



PLÁN [OBNOVY]

Nitrianske kompetenčné centrum kybernetickej bezpečnosti
Fakulta prírodných vied a informatiky
Univerzita Konštantína Filozofa v Nitre
Tr. A. Hlinku 1, 949 01 Nitra

KYBERNETICKÁ BEZPEČNOSŤ V MINECRAFT EDUCATION

Predmet: KI/bUZDHV/22 – Digitálne hry vo vzdelávaní

Téma

Vstavaná knižnica herného prostredia Minecraft Education obsahuje vzdelávacie svety zamerané na rôzne témy z oblasti kybernetickej bezpečnosti. Študenti učiteľstva si vybrané svety vyskúšajú v roli žiaka. Svoju skúsenosť s učením sa založeným na hre reflektujú aj z pedagogického hľadiska.

Viera Michaličková
vmichalickova@ukf.sk

Obsah

Abstrakt	2
Cieľová skupina	2
Požiadavky	3
Rozsah a formát	3
Obsah	3
Kybernetická bezpečnosť v minecraftových vzdelávacích svetoch.....	4
Kybernetická bezpečnosť (Cyber Safe)	4
Kybernetické základy (Cyber Fundamentals).....	5
Kybernetický expert (Cyber Expert).....	5
Práca so vzdelávacími svetmi	5
Charakteristika vybraného sveta – Všade dobre, doma .. hmm	6
Charakteristika vybraného sveta – Sieťoví hrdinovia.....	9

Abstrakt

Tento materiál je určený pre študentov bakalárskeho štúdia učiteľstva akademických predmetov so záujmom o využívanie digitálnych hier vo vzdelávaní a kybernetickú bezpečnosť. Cieľom je predstaviť študentom vzdelávacie svety zo vstavanej knižnice Minecraft Education, ktoré hravou formou sprostredkujú vedomosti o ochrane osobných údajov, bezpečnej komunikácii v online prostredí a prevencii kybernetických útokov. Študenti zažijú aktivity vo vybranom vzdelávacom svete v roli žiaka. Analyzujú ich z obsahovej aj formálnej stránky, hodnotia ich vzdelávací potenciál. Aktivity vo vzdelávacích svetoch podporujú kritické myslenie, budovanie návykov bezpečného správania sa na internete a motivujú k ďalšiemu štúdiu. Materiál kladie dôraz na praktické skúsenosti, metodickú prípravu a reflexiu zážitku z hry.

Autori

Autor: PaedDr. Viera Michaličková, PhD.

Email: vmichalickova@ukf.sk

Univerzita: Fakulta prírodných vied a informatiky, Univerzita Konštantína Filozofa v Nitre

Cieľová skupina

Obsah tohto materiálu je určený pre študentov v bakalárskom študijnom programe Učiteľstvo akademických predmetov (bez ohľadu na aprobačné predmety), ktorí navštevujú povinne voliteľný predmet *Digitálne hry vo vzdelávaní*. Osobitnou skupinou sú študenti učiteľstva informatiky, od ktorých sa očakáva hlbší záujem o tému kybernetickej bezpečnosti a metodiku vyučovania tejto témy v predmete informatika na základnej a strednej škole.

Vzdelávacie ciele

- Študenti získajú prehľad o obsahu a dizajne vzdelávacích svetov zameraných na tému kybernetickej bezpečnosti, ktoré sú dostupné vo vstavanej knižnici herného prostredia Minecraft Education. Vybrané vzdelávacie svety zažijú v roli žiaka a zhodnotia jeho kvalitu a použiteľnosť z pohľadu budúceho učiteľa.
- Študenti budú schopní vybrať vhodný vzdelávací svet a použiť ho v praxi vo formálnom alebo neformálnom vzdelávaní.
- Študenti sa zoznámia alebo si zopakujú koncepty a postupy súvisiace s kybernetickou bezpečnosťou, ktoré sú užitočné aj pre ich osobný alebo pracovný život.

