Erasmus+ Programme of the European Union

IO4: НАСОКИ ЗА ПАРТНЬОРИ С ИНСТРУМЕНТАРИУМ

DiSCVET

Развитие на компетенциите в Дигиталния суверенитет на учителите и обучителите в ПОО

Създаден от MIITR
май 2023

Този проект е финансиран с подкрепата на Европейската комисия. Настоящата публикация отразява единствено възгледите на автора и Комисията не носи отговорност за използването на съдържащата се в нея информация [Номер на проекта: 2020-3-BE05-KA205-003110].

Co-funded by the Erasmus+ Programme of the European Union

1 Съдържание

DiSCVET ИНСТРУМЕНТАРИУМ

ПРОЕКТ: Развитие на компетенциите за цифров суверенитет на учители и обучители в ПОО

Предлага се на BG, DE, EN, GR, IT, SI!

ЗАЩО?

Цифровият суверенитет е нова концепция в цифровата ера, която предполага, че страните трябва да имат суверенитет върху собствените си цифрови данни. На индивидуално ниво цифровият суверенитет демонстрира способността на хората да притежават своите лични данни и да контролират използването им. Хората често се борят да оценят значението на неприкосновеността на личния живот, тъй като последствията от нарушенията на неприкосновеността на личния живот са трудни за измерване поради тяхната неуловима природа.

КАКВО

АНова иновативна форма на съдържание за обучение заедно с онлайн платформа за симулация

ЗА КОГО

учители/обучители в ПОО, организации на ПОО, доставчици на образование, власти, експерти/лица, вземащи решения

КЪДЕ

discvet-hub.eu
discvet.eu
facebook.com/discvet

Включва материали за:

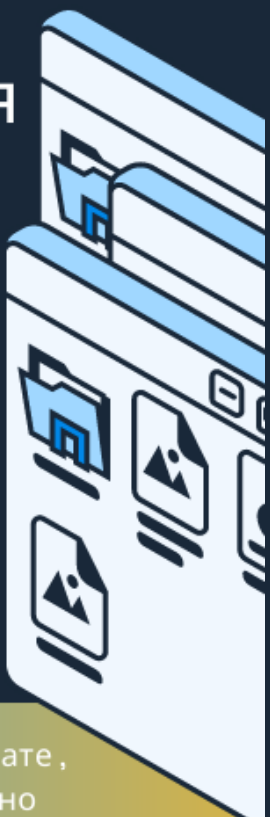
- Управление на цифрови ресурси
- Лични данни и поверителност
- Управление на информационната сигурност
- Управление на риска
- Управление на информация и знания

IO2 Онлайн платформа и учебни материали

Творчески обучителен материал, който има за цел да предостави на учителите/обучителите в ПОО необходимите компетенции, за да повишат цифровия си суверенитет и да им позволят да обучават други. Учебният материал се състои от пакет от дигитални учебни ресурси, които използват концепцията за микрообучение. Тези късчета за дигитално обучение включват различни ресурси като интерактивни игри, видеоклипове за електронно обучение, интерактивни казуси, инфографски ресурси и др.

IO3 Симулационни упражнения

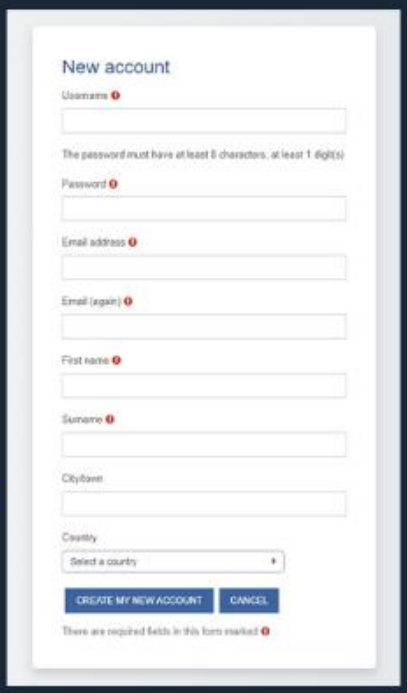
Преходът към практическа настройка беше направен чрез симулационни упражнения, имитиращи употреба в реалния живот, въвеждащи нови приложения, методи или инструменти и позволяващи на потребителите да придобият практически опит. Упражненията подобряват запазването на знания, тъй като потребителите ще могат да прилагат принципите на цифров суверенитет и цифрова сигурност в практически ситуации, като кибератаки, пробиви в сигурността, фишинг, зловреден софтуер и други.



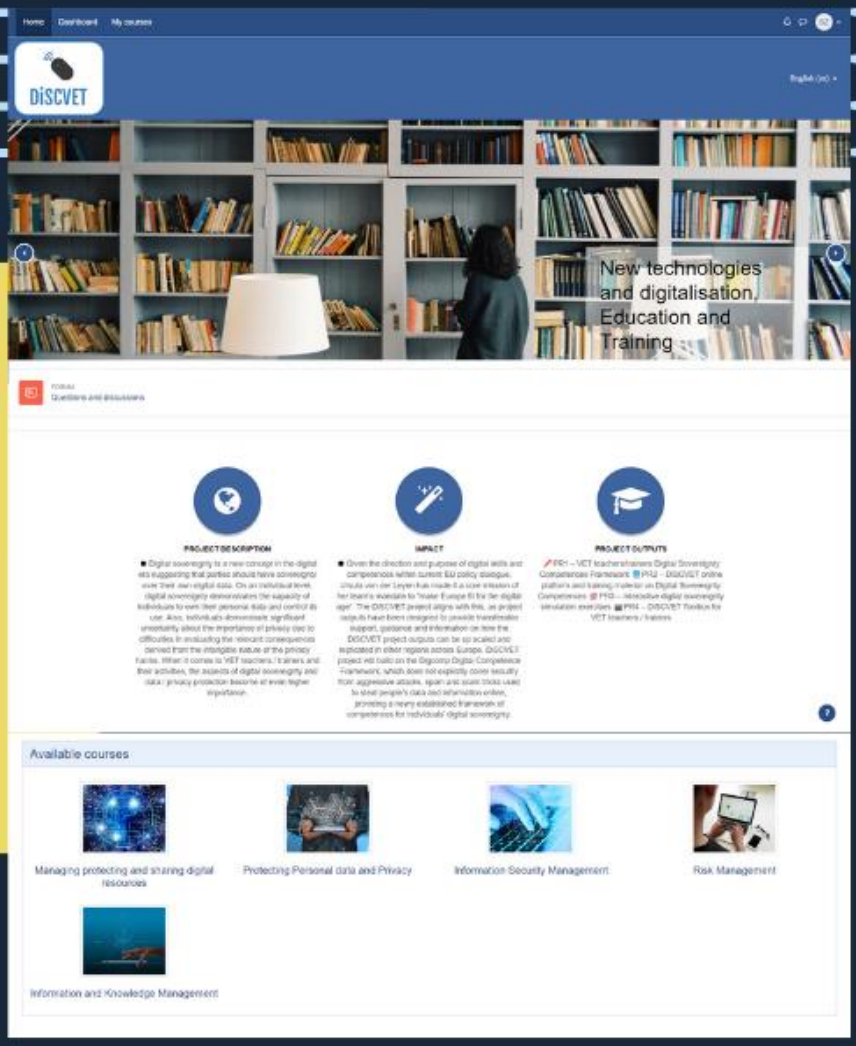
Научете повече за резултатите, как да ги използвате, пилотно тестване и национални инициативи относно обучението по дигитална сигурност! ⟶

Как да използваме платформата?

(discvet-hub.eu/)

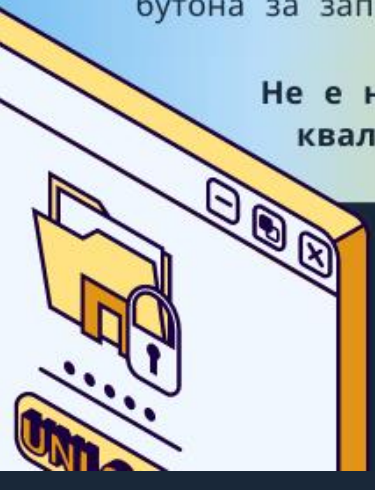


За достъп до материалите потребителите трябва да се регистрират в платформата. След като предоставите цялата необходима информация за създаване на акаунт, ще получите имейл за потвърждение (проверете папката си със спам!), който ще включва връзка за активиране на вашия акаунт.



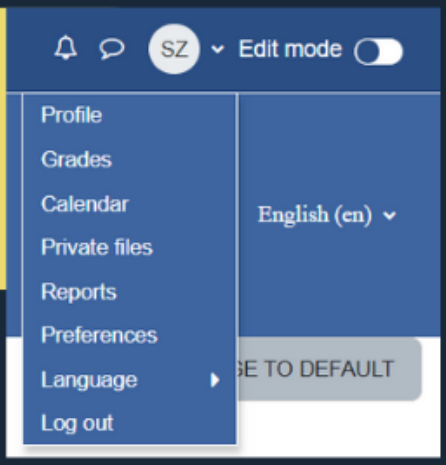
На началната страница можете да намерите информация за проекта и 5 налични курса. За достъп до учебния материал щракнете върху курс и натиснете бутона за записване.

Не е необходима квалификация!



Всеки модул се състои от няколко малки модула, като всички имат теоретична учебна част (PDF и цифрови късове), последвана от симулационни упражнения. Това е мястото, където ще проверите придобитите знания, като получите незабавна обратна връзка относно вашия резултат.

