Prevencinės priemonės kovai su fišingu 4-osios pramonės revoliucijos amžiuje (CyberPhish)

„CyberPhish“ mokymo programos išplėstinė versija

Projekto trukmė: 2020 lapkritis – 2022 lapkritis

Projekto Nr.: 2020-1-LT01-KA203-078070

Funded by the Erasmus+ Programme of the European Union

Projektas finansuojamas Europos Komisijos lėšomis. Leidinyje atspindimos tik autoriaus pažiūros, Komisija negali būti laikoma atsakinga už jame pateikiamą informaciją.

Dokumentų valdymas			
Revizija #	**Revizijos data**	**Apibūdinimas**	**Pavadinimas**
1 Juodraščio versija 1.0	**2021-05-02**	**Pirminis juodraštis**	**MECB Ltd (MT)**
2 Juodraščio versija 2.0	**2021-05-07**	**Atnaujintas juodraštis**	**MECB Ltd (MT)**
3 Juodraščio versija 3.0	**2021-05-09**	**Atnaujintas juodraštis**	**MECB Ltd (MT)**
4 Juodraščio versija 4.0	**2021-05-10**	**Juodraštis atnaujintas remiantis partnerių atsiliepimais**	**MECB Ltd (MT)**
5 Juodraščio versija 5.0	**2021-05-31**	**Juodraštis atnaujintas remiantis ekspertų atsiliepimais**	**MECB Ltd (MT)**
6 Galutinė versija 1.0	**2021-06-08**	**Galutinė versija, skirta platinimui**	**MECB Ltd (MT)**

Turinys

ĮVADAS

„CyberPhish“ išplėstinėje mokymo programoje pateikiama kibernetinio saugumo programa apimanti tris dalis:

- *Error! Reference source not found.* – rekomenduojamas lektorių pasirengimas prieš mokymus.
- ***Error! Reference source not found.*** – rekomendacijos, kaip mokymo programa turėtų būti dėstoma.
- ***Error! Reference source not found.*** – mokymo programos struktūros detalus išdėstymas.

Atkreipiame dėmesį tai, kad mokymo programa yra pritaikyta mokyti taikant mišrųjį būdą, tačiau, dėl savo struktūros programa yra lanksti ir gali būti taikoma tiek netoliniam, tiek kontaktiniam mokymui.

Viso kurso tikslas – supažindinti su kibernetine sauga, didelį dėmesį skiriant sukčiavimo (angl. phishing) atakoms. Kursas skirtas individualiems asmenims, verslininkams, ir sieks pasirengti ketvirtosios pramonės metu kylančiomis saugumo grėsmėmis.

Kurso metu besimokantieji įgis įgūdžių, kaip atpažinti ir valdyti kibernetines atakas, kaip apsaugoti įrenginius ir duomenis.

1. LEKTORIŲ PASIRENGIMAS MOKYMAMS

Šioje dalyje išdėstyta struktūra, kuri skirta pasiruošti mokymo kursui; ši programa yra suformuota taip, jog medžiagą galima dėstyti tiek kontaktiniu, tiek nuotoliniu būdu. Rekomenduojama jo trukmė gali skirtis priklausomai nuo dalyvių skaičiaus, pasirengimo ar pristatymo reikalavimų. Patariama, jog vienoje grupėje neturėtų būti daugiau negu dvylika lektorių.

Mokymų struktūra pateikiama žemiau esančioje lentelėje, kurioje **rekomenduojamos susitikimo su lektoriais temos** ir rekomenduojama paruošimo trukmė. Tačiau mokslo įstaiga ar lektoriai (dėstytojai) gali savo nuožiūra naudoti, pratęsti, sutrumpinti ar pailginti lektorių rengimo trukmę ir turinį, kaip mano esant tinkama ir atsižvelgiant į pačių lektorių ir besimokančiųjų pasirengimą

Svarbu paminėti, jog „lektorių pasirengimas mokymams“ programa skirta asmenims, jau turintiems bendrinių žinių apie kibernetinę saugą.

Mokymų organizatoriai, siekdami nustatyti dėstytojų gebėjimus bei sužinoti, ko tikimasi iš šios programos, galėtų jiems išsiųsti su šiomis temomis susijusį klausimyną. Sulaukę grįžtamojo ryšio, organizatoriai galėtų tinkamai pakoreguoti mokymo renginio darbotvarkę.

Struktūra	„Lektorių pasirengimas mokymams“ programos rekomenduojama keturių dienų trukmė. Mokymų metu siekiama išugdyti tinkamus lektorių įgūdžius bei kompetencijas.	
Tikslas	Išmokyti dėstytojus bazinių tarpininkavimo gebėjimų bei kuo labiau supažindinti su mokymo programa, jog jie galėtų efektyviai mokyti temomis, susijusiomis su kibernetine sauga.	
Programa		
1-oji diena	Lektorius studento vaidmenyje	
Užsiėmimo Nr.	*Užsiėmimas*	*Rekomenduojama trukmė*
D1-01	Įžanga ir susipažinimas • „Ledų pralaužimo“ ar komandos formavimo veiklos, skirtos susipažinimui. - *Socialinio tinklo imitacijos žaidimas („ledų pralaužimas“).* - *„Marshmallow Challenge“ (komandos formavimas).*	30 min.