Východiskové predpoklady a požiadavky na účastníkov

- Študent vie charakterizovať učenie sa založené na hre (*game-based learning*), špeciálne na digitálnej hre, pozná jeho benefity aj možné riziká, je schopný uviesť rôzne príklady digitálnych hier používaných vo formálnom a neformálnom vzdelávaní.
- Študent je zručný v používaní prostredia Minecraft Education. Dokáže vytvárať a budovať vlastný svet, pracovať vo svete z knižnice, identifikovať vzdelávacie ciele aktivity realizovanej v hre, vyhľadať a zhodnotiť zdroje pre vyučovanie v prostredí Minecraft Education, importovať/exportovať svet, zdieľať svet s inými hráčmi (žiakmi).
- Študent pozná nástroje prostredia Minecraft Education pre formatívne hodnotenie, spätnú väzbu a kolaboráciu. Je schopný uviesť príklady ich zmysluplného použitia v praxi.

Použité metódy

- prednáška, práca vo dvojici, diskusia

Požiadavky

Prístrojové vybavenie

- počítače alebo tablety so softvérom Minecraft Education (dostupné v Microsoft Store)

Priestorové požiadavky

- interiér, počítačová učebňa

Veľkosť skupiny

- prezentované aktivity je vhodné realizovať so skupinou 6 – 20 študentov

Ďalšie požiadavky

- študenti musia mať školské Office 365 účty, ktorými sa prihlásia do Minecraft Education

Rozsah a formát

- Trvanie: 3 hodiny
- Forma: prezenčne

Obsah

Kybernetická bezpečnosť je súbor procesov, osvedčených postupov a technologických riešení, ktoré pomáhajú chrániť kritické systémy a počítačovú sieť pred útokmi. V online priestore sme z rôznych dôvodov prítomní a aktívni denne. A to nielen dospelí používatelia, ale aj mladí ľudia a deti. Riziko kybernetických útokov, ktoré sa môžu priamo dotknúť každého z nás (príp. školy, organizácie, firmy, v ktorej študujeme alebo pracujeme) je potrebné nielen poznať, ale naučiť sa mu aj účinne čeliť. Tejto téme je preto nutné venovať mimoriadnu pozornosť aj v školskom vyučovaní alebo v neformálnom vzdelávaní, spôsobom primeraným veku žiakov.

Minecraft Education ponúka kvalitné vzdelávacie svety (mapy), v ktorých sa žiaci oboznamujú s konceptami kybernetickej bezpečnosti formou atraktívnej digitálnej hry. Sú vtiahnutí do príbehu, získavajú potrebné informácie a praktické rady, riešia konkrétne problémy, rozvíjajú si kritické myslenie. Zažívajú úspech z odvrátenia hrozby útoku či vyriešenia bezpečnostného incidentu. Táto skúsenosť môže byť motivujúca aj pre ich ďalšie štúdium či budúcu kariéru v oblasti kybernetickej bezpečnosti.

Na Obr. 1 vidíme aktuálny obsah kategórie *Kybernetika* v knižnici vstavaných svetov prostredia Minecraft Education, ktoré boli vytvorené v súlade so štandardami Cyber.org a CSTA. Vzdelávacie štandardy na Slovensku nemusia korešpondovať s tými, aké predpokladajú autori vzdelávacích svetov, učiteľ musí preto sám zvážiť, ktorý zo svetov môže do svojho vyučovania integrovať.



Obr. 1 Gradovaná séria vzdelávacích svetov o kybernetickej bezpečnosti v Minecraft Education¹

Kybernetická bezpečnosť v minecraftových vzdelávacích svetoch



Úloha 1:

Vyhľadajte v knižnici Minecraft Education kategóriu vzdelávacích svetov zameraných na kybernetickú bezpečnosť.

Koľko svetov obsahuje?

Pre koho sú určené?

Na aké témy sú zamerané?

Kybernetická bezpečnosť (Cyber Safe)

V tejto kolekcií sa nachádzajú svety vhodné najmä pre žiakov nižšieho sekundárneho vzdelávania (resp. 2. a 3. cyklus podľa aktuálnej kurikulárnej reformy). Sú úvodom do problematiky. Zameriavajú sa na základné koncepty a postupy, ktoré sú dôležité pre ochranu osobných údajov a bezpečnú komunikáciu detí v prostredí internetu. Stavajú na konkrétnych skúsenostiach detí z bežného života:

Všade dobre, doma ... hmm – žiaci sa učia, ako sa správať, aby boli na internete v bezpečí, trénujú si stratégiu: „Najprv sa zastav, porozmýšľaj a až potom klikaj!“

Fenomén v oblasti ochrany osobných údajov – žiaci sa dozvedia, čo sú to osobné údaje, kto by mal mať prístup k ich osobným údajom a ako ich chrániť.

