#ТЕМА 1

АДМИНИСТРАТИВНИ И ТЕХНОЛОГИЧНИ АСПЕКТИ НА ЗАЩИТАТА НА ДАННИТЕ НА УЧАЩИТЕ_ADMINISTRATIVE AND TECHNOLOGICAL SECURITY

Съфинансирано от Европейския съюз

Финансирано от Европейския съюз. Изразените възгледи и мнения обаче принадлежат изцяло на техния(ите) автор(и) и не отразяват непременно възгледите и мненията на Европейския съюз или на Европейската изпълнителна агенция за образование и култура (EACEA). За тях не носи отговорност нито Европейският съюз, нито EACEA.

Административни и технологични аспекти на сигурността за защита на данните на учащите се

Инструмент 1:

Тема	**Административни и технологични аспекти на сигурността за защита на данните на учащите се**
Описание на темата	Защитата на данните на учащите се изисква балансиран подход, който съчетава административен надзор с технологични предпазни мерки. В административен план това включва създаване на ясни протоколи за работа с данни, възлагане на отговорности на персонала в зависимост от ролята му и осигуряване на редовно обучение, за да се гарантира, че всеки разбира ролята си в поддържането на сигурността на данните. От технологична гледна точка се прилагат мерки като криптиране, сигурни комуникационни канали и контрол на достъпа, за да се защитят данните от неоторизиран достъп и нарушения. Заедно тези измерения създават съгласувана рамка за защита на информацията за учащите.
Заглавие на инструмента	Шаблони за DPIA
Връзка към инструмента	• Шаблон за DPIA на GDPR.eu • Шаблон за DPIA на Ubenda • Шаблони на TechTarget DPIA • Шаблон на SETU DPIA
За инструмента	Оценките на въздействието върху защитата на данните (ОВЗД) са основни инструменти, които се използват за оценка на потенциалните рискове за данните на обучаемите преди започване на курс или проект. Те помагат на организациите да идентифицират и намалят рисковете, свързани с обработката на данни, като гарантират спазването на разпоредби като Общия регламент относно защитата на данните (GDPR). DPIA са особено важни в образователните среди, където често се обработват чувствителни лични данни. Чрез провеждането на DPIA преподавателите могат да разберат по-добре рисковете за защита на данните, свързани с техните проекти, да изчислят методите за намаляване или

	премахване на тези рискове и да документират мерките за защита на данните, за да докажат съответствието пред надзорните органи.

Инструмент 2:

Тема	**Административни и технологични аспекти на сигурността за защита на данните на учащите се**
Описание на темата	Защитата на данните на учащите се изисква балансиран подход, който съчетава административен надзор с технологични предпазни мерки. В административен план това включва създаване на ясни протоколи за работа с данни, възлагане на отговорности на персонала в зависимост от ролята му и осигуряване на редовно обучение, за да се гарантира, че всеки разбира ролята си в поддържането на сигурността на данните. От технологична гледна точка се прилагат мерки като криптиране, сигурни комуникационни канали и контрол на достъпа, за да се защитят данните от неоторизиран достъп и нарушения. Заедно тези измерения създават съгласувана рамка за защита на информацията за учащите.
Заглавие на инструмента	Инструменти за управление на пароли
Връзка към инструмента	• LastPass • 1Парола • Bitwarden
За инструмента	Инструменти за управление на пароли като LastPass, 1Password и Bitwarden осигуряват силни и уникални пароли за достъп до образователни системи и бази данни, като намаляват риска от неоторизиран достъп. Тези инструменти предлагат функции като хранилища за пароли и възможности за автоматично попълване, което улеснява управлението на множество сигурни пароли. Като използват тези инструменти, преподавателите могат да поддържат надеждна сигурност, като същевременно опростяват процесите за влизане в системата. Това помага да се предотвратят често срещани проблеми със сигурността, свързани със слаби или повторно използвани пароли.

Инструмент 3:

Тема	**Административни и технологични аспекти на сигурността за защита на данните на учащите се**
Описание на темата	Защитата на данните на учащите се изисква балансиран подход, който съчетава административен надзор с технологични предпазни мерки. В административен план това включва създаване на ясни протоколи за работа с данни, възлагане на отговорности на персонала в зависимост от ролята му и осигуряване на редовно обучение, за да се гарантира, че всеки разбира ролята си в поддържането на сигурността на данните. От технологична гледна точка се прилагат мерки като криптиране, сигурни комуникационни канали и контрол на достъпа, за да се защитят данните от неоторизиран достъп и нарушения. Заедно тези измерения създават съгласувана рамка за защита на информацията за учащите.
Заглавие на инструмента	Модули за обучение на персонала относно GDPR и обработката на данни
Връзка към инструмента	• Coursera • Udemy • TalentLMS • Articulate 360
За инструмента	Модулите за обучение на персонала по GDPR и обработката на данни, достъпни в платформи като Coursera и Udemy, са от съществено значение, за да се гарантира, че преподавателите разбират и спазват разпоредбите за защита на данните. Тези модули осигуряват интерактивно обучение, което помага на персонала да развие уменията, необходими за сигурно боравене с данните на обучаемите. Като използват платформи като TalentLMS или Articulate 360, институциите могат да създават персонализирани програми за обучение, които да отговарят на специфичните им нужди. Това обучение е от жизненоважно значение за поддържане на култура на сигурност на данните в образователните институции.