D1-02	Skirtingų mokymosi metodų supratimas ir jų panaudojimas • Trumpas supažindinimas su skirtingais mokymosi metodais - *Pristatomi skirtingi mokymosi stiliai (pavyzdžiui, 7 mokymosi būdai, Kolb'o modelis), kurie bus naudojami vėlesniuose užsiėmimuose.*	30 min.
D1-03	Lektorius studento vaidmenyje – mokymo metodologijos pritaikymas (1-oji dalis). *Užsiėmimo tikslas – skatinti dėstytojus suprasti ir taikyti skirtingas pedagogines strategijas bei mokymo būdus žvelgiant iš studento perspektyvos. Veikla vyks kontaktiniu arba nuotoliniu būdu, o dėstytojai turės įsijausti į besimokančiojo rolę.* • Įžanga apie skirtingas pedagogines strategijas bei mokymo būdus. - *Pirmoje susitikimo dalyje, mokymus vedantis dėstytojas pristatys skirtingas pedagogines strategijas ir jų taikymo būdus (pavyzdžiui, praktiniai užsiėmimai, diskusijos, debatai, konkrečių pavyzdžių analizavimas ir pan.).* • Skirtingų mokymo būdų taikymas. - *Antroje dalyje lektoriai/besimokantieji taikys šiuos skirtingus mokymo būdus.*	3 valandos
D1-04	Pertrauka	30 min.
D1-05	Lektorius studento vaidmenyje – mokymo metodologijos pritaikymas (2-oji dalis) • Aptarimas, grįžtamasis ryšys, dalinimasis geriausiais būdais. - *Dalinimasis įspūdžiais, nuomone, atsiliepimais apie pirmąją dalį.* - *Dalinimasis geriausiomis strategijomis, kaip pagerinti besimokančiųjų ugdymą.*	1 valanda
D1-06	1-oji diena – apžvalga ir apibendrinimas	30 min.
2-oji diena	Būtinųjų „minkštųjų įgūdžių“ atnaujinimas	
Užsiėmimo Nr.	*Užsiėmimas*	*Rekomenduojama trukmė*
D2-01	2-sios dienos įžanga – „minkštųjų įgūdžių“ svarba • Trumpa įžanga apie „minkštuosius įgūdžius“, kai jie naudojami paskaitos dėstymo metu. - *Trumpas supažindinimas su tokiais metodais, kaip pateiktis, bendradarbiavimas, auditorijos valdymas ir konstruktyvaus grįžtamojo ryšio teikimas.*	30 min.
D2-02	Būtinieji „minkštieji įgūdžiai“, reikalingi mokymo metu (1-oji dalis) • Pranešimų rengimo gebėjimai. - *Pateikties struktūra (pavyzdžiui, skaidrių skaičius, jų formatas, internetinių įrankių nauda).* - *Elgesys pranešimo metu (pavyzdžiui, kūno kalba, balso tonas).* - *Trumpo pranešimo pristatymas (kontaktiniu arba nuotoliniu būdu), po kurio besimokantieji pateikia atsiliepimus bei grįžtamąjį ryšį.* • Bendradarbiavimo gebėjimai. - *Pagalba grupinės diskusijos metu (pavyzdžiui, klausimų analizavimas, peradresavimas ir perfrazavimas).* - *Bendradarbiavimo skatinimas (pavyzdžiui, minčių lietus, minčių žemėlapis, šešios mąstymo skrybėlės ir pan.).*	2 valandos

	• Skaitmeninių įrankių naudojimas, siekiant ugdyti „minkštuosius įgūdžius“. - *Skaitmeninių įrankių naudojimas pateikčių ir diskusijų metu.* - *Pagal poreikį, supažindinimas su skaitmeniniais (internetiniais) įrankiais, įskaitant „Microsoft Teams“, „Zoom“, „Skype“, „Google Meet“, „Mentimeter“, „Kazoom“ ir pan.*	
D2-03	Pertrauka	30 min.
D2-04	Būtinieji „minkštieji įgūdžiai“, reikalingi mokymų metu (2-oji dalis). • Auditorijos valdymas. - *Dalinimasis geriausiomis strategijomis, kaip valdyti, sudominti ir įtraukti besimokančiuosius tiek kontaktiniu, tiek nuotoliniu būdu.* • Konstruktyvaus grįžtamojo ryšio teikimas. - *Trumpa grupinė diskusija (kontaktiniu arba nuotoliniu būdu), kurios metu analizuojami efektyvūs ir konstruktyvūs grįžtamojo ryšio teikimo būdai.*	2 valandos
D2-05	2-oji diena – apžvalga ir apibendrinimas.	30 min.
3-oji diena	Mokymo programos apžvalga	
Užsiėmimo Nr.	*Užsiėmimas*	*Rekomenduojama trukmė*
D3-01	Įžanga apie mokymo programos struktūrą ir mokymo ypatybes. *Trumpas užsiėmimas kontaktiniu arba nuotoliniu būdu, kuris skirtas pristatyti mokymo programos struktūrą, aptarti mokymosi rezultatų svarbą bei ugdymo ypatybes.*	1 valanda
D3-02	Detali mokymo programos temų analizė (1-oji dalis). *Užsiėmimas, skirtas supažindinti su pirmaisiais dviem mokymo programos dalykais (moduliais).*	1 valanda
D3-03	Pertrauka	30 min.
D3-04	Detali mokymo programos temų analizė (2-oji dalis). *Užsiėmimas, skirtas supažindinti su paskutiniaisiais dviem mokymo programos dalykais (moduliais).*	3 valandos
D3-05	3-oji diena – apžvalga ir apibendrinimas	30 min.
4-oji diena	Baigiamasis seminaras – „minkštųjų įgūdžių“ vertinimas pasitelkiant mokymo programą	
Užsiėmimo Nr.	*Užsiėmimas*	*Rekomenduojama trukmė*
D4-01	Įžanga. *Paskutinių užsiėmimų metu, dalyvių bus prašoma pakartoti informaciją, gautą 1-osios dienos metu, pasitelkti įgūdžius, kuriuos lavino 2-ąją dieną, naudotis mokymo programa, apie kurią buvo dėstoma 3-ąją dieną.* *Įvertinimas bus grindžiamas grįžtamuoju ryšiu, gautu iš dalyvaujančių lektorių.* *Užsiėmimų trukmė priklausys nuo to, kiek besimokančiųjų žmonių atvyks.*	30 min.
D4-02	Pranešimo pristatymo įgūdžiai. *Lektorių bus paprašyta paruošti ir pristatyti 10-ies minučių pranešimą. Dalyviai galės rinktis iš visų mokymo programos temų. Nešališkas vertinimas ir grįžtamasis ryšys, įskaitant novatoriškus metodus, bus pateikiami po kiekvieno pristatymo.* Priklausomai nuo dėstytojo nuožiūros, gali būti naudojami kiti įvertinimo būdai.	25 min. kiekvienam dalyviui *(daugiausiai 3 valandos)*