¹ Zdroj: <https://learn.microsoft.com/en-us/training/modules/teach-cybersecurity-concepts-minecraft-education/cybersecurity-learning-pathway-minecraft-education>

Dobrá hra – žiaci sa učia o budovaní zdravých návykov a bezpečných postupoch pri hraní online hier s cieľom vytvoriť lepšiu online komunitu.

Cloudcraft – žiaci zisťujú, akú dôležitú úlohu zohrávajú dátové centrá v 21. storočí, čo všetko je potrebné pre ich bezpečnú prevádzku a garantovanie prístupnosti cloudových služieb.

Hlbšie skúmanie – žiaci sa kriticky zamýšľajú nad zmysluplným, etickým a bezpečným používaním nástrojov umelej inteligencie pri práci na školskom STEAM projekte.

Zlé pripojenie – príbeh je rozdelený do štyroch dejstiev. V úvodnej časti sa žiaci zoznamujú s hlavnými postavami a pripájajú sa do školského chatu. Následne sa stretávajú s prvými varovnými signálmi, keď neznáma osoba žiada osobné údaje, a učia sa využívať nástroje na nahlasovanie nevhodného správania. V ďalšej fáze čelia rastúcemu tlaku zo strany rovesníkov, kyberšikane a toxickej skupinovej atmosfére. Záverečné dejstvo ukazuje eskaláciu vyhrážok a zdôrazňuje význam zverenia sa dôveryhodnej dospeléj osobe, pričom ponúka viacero možných zakončení príbehu

Kybernetické základy (Cyber Fundamentals)

V tejto kolekcií sa nachádzajú svety, ktoré na seba obsahovo nadväzujú. Sú vhodné pre vyučovanie základov kybernetickej bezpečnosti v sekundárnom vzdelávaní:

Sieťoví hrdinovia – žiaci sa dozvedia o sieťových komponentoch, ochrane prístupu silným heslom, šifrovaní komunikácie a škodlivom softvéri (malvéri).

Interceptory – žiaci sa zaoberajú významom viacfaktorovej autentifikácie, spoznávajú typické zloženie a náplň práce tímov pre riešenie bezpečnostných incidentov.

Šampióni cloudu – žiaci uvažujú o digitálnych stopách, spôsoboch ukladania a význame zálohovania dát, o internete vecí a ich zraniteľnostiach.

Kybernetický expert (Cyber Expert)

V tejto kolekcií sa nachádzajú svety, ktoré zaujmú spracovaním aj starších študentov strednej školy:

Kryptické šifry – žiaci sa zaoberajú témami šifrovania a dešifrovania, integritou dát a sociálnym inžinierstvom.

Odvážna obrana – žiaci sa učia o firewall, útokoch DoS/DDoS a systémoch kontroly prístupu.

Malvérový chaos – žiaci sa dozvedia viac o malvéri, ransomvéri a zálohovaní dát.

Kybernetický obranca – svet môžeme zaradiť obsahovo do tejto kolekcie, hoci v knižnici tvorí samostatnú položku. Pokrýva problematiku kybernetickej bezpečnosti komplexne, formou taktickej hry typu „tower defence“.

Práca so vzdelávacími svetmi



Úloha 2:

Preskúmajte vybrané svety z prvej kolekcie (*Cyber Safe*). Pracujte v dvojčlenných tímoch.

1. prezrite si metodickú podporu pre vzdelávací svet dostupnú na webe,

2. prejdite aktivitami vo svete tak, ako by ich realizoval žiak,
3. priebežne sledujte, aký cieľ, obsah a formu majú jednotlivé aktivity,
4. všímajte si vzdelávacie prvky vložené do prostredia hry.

Pripravte a prezentujte stručnú správu so svojimi zisteniami a kritickým hodnotením zvoleného vzdelávacieho sveta.

Metodická poznámka

Zadanie úlohy v uvedenej podobe je vhodné pre skupinu študentov, ktorí neštudujú učiteľstvo informatiky. Svety z prvej kolekcie sú určené pre mladších žiakov a nevyžadujú od učiteľov, ktorí by ich vo vyučovaní použili, odborné informatické vzdelanie.