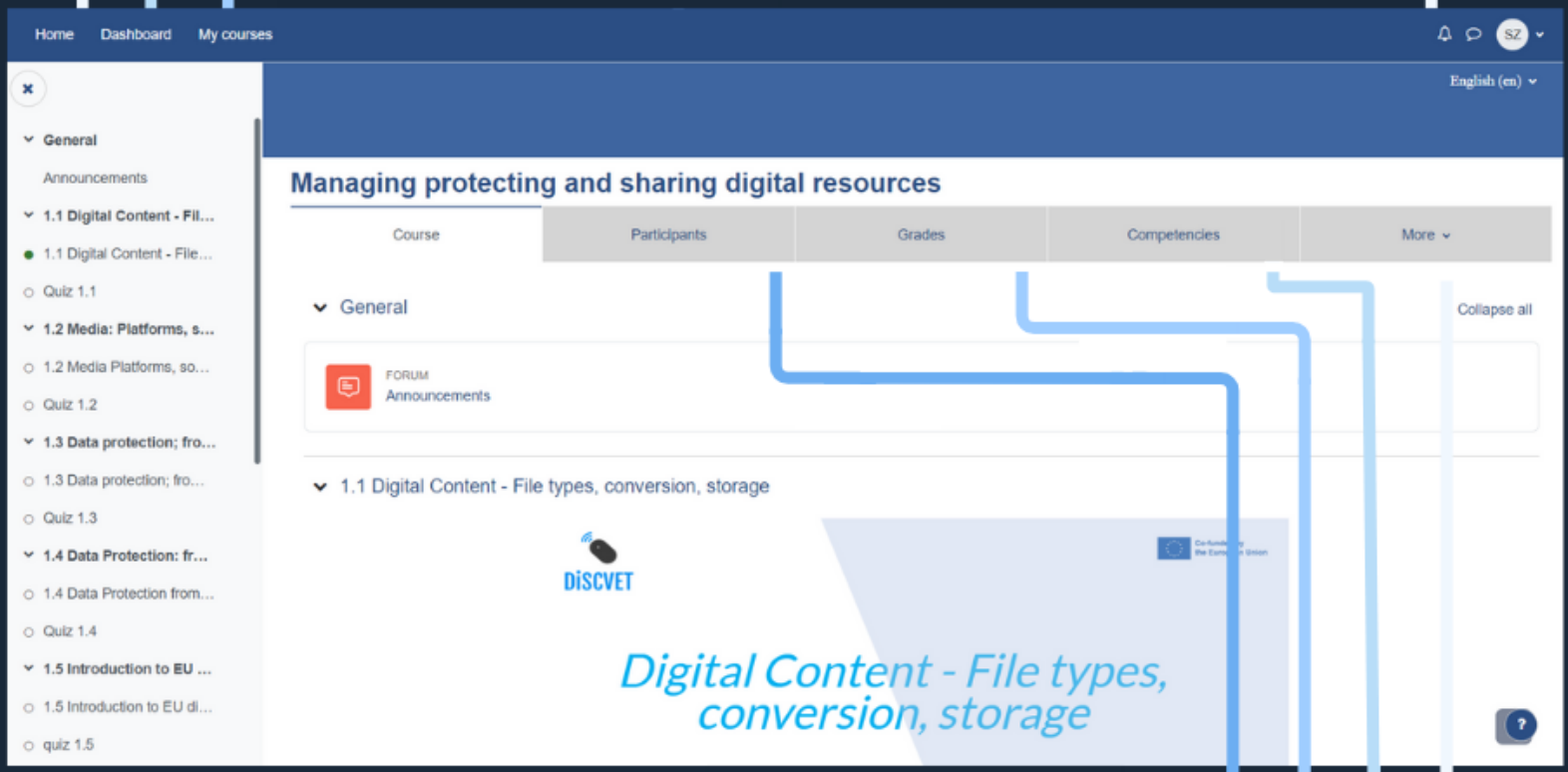
За достъп до вашия профил и настройки щракнете горе вдясно върху светлинния кръг с вашите инициали. До него можете да намерите известия (символ на звънец) и чатове (символ на балонче за чат).



Върнете се на началната страница

Достъп до календара и планираните дейности

Курсове, в които сте се записали, и вашият напредък [%]



Намерете други хора, участващи в този курс

Резултатите от вашите симулационни упражнения

Списък с вашите нови компетенции

Отпишете се от курса

Co-funded by the Erasmus+ Programme of the European Union

4 Доказателства и данни от пилотните дейности

4.1 Методика

Целта на този доклад е да представи отговорите, събрани във фазата на пилотното тестване на резултатите от проекта. Пилотната тестова дейност за проекта DiscVet се проведе през периода февруари-април 2023 г.

Общата цел на този обобщаващ доклад е да запише възприеманото ниво на удовлетворение и качество на резултатите от проекта, както и тяхната полезност, за да можете да се съсредоточите върху възникнали проблеми и да намерите възможни решения, за да доставите резултатите от проекта в окончателния и окончателна версия.

Проектът _ резултати тестван бяха :

- **IO2: DiSCVET онлайн платформа и обучителни материали относно компетенциите за цифров суверенитет**
- **IO3: Разработване на интерактивни упражнения за симулация на цифров суверенитет**

Пилотният тест на IO2 е приложен чрез структуриран въпросник под формата на **формуляр на Google** (за да се гарантира по-добра достъпност и достъпност на групата за целите), наличен в ПРИЛОЖЕНИЕ I към този доклад. Въпросникът имаше за цел да получи полезна обратна връзка от участниците в пилотните дейности, като се фокусира върху оценката на няколко характеристики на материала, като например:

- яснотата на структурата му;
- ефективността на цифровите ресурси, които включва;
- Лесното използване и навигация в платформата;
- Количеството време, прекарано в платформата и в нейните дейности/компоненти;
- Лесното въвеждане на нови данни / информация;
- Цялостната структура и естетика на платформата;
- Свързването/зареждането на компонентите и/или техните страници.

Пилотният тест на IO3 е проведен чрез съответен структуриран въпросник, като се фокусира върху оценката на няколко характеристики на симулационните упражнения, като например:

- Съответствие с темата и нуждите на целевата група;
- Лекота на използване;
- Дизайн.

Участниците бяха помолени да оценят различните аспекти на IO2 и IO3 по скала от 1 до 5, където
1 = най-ниското, незадоволително впечатление
3 = адекватно впечатление
5 = най-високото, много добро впечатление

Структурираният въпросник е с вградена връзка към онлайн платформата https://discvet-hub.eu/login/index.php съдържащи материала, за да може да се следи постигането на **KPIs** , предвидени за тази дейност по проекта.

KPI IO2

KPI 7: Добре дефиниран курс на обучение и материали, които отговарят на нуждите, разпознати в дейностите на IO1 (качествени) - Инструмент за измерване: вътрешна оценка от партньорите по проекта и външна оценка от членовете на NSAGs

KPI 8: Най-малко 180 учители/обучители в ПОО, които ще участват в пилотните дейности (количествени) – Инструмент за измерване: брой хора, които са се регистрирали в платформата и са завършили курса на обучение

KPI 9: 85% удовлетвореност на участниците от пилотните дейности (количествено) - Инструмент за измерване: попълнени структурирани въпросници за оценка на пилотните дейности

KPI IO3

KPI 10: Най-малко 180 учители/обучители в ПОО, които ще участват в пилотните дейности (количествени) – Инструмент за измерване: брой хора, които са се регистрирали в платформата и са завършили симулационните упражнения

KPI 11: 85% удовлетворение от функционалността на платформата (количествено) - Инструмент за измерване: попълнени структурирани въпросници за оценка на платформата

Всяка държава партньор проведе няколко пилотни сесии (онлайн или лице в лице), поради трудността да се наемат 30 участници едновременно.

В **Италия** бяха създадени материали за разпространение, за да рекламират събитието и да дадат инструкции как да се проведе пилотният тест. Беше организирана една присъствена сесия с участието на студенти, учители и заинтересовани страни за тестване на резултатите от проекта.

В **България** се проведоха общо три пилотни сесии – 1 присъствена и 2 онлайн, с участието на участници от учители по ПОО, обучители в обучението на възрастни и заинтересовани страни.

В **Словения** целевата група, участваща в пилотното тестване, се състоеше от преподаватели в ПОО, учители от местни институции за ПОО и гимназии, както и мрежа от други словенски неправителствени организации, заинтересовани от подобни теми, Местната търговско-промишлена камара. Пилотните сесии за тестване се проведоха в отделни моменти, според наличността на участниците бяха организирани 3 сесии лице в лице и 2 сесии онлайн.

4.2 Резултати

Достъп до платформата за електронно обучение по държава

Държава	**Брой влизания**
Гърция	40
Словения	32
Италия	36
Германия	11
Кипър	23

Co-funded by the Erasmus+ Programme of the European Union

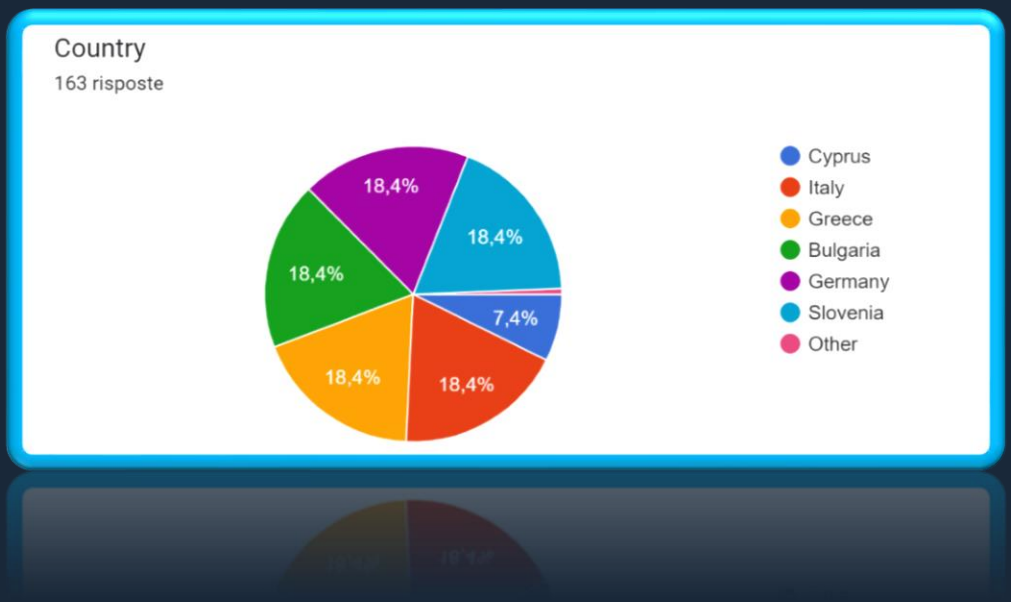
България	35

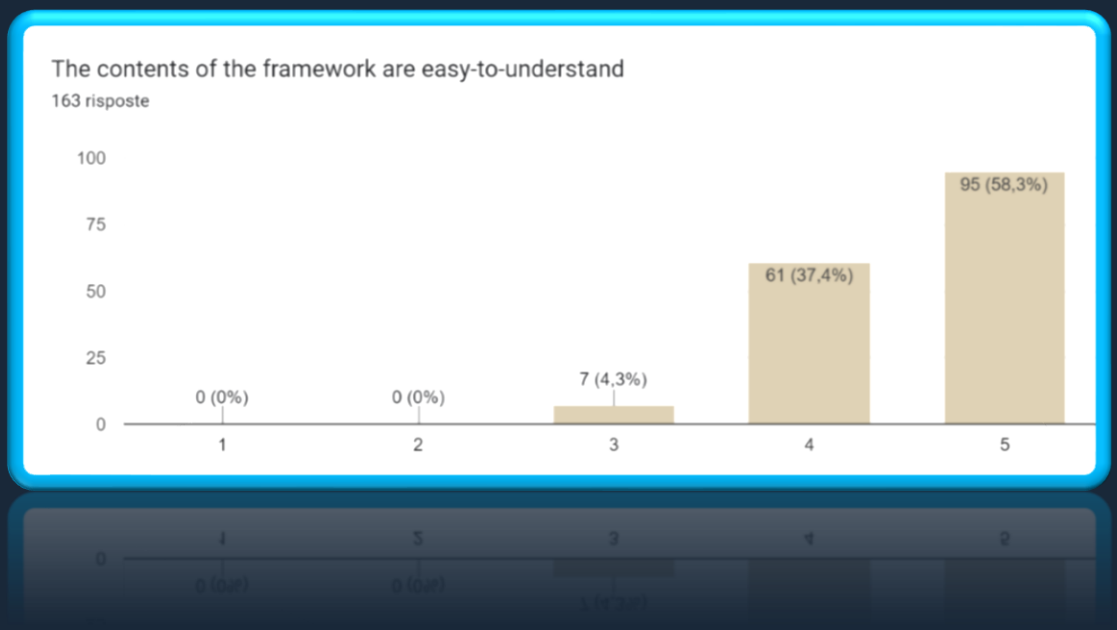
Обратна връзка на участниците.

