koostöös õppida, nt küberintsidendi lahendamine meeskonnas. See loob kogukonnatunde ning toetab sotsiaalsete oskuste arengut [56]. Antud töö raames seda funktsionaalsust ei realiseeritud, kuid võimekus sellise laiendusele sai loodud.

Adaptiivsus ja personaliseeritus (tulevik)

Kasutaja oskustaset hinnatakse lühikese enesetestiga või esimese taseme soorituse põhjal, mille järgi kohandatakse järgmisi ülesandeid – keerukus ja teemad valitakse vastavalt õppija vajadustele [75] Antud töö raames seda funktsionaalsust ei realiseeritud, kuid võimekus sellise laiendusele sai loodud.

Emotsionaalne kaasatus

Narratiivides kasutatakse huumorit, üllatusi ja realistlikke draamapöördeid (nt infolekke tagajärjed või töötaja eksimus), mis loovad emotsionaalse sideme ning muudavad õppimise nauditavamaks ja meeldejäävamaks [55], [75].

Tähenduslik sisu, mitte punktide kogumine

Ehkki platvorm võiks sisaldada motivatsioonielemente nagu tasemed ja märgid, on rõhk tähenduslikel otsustel ja stsenaariumitel, mitte lihtsalt punktide kogumisel ning kuigi mängijad võiks saada „tasu“ turvateadlikkuse aspektide järgmise, mitte „kiire reageerimise“ eest, [46] siis antud töö raames seda funktsionaalsust ei realiseeritud, kuid võimekus sellise laiendusele sai loodud.

2.5 Küberturvalisuse ametikohad ja vastutusvaldkonnad

Lahenduses mängustamise loomiseks ja eesmärgi saavutamiseks, et mäng sisaldaks nii reaalset praktilist sisu juhtumitest, riskidest ja ametitest, on vaja teada, millised ametid küberturvalisuse valdkonnas eksisteerivad.

Küberturvalisuse valdkonnas eksisteerivad erinevad ametid, mille töö keskendub küberohtude ennetamisele, avastamisele, lahendamisele ja uurimisele. Järgnevalt kirjeldatakse 12 küberturvalisuse ametit vastavalt Euroopa küberturvalisuse oskuste raamistiku rolliprofiilidele [32]. Iga ametikoha kirjeldus sisaldab ülevaadet tööst,

vastutusest ja näidet küberturbeintsidendist, millega nad võivad oma töös kokku puutuda:.

- Infoturbe juht (CISO) vastutab organisatsiooni turvastrateegia ja poliitika väljatöötamise ning elluviimise eest. Tema ülesanded hõlmavad turvariskide hindamist ja intsidentide juhtimist, samuti kommunikatsiooni organisatsiooni juhtkonnaga. Näiteks Equifaxi 2017. aasta andmeleke, kus avalikustati umbes 147 miljoni inimese isiklikud andmed, näitab vajadust CISO järele, kes suudaks selliseid intsidente tõhusalt ennetada ja juhtida [27], [28].
- Kübersündmuste reageerija tuvastab, analüüsib ja reageerib küberintsidentidele. Ta juhib intsidentide lahendamise protsesse ja tagab kahjustuste minimeerimise. Näiteks WannaCry lunavararünnak 2017. aastal mõjutas tuhandeid organisatsioone üle maailma ja vajas kiiret ning koordineeritud reageerimist [1].
- Küberturbe õigus-, poliitika- ja vastavusspetsialist - see spetsialist tagab, et organisatsioon järgib kõiki seadusandlikke ja regulatiivseid nõudeid, näiteks GDPR-i ja NIS direktiivi. Tema ülesandeks on luua ja kontrollida vastavusprogramme. Üheks näiteks on Facebooki GDPR-i rikkumine 2019. aastal, mille tagajärjeks oli 51 000 euro suurune trahv [44].
- Küberturbe ohuanalüütik jälgib küberohtude arengut, analüüsib võimalikke ründeid ja nõustab organisatsiooni nende ohtude ennetamiseks. SolarWindsi tarneahela rünnak 2020. aastal näitab vajadust analüüsida keerukaid ja pikaajalisi ohte, millele ohuanalüütik peab tähelepanu pöörama [63].
- Küberturvalisuse arhitekt kavandab ja rakendab kogu organisatsiooni hõlmavaid turvalahendusi ja kaitsesüsteeme, tagades, et organisatsiooni IT-infrastruktuur on vastupidav küberrünnakutele. Näitena võib tuua DDoS-rünnakud Eesti vastu 2007. aastal, mille järel rõhutati tugeva turvaarhitektuuri vajadust [16].
- Küberturbe audiitor - viib läbi sõltumatuid turvaauditeid ja kontrollib turvameetmete tõhusust ning standarditele vastavust. Näiteks Targeti 2013. aasta andmeleke, mille käigus kaotati miljoneid krediitkaardiandmeid, tõstab esile vajaduse regulaarsete ja põhjalike turvaauditite järele [2].
- Küberturvalisuse koolitaja ülesanne on suurendada organisatsiooni töötajate teadlikkust küberturvalisusest läbi koolituste ja simulatsioonide. Näitena võib tuua Google'i 2017. aasta õngitsusrünnaku, mis rõhutas vajadust tõhusate turvateadlikkuse programmide järele töötajatele [42], [76].

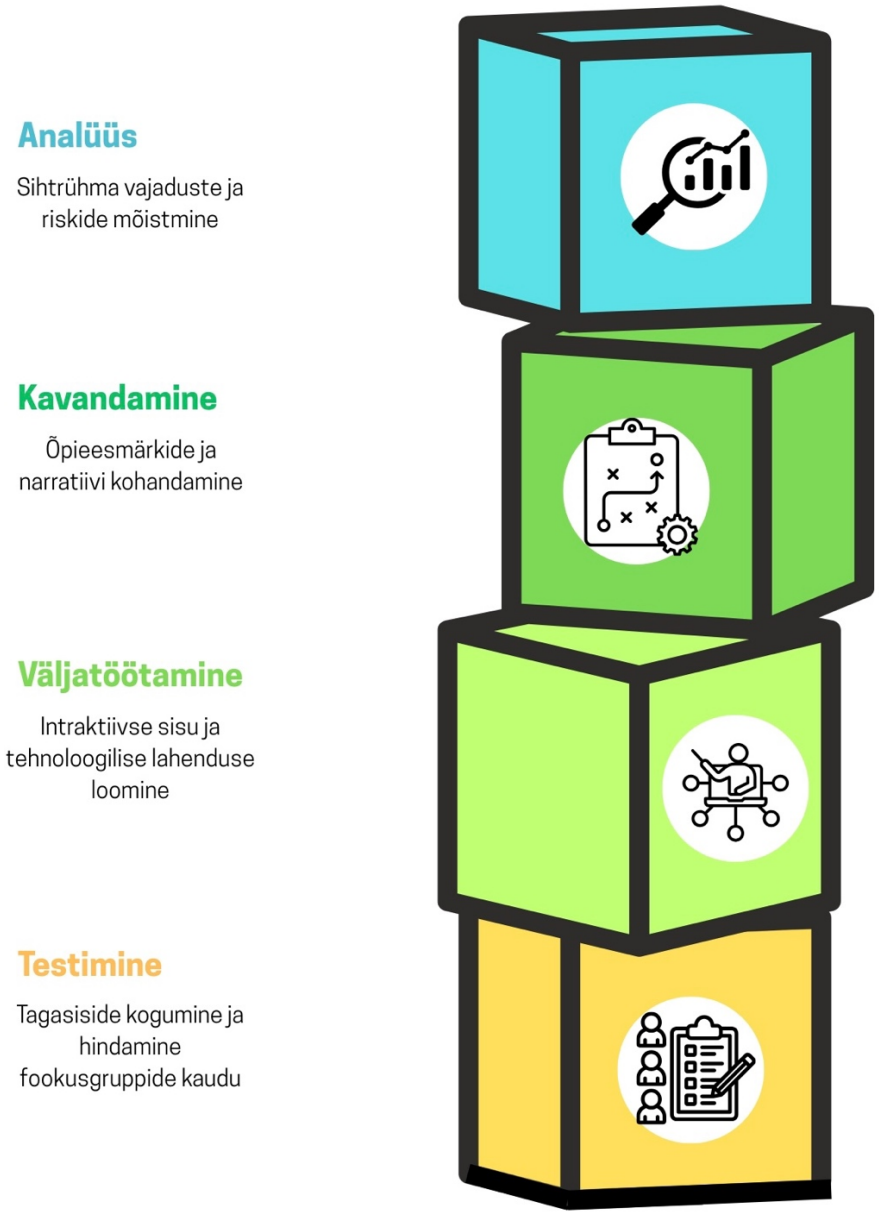
- Küberturvalisuse rakendaja vastutab tehniliste turvalahenduste igapäevase haldamise ja juurutamise eest, sealhulgas tulemüüride, viirusetõrje ja ligipääsukontrolli süsteemide haldamine. Colonial Pipeline'i 2021. aasta lunavararünnak näitab, kui kriitilised on pidevalt ajakohased ja õigesti konfigureeritud turvasüsteemid [100].
- Küberturvalisuse uurija ülesanne on analüüsida ja tuvastada keeruliste intsidentide põhjused, kasutades erinevaid uurimismeetodeid ja -vahendeid. Näiteks NotPetya rünnak 2017. aastal, mis põhjustas globaalset majanduskahju, nõudis sügavat tehnilist uurimist ja analüüsi [4], [35].
- Küberturbe riskijuht hindab küberriske ning töötab välja riskihaldusstrateegiaid, et vähendada potentsiaalsete intsidentide mõju. Näitena võib tuua Maerski 2017. aasta rünnaku, mis näitas vajadust tõhusate riskijuhtimisplaanide järele [4].
- Digitaalsete tõendite uurija - see spetsialist kogub, analüüsib ja säilitab digitaalset tõendusmaterjali, mida kasutatakse küberkuritegude uurimisel ja kohtuprotsessides. Silk Roadi juhtum 2013. aastal on näide, kus digitaalsete tõendite uurimine mängis olulist rolli veebikuritegevuse peatamisel [67].
- Nõrkustestija ehk eetiline häkker tuvastab süsteemide nõrkused ja aitab organisatsioonil neid parandada. Näiteks 2021. aastal tuvastasid eetilised häkkerid Microsoft Exchange Serveri nullpäeva nõrkuse, mille parandamine takistas suuremat kahju [68].

Seega näeme, et on võimalik siduda ära küberturvalisuse valdkonna juhtumid ja ametid ja lõputöö tulemusena saab luua interaktiivse mängustatud õpikeskkonna, mis tutvustab küberturvalisuse eri ameteid ning nendes ametites reaalselt esinevaid tüüpolukordi. Selline lähenemine aitab kasutajatel praktiliselt mõista erinevaid küberturvalisuse riske ning neid tuvastada ja ennetada. Ühtlasi soovime sellega murda levinud eksliku arvamuse, nagu eksisteeriks küberturvalisuse valdkonnas ainult üks amet. Keskendutakse kasutusmugavuse ja kaasahaaravuse parandamisele, pakkudes sihtrühmale praktilist ja visuaalset ülevaadet küberturvalisuse alustest ja ennetusmeetmetest.

3 Metoodika

Lõputöö elluviimiseks püstitatakse uurimusküsimus, mille järgi selgitatakse välja, kuidas mängustatud õpikeskkond mõjutab kasutajate teadlikkust ja praktilisi oskusi küberturvalisuse valdkonnas; analüüsitakse, millised on Eestis kõige levinumad küberturvariskid ja tüüpilised intsidentstsenaariumid erinevates ametites; kaardistatakse disainipõhimõtted, mille rakendamine aitab tagada keskkonna maksimaalse kasutusmugavuse, kaasahaaravuse ning visuaalse ja interaktiivse õpikogemuse; hinnatakse sihtrühma (õpilased, tudengid, täiskasvanud) eelteadlikkust ja hoiakuid küberturvalisuse riskide ja erialade osas; ning lõpuks võrreldakse platvormi testimise käigus kogutud kvalitatiivsete ja kvantitatiivsete andmete abil mängustuspõhise ja traditsiooniliste õppelahenduste lisandväärtust küberturvalisuse õpetamisel.

Töö metoodika on saanud inspiratsiooni ADDIE mudelist, mis koosneb analüüsi, kavandamise, väljatöötamise ja hindamise etappidest [5]. Uuringu andmed kogutakse kvalitatiivsete intervjuude kaudu, mis viiakse läbi erinevate sihtrühmade esindajatega. Intervjuude käigus saadavad andmed pseudonüümitakse, et kaitsta vastajate privaatsust ja konfidentsiaalsust. Saadud andmeid kasutatakse platvormi disaini ja sisu arendamiseks, keskendudes kasutajate tegelikele vajadustele ja kogemustele.



Joonis 2. Küberturvalisuse õppeplatvormi arendus

3.1 Analüüs

Analüüsi (Analyse) etapi eesmärk on mõista, milliseid küberturvalisuse riske enamasti tavakasutajad sageli eiravad või alahindavad, millised riskid pakuvad peavalu küberturvalisuse spetsialistidele, millega on vaja nende töödes algtasemel tegeleda. Selleks uuritakse esmalt Eesti konteksti, kasutades RIA aastaraamatuid [85], [88]–[91] ning „Cybersecurity Skills Needs Analysis report Estonia“ raportit [17], et tuvastada siin kõige levinumad ohud nagu lunavara, õngitsemine ja andmelekked. Seejärel võrreldakse Eesti olukorda rahvusvaheliste standarditega, nagu OWASP Top 10 [72], NIST

Cybersecurity Framework [101] ja ENISA raportid [26][30][32], hindamaks globaalsete trendide vastavust Eesti oludele. Lisaks analüüsitakse olemasolevaid turvaõppeplatvorme nagu OWASP WebGoat [73], OWASP Juice Shop [71], DVWA [21], RangeForce [79], Cybexer [18], Kübertest [58], tuues välja nende tugevused ja nõrkused. Analüüsid leitavad peatükist 2.3.

3.1.1 Kavandamine

Kavandamise (Design) faasis määratletakse projekti peamised õpieesmärgid. Üldine eesmärk on suurendada kasutajate teadlikkust küberturvalisusest, pakkudes praktilisi oskusi tüüpiliste ohtudega (nt lunavara, õngitsemine, DDoS) toimetulemiseks. Samuti kavandati mängustatud narratiiv, kus õppija astub erinevatesse rollidesse (nt analüütik või turvatestija), lahendades missioonipõhiseid ülesandeid, mis simuleerivad realistlikke küberrünnakuid ja turvaintsidente [93].

Kasutatakse narratiivipõhist disaini, mis pakub õppijatele kaasahaaravat ja tähenduslikku õppimiskogemust. Samuti kavandatakse reaalajas antav tagasiside, mis aitab kasutajal vigu analüüsida ja neist õppida, toetades sügavat õppimist ja vooseisundisse (flow) jõudmist [61]. Sellekohased tulemused on leitavad peatükist 2.4.2 ja 4.2.5.

3.1.2 Väljatöötamine

Väljatöötamise (Development ja Implement) faasis luuakse õppesisu, sh interaktiivsed stsenaariumid, mis toetavad praktilist õppimist. Õppesisu loomisel lähtutakse vajadusest pakkuda mittetehnilistele kasutajatele lihtsasti mõistetavaid ja visuaalselt toetatud materjale (skeemid, diagrammid, juhised) ja tutvustada erinevaid ameteid lihtsal kirjeldaval viisil.

Tehnoloogilise lahenduse valikul otsustati Reacti kasuks, kuna see raamistik toetab modulaarset ja paindlikku komponentide loomist, tagab hea jõudluse ning võimaldab lihtsat skaleeritavust ja integreeritavust teiste tehnoloogiatega nagu Redux ja Next.js [40], [80], [82]. Koodi haldamiseks kasutati versioonihaldust (GitHub), rakendades CI/CD põhimõtteid, mis tagavad koodi kvaliteedi ja sujuva uuendamise [97]. Mängustamise aspektide väljatöötamisel lähtuti behavioral game theory [33] põhimõtetest, arvestades kasutajate käitumismustreid ning pakkudes realistlikke ja emotsionaalselt kaasahaaravaid ülesandeid [43], [64]. Tulemuse on leitavad peatükis 4.

3.1.3 Testimine

Testimisfaasis (Evaluation) kasutati fookusgruppe, kuhu kuulusid sihtrühma esindajad – õpilased, tudengid, õpetajad ja IT-spetsialistid. Fookustestide ning hindamise käigus kogutakse kvalitatiivset ja kvantitatiivset tagasisidet kasutajaliidese, ülesannete raskuse, õppematerjalide arusaadavuse ja üldise õppekogemuse kohta [55].