Aby bola praktická časť vyučovacej hodiny efektívna, odporúčame pripraviť študentom pracovný hárok, do ktorého by priebežne a prehľadne zaznamenávali svoju skúsenosť. Práca vo dvojici je výhodná aj preto, aby sa študenti pri aktivitách v hernom prostredí a zapisovaní poznámok mohli vystriedať.

Výber svetov môžeme realizovať žrebovaním alebo dohodou tak, aby študenti v skupine preskúmali viaceré svety z tejto kolekcie. Niektoré (najnovšie) svety nemusia byť preložené do slovenského jazyka, resp. zatiaľ nepodporujú automatický preklad. V niektorých dialógoch s NPC sa zriedkavo objavujú štylistické chyby spôsobené automatickým prekladom. Texty na tabuliach nie sú prekladané automaticky. Pre preklad textu alebo jeho prečítanie je možné použiť imerznú čítačku. Metodické materiály na oficiálnom webe sú v anglickom jazyku, sú spracované názorne, s náhľadmi obrazoviek z hry, návodmi na riešenie, s pomocnými pracovnými listami a prezentáciami, ktoré je po preklade alebo adaptovaní možné využívať pri práci so žiakmi.

Po skončení práce vo vzdelávacích svetoch jednotlivé tímy stručne predstavia skúmaný svet spolužiakom a zhodnotia jeho herný dizajn a vzdelávací potenciál.

Charakteristika vybraného sveta – Všade dobre, doma .. hmm



Obr. 2 Vzdelávací svet Všade dobre, doma .. hmm

Žiaci realizujú v tomto svete postupne 4 aktivity:

Aktivita 1: Grieferi (používatelia, ktorí zámerne kazia zážitok ostatným, napr. v online hrách), trollovia (ľudia, ktorí provokujú a vyvolávajú konflikty), cudzinci (neznáme osoby na internete). Čo s nimi? V tejto aktivite sa žiaci dozvedia, aké dôležité je overovať si identitu v prípade žiadosti o priateľstvo a nekomunikovať s neznámymi osobami. Žiak sa rozhoduje medzi viacerými žiadosťami o priateľstvo od používateľov s podobnými nickmi ako spolužiak zo školy, s ktorým sa chce hrať.

Aktivita 2: Je v poriadku zdieľať svoje heslo? V tejto aktivite majú žiaci za úlohu prejsť údajne nezvládnuteľným bludiskom. Neznámy hráč (NPC) im ponúka cheatovacie kódy výmenou za poskytnutie hesla. Žiaci sa dozvedia, aké dôležité je uchovávať svoje osobné údaje v bezpečí (nerozumné správanie má následky). Žiak má možnosť úspešne prejsť bludiskom aj sám, bez poskytnutia hesla neznámej osobe a vyslúži si pochvalu od autora bludiska. V prípade, že heslo poskytne, získa spätnú väzbu s vysvetlením. Aby zachránil situáciu, musí pozbierať v miestnosti rozhádzané osobné údaje s cieľom ochrániť ich. Popritom sa naučí, čo všetko sú jeho osobné údaje.

Aktivita 3: Objednávanie vecí online je pre mnohých ľudí bežnou činnosťou, ktorú realizujú veľmi často a automaticky. Ak si však nedáme pozor, pri takýchto nákupoch môže dôjsť k zneužitiu osobných údajov a prideme o peniaze! V tejto aktivite žiaci dostanú e-mailovú správu o svojej nedávnej objednávke. V správe sa požadujú informácie o bankovom účte, aby sa „vyriešil problém s dorúčením“. Žiaci sa dozvedia o nebezpečenstvách phishingových schém (keď sa útočník vydáva za súčasť skutočnej spoločnosti, aby ukradol informácie o účte). Objednávka v hre sa týka emeraldového brnenia. Žiak vyrieši problém tak, že priamo vo firme, kam sa v hre dostane, komunikuje s pracovníkom, ktorý má dodávku na starosti. Naliehajúcemu podvodníkovi prihlasovacie údaje neposkytne.