Професия на целевата група

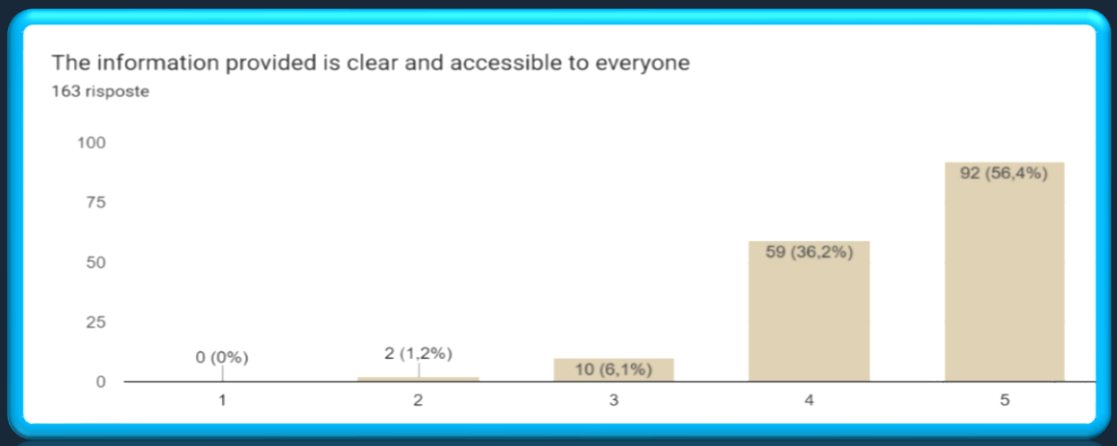
Общо бяха събрани 163 отговора от всички страни партньори, като най-високият процент, представляващ професията на целевата група, е 25,2% от учителите, следван от 23,3% от учителите в ПОО.

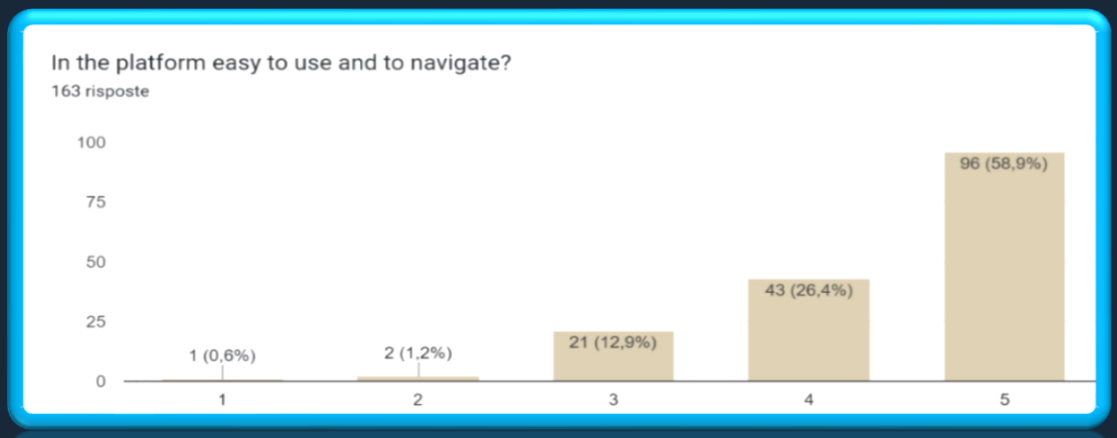
Регистрирани участници в пилотния тест от всички страни партньори. Малък процент (1 респондент) се е регистрирал от Франция.

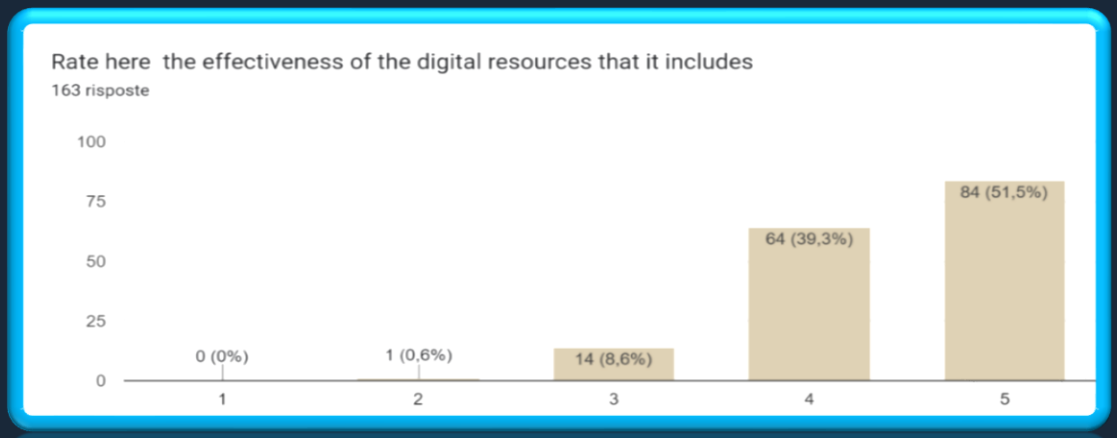




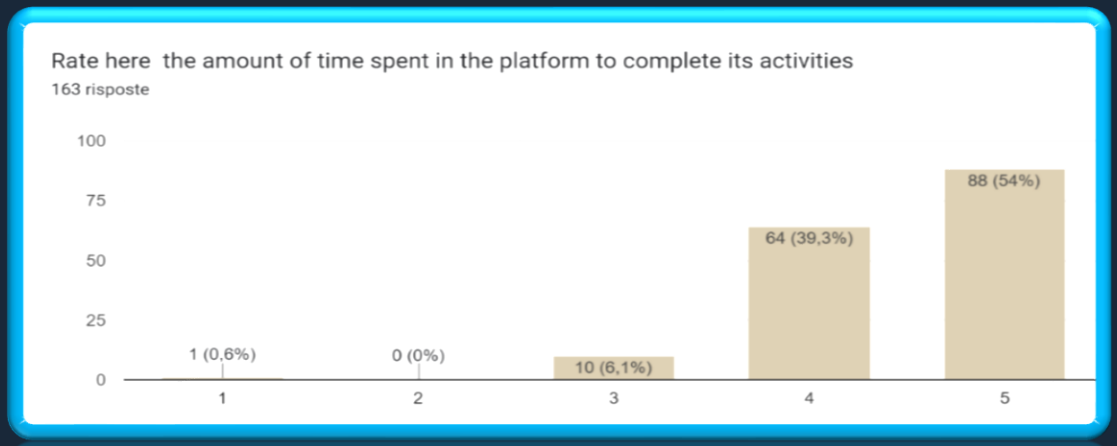
Co-funded by the
Erasmus+ Programme
of the European Union