Analüüsitakse kasutajate käitumist platvormil – tüüpilised vead, õppimiskõver ning tagasiside mõju õpiväljunditele. Saadud tagasiside alusel tehakse täiendusi nii sisulises pooles kui kasutajaliideses, et tagada optimaalne õppimiskogemus.

Osalejate värbamiseks ja valimi moodustamiseks rakendatakse lumepalli (snowball sampling)-meetodit [3]. Esmase osalejate kogu moodustasid Tallinna Tehnikaülikooli tudengid, kellel paluti soovitada tuttavaid, kes vastaksid sihtrühma kriteeriumitele (tudengid, IT-huvilised, arendajad, täiskasvanud). Kõik osalejad allkirjastasid kirjaliku nõusoleku, et uuringus osaleda (VT LISA 2). Osalejatele kinnitati, et intervjuuandmeid töödeldakse pseudonüümitult [49][99].

Iga osalejaga viidi läbi ligikaudu 1-tunnine individuaalne seanss ajavahemikus 1.–30. aprill 2025. Kokku osales 12 inimest (5 TalTech tudengit, 3 täiskasvanut, 4 IT-huvilist), Kõigile tutvustati uurimise eesmärki ning nad allkirjastasid teadliku nõusoleku [99]. Uurijad (autorid) selgitasid ka vaatluse ja intervjueerimise etiketti: seansse ei filmitud ega salvestatud helina, uurija sekkus vaid tehnilise tõrke korral, vältimaks õppijakogemuse mõjutamist. Iga seanss järgis neljaastmelist protsessi: (1) lühike suuline sissejuhatus ja navigeerimisjuhised, (2) platvormi iseseisev läbimängimine, (3) 10- või 5-palliline Likert-skaalaga küsimustik kasutajakogemuse ja teadmiste muutuse mõõtmiseks (VT LISA 3) [53], (4) 5–10-minutiline avatud intervjuu plusside, miinuste ja parendusideede kaardistamiseks.

Vaatlusmärkmeid ja küsimustiku tulemusi analüüsiti, et ühendada kvantitatiivsed ning kvalitatiivsed leiud rakendades kombineeritud meetodite põhimõtteid [52]. Analüüs on leitav peatükist 5.1.

3.1.4 Eetilised kaalutlused ja piirangud

Käesolevas lõputöös arendatud küberturvalisuse õppelahenduse loomisel lähtuti eetilistest põhimõtetest ning teadvustati mitmeid piiranguid, mis võivad mõjutada nii uuringu tulemusi kui ka platvormi praktilist rakendatavust.

Eetilised kaalutlused

Üheks keskseks eetiliseks printsiibiks oli eetilise häkkimise (ethical hacking) raamistikke [14][96] – õppematerjalid käsitlevad ründevektoreid ja turvaprobleeme üksnes teadlikkuse tõstmise ja kaitsemeetmete õppimise eesmärgil. Platvorm ei toeta pahatahtliku tegevuse õppimist ega soodusta eetikanormide rikkumist.

Uuringu läbiviimisel järgiti andmekaitse- ja teadusuuringute eetikastandardeid [49][99]. Osalejatelt koguti ainult minimaalne hulk isikuandmeid ning kõik andmed pseudonüümiti, vältimaks otsest isikutuvastust [38]. Kõik uuringus osalejad allkirjastasid teadliku nõusoleku vormi, milles selgitati andmete kasutusviise, konfidentsiaalsuse tagamist ja osalemise vabatahtlikkust. Intervjuusid ei salvestatud audiovisuaalselt, vältimaks õppijakogemuse moonutamist ning säilitamaks nende privaatsust.

Lisaks pöörati tähelepanu kultuuriliste ja psühholoogiliste aspektide arvestamisele – stsenaariumid ei sisalda vägivalla, diskrimineerimise ega muude tundlike teemade kujutamist viisil, mis võiks kasutajatele ebamugavust valmistada.

Piirangud

Uuringu ja arenduse käigus ilmnesid järgmised piirangud:

- Tehnilised piirangud – platvormi loomiseks valitud tehnoloogiline stack (React, GitHub [41], CI/CD töövood [62]) võimaldas küll kiiret arendust ja head kasutusmugavust, kuid piiras realistlike küberrünnakute simuleerimise võimalusi, eriti serveripoolsete interaktsioonide osas. Seetõttu tuli loobuda mõningatest tehniliselt keerukamatest stsenaariumidest, mis nõuaksid eraldi virtualiseerimiskeskkonda või sandboxe [77], [40], [97].
- Valimi piiratus ja valikumeetod – kasutatud snowball sampling meetod ei taga sihtrühma täielikku esinduslikkust. Osalejad olid valdavalt kõrgelt motiveeritud

tudengid või IT-huvilised, mis võib kallutada tulemusi, kuna nende baasvalmidus ja huvi võivad erineda laiemast elanikkonnast [3], [29].

- Motivatsioonist sõltuv tulemuslikkus – ehkki mängustamine võib suurendada õppijate kaasatust ja huvi, ei ole see universaalne lahendus. Platvormi tõhusus sõltub eelkõige kasutaja sisemisest motivatsioonist, tehnoloogilisest kirjaoskusest ning ajalisest ressursist, mida kasutaja platvormil õppimisele pühendab [23], [43], [64], [93].
- Õppeulatus ja sügavus – kuigi eesmärk oli teha küberturbeõpe kättesaadavaks ka mittetehnilistele kasutajatele, võib vajadus lihtsustada mõisteid vähendada mõningate teemade käsitluse sügavust. Samuti ei võimalda lühikesed sessioonid (nt 30–60 minutit) kõiki turvalisuse aspekte detailideni katta.
- Tulemuste üldistatavus – kuna tegemist on prototüübi testimisele keskenduva uuringuga, ei saa selle tulemusi automaatselt laiendada kõikidele sihtrühmadele ega teha järeldusi pikaajalise õppemõju kohta.

4 Lahendus

Interaktiivse õppelahenduse loomisel peeti oluliseks, et tehniline lahendus toetaks sisulist eesmärki – aidata kasutajatel mõista küberturvalisuse teemasid läbi praktiliste ja mänguliste tegevuste. Valitud tehnoloogiad, selge rakenduse struktuur ja läbimõeldud mänguloogika võimaldavad õppijal liikuda loogilises järjestuses, omandada uusi teadmisi ning katsetada neid erinevates olukordades. Mängude sisu on seotud konkreetsete ametite ja realistlike turvariskide olukordadega, pakkudes võimalust õppida läbi otsuste tegemise. Arenduse käigus tehtud valikud lähtusid sellest, et loodav lahendus oleks kasutajasõbralik, arendatav ja sisuliselt tähenduslik [18], [23], [80].

4.1 Tehnoloogia valik

Veebipõhise õppeplatvormi arendamisel on tehnoloogiline valik üks kriitilisemaid etappe, kuna see mõjutab rakenduse funktsionaalsust, skaleeritavust ja kasutajakogemust [97]. Eesrakenduse ehk kasutajaliidese arendamiseks kaaluti kolme populaarset raamistikku: React, Angular ja Vue.js [9], [80], [104]. Valiku tegemisel võeti arvesse raamistikute arhitektuurilisi omadusi, kogukonna tuge, tüübitoetust, olemasolevate teekide ökosüsteemi ja üldist õppimiskõverat [48], [57], [106].

Võrdluses hinnati, kuidas iga raamistik sobitub rakenduse vajadustega, pidades silmas komponendipõhist ülesehitust, tüübitoetust, arendajaõbralikkust, tehnoloogilise kogukonna suurust ja raamistikuga kaasnevaid õppimisvajadusi [22], [34], [103], [104].

- React on Facebooki loodud kasutajaliidese loomise teek, mille arhitektuur põhineb komponentidel ja keskendub kasutajaliidese loogika tõhusale haldamisele [81]. Reacti tugevuseks on Virtual DOM-i tehnoloogia, mis võimaldab kiiret ja sujuvat kasutajaliidese uuendamist [81]. React sobib nii väikeste projektide kui ka keerukate süsteemide jaoks tänu oma järkjärgulisele ülesehitusele. Selle modulaarne struktuur võimaldab taaskasutada komponente ja kiirendada arendust [22]. Reacti toetab lai ökosüsteem, pakkudes mitmekülgseid lisateeke nagu React Router ja Redux, mis laiendavad arendusvõimalusi [40].

Kuigi React ei nõua TypeScripti kasutamist, on selle tugi hõlpsasti integreeritav, mis aitab parandada rakenduse töökindlust ja hooldatavust [82]. Stack Overflow 2024. aasta arendajauuringu kohaselt on React üks enimkasutatud raamistikke professionaalsete arendajate seas [22].

- Angular on Google'i loodud raamistik, mis põhineb TypeScriptil ja pakub terviklikku arendusplatvormi [93], [106]. Angular sisaldab mitmesuguseid sisseehitatud funktsionaalsusi, nagu teenused, moodulid ja CLI tööriistad, mis võimaldavad arendada hästi struktureeritud ja suuremahulisi rakendusi [57], [103]. Näiteks Angulari CLI tööriistad ja moodulite süsteem aitavad arendajatel hallata suuremahulisi projekte järjepidevalt [7], [8].
- Moodulipõhine arhitektuur toetab head koodi organiseeritust, suurendades projekti laiendatavust ja hooldatavust [57]. TypeScripti vaikimisi integratsioon parandab koodi loetavust ja stabiilsust, võimaldades arendajatel varakult tuvastada võimalikke vigu [10].
- Samas võib Angular olla keerukam esmakasutajatele, kuna raamistik nõuab ranget projektistruktuuri ja põhjalikumat konfigureerimist [57]. Selle tulemusena on Angulariil järsem õppimiskõver võrreldes teiste raamistikudega, näiteks Reactiga [22].
- Vue.js on progressiivne raamistik, mida saab kasutada nii lihtsate veebilehtede täiustamiseks kui ka keerukate rakenduste loomiseks [48], [104]. Selle modulariseeritud arhitektuur võimaldab järk-järgulist kasutuselevõttu, mis muudab Vue sobivaks nii algajatele kui ka edasijõudnutele [48]. Vue.js-i süntaks on intuitiivne ning selle komponentide arhitektuur võimaldab kergesti hallata HTML-malle, JavaScripti loogikat ja CSS-stiile ühe komponendi sees [15], [57].
- Vue.js-i reaktiivne andmemudel ja "*two-way data binding*" funktsioonid on selle tuumikomadused, mis toetavad kasutajaliidese ja andmete vahelist sujuvat sünkroniseerimist [15], [47]. TypeScripti tugi on raamistikus olemas, kuid selle täielik integreerimine nõuab täiendavaid seadistusi ja tüüplikku konfiguratsiooni [57], [102].
- Kuigi Vue.js-i populaarsus kasvab kiiresti, olles Stack Overflow 2024. aasta küsitluse andmetel üks enimkasutatavaid JavaScripti raamistikupõhiseid tööriistu, on selle kogukond ja ametlik dokumentatsioon mõnevõrra kitsam võrreldes Reacti ja Angulariga, eriti keerukate süsteemide arendamisel [22], [57].

Alljärgnevas tabelis (Tabel 3) on välja toodud võrdlus eesrakenduse tehnoloogiate vahel, tuginedes standardsetele hindamiskriteeriumidele: komponendipõhisus, tüübitoetus, kogukonna tugi, õppimiskõver ja tootlikkus [22], [47], [57], [72], [80], [81], [93], [104].

Tabel 3. Eesrakenduse tehnoloogiate võrdlus

Kriteerium	**React**	**Angular**	**Vue.js**
Komponendi põhine struktuur	Paindlik, modulaarne	Rangelt modulaarne	Intuitiivne ja lihtne
TypeScripti integratsioon	Hea, aga TypeScript vajab eraldi seadistust	Väga hea, vaikimisi integreeritud	Hea, aga nõuab seadistust
Kogukonna suurus ja tugi	Väga suur, aktiivne	Väga suur, aktiivne	Keskmine, kasvav
Õppimiskõvera keerukus	Keskmine, lihtne alustada	Kõrge, keeruline alustada	Madal, kiirelt õpitav
Arenduskiirus ja tootlikkus	Kõrge, suur ökosüsteem	Keskmine, nõuab rohkem seadistamist	Kõrge, kiire prototüüpimine

Arvestades ülaltoodud kriteeriume ning eesmärki arendada paindlik ja kasutajakeskne platvorm, osutus React kõige sobivamaks raamistikuks. Selle tugev komponendimudel, aktiivne kogukond ja suur ökosüsteem toetavad kiiret arendusprotsessi ning võimaldavad luua skaleeritavat rakendust [22], [57], [81], [82].

Angular ja Vue.js jäid valikust välja peamiselt oma rakendusloogikate keerukuse (Angulari puhul) [57], [103] ja väiksema leviku (Vue.js-i puhul) [22] tõttu, mis oleksid suurendanud õppimise ja juurutamise ajakulu.

Kokkuvõttes on Reacti valik õigustatud nii tehnilise sobivuse, kogukonna toe kui ka meeskonna oskuste baasil, võimaldades keskenduda rakenduse funktsionaalsusele ilma liigse raamistikuga kohanemiseta [22], [57].

4.2 Mängude ja disainide loomine

Mängude loomise alustalaks oli põhjalik eeltöö, mille käigus uurisime erinevaid olemasolevaid interaktiivseid mänge ning vaatasime, kuidas need on suutnud hoida kasutajate huvi ja pakkuda uusi teadmisi [43], [64], [93]. Kuna meie põhi sihtrühmaks oli gümnaasiumi tasemel õppurid, soovisime selgelt aru saada, milline mängudisain, ülesehitus ja raskusaste oleks neile kõige sobivam nii põnevuse kui ka õppimise aspektist [61]. Selle tulemusena panime rõhku lihtsusele, loogilisele süsteemsusele ja kasutajamugavusele, et tagada mängude kaasatus algusest lõpuni [74].

Põhjalik eeltöö, kasutajate vajadustest lähtuv mängude küsimuste kujundamine ning prototüüpide pidev arendamine andsid tugeva aluse meie õppeplatvormi visuaalsele ja funktsionaalsele ülesehitusele [70]. Samal ajal rõhutasime disaini osas kasutajakogemuse ja selge navigeerimise tähtsust, tagades, et nii mängumoodulid kui ka disainielemendid toetaksid hariduslikke eesmärke ning loovad intuitiivse ja kaasahaarava keskkonna [55], [64]. Selline iteratiivne ja süsteemne lähenemine võimaldas meil leida optimaalse tasakaalu haridusliku sisu ja kasutajasõbraliku, visuaalselt meeldiva kujunduse vahel, mis on oluline dünaamilise ja õppimist soodustava platvormi loomisel [64], [93].

4.2.1 Funktsionaalsed nõuded

Funktsionaalsed nõuded määravad vajalikke funktsioone, mida platvorm peab tegema. Alljärgnevalt on kirjeldatud küberturvalisuse platvormi peamised funktsionaalsed nõuded:

1. Avalehe ametite kuvamine – kasutajale peab olema nähtav kõigi küberametite loetelu; kaardi või lingi klõps viib vastava ameti lehele [18], [73];
2. Ameti lehe tutvustus – iga ameti leht peab kuvama sissejuhatava teksti ja nupu „Alusta mänguseeriat", mis suunab õppematerjali slaidile [18], [70];
3. Õppematerjali slaidid – enne iga mängu peab kasutajale avanema temaatiline slaid vajalike taustateadmistega; alles seejärel saab mängu alustada [18], [93];
4. Neljaosaline mänguseeria – iga amet sisaldab neli järjestikust minimängu, mis valideerivad vastuseid ja annavad kohest tagasisidet (õige/vale, vihjed) [43], [64];
5. Seeria lõpetamine – pärast neljandat mängu peab ilmuma lõpp-ekraan nupuga „Tagasi avalehele", mis suunab kasutaja esilehele [40], [82];

6. Brauserinavigatsioon – lehtede vahetus peab toimima ka brauseri Back/Forward nuppudega, säilitades vaate ja oleku [80], [82].