D4-03	Pertrauka	30 min.
D4-04	Bendradarbiavimo įgūdžių vertinimas. *Dėstytojų bus prašoma suorganizuoti 10-ies minučių užsiėmimą. Dalyviai galės rinktis iš visų mokymo programos temų. Nešališkas vertinimas ir grįžtamasis ryšys, įskaitant novatoriškus metodus, bus pateikiami po kiekvieno užsiėmimo.* Priklausomai nuo dėstytojo nuožiūros, gali būti naudojami kiti vertinimo būdai.	25 min. kiekvienam dalyviui *(daugiausiai 3 valandos)*
D4-05	4-oji diena – „Lektorių pasirengimas mokymams“ kurso apžvalga ir apibendrinimas.	30 min.

2. KONTAKTINIS / NUOTOLINIS MOKYMAS

Siekiant besimokantiesiems geriau pritaikyti mokymo programą, naudojamas **4 etapų metodas**. Trumpai apie tai:

VIRTUALUS ĮVADINIS UŽSIĖMIMAS	STUDENTŲ SUTIKIMO RENGINYS	DALYKŲ (MODULIŲ) PRISTATYMAS	INTEGRACINIAI UŽSIĖMIMAI	DALYKŲ (MODULIŲ) PRISTATYMAS	KURSO UŽBAIGIMAS	BAIGIAMASIS TINKLO UŽSIĖMIMAS
Informacija apie mokymo įstaigą - *Tikslai* - *Veiklos kryptis* - *Darbo tvarka*	Įžanga – lektorių prisistatymas Mokymo įstaigos informacijos valdymo sistema - *Informacija sistemoje* - *ID / Slaptažodis* - *Ištekliai* - *Naudojimo politika* - *DUK/Problemų sprendimas* Oficiali kurso programa Vertinimo metodologija Susisiekimo būdai	Dalykų (modulių) pristatymas priklausomai nuo dienai paskirto valandų skaičiaus. 1-oji dalis (15 valandų)	Internetinė gerų mokymo būdų ir kitų strategijų grįžtamojo ryšio forma. Diskusija su besimokančiaisiais.	Dalykų (modulių) pristatymas priklausomai nuo dienai paskirto valandų skaičiaus. 2-oji dalis (15 valandų)	Informacijos surinkimas - *Iš dėstytojų vertinimų* - *Iš studentų skaitmeninių mokymų vertinimo formos*	Grupės diskusija - *Išmoktų dalykų aptarimas* - *Išvados* - *Tolimesni veiksmai*
NUOLATINĖ LEKTORIAUS PARAMA						
TĘSTINIS SISTEMOS PALAIKYMAS						

i. Savarankiškas ir virtualus įvadinis užsiėmimas

Pirmasis orientavimosi žingsnis – dalyvauti **virtualiame įvadiniame** susitikime. Kaip jau atspindi pavadinimas, tai bus savarankiška patirtis, studentai turės galimybę mokytis laisviau ir įgauti žinių apie instituciją (mokymo įstaigą), kuri atsakingą už mokymosi programą.

Besimokantieji turės galimybę labiau įsisavinti informaciją, kuri susijusi su mokymo įstaiga bei konkrečiu jai priklausančiu padaliniu. Išskiriami organizacijos lūkesčiai, tikslai, veiklos kryptis ir darbo tvarka. Be to, užsiėmimas pritaikytas regos ar klausos negalią turintiems studentams, kadangi visa medžiaga bus pasiekiama ekrano skaitytuvais bei pateikiama specialiais subtitrais.

ii. Sutikimo renginys

Naujai studentų grupei rengiamas **sutikimo renginys**. Jis gali vykti tiek kontaktiniu, tiek nuotoliniu būdu. Renginys suteikia puikią galimybę studentams pabendrauti su kitais grupės nariais ar lektoriais, užduoti klausimų bei susipažinti su kurso ypatybėmis.

Svarbu tai, jog gavęs leidimą naudotis mokymo institucijos informacine sistema, lektorius trumpai supažindins su šia sistema. Studentai gaus specialiu naudotojo ID bei galės nustatyti slaptažodžius. Be to, dalyviams bus pateikiami specialūs nurodymai, atsižvelgiant į tai, kokiais ištekliais jie galės naudotis. Taip pat perskaitoma ir pasirašoma naudojimo politika. Atsižvelgiant į tai, kad gali kilti daugybė techninių klausimų, bus sudarytas specialus DUK (dažniausiai užduodamų klausimų) bei problemų sprendimo dokumentas.

Lektorius gali baigti užsiėmimą tuomet, kai atidžiai išdėsto oficialią kurso programą, vertinimo metodologiją bei susisiekimo būdus.

iii. Studentų kompetencijų ugdymas su nuolatinė parama besimokantiesiems

Mokymo įstaiga ne tik ugdo besimokančiųjų žinias, įgūdžius ir požiūrį, susijusius su kibernetinio saugumo studijų dalyku, bet ir pripažįsta, kad svarbu nustatyti besimokančiųjų besikeičiančius poreikius ir į juos reaguoti. Besimokantieji turės galimybę reguliariai susisiekti su dėstytojais, kurie teiks reikalingą pagalbą.