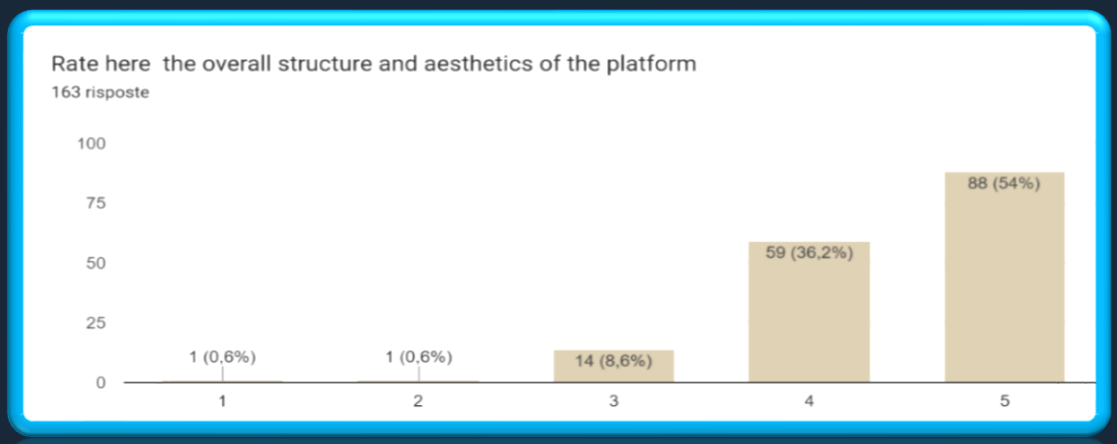


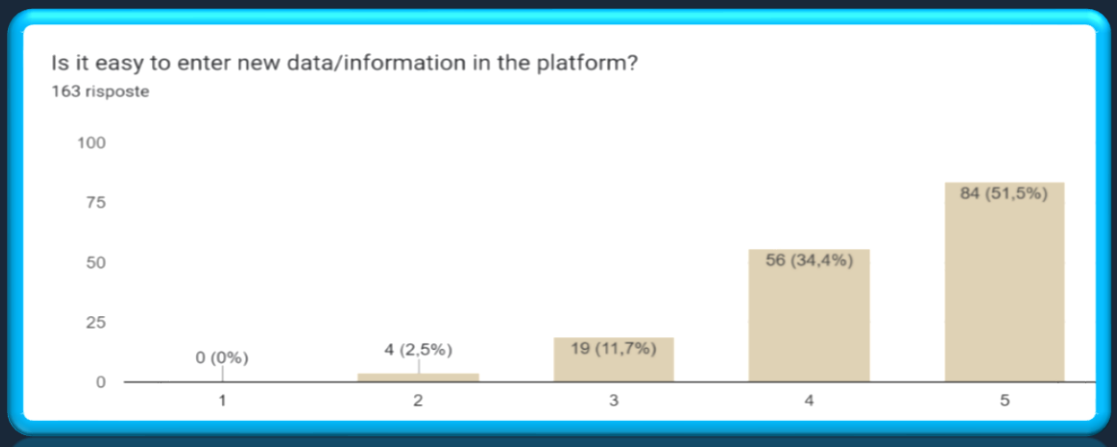




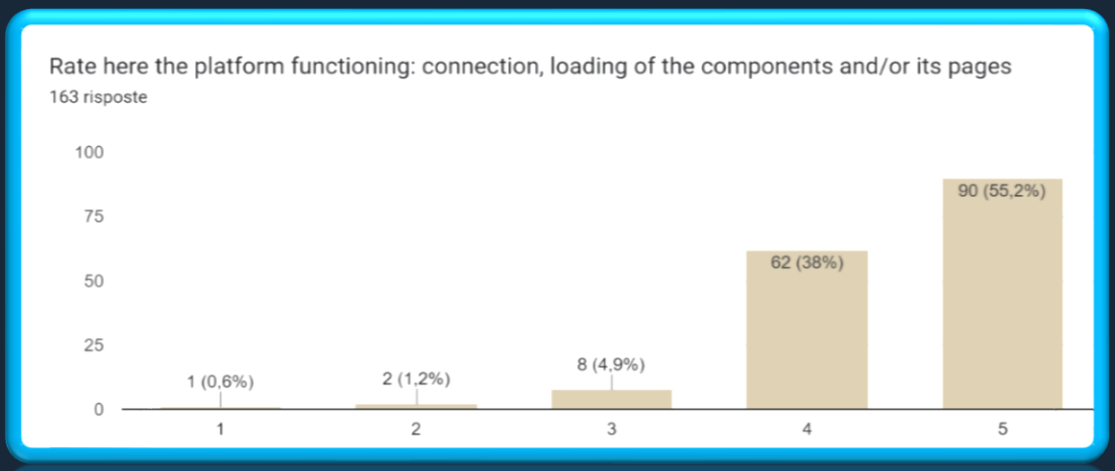
Co-funded by the
Erasmus+ Programme
of the European Union

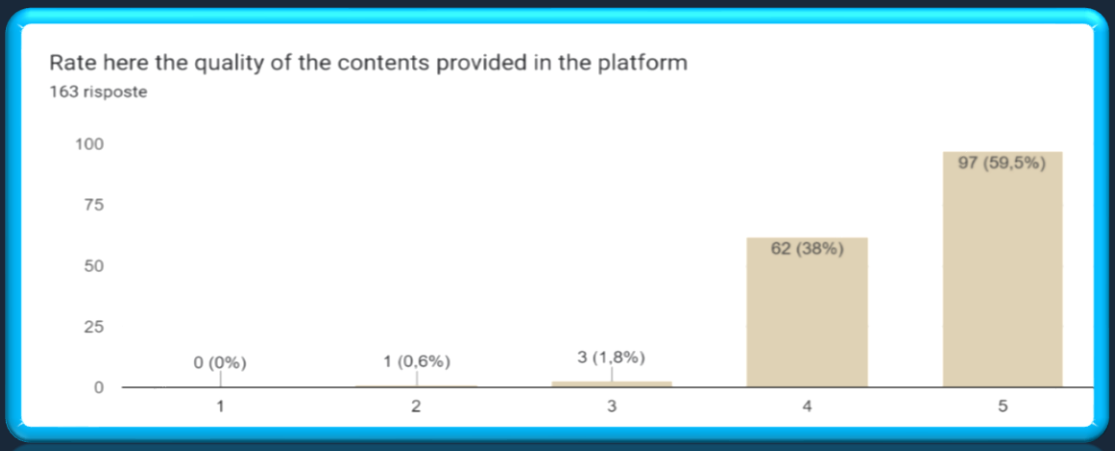


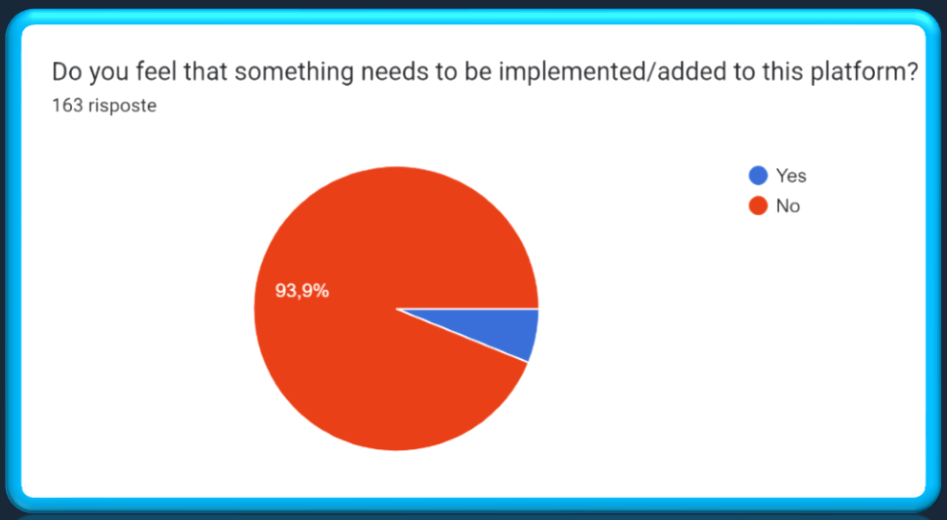


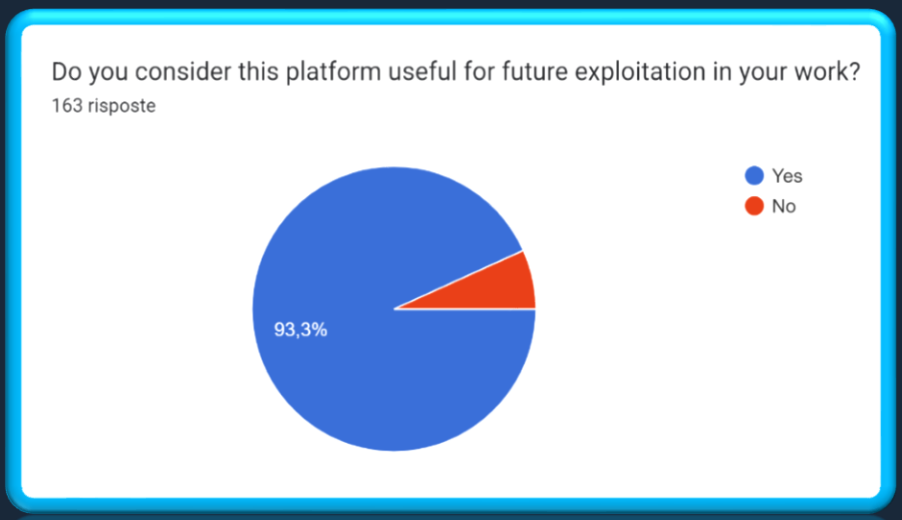


Co-funded by the
Erasmus+ Programme
of the European Union









Както може да се види от фигурите по-горе, представящи отговорите, събрани след сесиите за пилотно тестване във всяка страна партньор, участниците в пилотния тест изразиха **високо ниво** на удовлетворение, като оцениха различните аспекти на платформата за електронно обучение, като нейното съдържание, лекота за използване и навигация, качеството на качените материали, функционирането на платформата, поставяне на точки **между 4 и 5** (където 5 е максималният резултат).

Също така участниците декларираха полезността на платформата за бъдеща експлоатация на тяхната работа. По-голямата част от участниците в пилотния тест не изразиха необходимостта от по-нататъшно внедряване на платформата, но 10 участници (6,1%) предложиха някои специфични корекции, които да се вземат под внимание според обратната връзка, докладвана по-долу:

- Липсват преводи на словенски
- липсващи български въпроси във викторините
- когато е избран език, трябва да се показва само информацията на този език
- Още информативни видеоклипове

Въпреки че въпросникът, използван за пилотния тест, показа високо ниво на цялостно удовлетворение, имаше някои аспекти, които трябва да се подчертаят и да се вземат под внимание за окончателното подобряване на платформата и нейното съдържание, както се вижда от специфичната обратна връзка, обобщена по-долу.

Положителна обратна връзка

- *интересна платформа*
- *Добър дизайн и много полезен*
- *Вярвам, че тази платформа е лесна за разбиране и използване, освен това е страхотна естетика*
- *Платформата е много лесна за използване и може да се използва лесно.*
- *много добре*
- *Мисля, че това е полезно и приятелско*
- *Много полезно и ясно разделяне на съдържанието в платформата*
- *Отлично*
- *прилагат реални случаи*
- *Симулацията на реалния живот е полезна*
- *Липсваше ми това знание*
- *Лесен за разбиране и практичен*
- *Интерактивната навигация и информацията, събрана от уебсайта, бяха отлични*
- *Наистина ми хареса да разглеждам уебсайта и научих много нови неща за данните и поверителността*
- *Определено ще използвам наученото за визуализацията на данни в бъдеще и ще използвам съветите за обучение на платформата*
- *Много интересно и пълно с информация, която всички учители трябва да знаят*
- *Интересно! Научих много за интерактивността и управлението на цифрови данни*
- *Дигиталният свят е навсякъде около нас и е важно да знаем как да управляваме нашите данни и информация! Платформата е много интересна и лесна за четене*

Аспекти, които се нуждаят от подобрение

- *открият някои граматически грешки*
- *Необходима е мобилна оптимизация.*
- *бутонът за връщане назад не работеше, "словенската страница" беше предимно на английски, странно форматиране, естетически неприятно*
- *Съдържанието изглежда полезно; но начинът, по който е представен, понякога е неудобен и объркващ. В някои глави тестът и презентацията на genial.ly са включени, в други изобщо не. Съдържанието в genial.ly и pdf се повтаря и е неясно.*
- *Не е съгласувано между модулите*
- *Тестът имаше странно форматиране (двойни числа).*
- *Някои тестове имаха липсващи отговори, други имаха въпроси с няколко 100% верни отговора, от които да избирате, което превръщаше теста в игра за отгатване (напр. 5.4)*

- *Зареждането на презентациите отне малко време, но иначе полезно съдържание.*
- *Зареждането на Genially отне доста време. Съдържанието изглежда полезно; но начинът, по който е представен, понякога е неудобен и объркващ. В някои глави тестът и презентацията на genial.ly са включени, в други изобщо не. Съдържанието в genial.ly и pdf се повтаря и е неясно.*

4.3 Заключение

Фазата на пилотния тест се оказа като цяло положителна, като подчерта удовлетворението на повечето от участниците, които оцениха положително резултатите от проекта и тяхната полезност.