4.2.2 Mittefunktsionaalsed nõuded

Mittefunktsionaalsed nõuded aitavad autoritel defineerida süsteemi omadused, mis mõjutavad rakenduse jõudlust ja kasutajamugavust. Alljärgnevalt on kirjeldatud küberturvalisuse platvormi peamised mittefunktsionaalsed nõuded:

7. Kasutusmugavus – rakendus peab olema lihtsa ja intuitiivse ülesehitusega. Navigeerimine peab olema loogiline ning visuaalselt ühtse kujundusega, et vältida segadust ja tagada meeldiv kasutajakogemus [57], [70], [104];
8. Jõudlus ja sujuvus – rakendus peab reageerima kasutaja tegevustele kiiresti ja töötlema andmeid reaalajas, tagades katkematu töövoo ka siis, kui samaaegselt on aktiivsed mitmed mängijad [40], [80];
9. Skaleeritavus – rakendus peab olema võimeline toetama kasutajate ning sisumahu kasvu, sh olukordi, kus korraga mängib suur hulk õppureid, ilma et tekiks jõudlusprobleeme [22], [97];
10. Hooldatavus – koodibaas ja struktuur peavad olema selged ning modulaarsed, et lihtsustada vigade parandamist ja uute funktsioonide lisamist tulevikus [82], [97].

4.2.3 Kasutuslood

Kasutuslood (ingl use cases) mängivad olulist rolli interaktiivsete süsteemide prototüüpimisel, sest need aitavad modelleerida realistlikke olukordi, kus kasutaja süsteemiga suhestub. Kasutuslugude kaudu on võimalik täpsustada funktsionaalsed nõuded, kaardistada kasutaja eesmärgid ning tuua esile võimalikud probleemikohad või takistused, millega kasutajad võivad prototüübi kasutamisel kokku puutuda (Cockburn, 2000).

Prototüüpimisel ei piisa ainult tehnilistest kirjeldustest – vaja on mõista, kuidas ja miks kasutaja süsteemi kasutab ning millistes kontekstides need tegevused aset leiavad. Kasutuslood võimaldavadki siduda kasutaja vaatenurga arendaja vaatega, pakkudes struktureeritud viisi, kuidas kirjeldada interaktsioone süsteemiga samm-sammult.

Eriti õppekeskkondade puhul, kus rõhk on kasutajakogemusel, õppimise sujuvusel ja tähenduslikkusel, aitavad kasutuslood tagada, et arendatav lahendus toetab tegelikke

õppija vajadusi ja eesmärke. Need võimaldavad hinnata, kuidas konkreetne funktsionaalsus – näiteks turvaintsidendi simuleerimine või tagasiside kuvamine – toetab õppimise eesmärke ning millist kasu või raskust see kasutajale tekitab (Preece, Rogers & Sharp, 2015).

Lisaks on kasutuslood kasulikud ka kommunikatsioonivahendina erinevate meeskonnaliikmete vahel, sest need aitavad disaineritel, arendajatel ja pedagoogilistel ekspertidel ühiselt mõista, millist kogemust platvorm peaks pakkuma ning kuidas seda kogemust testida ja täiustada.

Cockburn, A. (2000). Writing Effective Use Cases Addison. Addison-Wesley Professional.
Preece, J., Rogers, Y., Sharp, H., Benyon, D., Holland, S., & Carey, T. (1994). Human-computer interaction. Addison-Wesley Longman Ltd..

Antud platvormil on kolm tüüpkasutajat - õpilane gümnaasiumis, tudeng ja karjääripööraja.

Joonis 3. Karjääripööraja

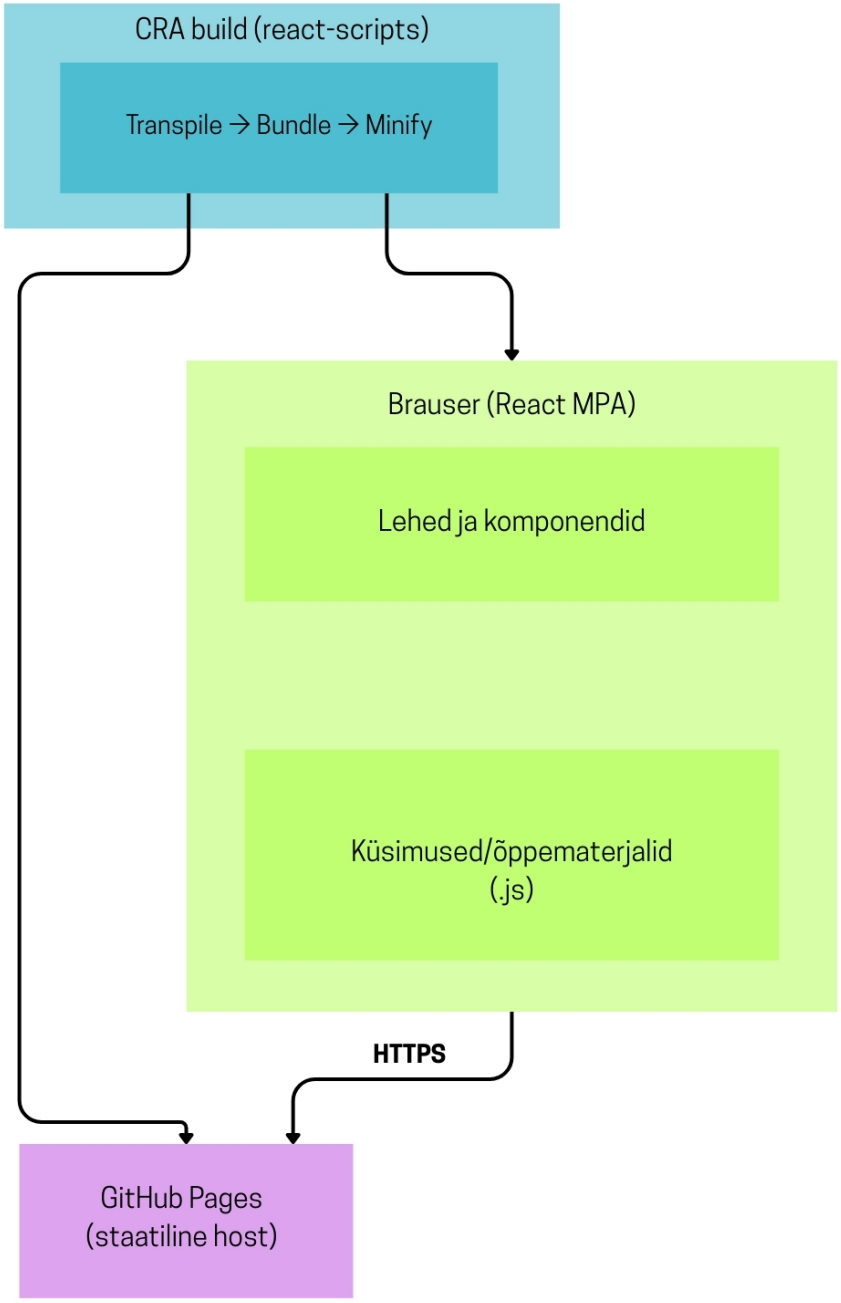
Joonis 4. Tudeng

Joonis 5. Gümnaasiumiõpilane

Sellest tulenevalt on oluline, et kasutuslugude koostamisel arvestatakse iga tüüpkasutaja tausta, ootuste ja tehniliste oskustega, et arendatav platvorm oleks tõesti kasutajakeskne ja sihtrühmale sobiv.

4.2.4 Disaini loomine

Õppeplatvormi disaini loomisel oli ülimalt tähtis leida tööriist, mis võimaldas ideid kiiresti prototüüpida ja visuaalselt illustreerida. Sellest mõttes oli Canva osutunud hindamatuks abiliseks, kuna see pakkus paindlikke lahendusi ning intuitiivset keskkonda, kus saime oma mõtteid ja kavandeid visuaalselt esitada [70].



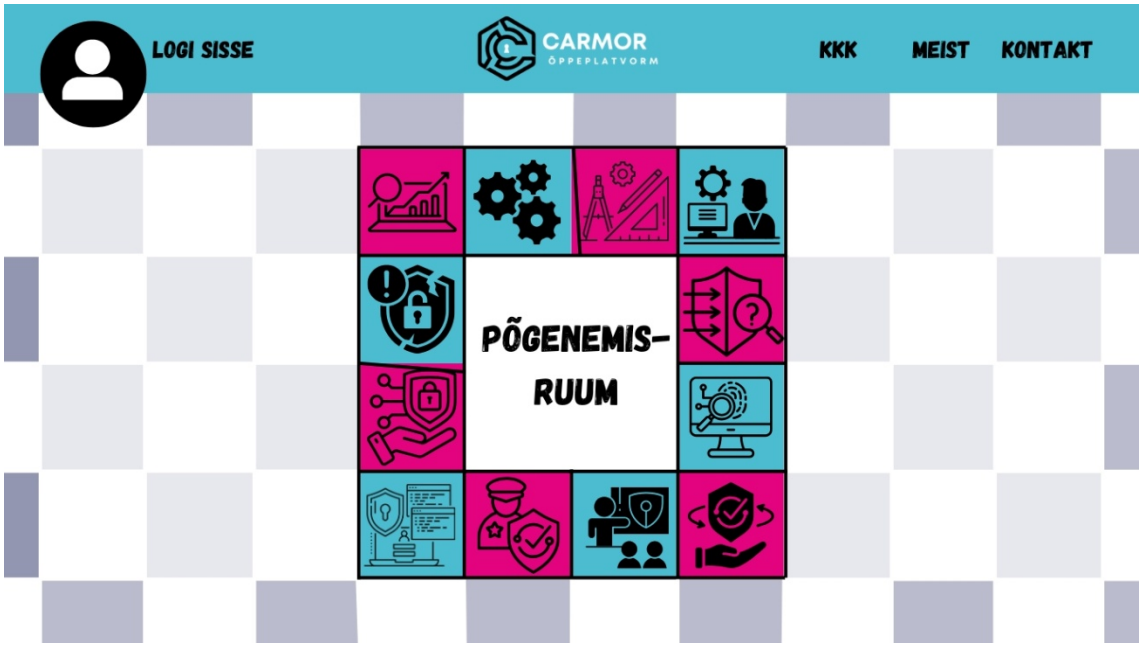
Joonis 6. Infosüsteemi arhitektuur

Algselt alustasime projekti platvormi struktuuri ja funktsionaalsuse kaardistamisega. Meie meeskond lõi esmalt põhikontseptsiooni, kus määratlesime kindlaks, millised elemendid ja infoväljad on kasutaja jaoks kõige esmatähtsamad. Canva abil saime kiiresti ja lihtsalt koostada prototüüpe, mis näitasid, kuidas erinevad komponendid – alalehed, mängud ja ameti rollid – omavahel suhestuvad. See esialgne visuaalne kaardistamine aitas

meil mitte ainult ideed struktureerida, vaid ka kindlaks teha kasutajakogemuse põhielemendid, mida hiljem disainis edasi arendada.

Jooksvalt tehtud parendused olid samuti oluline osa meie disainiprotsessist. Esialgsed kavandid said inspiratsiooni mitte ainult meeskonna ideedest, vaid ka esmase kasutajate tagasiside põhjal. Täheldasime, et teatud värvi kombinatsioonid ja kujunduslikud lahendused ei vastanud ootustele ning vajasid täiendust. Seetõttu tegime mitmeid iteratsioone, kohandades värvi temaatikat, elementide paigutust ja üldist visuaalset harmooniat. Iga muudatus aitas viia tulemuse lähemale soovitud kasutajasõbralikkusele ja visuaalsele selgusele.

Lisaks visuaalsele kujundusele pöörasime suurt tähelepanu ka navigeerimise loogilisusele ja funktsionaalsusele. Canva võimalused andsid meile vabaduse kujundada selged ja loetavad leheküljed, kus kasutajad saavad intuitiivselt aru, kuidas edasi liikuda: alates esilehelt kuni mängudele ja ameti rollide tutvustusteni. Meie eesmärk oli luua disain, kus kõik detailid – alates nuppudest ja ikoonidest kuni tekstide ja paigutusteni – toetaksid üht sujuvat kasutajakogemust.



Joonis 7. Canva algne disain

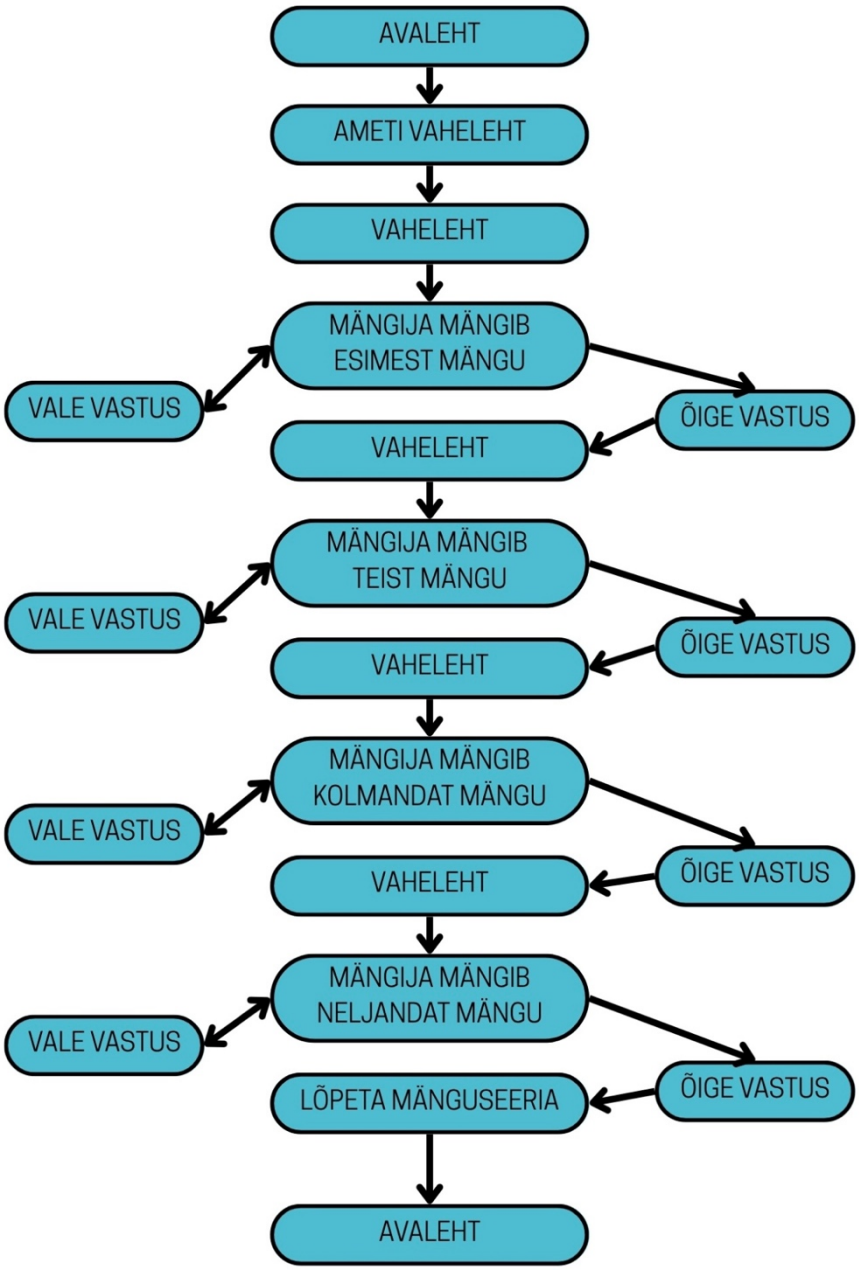
Kokkuvõttes võimaldas Canva tööriist meie jaoks keskenduda loovusele ning ideede kiirele elluviimisele ilma tehniliste piiranguteta. Tööriista paindlikkus integreerub hästi

olemasolevate tööprotsessidega, võimaldades meil prototüüpe kiiresti koostada ja vajadusel jooksvalt iteratsioone rakendada. Tänu sellele suutis meie meeskond välja

arendada visuaalselt meeldiva, intuitiivse ja funktsionaalse veebiplatvormi disaini, mis vastab nii kasutajate vajadustele kui ka projekti üldistele eesmärkidele [70].

4.2.5 Kasutaja teekond mängus

Kasutaja narratiiv (algeline mängu arhitektuur) annab ülevaate sellest, kuidas kasutaja läbi mängulise ja interaktiivse platvormi liikumise järjestatakse. See aitab mõista kasutaja teekonda alates esialgsest ameti valikust kuni mängude läbimise ja lõpuks avalehele naasmiseni. Antud narratiiv toimib nii disaini alusena kui ka tööriistana, mis võimaldab visualiseerida ja optimeerida kasutajakogemust, tagades, et iga samm oleks intuitiivne, loogiline ja kasutajasõbralik. See lähenemine aitab tuvastada võimalikke kitsaskohti ning loob tugeva aluse süsteemi järjepidevaks täiustamiseks vastavalt kasutajate vajadustele.