Atlikus nustatytą skaičių užsiėmimų, bus organizuojamas **integracijos seminaras**. Besimokantieji pateiks atsiliepimus bei grįžtamąjį ryšį, iš kurio planuojama nustatyti, ar kurso metu įgytos kompetencijos atitinka studentų lūkesčius bei mokslo institucijos standartus.

Integracijos seminaro metu gali būti pasitelkiami įvairūs vertinimo įrankiai, skirti palengvinti duomenų surinkimo procesą. Programos efektyvumą parodys tokie rodikliai, kurie tiria studentų naujų gebėjimų ir žinių įsisavinimą, dalyvių skaičių, palankiai vertinančių mokymosi patirtį bei jos efektyvumą.

Visi šie duomenys savo ruožtu bus pasitelkiami siekiant pagerinti programos kokybę.

iv. Kurso apibendrinimas ir išvados

Kurso užbaigimas savaime laikomas reikšmingu pasiekimu.

Baigiamasis užsiėmimas turės du tikslus. Pirmiausia besimokantieji tarpusavyje galės porą valandų pasidalinti kurso įspūdžiais. Bet tuo pačiu mokslo įstaiga pasinaudos galimybe įvertinti mokymo programos pasisekimą. Šiam tikslui bus pasitelkiamas Donaldo Kirkpatricko[1] „Keturių etapų vertinimo modelis“.

Prieš užsiėmimą, mokslo įstaiga nagrinės duomenis, gautus iš:

- *lektorių, kurie susiję su besimokančiųjų vertinimu.*
  Šie duomenys pasitarnaus kaip rodiklis, siekiant nustatyti, kaip pasikeitė studentų žinios nuo studijų programos pradžios.
- *studentų.*
  Šiam tikslui bus parengta skaitmeninė programos vertinimo forma. Bus siekiama nustatyti, kaip palankiai besimokantieji vertina šią mokymosi patirtį ir jos pritaikomumą darbovietėse.

Gavus šiuos duomenis, baigiamojo tinklo užsiėmimo metu bus surengta **grupinė diskusija**, kurioje mokslo įstaiga galės kokybiškai ištirti įvairius rodiklius, susijusius su programa, tokius kaip produktyvumas, kokybė ir efektyvumas.

[1] Kirkpatrick, D. L. (1994). *Evaluating training programs: the four levels*, San Franciskas: Berrett-Koehler.

3. MOKYMO PROGRAMOS (NUOTOLINIU BŪDU) STRUKTŪRA

3.1 Programos pagrindinės temos

Mokymo programos tikslas – suteikti daugiau žinių tiek individualiems asmenims, tiek verslininkams, kurie patiria neišvengiamas teigiamas ir neigiamas Pramonės 4.0 pasekmes ir nori pagerinti savo įgūdžius, susijusius su kibernetine sauga.

Mokymo programa sudaryta iš keturių atskirų dalių, pradedant įvadu į kibernetinio saugumo sritį ir su ja susijusius iššūkius, kylančius dėl Pramonės 4.0. Joje gilinamasi į kibernetinį saugumą ir jo teisinius aspektus Europos lygmeniu, taip pat į tai, kaip kibernetinis saugumas skatinamas Europos Sąjungoje.

Atsižvelgiant į socialinės inžinerijos svarbą ir poveikį bei jos ryšį su kibernetinėmis atakomis, šiame kurse aiškinama, kaip atpažinti kibernetines atakas ir kaip su jomis elgtis, kad būtų išvengta didelių ir negrįžtamų padarinių.

Kartu su glaustu įvairių modulių aprašymu, mokymo programoje pateikiami kiekvieno modulio mokymosi rezultatai, siūlomos rekomenduojamos valandos ir mokymosi būdai. Reikėtų pažymėti, kad nors mokymo programoje nurodytas valandų skaičius kiekvienam moduliui, šios valandos laikytinos kontaktinėmis valandomis. Visą mokymo programą sudaro 30 valandų, kurios atitinka 1 ECTS. Rekomenduojama, kad toks pat valandų skaičius kiekvienam moduliui būtų skirtas savarankiškam mokymuisi ir vertinimui.

Dalykas (modulis)	***Dalyko (modulio) tikslas***
1.0 Kibernetinio saugumo įvadas	Supažindinti su kibernetiniu saugumu bei įvairiomis temomis tiek dėstytojus, tiek studentus, besimokančius aukštosiose mokyklose. Pradedama nuo trumpos kibernetinių nusikaltimų tobulėjimo istorijos ir priežasčių, kurios lėmė spartų jų masto augimą, įvairių istorinių etapų bei dabartinės situacijos apibūdinimo. Apibūdinami dėl 4.0 Pramonės kylantys sunkumai, su kuriais susiduria tiek individualūs asmenys, tiek verslininkai. Vieni iš jų yra globalizacija, augantis mobiliųjų technologijų poreikis, debesijos platformos, daiktų internetas ir didieji duomenys. Be to galima paminėti trečiųjų šalių ir nacionalinio masto grėsmes. Dėstytojai galės rasti reikiamos medžiagos, kad supažindintų besimokančiuosius su kibernetinio saugumo sąvoka kartu su įprastais iššūkiais, su kuriais susiduria įmonės, jei įmanoma, pasitelkdami realių atvejų scenarijus. Taip pat bus nagrinėjamos įvairios sąvokos bei žargonai, kurie susiję su kibernetiniu saugumu.
2.0 Kibernetinė sauga Europos Sąjungoje (ES)	Šis modulis supažindina su esama ES politika ir iniciatyvomis, kuriomis siekiama skatinti kibernetinio saugumo koncepciją. Jame taip pat aptariami teisiniai kibernetinio saugumo aspektai tiek ES, tiek visame pasaulyje, supažindinama su daugybe realių šios srities scenarijų ir atvejų analizių. Modulyje apžvelgiamos Kibernetinio saugumo srities tendencijos, įskaitant, bet neapsiribojant statistiniais duomenimis, tendencijomis, atitinkamomis grėsmėmis, teisine, reputacijos ir finansine rizika bei atvejų analize.
3.0 Kibernetinės atakos (socialinė inžinerija ir sukčiavimas (angl. phishing)	Šiame modulyje mokiniai supažindinami su kibernetinėmis atakomis, ypatingą dėmesį skiriant sukčiavimo (angl. phishing) atakoms. Modulyje taip pat išsamiai aptariama socialinės inžinerijos ir atvirkštinės socialinės inžinerijos sąvoka bei aiškinamasi, kaip socialinė inžinerija susijusi su kibernetinėmis atakomis. Modulyje taip pat pristatomos įvairių tipų sukčiavimo (angl. phishing) atakos ir metodai, taip pat pateikiami keli realūs pavyzdžiai iš projekto partnerių šalių.
4.0 Kibernetinių atakų atpažinimas ir apsauga	Šiame modulyje studentai supažindinami su e. saugos sąvoka ir aktyvaus požiūrio į kibernetines grėsmes svarbą, taikant kibernetinės higienos koncepciją. Modulyje taip pat išsamiai aprašoma, kaip atpažinti kibernetines atakas ir kaip su jomis elgtis. Modulis supažindina su reagavimo į incidentus planų kūrimu ir įgyvendinimu, siekiant sumažinti kibernetinių atakų poveikį.