Aktivita 4: Keď nakupujeme online, vyhľadávače nám môžu pomôcť nájsť vhodný e-shop. Spoločnosti však môžu zaplatiť za umiestnenie svojej stránky na popredných miestach vo vyhľadávaní a úmyselne spotrebiteľa oklamať! V tejto aktivite sa žiaci naučia, aké dôležité je pri vyhľadávaní overovať dôveryhodnosť zdrojov a nie vždy veriť všetkému, čo vidia alebo čítajú na internete. Žiak má cez internet objednať tekvicový koláč od konkrétnej reštaurácie. Vo výsledkoch vyhľadávania sú však aj úplne iné firmy, ktoré lákajú reklamou. Žiak sa musí rozhodnúť, od koho bezpečne nakúpi. Jednotlivé klamlivé reklamy reprezentujú NPC postavy, ktorých ponuky musí žiak aktívne odmietnuť.

Žiaci si v týchto aktivitách precvičujú kritické myslenie, aby mohli prijímať zodpovedné a bezpečné rozhodnutia. Do hry je zakomponovaná postava dôveryhodného dospelého, na ktorého sa žiak môže obrátiť so žiadosťou o pomoc (tak ako to má robiť v skutočnom živote).

Dôveryhodný dospelý sprevádza žiaka medzi aktivitami, vždy upozorní na to, čo bude alebo čo bolo dôležité. Ak sa v hre žiak nevie samostatne rozhodnúť, môže požiadať o dodatočnú radu, ako má postupovať. Ak sa rozhodne zle, má možnosť rozhodnutie napraviť.

Hra rozpráva príbeh a vŕha žiaka do scenárov, v ktorých musí riešiť konkrétne problémy a upevňovať si návyky bezpečného správania sa v prostredí internetu. Dôraz sa kladie na to, aby sa žiak vždy najprv zastavil a porozmýšľal o tom, prečo je vyzývaný na kliknutie. V hre sa upriamuje pozornosť aj na limitovanie času stráveného pri obrazovke (dôveryhodný dospelý musí dať súhlas na použitie počítača, spoluhráč z online hry sa rozlúči po dohratí hry s tým, že musí ísť robiť domácu úlohu a pod.).

Svet obsahuje zaujímavé prvky – počítač, na ktorom žiak číta e-mailové správy, presuny do kontextu scenárov na banskom vozíku jazdou po horskej dráhe, možnosť zahrať si minihry (bludisko, parkúr).

Závěrečnou odmenou je okrem certifikátu aj brnenie, ktoré si postava hráča môže obliecť a koláč, ktorý môže v hre zjesť. Postavy, ktoré žiak stretol v hre, na konci hry zopakujú užitočné tipy pre bezpečné správanie sa na internete.

Prácu vo svete je potrebné ukončiť spoločnou reflexiou so žiakmi a zhrnutím problémových situácií, podstatných konceptov a odporúčaných postupov. Príklady otázok:

- Ktorá aktivita sa vám páčila najviac?
- Uveďte príklad pozitívnej (dobrej) veci na internete.
- Uveďte príklad nebezpečnej situácie, ktorá sa môže stať na internete.
- Prečo je dôležité chrániť svoje osobné údaje? Aké osobné údaje máme?



Úloha 3:

Preskúmajte vybrané svety z druhej kolekcie (*Cyber Fundamentals*). Pracujte v dvojčlenných tímoch.

1. prezrite si metodickú podporu pre vzdelávací svet dostupnú na webe,
2. prejdite aktivitami vo svete tak, ako by ich realizoval žiak,
3. priebežne sledujte, aký cieľ, obsah a formu majú jednotlivé aktivity,
4. všímajte si vzdelávacie prvky vložené do prostredia hry.

Pripravte a prezentujte stručnú správu so svojimi zisteniami a kritickým hodnotením zvoleného vzdelávacieho sveta.

Metodická poznámka

Zadanie úlohy v uvedenej podobe je vhodné pre skupinu študentov, ktorí študujú učiteľstvo informatiky. Ide o kolekciu svetov s pokračujúcim príbehom so systematickým výkladom tém z kybernetickej bezpečnosti. V záverečnom hodnotení skúsenosti z hrania je vhodné ich v rámci skupiny prezentovať v pôvodnom poradí.

Charakteristika vybraného sveta – Sieťoví hrdinovia



Obr. 3 Vzdelávací svet Sieťoví hrdinovia

Hra vtiahne žiakov do napínavého príbehu. Žiaci ako hráči nastupujú do novej školy. Zoznámia sa so svojím učiteľom a spolužiakmi, prídu do novej triedy. V škole sa hneď v prvý deň dejú zaujímavé veci. Žiaci musia prevziať zodpovednosť za záchranu školskej siete, odolať hrozbám zlých útočníkov.