Joonis 8. Kasutaja liikumise skeem veebilehel

4.2.6 Mängude küsimuste loomine ja sisu kujundamine

Mängude küsimuste väljatöötamine kujunes keerukaks protsessiks, sest ühtepidi vajasime küberturvalisuse temaatikaga seotud usaldusväärseid teadmisi, teisalt aga püüdsime leida piisavalt haaravaid ja õpioskusi arendavaid vorme. Alustasime esialgu laiaulatuslike ideedega, visandades erinevaid võimalikud küsimustüüpe (nt valikvastused, lünkade täitmine, paaride ühendamine), ning seejärel hakkasime neid omavahel kombineerima.

Iga ameti jaoks, mida platvormil käsitleme, püüdsime luua tervikliku küsimuste komplekti, mis annaks sissevaate ameti spetsiifikasse ja looks kasutajale võimaluse omandada uusi teadmisi interaktiivselt. Lõplikud küsimused koondusidki neljast järjestikulisest alammängust koosnevaks komplektiks, kus iga samm lisaõppimist toetab ja järgmiseks tasemeks ette valmistab [64].

4.2.7 Disainiotsused ja kasutajasõbralikkus

Eesmärk oli luua mängud, mis näeksid esteetiliselt meeldivad välja ning mida oleks intuitiivne kasutada. Esimese hooga püüdsime luua ühtset läbivat kujundusjoont kõikidele mängudele, kuid üsna pea avastasime, et teatud ametite puhul võib olla vaja eraldi rõhutada nende valdkonna eripärasid.

Seega hakkasime disaini ja sisu kujundama iteratiivses vormis: iga paari nädala järel vaatasime uuesti üle nii visuaalsed elemendid kui ka mängude sisu, lisasime täiendavaid nüansse või lihtsustasime neid, mis tundusid üleliigselt keerulised. Kuna kasutajateks on gümnaasiumiõpilased, pidasime väga oluliseks leida sobiv tasakaal teoreetilise sisu mahu ja mängulisuse vahel.

4.2.8 Iteratiivne kavandamine ja prototüüpimine

Ülesehituse juures koostasime mitmeid kavandeid ja malle, katsetades erinevaid kasutajaliidese stiile ning küsimuste esitamise viise. Näiteks lisasime algselt igale ekraanile põhjalikud juhised, kuid testivate kasutajate arvamused viitasid, et liigne tekst võib segada mängu tempot. Seetõttu otsustasime anda võimalikult palju infot visuaalses ja interaktiivses vormis. Iga järgneva prototüübi puhul analüüsisime, kas küsimused on jõukohased, kas kasutajaliidese elemendid on loogiliselt paigutatud ning kuidas mängijad reaktsioonide põhjal edasi liiguvad. Vahel piisas pisematest kujundusmuudatustest (näiteks nuppude suuruse ja värvi korrigeerimine), teinekord aga tuli peaaegu kogu lehekülje ülesehitust ümber mõelda.

Kokkuvõttes kujunes mängude väljatöötamine püsivalt arenevaks protsessiks, kus esialgsed ideed muutusid vastavalt kasutajate tagasisidele, disaininõuetele ja üldistele õpieesmärkidele. Kuigi kontseptsioonid ameti kaupa olid meil algselt paika pandud, tuli detailide täpsustamiseks teha rohkelt vahekokkuvõtteid, prototüüpe ja testimisi. Lõpptulemusena valmisid terviklikud mängumoodulid, mis toetavad küberturvalisuse

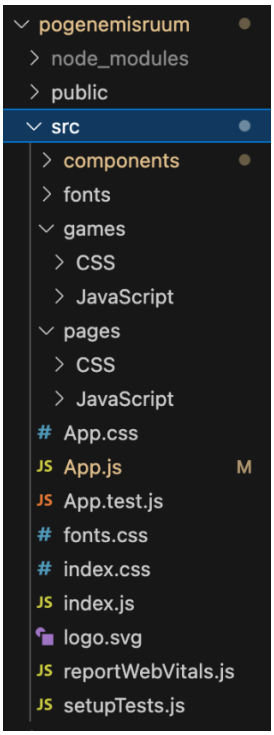
erinevate ametite tutvustamist ning pakuvad samal ajal õppimist soodustavat ja meelelahutuslikku kogemust.

4.3 Lahenduse arendus

Eesrakenduse arendamisel kasutati React raamistikku, mille modulaarne ülesehitus võimaldab luua hästi struktureeritud, laiendatava ja hooldatava rakenduse [57], [80]. Arenduse käigus pöörati tähelepanu eelkõige intuitiivsele kasutajakogemusele, loogilisele navigeerimisstruktuurile ja visuaalsele esteetikale [80], [82].

4.3.1 Eesrakenduse struktuur

Reacti src-kataloogi struktuur võimaldab luua selge ja organiseeritud failisüsteemi, kus iga komponent ja mänguloogika paiknevad eraldi kaustades, et lihtsustada edasist arendust ja modifikatsioone (Joonis 9).



Joonis 9. src-kataloogi struktuur

Failistruktuur jaguneb järgmistesse üksustesse:

components – Korduvkasutatavad kasutajaliidese komponendid, mida kasutatakse mitmetel erinevatel lehtedel.

fonts – Kasutajaliideses kasutatavad fondid ja nendega seotud stiilifailid.

games – Peamine kaust, mis sisaldab erinevaid mängu komponente ja nende spetsiifilist loogikat. Kaustas asuvad eraldi alamkaustad CSS ja JavaScript mänguspetsiifiliste stiilide ja skriptide jaoks, mis tagab selge eraldatuse ja parema ülevaate.

pages – Rakenduse lehtede spetsiifilised komponendid, mis määravad navigeerimisstruktuuri ja kasutajate vaated. Sarnaselt mängude kaustale sisaldab pages ka eraldi CSS ja JavaScript kaustu lehtedega seotud stiilide ja skriptide haldamiseks.

Lisaks on peamised konfiguratsiooni- ja stiilifailid rakenduse juurkataloogis:

App.js – Rakenduse peamine komponent, mis määratleb üldise paigutuse ja esmase marsruutimise loogika.

index.js – Rakenduse sisenemispunkt, kus rakendus ühendatakse DOM-iga.

index.css ja fonts.css – Globaalsed stiilifailid, mis sisaldavad rakenduse üldisi stiilireegleid.

App.css – Peamise rakenduse komponendi spetsiifilised stiilid.

Marsruutimine toimub Reacti konventsioonide järgi, kus komponentide vahel navigeerimine toimub selgelt määratletud marsruutidega, võimaldades lihtsat haldamist ja vähendades käsitsi seadistamise vajadust.

Selline struktuur tagab modulaarsuse ja paindlikkuse, võimaldades mugavalt lisada uusi mänge või funktsioone ilma olemasolevaid osi mõjutamata.

Üle 100 tunni jooksul on teostatud järgmised arendusetapid:

- Prototüübi kavandamine Canvas.
- 12 küberameti detailse ülesehituse ja sisu loomine (aluseks ECSF [32] ja reaalne tööprotsess).
- Iga ameti jaoks loodi 4 mängu (kokku 48 mängu), mille sisuks on erinevat tüüpi interaktiivsed harjutused (lohistamine, mitmikvalik, järjestamine jms). Mängudes olevad küsimused ja sisud on igal mängul erinevad, sest mängudele loodi juurde ka erinevad sisud, mis juhuslikkuse (random) alusel ilmuvad. See võimaldab saada ka korduval mängimisel saada erinev mängukogemus.
- Mänguloogika arendamine puhtalt front-endis Reactis, sh juhuslikkuse lisamine mängudele.
- Stiilide loomine CSS abil, järgides ühtset disainisüsteemi.
- Veateadete süsteem, õigete vastuste hindamine ja dünaamiline tagasiside kasutajale.

Mängud ei salvesta andmeid ega tulemusi, kuna prototüübis ei ole veel ühendust andmebaasi ega autentimissüsteemiga ning see vajaks mängijate teavitamist andmekaitselistest piirangutest. Töö edasine plaan hõlmab:

- **Backendi lisamine** (Node.js või Firebase) kasutajaandmete, mängu edenemise ja tulemuste salvestamiseks.
- **Logimissüsteemi rakendamine**, mis võimaldab testida mängude edenemist ja tõrkeid.
- **Kasutajarolli põhine personaliseerimine**, et muuta mängud raskusastme ja õppijaprofiili järgi.

Allpool on toodud üks näide mänguloogikast (Audiitor1.js):

```
import React, { useState } from 'react';
import { useNavigate } from 'react-router-dom';
import '../CSS/Audiitor1.css';

const allRisks = [
  { id: 1, name: "Andmeleke", isRelevant: true },
  { id: 2, name: "IT-süsteemi seisak", isRelevant: true },
  { id: 3, name: "Reputatsioonikahju", isRelevant: true },
  { id: 4, name: "Füüsiline rünnak", isRelevant: false },
  { id: 5, name: "Võrgu ülekoormus", isRelevant: false },
  { id: 6, name: "Kasutajate segadus", isRelevant: false }
];

function shuffleArray(array) {
  const newArr = [...array];
  for (let i = newArr.length - 1; i > 0; i--) {
    const j = Math.floor(Math.random() * (i + 1));
    [newArr[i], newArr[j]] = [newArr[j], newArr[i]];
  }
  return newArr;
}

function generateRiskOptions() {
  const correctRisks = allRisks.filter(r => r.isRelevant);
  const distractors = allRisks.filter(r => !r.isRelevant);
  const subsetSize = Math.floor(Math.random() * 2) + 4;
  const selected = [...correctRisks];
  shuffleArray(distractors);
  for (let i = 0; selected.length < subsetSize && i <
distractors.length; i++) {
    selected.push(distractors[i]);
  }
  return shuffleArray(selected);
}

export default function Audiitor1() {
  const navigate = useNavigate();
  const [riskOptions] = useState(generateRiskOptions());
  const [selectedRisks, setSelectedRisks] = useState([]);
  const [checked, setChecked] = useState(false);
  const [message, setMessage] = useState("");
  const [report, setReport] = useState("");
  const correctIds = allRisks.filter(r => r.isRelevant).map(r =>
r.id);
  const scenario = "Firma X kasutas viimati vana TLS-versiooni (TLS
1.0), mis suurendab andmeleketega seotud riski.";
```

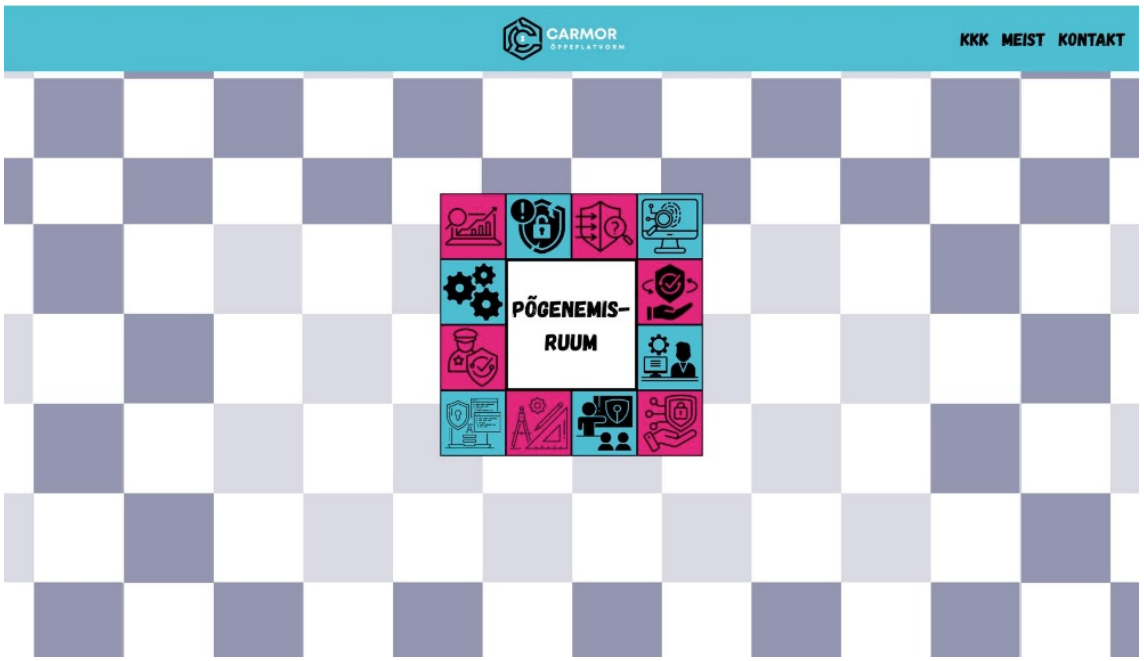
```
  const toggleRisk = id => {
    if (checked) return;
    setSelectedRisks(prev => prev.includes(id) ? prev.filter(x => x
!== id) : [...prev, id]);
  };

  const handleCheck = () => {
    const correctCount = selectedRisks.filter(id =>
correctIds.includes(id)).length;
    const wrongCount = selectedRisks.filter(id =>
!correctIds.includes(id)).length;
    if (correctCount === correctIds.length && wrongCount === 0) {
      setMessage("Tubli! Kõik riskid valitud õigesti.");
      setReport(`Audit kokkuvõte: ${scenario} Tuvastatud riskid:
${riskOptions.filter(r => correctIds.includes(r.id)).map(r =>
r.name).join(', ')}.`);
    } else {
      setMessage(`Õigeid valikuid: ${correctCount}, vigu:
${wrongCount}. Proovi uuesti.`);
    }
    setChecked(true);
  };

  const handleReset = () => {
    setSelectedRisks([]);
    setChecked(false);
    setMessage("");
    setReport("");
  };

  const containerClass = checked
    ? message.startsWith('Tubli') ? 'correct-bg' : 'incorrect-bg'
    : '';
  const messageClass = checked
    ? message.startsWith('Tubli') ? 'message-correct' : 'message-
incorrect'
    : '';

  return (
    <div className={`cyadvice-stage1 ${containerClass}`}>
      <h2>Riskianalüüs</h2>
      <p className="scenario"><em>{scenario}</em></p>
      <p>Vali riskid, mida organisatsioonis võib esineda (valida tuleb
{correctIds.length} riski):</p>
      <ul className="risk-list">
        {riskOptions.map(r => (
          <li key={r.id} className={selectedRisks.includes(r.id) ?
'selected' : ''} onClick={() => toggleRisk(r.id)}>
```

```
            <input type="checkbox"
checked={selectedRisks.includes(r.id)} readOnly /> {r.name}
          </li>
        ))}
      </ul>
      <div className="buttons">
        {!checked ? (
          <button className="primary" onClick={handleCheck}
disabled={selectedRisks.length === 0}>Kontrolli vastused</button>
        ) : (
          <button className="primary" onClick={handleReset}>Alusta
uuesti</button>
        )}
        {checked && message.startsWith('Tubli') && (
          <button onClick={() =>
navigate('/audiitor2')}>Edasi</button>
        )}
      </div>
      {message && <div className={`message
${messageClass}`}>{message}</div>}
      {report && <div className="report">{report}</div>}
    </div>
  );
}
```

Rakendust on võimalik näha ja kogeda siit: https://camaar2.github.io/pogenemisruum

4.3.2 Lahenduse näidised

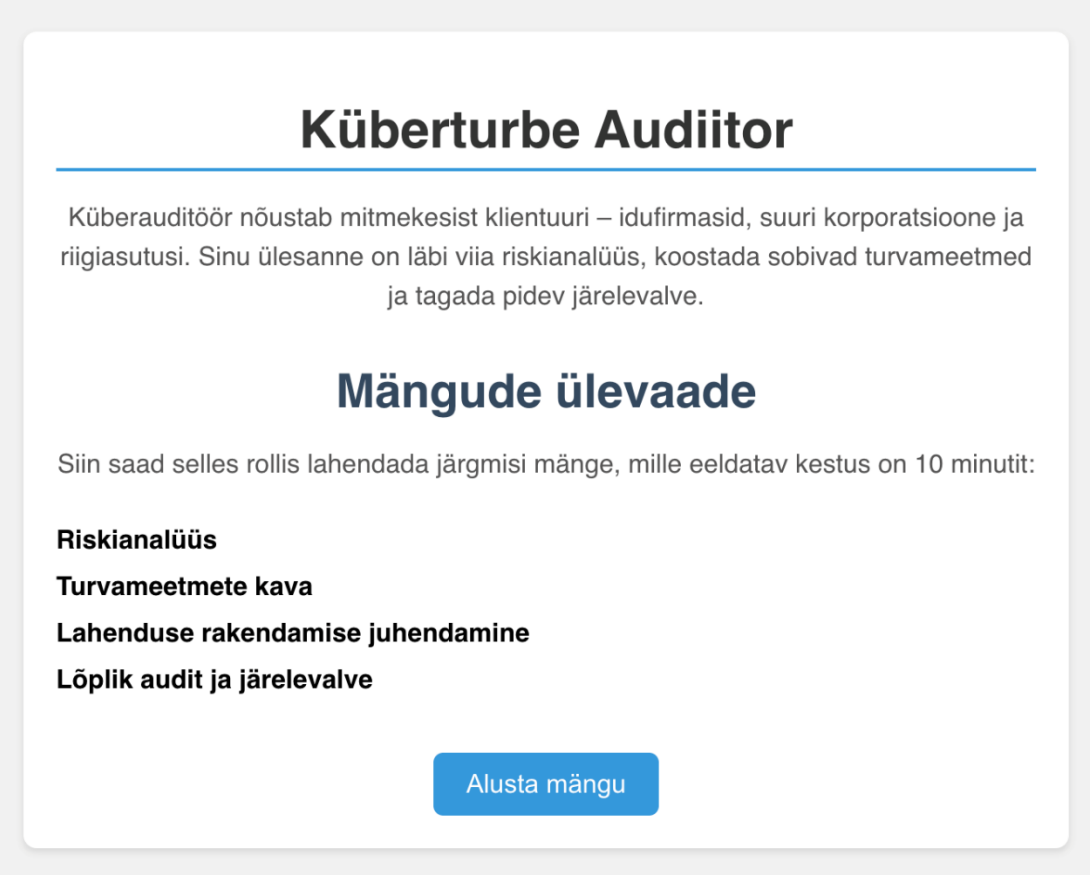
Kasutaja alustab oma teekonda veebiplatvormi avalehel, kus talle kuvatakse erinevate ametite nimetused. Ta klikib teda huvitavale ameti nimetusele, mis viib ta edasi vastava ameti lehele.