3.2 Detali mokymo nuotoliniu būdu programos struktūra

3.2.1 Kibernetinio saugumo įvadas

Dalyko (modulio) pavadinimas	1.0 Kibernetinio saugumo įvadas
Bendra trukmė *(valandomis / skaidrėmis)*	3 valandos 46–60 skaidrių
Mokymo metodai	Kontaktiniu būdu, Nuotoliniu būdu, Mišriuoju būdu.
Vertinimas	Kontaktiniu būdu ar internetiniu testu.
Dalyko (modulio) siekiniai	• Turėti bendrų kibernetinio saugumo žinių. • Suprasti kibernetinio saugumo keliamus iššūkius. • Suprasti, kaip laikui bėgant keitėsi kibernetinės atakos, dėl kurių atsirado daugiau priemonių, taigi ir kovos su kibernetinėmis atakomis priemonių. • Suprasti, kodėl svarbu sekti kibernetinio saugumo situaciją, ir kodėl būtina nuolat atnaujinti kibernetinio saugumo žinias. • Suprasti įvairias su kibernetiniu saugumu susijusias apibrėžtis.
Išankstiniai reikalavimai	Nėra
Dalyko (modulio) aprašas	Šio modulio tikslas – supažindinti aukštųjų mokyklų dėstytojus ir studentus su kibernetinio saugumo kursu ir jo temomis. Jis pradedamas trumpa kibernetinio saugumo raidos istorija ir jo spartaus augimo priežastimis, taip pat istoriniais etapais ir dabartine padėtimi. Taip pat apibūdinami kibernetinių atakų iššūkiai, su kuriais susiduria asmenys ir įmonės Pramonės 4.0 amžiuje, įskaitant, bet neapsiribojant, sumažėjusias pasaulines ribas, plačiai naudojamas mobiliąsias technologijas, debesų kompiuteriją, daiktų internetą (IoT) ir didžiuosius duomenis. Kiti iššūkiai apima trečiųjų šalių riziką ir didėjančias grėsmes, įskaitant nacionalinių valstybių (angl. nations-states) grėsmes. Dėstytojai galės rasti reikiamos medžiagos, kad supažindintų besimokančiuosius su kibernetinio saugumo sąvoka kartu su įprastais iššūkiais, su kuriais susiduria įmonės, jei įmanoma, pasitelkdami realių atvejų scenarijus. Modulyje taip pat gilinamasi į daugybę Kibernetinio saugumo srityje vartojamų ir sutinkamų apibrėžčių ir žargono.

<table>
<tr><th colspan="4">DALYKO (MODULIO) TEMOS</th></tr>
<tr><td>1.1 Įvadas: ketvirtosios pramonės revoliucijos iššūkiai</td><td colspan="3">• Kibernetinio saugumo įvadas.
• Trumpa kibernetinių nusikaltimų istorija bei priežastys, kurios lėmė spartų jų masto augimą bei dabartinė situacija.
• Problemos su kuriomis susiduria verslas, prieš kurį nukreipiamos kibernetinės atakos.
• Verslui kylantys iššūkiai:
- išnykusios ribos,
- technologijos ir platus jų naudojimas (mobiliosios technologijos),
- debesų kompiuterija,
- sunkumai, susiję su didžiaisiais duomenimis,
- trečiųjų šalių grėsmė,
- daiktų internetas.
• Didėjančių grėsmių iššūkiai.
• Valstybinio mąsto grėsmės.</td></tr>
<tr><td></td><td>Rekomenduojama trukmė
1 val. 30 min.</td><td>Mažiausiai skaidrių
23</td><td>Daugiausiai skaidrių
30</td></tr>
<tr><td>1.2 Kibernetinio saugumo istorija</td><td colspan="3">• Trumpa kibernetinio saugumo istorija, dėl kurios laikui bėgant, keitėsi požiūris į tokio pobūdžio atakas, bei kokie metodai taikomi, siekiant apsisaugoti nuo atakų.
• Lokalių, Europos, tarptautinių atvejų analizė.</td></tr>
<tr><td></td><td>Rekomenduojama trukmė
1 valanda</td><td>Mažiausiai skaidrių
15</td><td>Daugiausiai skaidrių
20</td></tr>
<tr><td>1.3 Kibernetinio saugumo apibrėžimai</td><td colspan="3">• Šioje dalyje nagrinėjami kibernetinio saugumo apibrėžimai ir žargonai bei statistika ir šaltiniai.</td></tr>
<tr><td></td><td>Rekomenduojama trukmė
30 min.</td><td>Mažiausiai skaidrių
8</td><td>Daugiausiai skaidrių
10</td></tr>
</table>