Postupne absolvujú tri lekcie:

Lekcia 1 – Sieťové komponenty: žiaci sa učia o LAN a WAN sieti, ako sa údaje posielajú z počítača do počítača a zo siete do siete. Umiestňujú počítače, ethernetové káble, routre, switch. Potom bojujú proti zlodejovi paketov, ktorý sa snaží získať dáta. Túto úlohu splnia tak, že komunikáciu medzi počítačmi zašifrujú.

Lekcia 2 – Ochrana heslom: žiaci sa dozvedia, prečo a ako vytvárať komplexné heslá, aká je ich úloha v zabezpečení siete a spoznajú ďalšie viacúrovňové bezpečnostné postupy (2FA, firewall), aby zabránili neoprávneným používateľom v prístupe do siete. Tvorbu hesla opakujú trikrát zostavovaním zo zozbieraných písmen, číslíc a ďalších znakov, s rastúcou zložitosťou hesla.

Lekcia 3 – Škodlivý softvér: žiaci sa učia identifikovať bežné typy malvéru a ako sa mu vyhnúť. Majú pomôcť učiteľom, ktorí sa stali obeťou malvéru. „Navštívia 2 webové lokality“ a zistia, že jeden z problémov je phishingový útok na sociálnej sieti. V druhom prípade ide o vyskakovacie okná s reklamami na stránke obchodu, ktoré je potrebné zatvárať a zabrániť tak nainštalovaniu malvéru.

Pri práci so svetom sa používa odborná terminológia, úlohy sú praktické, dobre napodobňujú reálne scenáre. Žiaci zapájajú počítače do siete, aktivujú šifrovanie, využívajú silné heslá, dvojfaktorovú autentifikáciu, firewall, odhaľujú malvér a dávajú ho do karantény.

Po každej lekcii je priestor na formatívne hodnotenie. Žiaci sú teleportovaní do miestnosti, kde majú nerušene zapísať, čo sa naučili, odpovedať na pripravené pomocné otázky (s využitím predmetu *Kniha a brko* alebo do pracovného listu). Vytvorené knihy s odpoveďami si žiaci zo sveta na záver môžu exportovať vo formáte .pdf a zdokumentovať tak výsledky svojej práce (odovzdať ich učiteľovi).

Prvky vo svete sú spracované realisticky (hardvérové komponenty, vybavenie budov), zadania riešených problémov vychádzajú z praxe, náročnosť úloh zodpovedá cieľovej skupine. Okrem animovaných sekvencií s uvedením lekcie NPC predstavujúcim učiteľa, sú v príbehu aj sekvencie

z centrály záškodníkov, ktorí chcú narušiť bezpečnosť školskej siete, ale sú vždy neúspešní. Žiaci sa stávajú hrdinami príbehu. Pre žiakov, ktorí nemajú skúsenosť s hraním hry Minecraft, je v úvode (po spustení sveta) zaradený krátky voliteľný tutoriál.



Úloha 4:

Ktorýkoľvek zo svetov z kategórie *Kybernetika* alebo *Umelá inteligencia* môžete spracovať ako tému svojej seminárnej práce.

Metodická poznámka

Študenti si ako tému svojej prezentácie v rámci seminára vyberajú vzdelávacie svety z knižnice podľa aprobačných predmetov, ktoré študujú. Vzdelávacie svety o kybernetickej bezpečnosti a umelej inteligencii bývajú zaujímavé najmä pre študentov učiteľstva informatiky, príp. prírodovedných predmetov. V rámci prezentácií spolužiakov, ktoré vychádzajú z autentickej skúsenosti, získavajú všetci študenti výborný prehľad o možnostiach minecraftových svetov pri implementácii učenia sa založenom na digitálnej hre v humanitných aj prírodovedných predmetoch, matematike a v informatike a v krúžkovej činnosti. Zvyšuje sa tým pravdepodobnosť, že takýmto spôsobom budú chcieť a budú schopní aj oni sami kompetentne vyučovať vo svojej vlastnej pedagogickej praxi.

Tento dokument bol vypracovaný pre projekt Nitrianske kompetenčné centrum pre kybernetickú bezpečnosť (17R05-04-V01-00003)



Nitrianske kompetenčné
centrum kybernetickej
bezpečnosti

Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]