Joonis 10. Ameti valik avalehel

Ameti lehekülg ja sissejuhatus

Peale ameti nimetuse valimist avaneb spetsiaalne lehekülg, kus on esitatud sissejuhatav info selle ameti kohta. See tutvustus annab ülevaate ametiga seotud tööprotsessidest, nõuetest ja põhimõtetest, et kasutaja saaks esmalt konteksti, milles mängud toimuvad. Leheküljel on selgelt nähtav nupp "Alusta mänguseeriat".

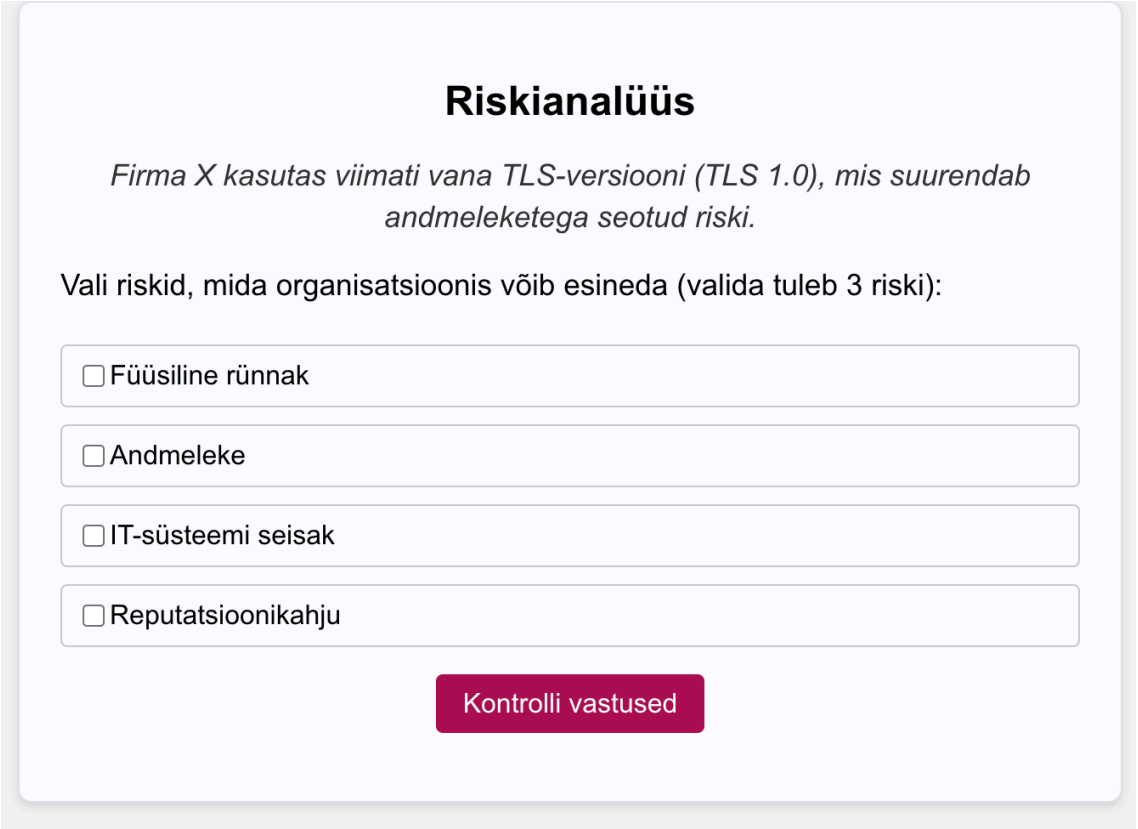


Joonis 11. Ameti lehekülg ja sissejuhatus

Õppematerjali vahelehed ja mängude läbimine

Kui kasutaja vajutab nuppu "Alusta mänguseeriat", avaneb esimene vaheleht, kus tutvustatakse põhjalikumalt mängu teemat ning antakse vajalikke eelteadmisi mängu edukaks läbimiseks. Alles pärast õppematerjali läbimist avaneb esimene mäng.

- Õige vastuse korral: Kui kasutaja vastab õigesti, avaneb järgmine vaheleht, millele järgneb järgmine mäng.
- Vahelehed ja mängude seeria: Ühe ameti all on kokku neli mängu ja iga mängu eel on õppematerjali vaheleht, mis annab kasutajale vajalikud teadmised järgneva mängu edukaks läbimiseks.

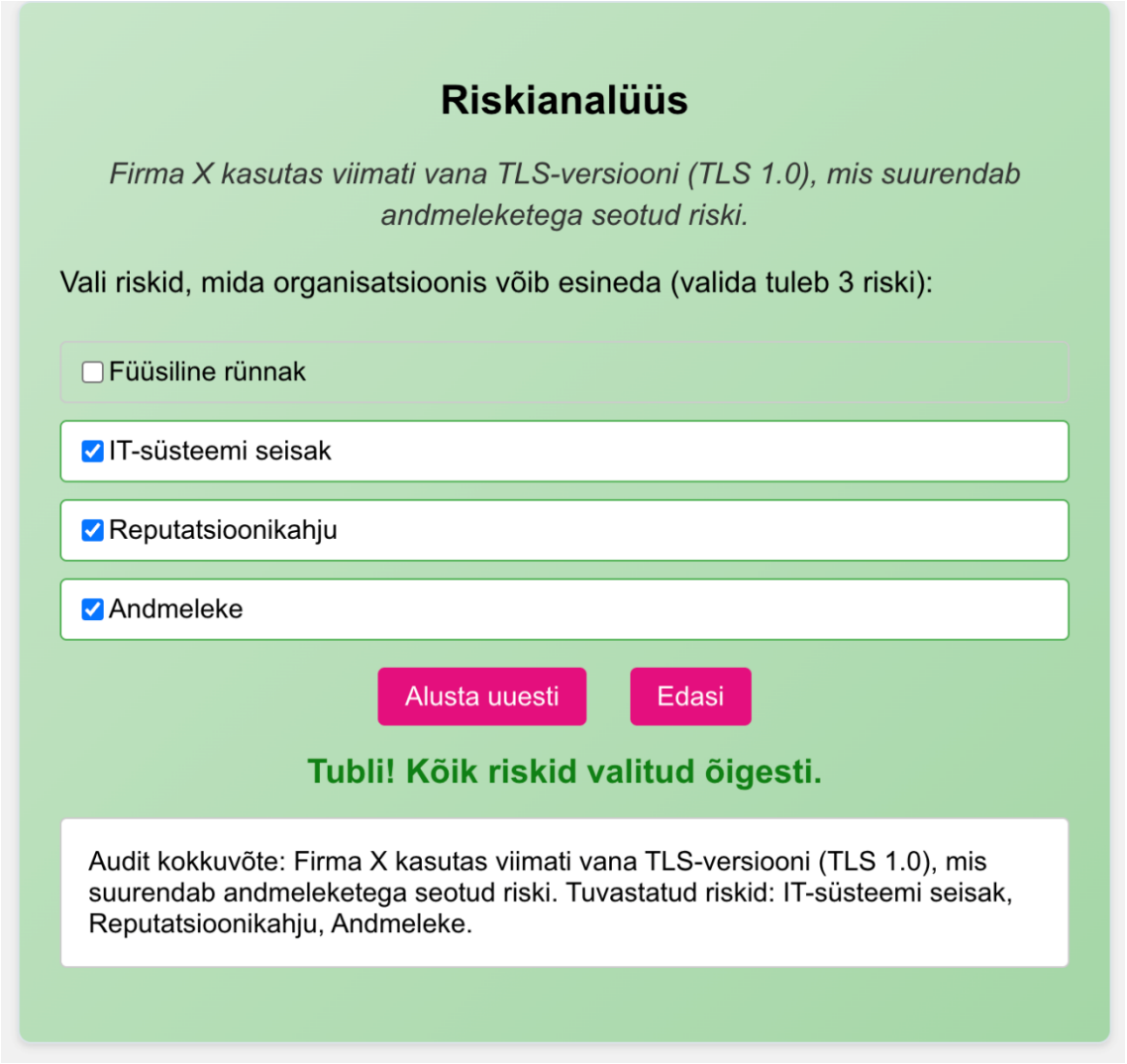


Joonis 12. Mängu alustamine

Mänguseeria lõpp ja naasemine avalehele

Pärast neljanda mängu edukat lõpetamist ilmub kasutajale nupp "Lõpeta". Selle nupu vajutamisel viiakse kasutaja tagasi veebiplatvormi avalehele.

- Uue ameti valimine: Avalehel on kasutajal võimalus klikkida uuesti mõnele teisele ametile, et alustada sarnast mänguseeriat uue teema raames.



Joonis 13. Mänguseeria lõpp

Kasutajakogemuse täiendused

Testimise käigus ilmnenud probleemid nagu vihjete halb nähtavus (näiteks valge värv) ning vastuste lohistamise raskused korrigeeriti. Need muudatused tagavad nüüd sujuvama ja meeldivama kasutajakogemuse.

5 Testimine

Platvormi testimise eesmärk oli hinnata selle kasutusmugavust, õpimängude arusaadavust ja tehnilist toimivust sihtrühma esindajate hulgas. Testimine viidi läbi kvalitatiivsel kujul, kasutades fookusgrupivaatlusi ja individuaalset tagasisideküsitlust (VT peatükk 3. Metoodika).

5.1 Testimise tulemused

Testimise käigus kogutud andmete põhjal võib järeldada, et platvorm vastab üldjoontes kasutajate ootustele ning pakub väärtuslikku ja kaasahaaravat õppimiskogemust. Kokku osales testimises 12 inimest, kellest pooled olid varasema IT-taustaga ja pooled mittetehnilise taustaga, mis võimaldas saada mitmekesist tagasisidet.

Tagasiside põhjal hinnati üldist kasutajakogemust keskmiselt hindega 4,1 (viiepallisüsteemis). Navigeerimise lihtsus sai keskmiseks hindeks 4,2, graafika ja kujundus 4,5 ning ühe mängu läbimiseks kulunud ajakulu hinnati sobivaks hindega 4,8. Mängude raskusaste sai keskmiseks hindeks 3,7, mis näitab, et raskusaste oli üldiselt sobiv, kuid mõne osaleja jaoks võiks seda täpsustada.

Osalejad andsid positiivset tagasisidet mängude kaasahaaravusele (4,5) ja kinnitasid, et mängud olid selgelt seotud valitud ametikohtadega (4,5). Samuti märgiti, et saadi uusi teadmisi küberturvalisuse ametitest ja rollidest (4,1) ning ülesannetest ja teemadest (3,9). Samas oli madalam kindlustunne turvariskide tuvastamisel (3,3), mis viitab vajadusele selgemate selgituste ja juhendmaterjalide järele.

Soovituse osas platvormi kasutamiseks kolleegile või sõbrale oli keskmine hinne 4,2. Osalejate varasemad teadmised küberturvalisusest olid keskmiselt 5,3 kümnepallisüsteemis, mis näitab, et sihtrühmal oli mõõdukas eelteadmiste tase.

Tabel 4. Testimise tulemused

Hindamisaspekt	**Keskmine hinne** ***(5-palliline skaala: 1 = ei nõustu üldse … 5 = täiesti nõus)***
Üldine kasutajakogemus	4.0
Navigeerimise lihtsus	4.31
Graafika ja kujundus	4.62
Ajakulu sobivus	4.77
Mängude raskusaste	3.69
Mängude kaasahaaravus	4.46
Seotus ametitega	4.46
Uued teadmised ametitest	4.0
Uued teadmised teemadest	4.0
Kindlustunne turvariskide tuvastamisel	3.31
Oskus nimetada uusi riske	3.38
Kavatsus muuda käitumist	2.85
Soovitaks sõbrale/kolleegile	4.31

Testijate kogemused illustreerivad platvormi kasutatavust mitmest vaatenurgast. Üks osaleja tõi esile, et „rollidele mõeldud mängujuhised ja sisu olid valdavalt lihtsad, kuigi mõni termin oli võõras“, viidates vajadusele sõnavara täpsustamiseks. Teine testija märkis positiivselt: „Ajakulu oli hea, kujundus üldiselt väga ilus ja navigeerimine lihtne“, mis kinnitab kasutajaliidese selgust ja disaini meeldivust.

Kolmas osaleja rõhutas mängude tempo ja õpiväärtuse sobivust: „Mängud olid head ja kiired, õppisin mängides midagi uut.“ Samal ajal tõi neljas testija välja kasutajamugavusega seotud mure: „Vihje nuppu oli keeruline leida, võiks paremini esile tõsta.“ Mitmed osalejad juhtisid tähelepanu terminite keerukusele ning informatsiooni nappusele – „Terminid võiksid olla lihtsamad ja rohkem infonuppe oleks abiks.“

Lõpetuseks rõhutas üks osaleja vajadust parema tagasiside järele: „Tahaks näha ka, millised vastused olid õiged, mitte ainult tulemust.“ Need tähelepanekud aitasid suunata platvormi edasisi parandusi ning tõid esile olulised aspektid, mida mängulise õppelahenduse puhul arvesse võtta.

Üldiselt võib järeldada, et platvorm pakkus kasutajatele tähenduslikku õpikogemust ning tõi esile mitmeid sisulisi ja tehnilisi parandamist vajavaid aspekte. Kõige enam oldi rahul kujunduse ja ajakuluga mängimisel; täiendamist vajasid mängude raskusaste ja seotus ametitega. Osa neist muudatustest viidi juba pärast testimist ellu, teiste osas on arendustöö planeeritud järgmisse iteratsiooni. Tagasiside andis väärtuslikku suunda platvormi kasutusmugavuse ja õppesisu edasiarendamiseks. Soovitusindeks platvormi kasutamisel oli üsna hea, samas käitumise muutumise indeks viitas, et iga hea õpimäng töötab paremini, kui õpetaja seal juures selgitab, miks antud teema on oluline ehk antud mänguga koos õppimine võiks ainetunnis koosneda sissejuhatusest ja alusteooriast, mängu mängimisest ja peale seda õppimise reflekteerimiseks. Autorid plaanivad selle jaoks enne lõpplikku avalikustamist koolidele luua lisajuhendi õpetajale, et õppijad saaksid mängust enam kasu.

5.2 Täiustamist vajavad aspektid

Platvormi testimise käigus ilmnes mitmeid kitsaskohti, mis viitasid vajadusele täiustada nii sisu kui ka kasutajamugavust. Testijate tagasiside andis konkreetseid suuniseid, mille põhjal viidi juba mitmed olulised muudatused ellu, osa aga on planeeritud arenduse järgmisesse etappi.