3.2.2 Kibernetinė sauga Europos Sąjungoje (ES)

Dalyko (modulio) pavadinimas	2.0 Kibernetinė sauga Europos Sąjungoje (ES)
Bendra trukmė *(valandomis / skaidrėmis)*	3 valandos 48–67 skaidrės
Mokymo metodai	Kontaktiniu būdu, Nuotoliniu būdu, Mišriuoju būdu, Diskusijomis.
Vertinimas	Kontaktiniu būdu ar internetiniu testu.
Dalyko (modulio) siekiniai	• Suprasti kibernetinio saugumo teisinius aspektus. • Suprasti dabartinės ES politikos kibernetinio saugumo klausimus. • Suprasti ES įstatymus, susijusius su kibernetine sauga. • Susieti ir palyginti kibernetinio saugumo vietos teisės aktus ir ES teisės aktus.
Išankstiniai reikalavimai	Pagrindinės IT ir verslo žinios gali būti naudingos norint geriau suprasti modulį
Dalyko (modulio) aprašymas	Šis modulis supažindina su esama ES politika ir iniciatyvomis, kuriomis siekiama skatinti kibernetinio saugumo koncepciją. Jame taip pat aptariami teisiniai kibernetinio saugumo aspektai tiek ES, tiek visame pasaulyje, supažindinama su daugybe realių šios srities scenarijų ir atvejų analizių. Modulyje apžvelgiamos Kibernetinio saugumo srities tendencijos, įskaitant, bet neapsiribojant statistiniais duomenimis, tendencijomis, atitinkamomis grėsmėmis, teisine, reputacijos ir finansine rizika bei atvejų analize.

<table>
<tr><th colspan="4">DALYKO (MODULIO) TEMOS</th></tr>
<tr><td rowspan="2">2.1 Kibernetinio saugumo ugdymas Europos Sąjungoje</td><td colspan="3">• Trumpas supažindinimas su ES strategijomis bei iniciatyvomis, kuriomis siekiama šviesti asmenis kibernetinio saugumo klausimais.</td></tr>
<tr><td>Rekomenduojama trukmė
1 valanda</td><td>Mažiausiai skaidrių
20</td><td>Daugiausiai skaidrių
30</td></tr>
<tr><td rowspan="2">2.2 Kibernetinio saugumo teisiniai aspektai</td><td colspan="3">• ES teisiniai aspektai bei atsakomybė, kuri gresia už jų nesilaikymą bei bendrinis tarptautinių teisinių aspektų aptarimas.
• ES ir tarptautinių kibernetinio saugumo įstatymų santykis, palyginimas ir skirtumai.</td></tr>
<tr><td>Rekomenduojama trukmė
30 min.</td><td>Mažiausiai skaidrių
5</td><td>Daugiausiai skaidrių
7</td></tr>
<tr><td rowspan="2">2.3 Kibernetinio saugumo tendencijų apžvalga</td><td colspan="3">• Realių pavyzdžių pristatymas bei atvejų analizė kartu su statistika, tendencijomis, potencialiomis grėsmėmis ir galima žala (teisine, įvaizdžio ar finansine prasme).
• Žvilgsnis į pastaruoju metu įvykdytas kibernetines atakas bei diskusija auditorijoje apie kompetencijos svarbą, kurią dėl kibernetinių atakų, asmenys privalo nuolatos gerinti.
Pastaba: diskusija gali vykti tiek kontaktiniu, tiek nuotoliniu būdu padedant dėstytojui, kuris nustato diskusijos tvarką ir pabrėžia, ko iš jos galima tikėtis.</td></tr>
<tr><td>Rekomenduojama trukmė
1 val. 30 min.</td><td>Mažiausiai skaidrių
23</td><td>Daugiausiai skaidrių
30</td></tr>
</table>

3.2.3 Kibernetinės atakos (socialinė inžinerija ir sukčiavimas (angl. phishing))

Dalyko (modulio) pavadinimas	3.0 Kibernetinės atakos (socialinė inžinerija ir sukčiavimas (angl. phishing))
Bendra trukmė *(valandomis / skaidrėmis)*	10 valandų 150–200 skaidrių
Mokymo metodai	Kontaktiniu būdu, Nuotoliniu būdu, Mišriuoju būdu, Interaktyvių įrankių naudojimas (pvz. internetinių situacijų įrankių), Diskusijos.
Vertinimas	Kontaktiniu būdu ar internetiniu testu.
Dalyko (modulio) siekiniai	• Suprasti kibernetinių atakų sąvoką. • Išmanyti socialinės inžinerijos ir atvirkštinės socialinės inžinerijos apibrėžimą. • Suprasti socialinės inžinerijos būdus ir jos ryšį su kibernetinėmis atakomis. • Suprasti dažniausiai pasitaikančias kibernetinio saugumo grėsmes. • Suprasti pagrindines kibernetinių atakų kategorijas ir metodus.
Išankstiniai reikalavimai	Pagrindinės IT ir verslo žinios gali būti naudingos, norint geriau suprasti modulį.
Dalyko (modulio) aprašas	Bus siekiama supažindinti studentus su kibernetinėmis atakomis, didelį dėmesį skiriant sukčiavimui (angl. phishing). Taip pat bus nagrinėjama socialinės inžinerijos bei atvirkštinės socialinės inžinerijos pritaikymas kibernetinių išpuolių metu. Dalyke bus nagrinėjami skirtingi sukčiavimo (angl. phishing) atakų tipai ir metodika kartu su pateikiamais realiais pavyzdžiais iš projekte dalyvaujančių partnerių šalių.