В същото време аспектите, които изискват подобрение, бяха подчертани и засягаха най-вече някои аспекти, свързани с викторините. В това отношение предоставените предложения се въртят около възможността „ *първо да се коригират по-очевидните проблеми като граматика, двойни числа в тестовете, липсващи отговори и т.н., всички споменати по-горе. След това преминете към надграждане на дизайна на сайта (направете горния банер по-малък, преместете модулите така, че да са най-горе, използвайте по-добре разстоянието и оформлението (на всички страници)). И накрая, разгледайте времето за зареждане на Genialys* ”

4.4 ПРИЛОЖЕНИЯ

Приложение I - I Въпросник за пилотен тест
https://docs.google.com/forms/d/e/1FAIpQLSdLMxrfoPSlRcKhAgGl_Ph0LJceFrdhE5wSCiV0lWbhORUElA/viewform

Приложение II - II IO1 Валидиране
https://drive.google.com/drive/folders/1rIvFJQheUiG38Ii7rAG5GxIAyW_e-y0o

5 ПОДХОД НА ЕС КЪМ ЦИФРОВАТА СИГУРНОСТ

5.1 Общ подход на ЕС към киберсигурността

ЕС възприе цялостен подход към киберсигурността с редица регламенти и директиви, насочени към защита на цифровата инфраструктура и личните данни. Някои ключови елементи от стратегията на ЕС за киберсигурност включват:

Общият **регламент за защита на данните (GDPR),** който определя правила за това как личните данни трябва да се обработват, съхраняват и защитават в рамките на ЕС. GDPR се прилага за всички бизнеси, работещи в рамките на ЕС, както и за всяка компания, обработваща лични данни на граждани на ЕС.

Директивата **за мрежова и информационна сигурност (NIS Директива)**, която установява мерки за киберсигурност за доставчиците на критична инфраструктура, включително секторите на енергетиката, транспорта и здравеопазването. Той изисква тези доставчици да докладват големи инциденти със сигурността на националните органи.

Законът **за киберсигурността** , който създава рамка за установяване на схеми за сертифициране на киберсигурност в целия ЕС за цифрови продукти, услуги и процеси.

Стратегията **на ЕС за киберсигурност** , която е цялостен план за подобряване на киберсигурността в целия ЕС. Той включва инициативи за подобряване на сътрудничеството между държавите-членки, насърчаване на научните изследвания и иновациите и укрепване на инфраструктурата за киберсигурност на ЕС.

5.2 План за действие за цифрово образование

В Европа все повече се признава значението на цифровото образование за подготовката на хората за бъдещето. Европейската комисия стартира нов План за действие за цифрово образование, който има за цел да насърчи използването на технологии в образованието и да подобри цифровите умения сред европейските граждани. Планът включва инициативи като осигуряване на всички училища с високоскоростен интернет достъп, увеличаване на използването на цифрови инструменти в преподаването и ученето и подкрепа за развитието на иновативни образователни технологии. Планът също така се фокусира върху подобряването на цифровите умения на учителите и насърчаването на възможностите за учене през целия живот за всички граждани. Инвестирайки в цифрово образование, Европейският съюз се надява да насърчи икономическия растеж, социалното включване и цифровото гражданство в целия регион.

Планът има 13 действия, 3 от които са пряко свързани с дигиталното образование и обучение:

Действие 5 (Планове за цифрова трансформация за институции за образование и обучение) – има за цел да подкрепи усилията за цифрова трансформация чрез проекти за сътрудничество по Еразъм+, създава академии за учители за развитие и сътрудничество и въвежда онлайн инструмент за самооценка, наречен SELFIE за учители, за идентифициране на области за подобрение.

Действие 6 (Етични насоки за използването на AI и данни в преподаването и ученето за преподаватели) – нараства необходимостта да се разбере потенциалът на AI и да се повиши осведомеността за възможните рискове, тъй като той може да трансформира образованието и обучението, както и нашето ежедневието. Насоките предоставят практическа подкрепа и насоки за използването на AI, помагат при преподаването и ученето, предлагат по-добри системи за поддръжка на административни процеси и представят етични съображения.

Действие 7 (Общи насоки за учители и преподаватели) – образованието и обучението са жизненоважни за култивирането на уменията за критично мислене на гражданите, необходими за навигация в онлайн света, като се имат предвид неговите уникални характеристики като алгоритми, „информационни балони“ и „ехо камери“. Следователно подкрепата на учителите и преподавателите с насоки и практически примери е от съществено значение за насърчаването на цифровата грамотност и борбата с дезинформацията. Насоките предлагат практически съвети и планове за дейности за начални и средни учители, независимо от техните познания по дигитално образование, и са допълнени от окончателен доклад, очертаващ основните констатации и препоръки на Експертната група.

Като цяло Планът за действие за цифрово образование е цялостна стратегия за насърчаване на цифровото образование и подобряване на цифровите умения в цяла Европа. Той признава значението на технологиите за подготовката на учениците за бъдещето и за насърчаване на икономическия растеж и социалното включване.

5.3 Рамки, съдържащи умения за цифрова сигурност

Експоненциалният растеж на цифровите технологии подчерта необходимостта от цифрова сигурност. Значението на развиването и подобряването на уменията за дигитална сигурност се споменава в рамките на компетенциите за цифрови технологии като Европейската цифрова компетентност, известна като DigComp 2.2, и Европейската цифрова компетентност за преподаватели, известна като DigCompEdu.

Рамката DigComp позволява на европейските граждани да разберат по-добре какво се има предвид под цифрова компетентност и как да оценят и развият собствената си цифрова компетентност. Петте основни области в рамката на компетенциите са информационна и информационна грамотност, комуникация и сътрудничество, създаване на цифрово съдържание, безопасност и решаване на проблеми.

Рамката **DigCompEdu** описва какво означава за преподавателите да бъдат дигитално компетентни и е насочена към всички преподаватели на всички нива на образование. Рамката изобразява 22 компетенции, които са организирани в шест области. Тези области са професионална ангажираност, цифрови ресурси, преподаване и учене, оценяване, овластяване на учащите и улесняване на дигиталната компетентност на учащите.

5.4 Финансиране на изследвания и иновации за цифрово обучение

ЕС финансира изследвания и иновации в областта на киберсигурността и цифровите технологии чрез програми като Horizon Europe, Digital Europe Programme и CEF (Connecting Europe Facility). Последният поддържа инфраструктура за киберсигурност и екипи за реакция при инциденти. InvestEU финансира важни вериги за киберсигурност в частния сектор. Хоризонт Европа, една от най-важните програми за финансиране на киберсигурността, финансира иновативни решения за киберзащита, целящи подкрепа на МСП, симулации и защита на критични данни. Тези програми работят с Европейския център за промишлени, технологични и изследователски компетенции в областта на киберсигурността, клъстер от експерти и организации за внедряване на киберсигурност в страните.

5.5 Полезни ресурси и инструменти (ВВВ)

Четвъртата индустриална революция донесе бързо развитие в областта на новите технологии, комуникацията и автоматизацията. Тези развития доведоха до прехода към цифров контекст в заетостта и образованието. Пандемията ускори този преход, като създаде по-голяма нужда от дистанционно обучение и работа. Това създаде нова динамика и предизвикателства с универсалната и широко разпространена употреба на цифровите инструменти (платформи, уебсайтове и др.).

В този контекст ЕС призна импулса и прие Плана за действие за цифрово образование (2021-2027 г.), който определя целите на Европейската комисия за постигане на ефективно, приобщаващо и достъпно цифрово образование в целия Европейски съюз. По-специално, ЕС създаде набор от цифрови инструменти за улесняване на операциите на ЕС, проблемите с обучението и комуникацията между организации и лица в целия ЕС. Основните цифрови инструменти, въведени от ЕС, са:

Портал за училищно образование . Това е „онлайн каталог“, където можете да правите справки с образователни материали, да участвате в онлайн курсове и да имате достъп до ресурси за обучение за учители и по-общо за хора, които се интересуват от училищно образование в Европа. Порталът за училищно образование включва публикации, ръководства, учебни материали, създадени от институции на ЕС, проекти, финансирани от ЕС, безплатни онлайн курсове, уебинари и най-новите новини, свързани с европейската училищна политика и образование.

eTwinning . Платформата е насочена към училищния персонал в европейските страни, за да позволи на учители и директори да общуват помежду си, да създадат мрежа, която позволява развитието на сътрудничество, споделяне и полезни проекти за европейската училищна система. eTwinning има за цел да насърчи училищното сътрудничество в Европа чрез използването на информационни и комуникационни технологии: чрез платформата всъщност училищният персонал може да комуникира, да обменя ресурси и да създава проекти на 30 езика.

Учебен кът . Това е платформа, насочена както към ученици, така и към учители. В зависимост от възрастовата група на учениците се предоставят различни материали, включително игри, състезания и учебници, които им позволяват да научат повече за различни аспекти на Европейския съюз, от законите до околната среда и историята. За учителите платформата е добър източник за намиране на образователни материали, посветени на ученици от началното или средното училище.

Подкрепа, възможности за напреднало обучение и обучение за младежи (Skip-Youth). Това е мрежа от седем центъра, всеки от които работи в приоритетна област в областта на младежта. По-конкретно, платформата предоставя ресурси за обучение на младежи, курсове за обучение и възможности за работа в мрежа.

Електронна платформа за обучение на възрастни в Европа (EPALE). Това е европейска онлайн общност, многоезична и отворена, към която могат да се присъединят професионалисти в областта на образованието за възрастни от цяла Европа. Платформата предоставя възможност за прилагане на дигитални умения чрез безплатни онлайн курсове, достъп до примери за добри практики в обучението на възрастни и ресурси за електронно обучение.

Саморефлексия върху ефективното учене чрез насърчаване на използването на иновативни образователни технологии (SELFIE) е безплатен инструмент, предназначен да помогне на училищата да внедрят цифрови технологии в преподаването, ученето и оценяването. SELFIE има силна изследователска основа и е разработен въз основа на рамката на Европейската комисия за насърчаване на обучението в дигиталната ера в образователните организации.