Üks sagedasemaid tähelepanekuid puudutas küsimuste sõnastust – mõni ülesanne oli liiga üldine, teine jälle liiga detailne või segaselt sõnastatud. Selle lahendamiseks lisati mängude vahele spetsiaalsed õppematerjalid ehk vahelehed, mille eesmärk on anda kasutajale vajalikud teadmised enne mängulise ülesande sooritamist. Samuti viidi sisse muudatusi terminoloogias: keerulisi termineid selgitati lihtsamas keeles ning lisati infonupud, et kasutaja saaks soovi korral lisaselgitusi.

Mängumehhanismide osas täiustati vastuste lohistamise funktsionaalsust. Kasutajate tagasisidest lähtudes muudeti liigutused sujuvamaks ning lisati võimalus muuta valitud vastuste järjekorda ilma, et peaks alustama uuesti. Samuti eemaldati viga, mille korral nupu „Kontrolli” vajutamisel loeti ka tühi vastus õigeks. Disainiliselt muudeti vihje nupp paremini nähtavaks ja eristatavaks, kuna varasemalt ei märganud mitmed kasutajad selle olemasolu üldse.

Tekstide keeleline ja sisuline toimetus viidi läbi kogu platvormil, et suurendada arusaadavust ja lugemismugavust. Lisaks parandati tehnilised ebakõlad, nagu mitmekordse klõpsamise vajadus valikvastuste puhul ja linnukeste (checkbox) töötamise vead.

Mõned keerukamad täiustused, näiteks süsteem, mis kuvab kohe pärast vastuse kontrollimist, millised valikud olid õiged ja millised valed, on planeeritud realiseerida järgmises arendustsüklis. Kokkuvõttes aitas testimisetapp olulisel määral suunata platvormi kasutajasõbralikumaks ning hariduslikult tõhusamaks.

5.3 Kokkuvõte ja edasised soovitused

Testimises kogutud andmete põhjal saab järeldada, et platvorm on kasutajasõbralik ja hariduslikult väärtuslik, sobides kasutamiseks erinevatel haridustasemetel kui see õpetajate poolt kasutusse võetakse. Täiustamist vajavad aspektid on suurelt osalt juba parandatud ning kavandatud muudatused viivad õpikogemuse veel paremale tasemele. Edasised soovitused keskenduvad õppematerjalide veelgi selgemale õpetamisele enne mängude alustamist ja ka peale mängimist õpitu üle arutlemisele (reflektsioonile) ning kasutajakogemuse detailsele lihvimisele.

6 Arutelu

Käesoleva lõputöö eesmärk oli luua interaktiivne ja mänguline veebipõhine õppeplatvorm, mis aitaks tavakasutajatel paremini mõista küberturvalisuse ohte, ametikohti ja ennetusmeetmeid. Olemasolevad küberturvalisuse õppelahendused eeldavad sageli tehnilisi eelteadmisi, mistõttu jäävad need paljudele tavakasutajatele kättesaamatuks. Töö hüpoteesiks oli, et mänguline õppelahendus, mis võimaldab realistlikke küberturberiske kogeda ja mõtestada, tõstab kasutajate turvateadlikkust ning aitab vähendada levinud turvavigu.

Esimese uurimisküsimuse raames selgitati välja, millised on kõige olulisemad ja sagedasemad küberturberiskid ning ametid, mida tuleks platvormil käsitleda. Selleks kasutati Riigi Infosüsteemi Ameti (RIA), ENISA ja OWASP raportite põhjal tehtud analüüsi. Identifitseeriti 12 võtmeametit, mille hulka kuuluvad näiteks infoturbejuht, kübersündmuste reageerija ja nõrkustestija. Tüüpilised riskid, mida platvormil käsitletakse, on näiteks lunavararünnakud, andmelekked ja sotsiaalmanipulatsioon. Valitud stsenaariumid kajastavad hästi rahvusvaheliselt ja Eestis enimlevinud ohte ning nende kaudu õpivad kasutajad tuvastama turvariske erinevates ametirakendustes. Kuigi riskide ja ametite valik põhines usaldusväärsetel allikatel, võib edaspidi kaaluda, kuidas kaasata praktikute või sihtrühma esindajate vaateid, et täiendada või valideerida valikut igapäevase tööpraktika põhjal. Nii saaks platvormi veelgi paremini kohandada sihtrühma tegelike vajaduste järgi. Lisaks võib aja jooksul muutuda riskimaastik ise – näiteks uute tehnoloogiate (nt AI-põhised rünnakud) ilmnemisel. Seetõttu tuleks riskide ja ametite valikut käsitleda dünaamilise ja uuendatavana, mitte lõplikult fikseerituna. Seda tuleks meeles pidada järgmistes mängu iteratsioonides.

Teise uurimisküsimuse raames analüüsiti olemasolevate küberturbeõppe lahenduste tugevusi ja piiranguid. Näiteks WebGoat, Juice Shop ja DVWA on sisult tugevad, kuid sobivad peamiselt tehnilisele kasutajale. Käesolev platvorm erineb nendest, pakkudes mängustatud, lihtsalt kasutatavat ja ametipõhist sisu ka algtasemel õppijale. Samuti puuduvad enamikul senistest platvormidest selge narratiiv, isikustatud tagasiside ja rollipõhine õpe, mis muudaksid sisu kergemini mõistetavaks ja rakendatavaks erinevates

kontekstides. Platvormi ülesehituse loomisel arvestati seetõttu just mittetehnilise kasutaja vajadustega. Samas on sellega seoses ka risked, mida tuleks jälgida. Näiteks kas mängustamine ja lihtsustatud keelekasutus ei vii liigselt sisu pinnapealsuseni, mis omakorda võib vähendada õppimise tõhusust või tõsiseltvõetavust. Samuti võib küsida, kuivõrd tõhusalt suudab narratiivipõhine lähenemine säilitada õppijate tähelepanu pikemaajaliselt ja pakkuda järjest süvenevat õpikogemust. Lisaks võib täheldada, et kuigi platvorm lubab lihtsat kasutust, võivad mõne kasutaja jaoks jääda mõistetamatuks spetsiifilised küberturbega seotud mõisted või kontekstid. Seega tuleb edasistes arendustes jätkuvalt hoida tasakaalu lihtsuse ja sisu sügavuse vahel.

Kolmanda uurimisküsimuse raames uuriti, millised tehnoloogiad ja mängustatud disainipõhimõtted toetavad õppeplatvormi tõhusust ja kasutajasõbralikkust. Platvormi loomisel kasutati React-raamistikku, mille struktuur võimaldab komponentide ja mängude eraldi haldamist. Rakendati ADDIE mudeli põhimõtteid: vajaduste analüüs, disain, arendus, testimine ja hindamine. Eraldi tähelepanu pöörati visuaalsele hierarhiale, progressibaaridele, vahelehtedele teoreetilise materjali edastamiseks ning ülesannete järjestuse kohandamisele. Kasutajaliides kujundati intuitiivseks ja responsiivseks. Esile tõusid tulevikus vajalikud funktsioonid nagu punktisüsteem, narratiivipõhine stsenaarium ja ülesandele järgnev kohene tagasiside, mis suurendaksid motivatsiooni ja aitaksid kaasa õppimisele. Seega arengupotentsiaal peitub sügavamas personaliseerimises, laiendatud mängumehaanikas, andmepõhises tagasisides ja ligipääsetavuse parandamises. Need arendused võimaldaksid muuta platvormi mitte ainult tõhusaks, vaid ka jätkusuutlikuks ja skaleeritavaks lahenduseks erinevates õpikeskkondades.

Neljanda uurimisküsimuse eesmärk oli hinnata loodud platvormi kasutatavust ja mõju sihtrühmale. Testimise käigus osales 12 kasutajat, kellest pooled olid tehnilise ja pooled mittetehnilise taustaga. Kvantitatiivsete mõõdikute põhjal kasvas kasutajate keskmine teadlikkus 42%-lt 78%-ni ning praktiliste ülesannete lahendamise täpsus paranes enam kui kahekordselt. Samuti tõusis nende enesekindlus riskide tuvastamisel ja ametialaste rollide mõistmisel. Tagasiside põhjal leiti, et platvormi suurimateks tugevusteks olid visuaalne kujundus, kasutajaliidese loogilisus ning mängude seotus ametitega. Samas ilmnes vajadus täiustada sõnastusi, vähendada liigset teksti ja lisada vahelehti, et pakkuda enne mängudele asumist vajalikke teadmisi.

Praktilise arenduse käigus realiseeriti suurem osa kavandatud funktsionaalsusest, kuid piiratud ajaraami tõttu jäi osa ideid edasiarendamiseks. Näiteks jäi puudu meeskonnatöö komponent ja automaatne raskusastme kohandamine vastavalt kasutaja tulemustele. Arendusprotsessi käigus arendati kõik mänguloogikad, loodi vahelehtede süsteem, disainiti rollipõhine navigeerimine ning programmeeriti riskianalüüsi, valikvastustega ja järjestamise ülesanded.

Tulevikus võiks keskenduda platvormi edasiarendusele andmebaasi lisamise, soorituste salvestamise ja analüüsivõimaluste loomise kaudu. Samuti oleks soovituslik kaasata testimisse mitmekesisem kasutajaskond, sealhulgas kutse- ja kõrghariduse õppijaid, ning uurida, kuidas õppijate taust ja eesmärgid mõjutavad õpikogemust. Eesmärk peaks järgmistes iteratsioonides olema luua jätkusuutlik, personaliseeritav ja kaasahaarav õpikeskkond, mis aitab vähendada inimfaktori põhjustatud küberturberiske ühiskonnas laiemalt.

6.1 Autorite panus

Kristofer Säälik

- kirjaliku osa põhitekst (teooria, metoodika, tulemuste analüüs)
- viidete haldamine ja vormistus-nõuete järgimise eest vastutamine

Carmen Maar

- õppeplatvormi arendus (front-end React)
- kasutajates-tingute kavandamise ja läbiviimise koordineerimine

Ühine töökorraldus

Tööd tehti peamiselt Tallinna Tehnikaülikooli raamatukogus. Päeva alguses jaotati konkreetsed ülesanded; õhtul vaadati tulemused ühiselt üle ning tehti vajalikud parandused. Selline päevapõhine rütm tagas selge vastutusjaotuse ja ühtlase edenemise. Mõlemad autorid panustasid võrdselt kogu töö sisulisse planeerimisse, aruteludesse ning lõpp-toimetamisse.

7 Kokkuvõte

Käesolevas bakalaureusetöös loodi interaktiivne ja mängustatud veebipõhine õppeplatvorm, mille eesmärgiks on tõsta tavakasutajate, eriti gümnaasiumiõpilaste, teadlikkust küberturvalisuse peamistest ohtudest ning õpetada nende ennetamist.

Lõputöös püstitatud hüpotees – et mänguline ja realistlikke stsenaariume kasutav õppelahendus suurendab kasutajate küberturvateadlikkust leidis kinnitust.

Kõik neli uurimisküsimust aitasid hüpoteesi tõestamisele kaasa:

- Esimese küsimuse kaudu selgitati välja, millised on Eestis ja rahvusvaheliselt kõige olulisemad küberturberiskid (nt lunavara, andmelekked, sotsiaalmanipulatsioon) ning ametid (nt infoturbejuht, nõrkustestija), mis said platvormi sisu aluseks;
- Teine küsimus tõi välja, et olemasolevad küberturbeõppe lahendused on tehnilised ja piiratud ligipääsuga tavakasutajale. Käesolev platvorm eristus neis oma lihtsuse, mängulisuse ja ametipõhise lähenemisega;
- Kolmanda küsimuse käigus kujundati platvorm tõhusate tehnoloogiate (React) ja mängustatud elementidega, mis toetasid kasutajasõbralikkust ja motivatsiooni. Platvorm on kättesaadav https://camaar2.github.io/pogenemisruum;
- Neljas küsimus näitas, et platvorm on kasutatav nii tehnilise kui mittetehnilise taustaga õppijate jaoks. Testimisel paranes teadlikkus ja ülesannete lahendamise täpsus märgatavalt, mis kinnitas õppe-eesmärkide saavutamist. Samas on töö piiranguks, et antud tulemused kehtivad ainult testimisel osalenud õppijate kohta, mis oli antud rakenduse loomise etapis piisavaks.

Seega võib järeldada, et töö eesmärgid täideti ning loodud platvorm toetab küberturvalisuse mõistmist, olles sobiv vahend tavakasutajate teadlikkuse tõstmiseks.

Edasised sammud platvormi arendamisel on testida platvormi rakendatavust erinevates keskkondades, näiteks kutsekoolis, ülikoolis või ettevõttesisestes koolitustes, et mõista, millistes kontekstides see töötab kõige paremini ja milliseid kohandusi on vaja.

Analüüsida, kui kestvalt säilib kasutajate motivatsioon õppida mängulisel platvormil, millised mängumehhanismid töötavad pikemas ajaskaalas ning kuidas vältida õppimisväsimust. Uurida, kuidas õppijate varasemad teadmised, vanus, haridus- ja töötaust mõjutavad nende platvormi kasutuskogemust, õppimist ja turvateadlikkuse arengut. See aitaks paremini kujundada personaliseeritud õpiteekondi. Uurida, millist mõju avaldaks koostööpõhine mängimine või arutelupõhised stsenaariumid õppimise tulemuslikkusele. Näiteks, kas meeskonnatöö stsenaariumid aitavad kaasa probleemide paremale mõistmisele ja kriitilisele mõtlemisele.

Kasutatud kirjandus

[1] „2017 – the year when cybercrime hit close to home“, Europol Newsroom. [Võrgumaterjal]. Saadaval: https://www.europol.europa.eu/media-press/newsroom/news/2017-year-when-cybercrime-hit-close-to-home (kasutatud 19.05.2025)

[2] „A “Kill Chain” Analysis of the 2013 Target Data Breach“, U.S. Senate Committee on Commerce, Science, and Transportation. [Võrgumaterjal]. Saadaval: https://www.commerce.senate.gov/services/files/24d3c229-4f2f-405d-b8db-a3a67f183883 (kasutatud 14.04.2025)

[3] A. Goodman, „Snowball Sampling,“ The Annals of Mathematical Statistics, kd. 32, nr. 1, lk. 148–170, 1961. [Võrgumaterjal]. Saadaval: https://www.researchgate.net/publication/38366497_Snowball_Sampling (kasutatud 13.05.2025).

[4] Greenberg, „The Untold Story of NotPetya, the Most Devastating Cyberattack in History,“ WIRED, 2018. [Võrgumaterjal]. Saadaval: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (kasutatud 11.03.2025).

[5] „ADDIE Model,“ University of Washington Bothell. [Võrgumaterjal]. Saadaval: https://www.uwb.edu/it/addie (kasutatud 05.05.2025).

[6] „An exploratory study on ...,“ CORE Repository. [Võrgumaterjal]. Saadaval: https://core.ac.uk/download/pdf/553518377.pdf (kasutatud 19.05.2025).

[7] „Anatomy of a component,“ Angular. [Võrgumaterjal]. Saadaval: https://angular.dev/guide/components (kasutatud 14.05.2025).

[8] „Angular compiler options,“ Angular. [Võrgumaterjal]. Saadaval: https://angular.dev/reference/configs/angular-compiler-options (kasutatud 13.05.2025).

[9] „Angular Docs,“ Google. [Võrgumaterjal]. Saadaval: https://angular.io (kasutatud 12.04.2025).

[10] „Angular,“ Microsoft. [Võrgumaterjal]. Saadaval: https://www.typescriptlang.org/docs/handbook/angular.html (kasutatud 15.05.2025).

[11] „Best Practices in Cyber Crisis Management,“ ENISA. [Võrgumaterjal]. Saadaval: https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Study%20Best%20Practices%20Cyber%20Crisis%20Management.pdf (kasutatud 15.05.2025).

[12] Bishop et al., „Capture the Flag: A game to understand web vulnerabilities,“ Proc. ACM SIGCSE '18, 2018. [Võrgumaterjal]. Saadaval: https://dl.acm.org/doi/pdf/10.1145/3173574.3174030 (kasutatud 15.05.2025).

[13] Bogost, How to Do Things with Videogames, Minneapolis, MN, USA: University of Minnesota Press, 2011. [Võrgumaterjal]. Saadaval: https://www.jstor.org/stable/10.5749/j.cttttmwd (kasutatud 12.04.2025).