<table>
<tr><th colspan="4">DALYKO (MODULIO) TEMOS</th></tr>
<tr><td>3.1</td><td>Kibernetinių atakų įvadas</td><td colspan="2">• Trumpas kibernetinių atakų įvadas skiriant didelį dėmesį sukčiavimui (angl. phishing).</td></tr>
<tr><td colspan="2"></td><td>Rekomenduojama trukmė
30 min.</td><td>Mažiausiai skaidrių
8
Daugiausiai skaidrių
10</td></tr>
<tr><td>3.2</td><td>Socialinės inžinerijos moduliai ir manipuliacija</td><td colspan="2">• Socialinės inžinerijos modelių apžvalga, skiriant didelį dėmesį:
a) R. Cialdini „Įtikinėjimo principai“[2]:
- apsikeitimas (angl. Reciprocation),
- įsipareigojimas ir nuoseklumas (angl. Commitment and consistency),
- priimtinumas (žmonės linkę pritarti daugumos nuomonei, angl. Social proof),
- simpatijoms (žmonės linkę padėti asmenims, kurie jiems patinka angl. Liking),
- valdžia, autoritetas (angl. Authority),
- trūkumas, stygius (žmonės neretai trokšta dalykų, kurių neturi).
b) Socialinės inžinerijos psichologiniai aspektai.
c) Atvirkštinės socialinės inžinerijos apžvalga.</td></tr>
<tr><td colspan="2"></td><td>Rekomenduojama trukmė
4 valandos</td><td>Mažiausiai skaidrių
60
Daugiausiai skaidrių
80</td></tr>
<tr><td>3.3</td><td>Skirtingi sukčiavimo (angl. phishing) atakų tipai ir kategorijos</td><td colspan="2">• Skirtingi kibernetinių atakų, ypač sukčiavimo (angl. phishing), tipai bei kaip juos atpažinti.
Kategorijos:
- su BDAR (Bendruoju duomenų apsaugos reglamentu) susijusios atakos,
- elektroniniai laiškai,
- tiesioginio susirašinėjimo žinutės,
- socialiniai tinklai,
- svetainės,
- netikrų loterijų pranešimai,
- SMS žinutės,
- telefoniniai skambučiai,
- gyvai vykstantys susitikimai,
- duomenų vagystė paslapčia stebint duomenis vedantį asmenį.
Atakų tipai:
- „Spray and pray“ (el. laiškai siekiant pavogti konfidencialią informaciją),
- „Spear phishing“ (personalizuotas sukčiavimas (angl. phishing)),
- „Whaling“ (bandymas pavogti konfidencialią informaciją ir dažnai nukreiptas į aukščiausią vadovybę),
- „Vishing“ (telefoninis sukčiavimas),</td></tr>
</table>

[2] Cialdini, R. B. (2016). *Pre-Suasion: A Revolutionary Way to Influence and Persuade*, Niujorkas: Simon & Schuster. ISBN 978-1501109799.

<table>
<tr><td></td><td colspan="3">- „Smishinf“ (sukčiavimas SMS žinutėmis),
- „Angler Phishing“ (sukčiavimas socialiniuose tinkluose),
- „Clone Phishing“ (tikrų laiškų turinio panaudojimas sukčiavimui),
- „Malwertising“ (kenkėjiškas turinys reklamose).</td></tr>
<tr><td></td><td>Rekomenduojama trukmė
4 valandos</td><td>Mažiausiai skaidrių
60</td><td>Daugiausiai skaidrių
80</td></tr>
<tr><td>3.4 Konkrečių pavyzdžių nagrinėjimas</td><td colspan="3">• Kelių skirtingų partnerių organizacijų pavyzdžių pristatymas ir nagrinėjimas.
• Kontaktiniu ar nuotoliniu būdu vykstanti diskusija nedidelėse grupėse (sudarytose iš 5-6 studentų).
Pastaba: studentų bus prašoma ne tik diskutuoti, bet ir analizuoti neseniai įvykdytą sukčiavimo (angl. phishing) ataką bei paminėti svarbias detales, tokias kaip atakos data, informacija apie auką, atakos pobūdis, kokios jos pasekmės, išmoktos pamokos ir pan. Po to, grupė išrinks vieną atstovą, kuris pristatys analizės rezultatus visai auditorijai. Tada dėstytojai ir kiti studentai pateiks konstruktyvų grįžtamąjį ryšį.</td></tr>
<tr><td></td><td>Rekomenduojama trukmė
1 val. 30 min.</td><td>Mažiausiai skaidrių
22</td><td>Daugiausiai skaidrių
30</td></tr>
</table>

3.2.4 Kibernetinių atakų atpažinimas ir apsauga

Dalyko (modulio) pavadinimas	4.0 Kibernetinių atakų atpažinimas ir apsauga
Bendra trukmė *(valandomis / skaidrėmis)*	14 valandų 210–255 skaidrės
Mokymo metodai	Kontaktiniu būdu, Nuotoliniu būdu, Mišriuoju būdu.
Įvertinimas	Kontaktiniu būdu ar internetiniu testu.
Dalyko (modulio) siekiniai	• Įgyti pagrindinių žinių apie e. saugą ir saugumas. • Suprasti skirtingą informacijos turinį. • Išmanyti tapatybės apibrėžimą bei gebėti atskirti atakas, nukreiptas prieš asmeninius duomenis. • Suprasti potencialių kibernetinių atakų pasekmes, kurios nukreipiamos prieš individualius asmenis ar/ir tam tikras organizacijas. • Apibrėžti ir suprasti kibernetinės higienos sąvoką bei aptarti jos svarbą gynybos prieš kibernetines atakas procese. • Suprasti ir taikyti įvairius apsaugos nuo kibernetinių atakų metodus. • Gebėti parengti ir pritaikyti kibernetinio incidento valdymo planą.
Išankstiniai reikalavimai	Ankstesni dalykai (moduliai)
Dalyko (modulio) aprašas	Dalyko metu siekiama supažindinti studentus su kibernetinio saugumo sąvoka bei su iniciatyvumo svarba, taikant kibernetinės higienos koncepciją ir siekiant apsisaugoti nuo virtualių atakų. Modulyje taip pat išsamiai aprašoma, kaip atpažinti kibernetines atakas ir kaip su jomis elgtis. Modulis supažindina su reagavimo į incidentus planų kūrimu ir įgyvendinimu, siekiant sumažinti kibernetinių atakų poveikį.