6 НАЦИОНАЛЕН КОНТЕКСТ

6.1 Словения

През последните години Словения работи активно за подобряване на своята инфраструктура за цифрова и киберсигурност. Страната е признала значението на киберсигурността като основен компонент на националната сигурност и е разработила различни инициативи за подобряване на своите способности за киберсигурност. Националните способности на Словения за киберсигурност и техните роли са определени на оперативно ниво: SI-CERT е националният актив за гарантиране на киберсигурността, а MORS отговаря в

областта на отбраната и защитата срещу природни и други бедствия (включително защитата на критични инфраструктура), полицията гарантира киберсигурността в контекста на обществената безопасност и борбата с киберпрестъпността, Словенската агенция за разузнаване и сигурност (SOVA) извършва контраразузнаване, а възникващият SIGOVCERT отговаря за киберсигурността в публичната администрация. В областта на ангажираността са включени и други заинтересовани страни, като например операторите на критична инфраструктура в частния и публичния сектор.

ИНИЦИАТИВА 1	
Име	В безопасност в Интернет
Местоположение	Национален
Продължителност	2011 –
Описание	SI-CERT повишава националната осведоменост и провежда образователна програма „Безопасно в Интернет“. Тази инициатива е насочена към широката общественост със специфично съдържание за малки предприятия, занаятчии и еднолични търговци за повишаване на осведомеността относно безопасното използване на интернет. Проектът е финансиран от Министерството на образованието, науката и спорта и участва и в кампаниите на Европейския месец на киберсигурността.
Резултати/въздействие	Досега инициативата си сътрудничи с няколко организации и институции, като: Агенция на Европейския съюз за мрежова и информационна сигурност, Европейски потребителски център, Агенция за комуникационни мрежи и услуги на Република Словения, Информационен комисар на РС, Служба за интелектуална собственост , Асоциация на банките на Словения, Асоциация на потребителите на Словения.
Линк към източника	https://www.varninainternetu.si/

ИНИЦИАТИВА 2	
Име	Име
Местоположение	Местоположение
Продължителност	Продължителност
Описание	Центърът за безопасен интернет (SIC) Словения е националният проект, който насърчава и осигурява по-добър интернет за децата. Проектът е съфинансиран от Европейската изпълнителна агенция по здравеопазване и цифрови технологии (HaDEA); в Словения

	финансовата подкрепа също идва от Службата за сигурност на информацията на правителството. Проектът се ръководи от консорциум от партньори, координиран от Факултета по социални науки към Университета в Любляна, Академичната и изследователска мрежа на Словения (ARNES), Словенската асоциация на приятелите на младежта (ZPMS) и Младежката информация и консултиране Център на Словения (MISSS). От 2005 г. SAFE.SI работи като национален център за повишаване на осведомеността на деца и тийнейджъри относно безопасното използване на интернет и мобилни устройства. Техните дейности са насочени към четири целеви групи: деца, юноши, родители и професионалисти (учители, социални работници, младежки работници и др.). Мисията на информационната кампания е да информира младите интернет и мобилни потребители как могат да се предпазят от рискове и да използват мрежата и другите нови технологии безопасно и отговорно.
Резултати/въздействие	SAFE.si насърчава сътрудничеството със словенските заинтересовани страни и институции от публичната и частната сфера, за да направят децата и юношите по-безопасни онлайн и да ги предпазят от потенциални опасности и рискове. Те си сътрудничиха с Агенцията за комуникационни мрежи и услуги на Република Словения, Асоциацията по педиатрия, Министерството на образованието, науката и спорта (изготвяне на план за действие за цифровизация на образованието) и др.
Линк към източника	https://safe.si/

ПРЕДЛОЖЕНИЯ ЗА ОЦЕНКА И ИЗПЪЛНЕНИЕ

Освен споменатите инициативи, Словения допринася за националните системи за киберсигурност чрез програми за висше образование (напр. Факултет по компютърни и информационни науки) и курсове по киберсигурност на всички нива на образование, както и резултатите от изследователски организации. Професионалните асоциации инициираха подобрения и помощ за повишаване на осведомеността сред различни целеви групи (напр. Търговско-промишлената камара на Словения, ISACA, SI-CERT). Въпреки че Словения положи усилия да образова своите граждани относно цифровата сигурност, все още има място за подобрение.

За да подобри нивото на знания сред гражданите, Словения би могла да приложи офлайн инициативи, като промоция в началните и средните училища. Цифровата сигурност може да стане задължителна част от училищната програма, за да се гарантира, че децата ще бъдат обучавани за рисковете за онлайн сигурността от ранна възраст. Инициативите трябва да се разширят до по-широки целеви групи, като

възрастни и предприятия. В Словения е разработена стратегия за киберсигурност, но без план за действие за нейното прилагане.

6.2 Гърция

В Гърция дигиталната и киберсигурността стават все по-важни през последните години, тъй като страната става все по-зависима от технологиите и интернет. Гръцкото правителство предприе стъпки за укрепване на мерките за киберсигурност и защита на критичната инфраструктура, като например енергийните и транспортните системи на страната. През 2019 г. гръцкото министерство на цифровата политика стартира нова национална стратегия за киберсигурност, която включва набор от инициативи за подобряване на киберсигурността в публичния и частния сектор. Стратегията се фокусира върху четири ключови области: защита, откриване, реакция и възстановяване. Той включва мерки като подобряване на сигурността на критичната инфраструктура, разработване на кампании за осведоменост относно киберсигурността и подобряване на способността на страната да реагира на киберзаплахи. Гръцкото правителство също така създаде Национален орган за киберсигурност, който отговаря за координирането на усилията за киберсигурност в публичния и частния сектор. Органът работи за идентифициране и смекчаване на рисковете за киберсигурността, разработва политики и разпоредби за киберсигурност и предоставя насоки и подкрепа на организации и лица.

ИНИЦИАТИВА 1	
Име	Национална стратегия за киберсигурност
Местоположение	Национален, публичен сектор
Продължителност	2019 –
Описание	Националната стратегия за киберсигурност на Гърция стартира през 2019 г. от Министерството на цифровата политика, телекомуникациите и информацията. Стратегията има за цел да подобри киберсигурността в публичния и частния сектор и да защити критичната инфраструктура от киберзаплахи. Стратегията се основава на четири основни стълба: защита, откриване, реакция и възстановяване. Тези стълбове се подкрепят от набор от инициативи, включително: Укрепване на сигурността на критичната инфраструктура Развиване на осведомеността за киберсигурността Подобряване на способността на страната да реагира на кибернетични заплахи Насърчаване на международното сътрудничество Националната стратегия за киберсигурност също така включва конкретни

	цели и срокове за изпълнение на своите инициативи. Като цяло стратегията представлява цялостен подход за подобряване на киберсигурността в Гърция и защита срещу киберзаплахи.
Резултати/въздействие	Подобрена информираност за киберсигурността Засилена сигурност на критичната инфраструктура: Подобрени възможности за реакция при инциденти Засилено международно сътрудничество Като цяло Националната стратегия за киберсигурност оказа положително въздействие върху киберсигурността в Гърция. Въпреки че има още работа за справяне с текущите заплахи и предизвикателства, стратегията спомогна за повишаване на осведомеността относно рисковете за киберсигурността, подобряване на сигурността на критичната инфраструктура, подобряване на способностите за реакция при инциденти и насърчаване на международното сътрудничество.
Линк към източника	https://www.trade.gov/market-intelligence/greece-cyber-security-strategy

ИНИЦИАТИВА 2	
Име	Национален орган за киберсигурност
Местоположение	Национален, публичен сектор
Продължителност	2019 –
Описание	Националният орган за киберсигурност (NCA) е гръцка правителствена агенция, отговорна за координирането и прилагането на политики и инициативи за киберсигурност в публичния и частния сектор. NCA беше създадена през 2019 г. като част от националната стратегия на Гърция за киберсигурност. Основните отговорности на НКО включват: Разработване и прилагане на политики и разпоредби за киберсигурност: NCA отговаря за разработването на политики и разпоредби за подобряване на киберсигурността в различни сектори в Гърция. Координиране на усилията за киберсигурност: NCA работи за координиране на усилията за киберсигурност между различни държавни агенции, както и с организации от частния сектор и международни партньори.

	Идентифициране и смекчаване на рисковете за киберсигурността: НКО отговаря за идентифицирането и смекчаването на рисковете за киберсигурността, включително тези, свързани с критична инфраструктура. Предоставяне на насоки и подкрепа: NCA предоставя насоки и подкрепа на организации и лица относно най-добрите практики за киберсигурност и реакция при инциденти.
Резултати/въздействие	Тъй като Националният орган за киберсигурност (NCA) в Гърция беше създаден през 2019 г., все още е сравнително рано да се оценят напълно резултатите и въздействието на неговите дейности. Има обаче няколко забележителни развития от създаването му, които предполагат, че НКО оказва положително въздействие върху киберсигурността в Гърция. NCA изигра роля в повишаването на осведомеността относно рисковете за киберсигурността и най-добрите практики в Гърция чрез кампании за информиране на обществеността, програми за обучение и други инициативи. Това спомогна за подобряване на общото ниво на киберсигурност в страната. Като цяло, НКО направи важни крачки в подобряването на киберсигурността в Гърция от създаването си през 2019 г. Въпреки че има още работа за справяне с текущите предизвикателства пред киберсигурността, НКО оказа положително въздействие и играе критична роля в защитата на Гърция от кибер заплахи.
Линк към източника	https://www.concordia-h2020.eu/consortium/national-cyber-authority-ncsa/

ПРЕДЛОЖЕНИЯ ЗА ОЦЕНКА И ИЗПЪЛНЕНИЕ

Въпреки че Гърция постигна напредък в повишаването на осведомеността за цифровата сигурност сред своите граждани, все още има място за подобрение. Ето някои възможни решения за подобряване на нивото на знания и осведоменост относно цифровата сигурност в Гърция, с акцент върху това как други държави/институции могат да прилагат подобни инициативи:

ОБРАЗОВАТЕЛНИ ИНИЦИАТИВИ: Едно възможно решение е да се засили акцентът върху цифровата сигурност в образователните институции, като училища и университети. Правителствата и институциите могат да разработят и прилагат образователни програми, които преподават на младите хора основни умения и практики за киберсигурност. Тези програми могат също да са насочени към възрастни, които може да не са имали възможност да научат за цифровата сигурност по-рано в живота си.

КАМПАНИИ ЗА ИНФОРМИРАНЕ НА ОБЩЕСТВЕНОСТТА: Правителствата могат да провеждат кампании за осведомяване на обществеността, за да повишат осведомеността относно важността на цифровата сигурност и да осигурят насоки как да се защитите онлайн. Тези кампании могат да приемат различни форми, като плакати, реклами и публикации в социалните медии.