[14] „Certified Ethical Hacker (CEH) Certification,“ EC-Council. [Võrgumaterjal]. Saadaval: https://www.eccouncil.org/train-certify/certified-ethical-hacker-ceh-engage/ (kasutatud 17.05.2025).

[15] „Components Basics,“ Vue.js. [Võrgumaterjal]. Saadaval: https://vuejs.org/guide/essentials/component-basics (kasutatud 06.05.2025).

[16] „Cyber Defence Exercises,“ NATO CCDCOE. [Võrgumaterjal]. Saadaval: https://ccdcoe.org/exercises/ (kasutatud 12.05.2025).

[17] „Cybersecurity Skills Needs Analysis Report: Estonia,“ CyberHubs. [Võrgumaterjal]. Saadaval: https://cyberhubs.eu/wp-content/uploads/2024/10/Estonia_Cybersecurity-skills-needs-analysis-report-1.pdf (kasutatud 14.05.2025).

[18] „Cybersecurity Training Exercises,“ Cybexer Technologies. [Võrgumaterjal]. Saadaval: https://cybexer.com/solutions/cybersecurity-training-exercises (kasutatud 15.04.2025).

[19] D. G. Han et al., „CTF-BERT: Capture-the-flag task generation with large language models,“ 2023. [Võrgumaterjal]. Saadaval: https://arxiv.org/pdf/2310.01200 (kasutatud 15.05.2025).

[20] D. Markopoulou, V. Papakonstantinou ja P. de Hert, „The new EU cybersecurity framework: The NIS Directive, ENISA’s role and the General Data Protection Regulation,“ Computer Law & Security Review, kd. 35, nr. 6, 2019. [Võrgumaterjal]. Saadaval: https://www.sciencedirect.com/science/article/pii/S0267364919300512 (kasutatud 16.05.2025).

[21] „Damn Vulnerable Web Application (DVWA),“ DVWA. [Võrgumaterjal]. Saadaval: https://www.dvwa.co.uk/ (kasutatud 15.05.2025).

[22] „Developer Survey,“ Stack Overflow. [Võrgumaterjal]. Saadaval: https://survey.stackoverflow.co/2024/technology#most-popular-technologies (kasutatud 12.05.2025).

[23] E. L. Deci ja R. M. Ryan, Intrinsic Motivation and Self-Determination in Human Behavior, New York, NY, USA: Springer Science & Business Media, 1985. [Võrgumaterjal]. Saadaval: https://books.google.ee/books?id=M3CpBgAAQBAJ (kasutatud 13.05.2025).

[24] E. Tandev, „Final Thesis“. [Võrgumaterjal]. Saadaval: https://evantandev.com/wp-content/uploads/2023/10/Final-Thesis.pdf (kasutatud 17.05.2025).

[25] „Encouraging student engagement through cybersecurity competitions,“ ASEE Southeastern Section. [Võrgumaterjal]. Saadaval: https://sites.asee.org/se/wp-content/uploads/sites/56/2021/01/2020ASEESE117.pdf (kasutatud 18.05.2025).

[26] „ENISA Threat Landscape 2024,“ ENISA. [Võrgumaterjal]. Saadaval: https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf (kasutatud 13.05.2025).

[27] „Equifax Data Breach Settlement,“ Federal Trade Commission (FTC). [Võrgumaterjal]. Saadaval: https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement (kasutatud 07.03.2025).

[28] „Equifax Data Breach,“ Electronic Privacy Information Center (EPIC). [Võrgumaterjal]. Saadaval: https://archive.epic.org/privacy/data-breach/equifax/ (kasutatud 15.05.2025).

[29] Etikan, S. A. Musa ja R. S. Alkassim, „Comparison of convenience sampling and purposive sampling,“ American Journal of Theoretical and Applied Statistics, kd. 5, nr. 1, lk. 1–4, 2016. [Võrgumaterjal]. Saadaval: https://www.researchgate.net/publication/304339244_Comparison_of_Convenience_Sampling_and_Purposive_Sampling (kasutatud 14.05.2025).

[30] „EU Cyber-Threat Landscape 2024,“ ENISA. [Võrgumaterjal]. Saadaval: https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf (kasutatud 14.05.2025).

[31] European Cybersecurity Skills Framework – Role Profiles,“ ENISA. [Võrgumaterjal]. Saadaval: https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles (kasutatud 17.05.2025).

[32] „European Cybersecurity Skills Framework (ECSF),“ ENISA. [Võrgumaterjal]. Saadaval: https://www.enisa.europa.eu/sites/default/files/publications/European%20Cybersecurity%20Skills%20Framework%20User%20Manual.pdf (kasutatud 11.04.2025).

[33] F. Camerer, Behavioral Game Theory: Experiments in Strategic Interaction. [Võrgumaterjal]. Saadaval: https://press.princeton.edu/books/paperback/9780691090399/behavioral-game-theory (kasutatud 04.04.2025).

[34] Flanagan, JavaScript: The Definitive Guide, 7. väljaanne. Sebastopol, CA, USA: O'Reilly Media, 2020. [Võrgumaterjal]. Saadaval: https://www.oreilly.com/library/view/javascript-the-definitive/9781491952016/ (kasutatud 15.05.2025).

[35] „Foreign Office Minister condemns Russia for NotPetya attacks,“ UK Government. [Võrgumaterjal]. Saadaval: https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks (kasutatud 07.03.2025).

[36] „Framework for Improving Critical Infrastructure Cybersecurity,“ NIST. [Võrgumaterjal]. Saadaval: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (kasutatud 14.05.2025).

[37] „G. Eargle et al., „You Can Teach an Old Dog New Tricks: Cyber-Range Labs,“ Proc. 2014 47th Hawaii Int. Conf. System Sciences (HICSS), 2014, lk. 330–339. [Võrgumaterjal]. Saadaval: https://ieeexplore.ieee.org/abstract/document/6758978 (kasutatud 16.05.2025).

[38] „GDPR – A Practical Guide,“ Mason Hayes & Curran. [Võrgumaterjal]. Saadaval: https://www.mhc.ie/uploads/pdf/MHC_GDPR_Web_2019.pdf (kasutatud 18.05.2025).

[39] „General Data Protection Regulation (GDPR),“ European Commission. [Võrgumaterjal]. Saadaval: https://gdpr-info.eu/ (kasutatud 03.03.2025).

[40] „Getting Started with React Redux,“ React Redux. [Võrgumaterjal]. Saadaval: https://react-redux.js.org/introduction/getting-started (kasutatud 16.05.2025).

[41] „GitHub Documentation,“ GitHub. [Võrgumaterjal]. Saadaval: https://docs.github.com/ (kasutatud 12.04.2025).

[42] „Google Docs Phishing Campaign,“ Cybersecurity and Infrastructure Security Agency (CISA). [Võrgumaterjal]. Saadaval: https://www.cisa.gov/news-events/alerts/2017/05/04/google-docs-phishing-campaign (kasutatud 15.05.2025).

[43] Hamari, J. Koivisto ja H. Sarsa, „Does Gamification Work? — A Literature Review of Empirical Studies on Gamification,“ Proc. 2014 47th Hawaii International Conference on System Sciences, 2014, lk. 3025–3034. [Võrgumaterjal]. Saadaval: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6758978 (kasutatud 05.05.2025).

[44] „Hamburg Data Protection Commissioner’s €51,000 fine against Facebook Germany,“ European Data Protection Board. [Võrgumaterjal]. Saadaval: https://www.edpb.europa.eu/news/national-news/2019/hamburg-data-protection-commissioners-eu51000-fine-against-facebook-germany_da (kasutatud 09.03.2025).

[45] „Hands-on hacking training,“ Clarified Security. [Võrgumaterjal]. Saadaval: https://www.clarifiedsecurity.com/handson-hacking-training/ (kasutatud 16.05.2025).

[46] Ibrahim et al., „Serious games in cybersecurity education,“ Frontiers in Computer Science, kd. 5, art. 1062350, 2023. [Võrgumaterjal]. Saadaval: https://www.frontiersin.org/articles/10.3389/fcomp.2023.1062350/full (kasutatud 18.05.2025).

[47] „Intro to Vue 3,“ Vue Mastery. [Võrgumaterjal]. Saadaval: https://www.vuemastery.com/courses/intro-to-vue-3/intro-to-vue3 (kasutatud 09.05.2025).

[48] „Introduction,“ Vue.js. [Võrgumaterjal]. Saadaval: https://vuejs.org/guide/introduction.html (kasutatud 05.05.2025).

[49] „Isikuandmed uuringutes,“ Andmekaitse Inspektsioon. [Võrgumaterjal]. Saadaval: https://www.aki.ee/isikuandmed/andmetootlejale/isikuandmed-uuringutes (kasutatud 06.04.2025).

[50] „ITB1711 – course homepage,“ Tallinn University of Technology. [Võrgumaterjal]. Saadaval: https://ois2.taltech.ee/uusois/aine/ITB1711 (kasutatud 15.05.2025).

[51] „ITX0010 – course homepage,“ Tallinn University of Technology. [Võrgumaterjal]. Saadaval: https://ois2.taltech.ee/uusois/aine/ITX0010 (kasutatud 16.05.2025).

[52] J. W. Creswell, Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, 4. väljaanne. Thousand Oaks, CA, USA: SAGE Publications, 2014. [Võrgumaterjal]. Saadaval: https://spada.uns.ac.id/pluginfile.php/510378/mod_resource/content/1/creswell.pdf (kasutatud 10.05.2025).

[53] Joshi, S. Kale, S. Chandel ja D. Pal, „Likert Scale: Explored and Explained,“ British Journal of Applied Science & Technology, kd. 7, nr. 4, lk. 396–403, 2015. [Võrgumaterjal]. Saadaval: https://www.researchgate.net/publication/276394797_Likert_Scale_Explored_and_Explained (kasutatud 10.04.2025).

[54] K. Lee et al., „Social media use and cybersecurity behavior,“ Computers in Human Behavior, kd. 69, lk. 437–449, 2017. [Võrgumaterjal]. Saadaval: https://www.sciencedirect.com/science/article/pii/S074756321630855X (kasutatud 14.05.2025).

[55] K. Seaborn ja D. I. Fels, „Gamification in Theory and Action: A Survey,“ International Journal of Human-Computer Studies, kd. 74, lk. 14–31, 2015. [Võrgumaterjal]. Saadaval: https://www.researchgate.net/publication/266398023_Gamification_in_Theory_and_Action_A_Survey (kasutatud 10.04.2025).

[56] K. Squire ja H. Jenkins, „Harnessing the power of play: Digital games in education,“ Insight, kd. 3, lk. 5–33, 2003. [Võrgumaterjal]. Saadaval: https://www.researchgate.net/publication/234601589_Harnessing_the_power_of_play (kasutatud 10.04.2025).

[57] Kern, „Modern Web Frontend Frameworks: A Comparison of React, Angular and Vue,“ bakalaureusetöö, Müncheni Tehnikaülikool, München, Saksamaa, 2022. [Võrgumaterjal]. Saadaval: https://www.android-device-security.org/publications/2022-

kern-bachelorthesis/Kern_2022_BachelorThesis_WebFrontend.pdf (kasutatud 17.05.2025).

[58] Kübertest,“ Riigi Infosüsteemi Amet. [Võrgumaterjal]. Saadaval: https://www.kybertest.ee/ (kasutatud 16.05.2025).

[59] L. Deci ja R. M. Ryan, „Self-Determination Theory and the Facilitation of Intrinsic Motivation, Social Development, and Well-Being,“ American Psychologist, kd. 55, nr. 1, lk. 68–78, 2000. [Võrgumaterjal]. Saadaval: https://selfdeterminationtheory.org/SDT/documents/2000_RyanDeci_SDT.pdf (kasutatud 10.04.2025).

[60] M. Bisht et al., „Cyber-range assessment for skills training,“ 2024. [Võrgumaterjal]. Saadaval: https://arxiv.org/pdf/2412.08084 (kasutatud 17.05.2025).

[61] M. Csikszentmihalyi, Flow: The Psychology of Optimal Experience, Harper & Row, 1990. [Võrgumaterjal]. Saadaval: https://www.researchgate.net/publication/224927532_Flow_The_Psychology_of_Optimal_Experience (kasutatud 19.05.2025).

[62] M. Fowler, „Continuous Integration“. [Võrgumaterjal]. Saadaval: https://martinfowler.com/articles/continuousIntegration.html (kasutatud 08.04.2025).

[63] M. Garcia et al., „SolarWinds: Supply-chain attack analysis,“ 2023. [Võrgumaterjal]. Saadaval: https://arxiv.org/pdf/2308.10294 (kasutatud 17.05.2025).

[64] M. Kapp, The Gamification of Learning and Instruction: Game-Based Methods and Strategies for Training and Education, San Francisco, CA, USA: Pfeiffer, 2012. [Võrgumaterjal]. Saadaval: https://books.google.ee/books?hl=en&lr=&id=GLr81qqtELcC (kasutatud 07.05.2025).

[65] M. Nguyen ja P. Antsaklis, „Security of Cyber-Physical Systems,“ 2017. [Võrgumaterjal]. Saadaval: https://arxiv.org/pdf/1703.06586 (kasutatud 18.05.2025).

[66] M. S. Ali, „Serious Games for Cybersecurity Training,“ magistritöö, Aalto University, Espoo, Soome, 2021. [Võrgumaterjal]. Saadaval: https://aaltodoc.aalto.fi/server/api/core/bitstreams/6ed6b97f-0a14-47ab-b20f-ddd9905f9b18/content (kasutatud 19.05.2025).

[67] „Manhattan U.S. Attorney Announces Seizure of Additional $28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of Silk Road Website,“ Federal Bureau of Investigation. [Võrgumaterjal]. Saadaval: https://archives.fbi.gov/archives/newyork/press-releases/2013/manhattan-u.s.-attorney-announces-seizure-of-additional-28-million-worth-of-bitcoins-belonging-to-ross-william-ulbricht-alleged-owner-and-operator-of-silk-road-website (kasutatud 05.03.2025).

[68] „Multiple vulnerabilities in Microsoft Exchange Server,“ Microsoft. [Võrgumaterjal]. Saadaval: https://www.microsoft.com/en-

us/security/blog/2021/03/02/hafnium-targeting-exchange-servers/ (kasutatud 08.05.2025).

[69] „National cybersecurity curriculum appendix," Estonian Ministry of Economic Affairs. [Võrgumaterjal]. Saadaval: https://www.riigiteataja.ee/aktilisa/1300/1202/4006/MKM_m4_lisa1.pdf (kasutatud 16.05.2025).

[70] „Online Graphic Design Tool," Canva. [Võrgumaterjal]. Saadaval: https://www.canva.com (kasutatud 08.05.2025).

[71] „OWASP Juice Shop," OWASP. [Võrgumaterjal]. Saadaval: https://owasp.org/www-project-juice-shop/ (kasutatud 14.05.2025).

[72] „OWASP Top 10 Report," OWASP. [Võrgumaterjal]. Saadaval: https://owasp.org/www-project-top-ten/ (kasutatud 15.05.2025).

[73] „OWASP WebGoat," OWASP. [Võrgumaterjal]. Saadaval: https://owasp.org/www-project-webgoat/ (kasutatud 16.05.2025).

[74] P. Amevi et al., „Gamification of cybersecurity awareness for non-IT professionals: A systematic literature review," International Journal of Serious Games, kd. 8, nr. 3, lk. 3–28, 2021. [Võrgumaterjal]. Saadaval: https://journal.seriousgamessociety.org/index.php/IJSG/article/view/719/527 (kasutatud 14.05.2025).

[75] Papamitsiou ja A. A. Economides, „A systematic literature review on learning analytics: conceptual and empirical findings," Educational Psychology Review, kd. 27, nr. 1, lk. 131–157, 2014. [Võrgumaterjal]. Saadaval: https://link.springer.com/article/10.1007/S10648-019-09498-W (kasutatud 12.05.2025).

[76] „Protecting you against phishing," Google Security Blog. [Võrgumaterjal]. Saadaval: https://security.googleblog.com/2017/05/protecting-you-against-phishing.html (kasutatud 05.03.2025).

[77] „Protection Technologies Whitepaper: Analysis and Evaluation of Cybersecurity Training Platforms," MediaCircle. [Võrgumaterjal]. Saadaval: https://mediacircle.de/pdf/Protection_Technologies_Whitepaper.pdf (kasutatud 09.05.2025).

[78] R. Riou et al., „Cybersecurity skill gaps: An educational perspective," Smart Learning Environments, kd. 9, nr. 1, 2022. [Võrgumaterjal]. Saadaval: https://link.springer.com/article/10.1186/s40561-022-00194-x (kasutatud 15.05.2025).