<table>
<tr><th colspan="4">DALYKO (MODULIO) TEMOS</th></tr>
<tr><td>4.1 Pagrindinės žinios apie e. saugumą</td><td colspan="3">

Informacijos turinio skirtumai (laisvai prieinami duomenys, asmeninė, verslo informacija ir kt.); intelektinė nuosavybė; autorių teisės.
Suprasti tapatybės sąvoką; žinoti apie tapatybės vagystę ir vagystės būdus. Žinoti apie šnipinėjimo programas, klaviatūros šnipinėjimą, sukčiavimo strategijomis, kurios naudojamos parduodant prekes, Trojos arklius. Žinoti įvairius būdus, kaip kenkėjiška programinė įranga gali patekti į įrenginį.
Žinoti apie tapatybės ir asmens duomenų vagysčių darbe ir internete priežastis ir pasekmes (apgaulingas informacijos naudojimas, informacijos praradimo grėsmė, tam tikri sąmokslai).
Žinoti apie grėsmes, susijusias su asmens duomenų atskleidimu.
Trumpai supažindinti su kibernetinių atakų poveikiu asmeniui ir organizacijai. Išsamesnė informacija bus nagrinėjama 4.4 skirsnyje.

<table>
<tr><td>Rekomenduojama trukmė
30 min.</td><td>Mažiausiai skaidrių
8</td><td>Daugiausiai skaidrių
10</td></tr>
</table>
</td></tr>
<tr><td>4.2 Prevencinės priemonės</td><td colspan="3">

Kibernetinė higiena internete (kuo mažiau informacijos apie asmenis, įskaitant asmenines paskyras socialinėje žiniasklaidoje, kadangi ši informacija gali tapti sukčių taikiniu).
Kibernetinė higiena darbo vietoje.
Speciali įranga ir technologijos (filtrai ir apgaulingų el. laiškų blokavimas).

<table>
<tr><td>Rekomenduojama trukmė
2 valandos</td><td>Mažiausiai skaidrių
30</td><td>Daugiausiai skaidrių
35</td></tr>
</table>
</td></tr>
<tr><td>4.3 Kibernetinių atakų atpažinimas</td><td colspan="3">

Atvejų analizė pasitelkiant 3.3 skyriuje „Skirtingi sukčiavimo (angl. phishing) atakų tipai ir kategorijos“ aprašytus metodus.
Kibernetinių atakų atpažinimas (atsižvelgiant į ankstesnio skyriaus punktus), įskaitant, bet neapsiribojant:

kritinis mąstymas,
laiške esančios nuorodos tikrinimas jos nepaspaudžiant,
supratimas, kas yra URL,
pranešimų analizė,
pagrindinių požymių (angl. red flags) atpažinimas.

<table>
<tr><td>Rekomenduojama trukmė
5 valandos</td><td>Mažiausiai skaidrių
75</td><td>Daugiausiai skaidrių
90</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td>4.4</td><td>Kibernetinių atakų valdymas</td><td colspan="3">

Kibernetinio saugumo vadovas, skirtas šios srities žinių gilinimui bei dalis, kurioje aptariama asmenims bei organizacijoms padaryta žala.
Dalis veiksnių, kurie padeda apsisaugoti nuo kibernetinių atakų:
- saugi navigacija,
- patikimi ir „stiprūs“ slaptažodžiai,
- atakų vengimas,
- saugus apsipirkimas internete,
- specialios programos, skirtos kovoti su kibernetinėmis atakomis,
- darbas su slapukais,
- atsarginių duomenų kopijų kūrimas,
- failų šifravimas,
- dviejų veiksnių (žingsnių) autentifikavimas,
- kenkėjiška programinė įranga,
- saugus naršymas.
Lokalių, Europos ir tarptautinių atvejų analizė.
Nuosekliai aptariamas kiekvienas instrukcijos žingsnis bei iliustracijos.
Pateikiami reagavimo į kibernetinę ataką veiksmai, kurių gali imtis nukentėjęs asmuo arba įmonė bei tai, kokių priemonių imtis siekiant atitaisyti žalą.

<table>
<tr><td>Rekomenduojama trukmė
5 valandos</td><td>Mažiausiai skaidrių
75</td><td>Daugiausiai skaidrių
90</td></tr>
</table>
</td></tr>
<tr><td>4.5</td><td>Žalos sumažinimas pasinaudojant incidento valdymo planu</td><td colspan="3">

Sukurti, parengti ir įgyvendinti reagavimo į incidentus planą, kuriame nurodomi siūlomi ir geriausios praktikos metodai, taikytini įvykus duomenų saugumo pažeidimo incidentui.
Pastaba: šią dalį galima pritaikyti priklausomai nuo šalyje taikomų būdų.

<table>
<tr><td>Rekomenduojama trukmė
1 val. 30 min.</td><td>Mažiausiai skaidrių
22</td><td>Daugiausiai skaidrių
30</td></tr>
</table>
</td></tr>
</table>