СЕРТИФИКАТИ ЗА КИБЕРСИГУРНОСТ: Друго решение е да се създадат сертификати за киберсигурност, които хората могат да получат след завършване на курс на обучение. Тези сертификати могат да предоставят на лицата призната квалификация, която демонстрира техните знания и умения в областта на киберсигурността.

СЪТРУДНИЧЕСТВО С ЧАСТНИЯ СЕКТОР: Правителствата могат да си сътрудничат с организации от частния сектор, за да предоставят обучение и подкрепа на гражданите относно цифровата сигурност. Например телекомуникационните компании могат да предоставят насоки за безопасно използване на интернет на своите клиенти.

МЕЖДУНАРОДНО СЪТРУДНИЧЕСТВО: Държавите могат да си сътрудничат по инициативи за подобряване на цифровата сигурност. Това може да включва споделяне на информация за кибернетични заплахи и най-добри практики, съвместни тренировъчни упражнения и координирани отговори на киберинциденти.

6.3 Италия

Италия предприе значителни стъпки към подобряване на цялостната си позиция в областта на цифровата/киберсигурността. Страната е осъзнала важността на киберсигурността и предприема различни инициативи за подобряване на своите способности за киберсигурност. През 2021 г. беше създадена Националната агенция за киберсигурност (ACN). Тя има за цел да повиши националната киберсигурност и устойчивост за цифровото развитие на страната, да постигне национална и европейска стратегическа автономия в цифровия сектор, да насърчи специфични курсове за обучение за развитието на работната сила в сектора, да подкрепи кампании за осведомяване, да насърчи широко разпространена култура на киберсигурност и разработване на международни действия и проекти за сигурно глобално киберпространство. Правителството също така представи Националната стратегия за киберсигурност (NCS), която има за цел да засили цифровата устойчивост и способности на страната срещу киберзаплахи. Той се фокусира върху защитата на критичната инфраструктура, споделянето на информация, научноизследователската и развойна дейност, както и обучението и образованието.

ИНИЦИАТИВА 1	
Име	Облачна стратегия Италия
Местоположение	За италианската публична администрация
Продължителност	15.12.2021 г. –
Описание	Облачната стратегия Италия, създадена от Департамента за дигитална трансформация и Националната агенция за киберсигурност (ACN), съдържа стратегическите насоки за миграционния път на данните и цифровите услуги на публичната администрация към облака чрез система за класифициране на данни на 3 нива . Стратегически: данни и услуги, чийто компромет може да повлияе на националната сигурност.

	Критични: данни и услуги, чийто компромет може да навреди на поддържането на функции, свързани с обществото, здравето, безопасността и икономическото и социално благополучие на страната. Обикновени: данни и услуги, чийто компромет не причинява прекъсване на държавните услуги или, във всеки случай, накърняване на икономическото и социалното благополучие на страната. С цел насочване и насърчаване на безопасното, контролирано и пълно приемане на облачни технологии от публичния сектор, в съответствие с принципите за защита на личните данни и с препоръките на европейските и национални институции.
Резултати/въздействие	Цифровите инфраструктури ще бъдат по-надеждни и сигурни, а публичната администрация ще може организирано да реагира на кибератаки, гарантирайки непрекъснатост и качество при използването на данни и услуги.
Линк към източника	https://www.acn.gov.it/

ИНИЦИАТИВА 2	
Име	Център за по-безопасен интернет – Свързани поколения
Местоположение	Национален
Продължителност	07.01.2016 г. –
Описание	Проектът Център за безопасен интернет (SIC) – Свързани поколения е съфинансиран от Европейската комисия по програма „Цифрова Европа“, координиран е от Министерството на образованието и заслугите и е член на мрежа, насърчавана от Европейската комисия в онлайн платформата „По-добър интернет за деца“, управляван от European Schoolnet, в тясно сътрудничество с INSAFE (мрежа, която обединява всички европейски SIC) и Inhope (мрежа, която обединява всички европейски горещи линии). Образователната мисия на SIC е да предоставя информация, съвети и подкрепа на деца, тийнейджъри, родители, учители и възпитатели, за да улесни докладването на незаконни материали онлайн. Общата цел е да се разработят услуги с иновативно и по-висококачествено съдържание, за да се гарантира онлайн сигурност на младите потребители, като в същото време се разглежда

	свързаната инвестиция като „добродетелна“ възможност за „социален“ и икономически растеж на цялата общност. .
Резултати/въздействие	Осигурете подкрепа и съвети за повишаване на осведомеността относно онлайн опасностите.
Линк към източника	https://www.generazioniconnesse.it/site/it/safer-internet-centre/

ПРЕДЛОЖЕНИЯ ЗА ОЦЕНКА И ИЗПЪЛНЕНИЕ

В Италия има няколко инициативи по отношение на киберсигурността. Беше разработена и Национална стратегия за киберсигурност 2022-2026 г., насочена към планиране, координиране и прилагане на мерки, целящи да направят страната по-сигурна и устойчива. Тази стратегия предвижда постигането на 82 мерки до 2026 г. Валидно предложение може да бъде включването на теми за онлайн безопасност и уроци по киберсигурност в училищните образователни планове, като не ги оставя само на преценката на допълнителни курсове, извънкласни дейности или учебната програма на училищата, в които учат предмети, свързани с ИТ обучението.

6.4 Кипър

Според OCECPR „Визията на Стратегията за киберсигурност на Кипър е използването на информационни и комуникационни технологии в Кипър с необходимите нива на сигурност в полза на всеки потребител“. Основната цел на стратегията е да развие и поддържа безопасна и сигурна електронна среда в Кипър за всички предприятия и граждани чрез разработване на политики в рамките на сътрудничеството между всички компетентни органи. В тази насока Кипър одобри редица действия, които бяха насърчавани на национално ниво, като например създаването на рамка за сигурността и целостта на информационните инфраструктури и повишаването на осведомеността на всички заинтересовани страни и кипърското общество относно съответните въпроси на сигурността и формирането на компютърни екипи за спешно реагиране (CCERTs/CSIRTs). Освен това Кипър се ангажира да допринесе за европейското и международното сътрудничество в отговор на заплахи в киберпространството.

ИНИЦИАТИВА 1	
Име	Национален координационен център за киберсигурност (NCCC-CY) за Република Кипър
Местоположение	Национален
Продължителност	21 декември 2021 г. –
Описание	Органът за цифрова сигурност (DSA) е определен като NCCC-CY с решение на Съвета на министрите на Кипър през декември 2021 г. Неговите основни отговорности са да предоставя знания и да

	улеснява достъпа до ноу-хау относно киберсигурността промишлени, технологични и изследователски въпроси. В допълнение е насърчаването и улесняването на участието на стартиращи предприятия, МСП и академични и изследователски общности на национално ниво в трансгранични проекти и в действия за киберсигурност, финансирани от съответните програми на Съюза. Освен това Центърът предоставя техническа помощ на заинтересованите страни, като ги подкрепя във фазата на кандидатстване за проекти, управлявани от Центъра за компетентност, и се стреми да установи сътрудничество със съответните дейности на национално, регионално и местно ниво, като национални политики за научни изследвания, развитие и иновации в областта на киберсигурността, и по-специално тези политики, посочени в Националната стратегия за киберсигурност .
Резултати/въздействие	От 4 май 2022 г. DSA в сътрудничество с Фондацията за научни изследвания и иновации - CY са в състояние да теглят и насочват наличните средства за киберсигурност след одобрението на нейното предложение от Европейската комисия. За да може DSA да функционира в тази посока, трябваше да бъде оценен задълбочено от Европейската комисия по отношение на способността му да управлява въпросните средства. Европейската комисия извърши оценката след подаването на предложението на 17 февруари 2022 г. и го одобри на 4 май.
Линк към източника	https://dsa.cy/en/activities/nccc

ПРЕДЛОЖЕНИЯ ЗА ОЦЕНКА И ИЗПЪЛНЕНИЕ

В допълнение към CCERT има различни инициативи, насочени към повишаване на информираността за киберсигурността и насърчаване на най-добрите практики. Те включват годишното Кипърско предизвикателство за киберсигурност, което се стреми да идентифицира и развие най-добрите таланти в областта на киберсигурността в страната, и създаването на Кипърската асоциация за киберсигурност, която има за цел да насърчава изследванията, образованието и иновациите в киберсигурността. DSA работи за повишаване на осведомеността за киберсигурността и за развитие на киберкомпетенции в различни бизнес области. Той организира обучения, семинари и уебинари и предлага информационни сесии за студенти, които се интересуват от изучаване на киберсигурност, МСП и възрастни граждани. Министерството на образованието и културата също е внедрило образователни програми за киберсигурност в училищата. Тези програми имат за цел да предоставят на студентите необходимите знания и умения, за да се защитят онлайн и да повишат осведомеността относно киберзаплахите.

Въпреки това все още има място за подобрение в областта на цифровата/киберсигурността в Кипър. По-конкретно, повече ресурси могат да бъдат отделени за програми за образование и обучение по киберсигурност, особено за МСП, които може да са по-уязвими на кибератаки. Освен това по-доброто

сътрудничество между правителството, академичните среди и частния сектор може да помогне за укрепване на цялостната позиция на киберсигурността на страната.

6.5 България

България постигна напредък в подобряването на киберсигурността с Националната стратегия за киберсигурност, Закона за защита на личните данни и Директивата за МИС. Държавната агенция за електронно управление координира политиките и осигурява обучения. CERT България открива и реагира на заплахи, докато Центърът за компетенции по киберсигурност има за цел да насърчи експертизата. Предизвикателствата включват недостиг на квалифицирани специалисти, ниска обществена осведоменост и скорошни кибератаки.