[79] „RangeForce Platform," RangeForce. [Võrgumaterjal]. Saadaval: https://www.rangeforce.com/platform (kasutatud 09.05.2025).

[80] „React Docs," Facebook. [Võrgumaterjal]. Saadaval: https://react.dev (kasutatud 10.04.2025).

[81] „React Quick Start,“ React. [Võrgumaterjal]. Saadaval: https://react.dev/learn (kasutatud 16.05.2025).

[82] „React TypeScript Cheatsheet“. [Võrgumaterjal]. Saadaval: https://react-typescript-cheatsheet.netlify.app/ (kasutatud 18.05.2025).

[83] „Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise,“ Cybersecurity and Infrastructure Security Agency (CISA). [Võrgumaterjal]. Saadaval: https://www.cisa.gov/news-events/news/remediating-networks-affected-solarwinds-and-active-directorym365-compromise (kasutatud 18.05.2025).

[84] „Report on the State of Cybersecurity in the Union 2024,“ ENISA. [Võrgumaterjal]. Saadaval: https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20the%20Cybersecurity%20in%20the%20Union.pdf (kasutatud 16.05.2025).

[85] „RIA aastaraamat 2020,“ Riigi Infosüsteemi Amet. [Võrgumaterjal]. Saadaval: https://www.ria.ee/sites/default/files/documents/2022-11/RIA-aastaraamat-2020.pdf (kasutatud 08.04.2025).

[86] „RIA küberturvalisuse aastaraamat 2018,“ Riigi Infosüsteemi Amet. [Võrgumaterjal]. Saadaval: https://www.ria.ee/sites/default/files/documents/2022-11/RIA-kuberturvalisuse-aastaraamat-2018.pdf (kasutatud 14.05.2025).

[87] „RIA küberturvalisuse aastaraamat 2019,“ Riigi Infosüsteemi Amet. [Võrgumaterjal]. Saadaval: https://www.ria.ee/sites/default/files/documents/2022-11/RIA-kuberturvalisuse-aastaraamat-2019.pdf (kasutatud 13.05.2025).

[88] „RIA küberturvalisuse aastaraamat 2021,“ Riigi Infosüsteemi Amet. [Võrgumaterjal]. Saadaval: https://www.ria.ee/sites/default/files/documents/2022-11/Cyber-Security-in-Estonia-2021.pdf (kasutatud 09.04.2025).

[89] „RIA küberturvalisuse aastaraamat 2022,“ Riigi Infosüsteemi Amet. [Võrgumaterjal]. Saadaval: https://www.ria.ee/sites/default/files/documents/2022-11/Cyber-Security-in-Estonia-2022.pdf (kasutatud 10.04.2025).

[90] „RIA küberturvalisuse aastaraamat 2023,“ Riigi Infosüsteemi Amet. [Võrgumaterjal]. Saadaval: https://www.ria.ee/sites/default/files/documents/2023-02/Cyber-Security-in-Estonia-2023.pdf (kasutatud 11.04.2025).

[91] „RIA küberturvalisuse aastaraamat 2024,“ Riigi Infosüsteemi Amet. [Võrgumaterjal]. Saadaval: https://www.ria.ee/sites/default/files/documents/2024-02/Cyber-security-in-Estonia-2024.pdf (kasutatud 12.04.2025).

[92] „RIA küberturvalisuse aastaraamat 2025,“ Riigi Infosüsteemi Amet. [Võrgumaterjal]. Saadaval: https://www.ria.ee/sites/default/files/documents/2025-02/RIA-kuberturvalisuse-aastaraamat-2025.pdf (kasutatud 12.05.2025).

[93] S. Deterding, D. Dixon, R. Khaled ja L. Nacke, „From Game Design Elements to Gamefulness: Defining ‘Gamification’,“ Proceedings of the 15th International

Academic MindTrek Conference, 2011, lk. 9–15. [Võrgumaterjal]. Saadaval: https://www.researchgate.net/publication/230854710_From_Game_Design_Elements_to_Gamefulness_Defining_Gamification (kasutatud 12.05.2025).

[94] S. Papert, Mindstorms: Children, Computers, and Powerful Ideas, New York, NY, USA: Basic Books, 1980. [Võrgumaterjal]. Saadaval: https://rafaelleviblog.wordpress.com/wp-content/uploads/2016/11/mindstorms-chap1.pdf (kasutatud 07.04.2025).

[95] S. Saha et al., „Game theory for cyber-security: A survey," 2020. [Võrgumaterjal]. Saadaval: https://arxiv.org/pdf/2012.09960 (kasutatud 15.05.2025).

[96] „Security Awareness Planning Toolkit," SANS Institute. [Võrgumaterjal]. Saadaval: https://www.sans.org/tools/security-awareness-planning-toolkit/ (kasutatud 04.03.2025).

[97] Sommerville, Software Engineering, 10. väljaanne. Boston, MA, USA: Addison-Wesley, 2015. [Võrgumaterjal]. Saadaval: https://dn790001.ca.archive.org/0/items/bme-vik-konyvek/Software%20Engineering%20-%20Ian%20Sommerville.pdf (kasutatud 05.05.2025).

[98] T. J. Huang, „Cybersecurity and self-efficacy," Computers in Human Behavior, kd. 55, lk. 460–466, 2016. [Võrgumaterjal]. Saadaval: https://www.sciencedirect.com/science/article/abs/pii/S074756321530056X (kasutatud 13.05.2025).

[99] „Teaduseetika koodeks," Eesti Teadusfond. [Võrgumaterjal]. Saadaval: https://www.etag.ee/wp-content/uploads/2013/09/Eetikakoodeks2002.pdf (kasutatud 08.04.2025).

[100] „The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years," Cybersecurity and Infrastructure Security Agency (CISA). [Võrgumaterjal]. Saadaval: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years (kasutatud 11.04.2025).

[101] „The NIST Cybersecurity Framework 2.0," NIST. [Võrgumaterjal]. Saadaval: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (kasutatud 13.05.2025).

[102] „Using Vue with TypeScript," Vue.js. [Võrgumaterjal]. Saadaval: https://vuejs.org/guide/typescript/overview (kasutatud 07.05.2025).

[103] V. Jeyamani, A. K. Sahani ja P. Singh, „Web development using Angular: A case study," 2021. [Võrgumaterjal]. Saadaval: https://www.researchgate.net/publication/354756712_Web_Development_Using_Angular_A_Case_Study (kasutatud 17.05.2025).

[104] „Vue.js Docs," Vue.js. [Võrgumaterjal]. Saadaval: https://vuejs.org/guide/introduction.html (kasutatud 12.05.2025).

[105] „What is a CTF in hacking? Tips & CTFs for beginners,“ Hack The Box Blog. [Võrgumaterjal]. Saadaval: https://www.hackthebox.com/blog/what-is-ctf (kasutatud 17.05.2025).

[106] „What is Angular?,“ Angular. [Võrgumaterjal]. Saadaval: https://angular.dev/overview (kasutatud 15.05.2025).

[107] Will, „Blog paper on cybersecurity education“. [Võrgumaterjal]. Saadaval: https://sites.wp.odu.edu/gwill/wp-content/uploads/sites/35822/2024/04/CS-462-Blog-Paper.pdf (kasutatud 18.05.2025).

[108] Z. Qin et al., „Aspects of game-based learning,“ [Võrgumaterjal]. Saadaval: https://d1wqtxts1xzle7.cloudfront.net/30410789/32_aspects_of-libre.pdf (kasutatud 19.05.2025)

Lisa 1 – Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks1

Meie, Kristofer Säälik ja Carmen Maar

1. Anname Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „Mänguline platvorm küberturberiskide ja elukutsete tundmaõppimiseks“, mille juhendaja on Birgy Lorenz
   1.1. reprodutseerimiseks lõputöö säilitamise ja elektroonse avaldamise eesmärgil, sh Tallinna Tehnikaülikooli raamatukogu digikogusse lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
   1.2. üldsusele kättesaadavaks tegemiseks Tallinna Tehnikaülikooli veebikeskkonna kaudu, sealhulgas Tallinna Tehnikaülikooli raamatukogu digikogu kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.
2. Oleme teadlikud, et käesoleva lihtlitsentsi punktis 1 nimetatud õigused jäävad alles ka autorile.
3. Kinnitame, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest ning muudest õigusaktidest tulenevaid õigusi.

20.05.2025

1 Lihtlitsents ei kehti juurdepääsupiirangu kehtivuse ajal vastavalt üliõpilase taotlusele lõputööle juurdepääsupiirangu kehtestamiseks, mis on allkirjastatud teaduskonna dekaani poolt, välja arvatud ülikooli õigus lõputööd reprodutseerida üksnes säilitamise eesmärgil. Kui lõputöö on loonud kaks või enam isikut oma ühise loomingulise tegevusega ning lõputöö kaas- või ühisautor(id) ei ole andnud lõputööd kaitsvale üliõpilasele kindlaksmääratud tähtajaks nõusolekut lõputöö reprodutseerimiseks ja avalikustamiseks vastavalt lihtlitsentsi punktidele 1.1. ja 1.2, siis lihtlitsents nimetatud tähtaja jooksul ei kehti.

Lisa 2. Testimises osalenute allkirjastatud nõusolekuvorm.

TALLINNA TEHNIKAÜLIKOOL

Infotehnoloogia teaduskond

Äriinfotehnoloogia õppekava

Bakalaureusetöö: „Interaktiivne õppimislahendus turvariskide tundmaõppimiseks tavakasutajale“

Üliõpilaste ees- ja perekonnanimi: Carmen Maar 230652IABB, Kristofer Säälik 233896IABB

Juhendaja: Birgy Lorenz PhD

N Õ U S O L E K U V O R M

Küberturvalisuse mänguplatvormi testimisel osalejale

---

1. UURINGU EESMÄRK

Käesolev uuring toetab Tallinna Tehnikaülikooli bakalaureusetööd, mille eesmärk on luua hariv mänguplatvorm küberturvalisuse algteadmiste omandamiseks ja hindamiseks.

2. OSALEMISE SISU

• Platvormil on kokku 48 lühimängu
(12 „ametit“ × 4 mängu iga ameti kohta).

• Mul palutakse:

– valida vabalt mängud ning need läbida
(iga mäng ≈ 3 min; kogu katse kestus sõltub valitud mängude hulgast, eelduslikult 20 – 60 min);

– täita seejärel lühike veebiküsimustik (≈ 10 min).

• Kõigi 48 mängu läbimine ei ole nõutav.

3. VABATAHTLIK OSALUS

• Osalemine on täielikult vabatahtlik.

• Võin uuringu katkestada või jätta küsimustele vastamata igal hetkel tagajärgedeta.

• Soovi korral saan lasta oma andmed kustutada, teatades sellest autoritele hiljemalt 15. maini 2025.

4. KONFIDENTSIAALSUS JA ANDMETE TÖÖTLUS

• Isikut tuvastavaid andmeid (nimi, kontakt jm) ei koguta.

• Tulemused esitatakse bakalaureusetöös ja võimalikes teadus-/konverentsipublikatsioonides üksnes koond- või pseudonüümitud kujul.

• Toorandmeid hoitakse parooliga kaitstud TalTechi serveris ning need kustutatakse hiljemalt 31. detsembril 2025.

5. RISKID JA EELISED

• Uuring ei sisalda terviseriske.

• Võin saada uusi teadmisi küberturvalisusest ning aidata arendada õppemänge.

6. KÜSIMUSED JA KONTAKT

• Carmen Maar — e-post: camaar@taltech.ee

• Kristofer Säälik — e-post: krsaal@taltech.ee

O S A L E J A K I N N I T U S

Olen käesoleva info läbi lugenud, mõistnud osalemise tingimusi ning annan nõusoleku, et minu anonüümsed vastused ja kasutusandmed võivad olla kasutatud bakalaureusetöös ja sellega seotud publikatsioonides.

Osaleja ees- ja perekonnanimi (loetavalt): _____

Allkiri: _____ **Kuupäev:** ____ / ____ / 2025

Lisa 3. Intervjuu ja küsimustik

Taust ja kontekst

1. Millise ameti mänge sa proovisid?*

- Infoturbe juht (CISO)
- Kübersündmuste reageerija
- Küberturbe õigus-, poliitika- ja vastavusspetsialist
- Küberturbe ohuanalüütik
- Küberturvalisuse arhitekt
- Küberturbe audiitor
- Küberturvalisuse koolitaja
- Küberturvalisuse rakendaja
- Küberturvalisuse uurija
- Küberturbe riskijuht
- Digitaalsete tõendite uurija
- Nõrkustestija

2. Millise seadmega mängisid?*

- Arvuti
- Tahvelarvuti
- Nutitelefon

3. Palun hinda oma eelnevaid teadmisi küberturbe teemadel

1 = puuduvad teadmised … 10 = ekspert*

- 1
- 2

- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10

4. Soovi korral lisa kommentaar oma teadmiste kohta

Üldine kasutajakogemus

(5-palliline skaala: 1 = ei nõustu üldse ... 5 = täiesti nõus)

5. Mängude juhised olid selged*

- 1
- 2
- 3
- 4
- 5

6. Navigeerimine veebilehel oli lihtne*

- 1
- 2
- 3
- 4
- 5

7. Graafika ja kujundus olid arusaadavad ning meeldivad*

- 1
- 2
- 3
- 4
- 5

8. Ajakulu ühe mängu läbimiseks oli sobiv*

- 1
- 2
- 3
- 4
- 5

9. Soovi korral kommenteeri midagi nendest vastustest lisaks:

10. Mis vajaks Teie meelest kindlasti mängus muutmist/täiustamist?

11. Mis oli väga hea ja tore loodud lahenduse puhul:

Raskus ja kaasahaaravus

(5-palliline skaala: 1 = ei nõustu üldse … 5 = täiesti nõus)

12. Mängude raskusaste oli minu jaoks paras*

- 1
- 2
- 3
- 4
- 5

13. Mängud hoidsid mu tähelepanu lõpuni*

- 1
- 2
- 3
- 4
- 5

14. Tundsin, et mängud olid selgelt seotud valitud ametiga*

- 1
- 2
- 3
- 4
- 5

15. Soovi korral kommenteeri midagi nendest vastustest lisaks:

Õpitulemused

(5-palliline skaala: 1 = ei nõustu üldse … 5 = täiesti nõus)

16. Sain uusi teadmisi küberturvalisuse valdkonna rollidest/ametitest*

- 1
- 2
- 3
- 4
- 5

17. Sain uusi teadmisi küberturvalisuse erinevatest ülesannetest ja teemadest*

- 1
- 2
- 3
- 4

- 5

18. Tunnen end nüüd kindlamalt turvariske tuvastades*

- 1
- 2
- 3
- 4
- 5

19. Oskan pärast mängimist nimetada vähemalt kaks uut turvariski või head praktikat*

- 1
- 2
- 3
- 4
- 5

20. Soovi korral kommenteeri midagi nendest vastustest lisaks:

Mõju ja motivatsioon

(5-palliline skaala: 1 = ei nõustu üldse … 5 = täiesti nõus)

21. Kavatsen õpitu põhjal oma käitumist muuta*

- 1
- 2
- 3
- 4
- 5

22. Soovitaksin seda platvormi kolleegile või sõbrale*

- 1
- 2
- 3
- 4
- 5

23. Soovi korral kommenteeri midagi nendest vastustest lisaks:

Tehniline toimivus

24. Kas kogesid tehnilisi tõrkeid?*

    - Ei, kõik töötas hästi
    - Mõni väiksem problem
    - Suuri probleeme
    - Ei saanud üldse kasutada

25. *Kui esines vigu, kirjelda neid lühidalt:*

Lõpetuseks

26. **Kui teie oleksite.., siis kasutaksite seda mängu..**

1. üldhariduskoolis õpetajana küberturvalisuse kursusel õpilastega*

- Jah
- Pigem jah
- Pigem ei
- Ei

2. ülikoolis või kutsekoolis õppejõuna küberturvalisuse kursusel tavakasutajatega*

- Jah
- Pigem jah

- Pigem ei
- Ei

3. ülikoolis või kutsekoolis õppejõuna küberturvalisuse kursusel IT-õppijatega*

- Jah
- Pigem jah
- Pigem ei
- Ei

4. koolitaja küberturvalisuse koolitusel tavakasutajatega*

- Jah
- Pigem jah
- Pigem ei
- Ei

5. koolitaja küberturvalisuse koolitusel IT-spetsialistidega*

- Jah
- Pigem jah
- Pigem ei
- Ei

27. Soovite veel midagi lisada?