ИНИЦИАТИВА 1	
Име	Държавна агенция за електронно управление (СЕГА)
Местоположение	Национален, публичен сектор
Продължителност	2016 –
Описание	Държавната агенция за електронно управление (SEGA) отговаря за политиките за електронно управление и киберсигурност на страната. Агенцията се координира с други държавни органи и предоставя обучение по киберсигурност на служителите в публичния сектор.
Резултати/въздействие	SAEG работи за подобряване на възможностите за киберсигурност на страната чрез насърчаване на сигурна електронна комуникация, прилагане на мерки за информационна сигурност и провеждане на редовни одити на правителствените информационни системи.
Линк към източника	https://www2.e-gov.bg/en/about_us

ИНИЦИАТИВА 2	
Име	Национална образователна програма по киберсигурност
Местоположение	Национални, гимназии (7-ми до 12-ти клас)
Продължителност	2016 –
Описание	Тази програма е насочена към ученици от 7 до 12 клас и се фокусира върху повишаване на осведомеността относно рисковете за киберсигурността, насърчаване на безопасно и отговорно поведение онлайн и насърчаване на учениците да обмислят кариера в киберсигурността. Състои се от 3 основни компонента: лекции,

	упражнения и състезания. Инициативата има за цел да насърчи култура на информираност и образование в областта на киберсигурността в България и да подпомогне изграждането на квалифицирана работна сила в областта на киберсигурността.
Резултати/въздействие	Програмата спомогна за повишаване на нивото на интерес към образованието и кариерите по киберсигурност сред младите хора в България, като същевременно насърчи националните организации да формират партньорства за укрепване на способностите на страната за киберсигурност. Това доведе и до появата на ново поколение специалисти по киберсигурност, които са оборудвани с необходимите знания и умения за защита на дигиталната инфраструктура на България.
Линк към източника	https://ccdcoe.org/uploads/2018/10/Bulgaria_National-program-Digital-Bulgaria-2025_2019_original.pdf

ПРЕДЛОЖЕНИЯ ЗА ОЦЕНКА И ИЗПЪЛНЕНИЕ

Въпреки че България предприема необходимите стъпки за напредък в киберсигурността, винаги има място за подобрение. Например Националната образователна програма за киберсигурност може да бъде разширена, за да достигне до по-широка аудитория, включително възрастни и предприятия. Като се има предвид това, добра идея е да се насочите към младата публика, тъй като те са тези, които оформят бъдещето. Това е нещо, което други страни също биха могли да прилагат. В допълнение към образователните инициативи има нужда от по-всеобхватни политики и регулации за киберсигурност в България за защита от киберзаплахи. Това включва по-строги закони и разпоредби за защита на данните, както и подобрени стандарти за киберсигурност за критична инфраструктура.

6.6 Германия

Въпросите, свързани с образованието по цифрова/киберсигурност, са приоритет за Германия, за да може да посрещне предизвикателствата, породени от новите развития в киберуправлението и цифровия преход. По-конкретно, германското правителство, в партньорство със заинтересованите страни в сектора, пристъпи към разработването на цифрова стратегия.

„Цифровата стратегия 2025“ очертава приоритетите на германското правителство, а именно да развива дигиталните компетенции и да насърчава използването на нови инструменти за подобряване на процесите на цифровизация в Германия. Стратегията се основава на 10 стълба, важни за цифровизацията, включително стълб, насочен към въвеждането на цифрово образование на всички етапи от живота на индивида.

Германската цифрова стратегия 2025 беше приета през 2016 г. за 10 години. Действията на стратегията имат за цел не само да дадат възможност на германската икономика да посрещне новите

предизвикателства, но и да осигурят водещата си позиция както в качеството, така и в технологиите за следващите години чрез комбиниране на традиционни конкурентни предимства с по-нова технология, модерни методи и специални програми за подпомагане.

INITIATIVE 1	
Име	Стратегия за киберсигурност за Германия
Местоположение	Национален
Дата	2021 г
Описание	На 8 септември 2021 г. федералният кабинет прие стратегията за киберсигурност за Германия за 2021 г., изготвена от федералния министър на вътрешните работи и общността. Той осигурява рамката за киберсигурност през следващите пет години. Киберсигурността е задача за настоящето и една от важните задачи за бъдещето. Това е ера, определена от новите възможности на дигиталния свят, като изкуствен интелект, свързани електронни устройства и нови, иновативни средства за комуникация. За да можете да се възползвате от тези възможности, от съществено значение е да минимизирате рисковете. Германската стратегия за киберсигурност 2021 заменя Германската стратегия за киберсигурност 2016. Стратегията определя основната дългосрочна насока на политиката за киберсигурност на федералното правителство, разбита на ръководни принципи, области на действие и стратегически цели. Стратегията за киберсигурност се фокусира върху четири области на действие: общество, частна индустрия, правителство и ЕС/международни въпроси. В тези области на действие са определени общо 44 стратегически цели.

Резултати/въздействие	Федералната служба за информационна сигурност ще се превърне в център за съвместна работа на федералните и щатските агенции за предотвратяване на киберпрестъпления, създавайки трети стълб в цялостната федерална архитектура за киберсигурност: тя ще заеме своето място заедно с Федералната служба на криминалната полиция (BKA), която вече играе тази роля в германския полицейски сектор и Федералната служба за защита на конституцията, която прави това във вътрешната германска разузнавателна общност. Стратегията укрепва цифровия суверенитет и по този начин сигурната цифрова трансформация на страната ни. Дигиталната икономика на Германия ще бъде укрепена чрез целенасочена подкрепа за ключови базови технологии и работа в мрежа със съответните изследователи. Подходът за сигурност при проектирането ще бъде приложен от самото начало към нововъзникващи и ключови базови технологии.

INITIATIVE 2	
Име	Изследователски центрове за киберсигурност
Местоположение	Национален
Дата	2011 г
Описание	Финансирането на научни изследвания има за цел да финансира развитието на нови идеи и технологии. Осигурено е финансиране на проекти в широк спектър от научни области. Гамата обхваща всичко от фундаментални изследвания в природните науки, екологосъобразно устойчиво развитие, нови технологии, информационни и комуникационни технологии, науки за живота, проектиране на работа, финансиране на структурни изследвания във висши учебни заведения до подкрепа за иновации и трансфер на технологии. Федералното министерство на образованието и научните изследвания (BMBF) финансира три Kompetenzzentren für IT-Sicherheitsforschung (Изследователски центрове за киберсигурност). Отделни изключителни университети или извънуниверситетски изследователски институции се финансират като изследователски центрове за киберсигурност. Центровете се фокусират тематично и организационно върху най-важните

	предизвикателства в областта на ИТ сигурността.
Резултати/въздействие	Задачата на тези центрове е да разработват дългосрочни стратегии за киберсигурност и да извършват свързани изследователски проекти, за да посрещнат настоящите и бъдещите предизвикателства.

ПРЕДЛОЖЕНИЯ ЗА ОЦЕНКА И ИЗПЪЛНЕНИЕ

Германия положи значителни усилия да образова своите граждани относно цифровата сигурност, но има място за подобрение. Докато инициативи като кампании за повишаване на осведомеността на обществото, училищни програми и финансирани от правителството ресурси са изпълнени, непрекъснато развиващият се характер на цифровите заплахи изисква постоянни усилия.

За да подобри нивото на познания на гражданите относно цифровата сигурност, Германия може да обмисли следните решения:

- Интегрирани програми за обучение за публичния и частния сектор
- Инициативи на публичния и частния сектор
- Платформи за обмен на информация
- Кампании за повишаване на осведомеността
- За да реализират подобни инициативи, други държави/институции могат:
- Адаптирайте съществуващите програми: Проучете успешни инициативи от Германия и други страни, за да ги адаптирате и приложите в собствените си образователни системи.
- Работете с експерти в областта: Сътрудничете с местни експерти от индустрията и специалисти по киберсигурност, за да разработите подходящо и практическо образователно съдържание.
- Насърчаване на публично-частни партньорства: Насърчаване на партньорства между държавни агенции, частни компании и организации с нестопанска цел.
- Адаптирайте комуникационните канали: Използвайте комбинация от комуникационни канали, за да достигнете до широка аудитория.
- Използвайте различни комуникационни канали, за да се възползвате от комбинация от канали: Редовно оценявайте ефективността на образователните инициативи за цифрова сигурност.

Co-funded by the Erasmus+ Programme of the European Union

7 ЗАКЛЮЧЕНИЕ

Основната цел на проекта DiscVET беше да предостави на учителите и обучителите в ПОО необходимите компетенции в цифровия суверенитет, за да обучават ефективно другите и да насърчават сигурна цифрова среда. С фокус върху създаването на иновативни материали за обучение и интерактивни симулационни упражнения, проектът има за цел да подобри готовността на участниците за цифрова сигурност. Нашата визия обаче се простира отвъд тази непосредствена цел. Ние се стремим да допринесем за образованието на по-осъзнатото и висококвалифицирано поколение европейци чрез овластяване на учителите и обучителите в ПОО със знанията и компетенциите, необходими за цифров суверенитет.

Признавайки значението на дигиталните умения, сигурните цифрови среди и възможностите за учене през целия живот, ЕС възприе цялостен подход към киберсигурността, цифровото образование и финансирането на научни изследвания и иновации. Този ангажимент е очевиден в стратегиите, регламентите и инициативите на ЕС, насочени към предоставяне на хората на необходимите цифрови умения и насърчаване на сигурни цифрови практики в цяла Европа.

За да гарантираме ефективността и качеството на проекта DiscVET, ние ценим обратната връзка и оценката, предоставена от участниците. Чрез внимателно анализиране и разглеждане на идентифицираните проблеми, ние се стремим да предоставим окончателната и окончателна версия на резултатите от проекта. Докладът за оценка ще служи като ценен ресурс, който ще ни насочи към подобряване на резултатите от проекта и ще гарантира високо удовлетворение и полезност от проекта сред целевата група.

8 БИБЛИОГРАФИЯ

- UpGuard: Киберсигурност на критична цифрова инфраструктура

Получено от: https://www.upguard.com/blog/cybersecurity-regulations-in-the-european-union#toc-3

- Европейска комисия: Дигитално обучение и ИКТ в образованието

Получено от: https://digital-strategy.ec.europa.eu/en/policies/digital-learning

- Европейска комисия: План за действие за цифрово образование – действие 5

Получено от: https://education.ec.europa.eu/focus-topics/digital-education/action-plan/action-5

- Европейска комисия: План за действие за цифрово образование – действие 6

оПолучено от:: https://education.ec.europa.eu/focus-topics/digital-education/action-plan/action-6

Европейска комисия: План за действие за цифрово образование – действие 7

Получено от: https://education.ec.europa.eu/focus-topics/digital-education/action-plan/action-7

- Европейска комисия: DigComp Framework

Получено от: https://joint-research-centre.ec.europa.eu/digcomp/digcomp-framework_en#ref-4-safety

- Кристин Редекер: Европейска рамка за дигитална компетентност на преподавателите: DigCompEdu

Получено от: https://publications.jrc.ec.europa.eu/repository/handle/JRC107466

- UpGuard: Правила за финансиране и научни изследвания (Подкрепа за научни изследвания и иновации)

Получено от: https://www.upguard.com/blog/cybersecurity-regulations-in-the-european-union#toc-4

- Франческа Бернаскони: Дигитално образование според ЕС: полезни инструменти

Получено от: https://www.elearningnews.it/en/news-C-27/digital-education-according-to-the-eu-useful-tools-AR-1488/

Co-funded by the
Erasmus+ Programme
of the European Union