Инструмент 4:

Тема	**Административни и технологични аспекти на сигурността за защита на данните на учащите се**
Описание на темата	Защитата на данните на учащите се изисква балансиран подход, който съчетава административен надзор с технологични предпазни мерки. В административен план това включва създаване на ясни протоколи за работа с данни, възлагане на отговорности на персонала в зависимост от ролята му и осигуряване на редовно обучение, за да се гарантира, че всеки разбира ролята си в поддържането на сигурността на данните. От технологична гледна точка се прилагат мерки като криптиране, сигурни комуникационни канали и контрол на достъпа, за да се защитят данните от неоторизиран достъп и нарушения. Заедно тези измерения създават съгласувана рамка за защита на информацията за учащите.
Заглавие на инструмента	Рамки за киберсигурност за институциите
Връзка към инструмента	• Ръководство за прилагане на контролите на CIS • Рамка за киберсигурност на NIST
За инструмента	Рамките за киберсигурност като Ръководството за прилагане на контролите на CIS и Рамката за киберсигурност на NIST предоставят насоки за защита на институционалните системи и данни. Тези рамки очертават най-добрите практики за киберсигурност, като помагат на институциите да прилагат надеждни мерки за сигурност, за да се предпазят от киберзаплахи. Като следват тези рамки, образователните институции могат да гарантират, че техните данни и системи са добре защитени и отговарят на индустриалните стандарти. Този проактивен подход помага да се предотвратят пробиви в данните и да се поддържа институционалната сигурност.

Инструмент 5:

Тема	**Административни и технологични аспекти на сигурността за защита на данните на учащите се**
Описание на темата	Защитата на данните на учащите се изисква балансиран подход, който съчетава административен надзор с технологични предпазни мерки. В административен план това включва създаване на ясни протоколи за работа с данни, възлагане на отговорности на персонала в зависимост от ролята му и осигуряване на редовно обучение, за да се гарантира, че всеки разбира ролята си в поддържането на сигурността на данните. От технологична гледна точка се прилагат мерки като криптиране, сигурни комуникационни канали и контрол на достъпа, за да се защитят данните от неоторизиран достъп и нарушения. Заедно тези измерения създават съгласувана рамка за защита на информацията за учащите.
Заглавие на инструмента	Инструменти за виртуална частна мрежа (VPN)
Връзка към инструмента	• NordVPN • ExpressVPN
За инструмента	Инструменти за виртуални частни мрежи (VPN) като NordVPN и ExpressVPN осигуряват интернет връзки по време на виртуални учебни сесии, особено в публични мрежи. Чрез криптиране на данните по време на преноса VPN мрежите предпазват от подслушване и атаки от типа "човек в средата", като гарантират, че поверителната информация остава поверителна. Това е особено важно за преподавателите, които често работят от разстояние или използват обществени мрежи. Използването на VPN помага за поддържане на сигурността на образователните комуникации.

Инструмент 6:

Тема	**Административни и технологични аспекти на сигурността за защита на данните на учащите се**
Описание на темата	Защитата на данните на учащите се изисква балансиран подход, който съчетава административен надзор с технологични предпазни мерки. В административен план това включва създаване на ясни протоколи за работа с данни, възлагане на отговорности на персонала в зависимост от ролята му и осигуряване на редовно обучение, за да се гарантира, че всеки разбира ролята си в поддържането на сигурността на данните. От технологична гледна точка се прилагат мерки като криптиране, сигурни комуникационни канали и контрол на достъпа, за да се защитят данните от неоторизиран достъп и нарушения. Заедно тези измерения създават съгласувана рамка за защита на информацията за учащите.
Заглавие на инструмента	Комуникационни инструменти, насочени към поверителността
Връзка към инструмента	• Сигнал • Microsoft Teams
За инструмента	Инструменти за комуникация с фокус върху поверителността като Signal и Microsoft Teams (с разширени настройки за сигурност) криптират видео и текстова комуникация с обучаемите. Тези инструменти осигуряват криптиране от край до край и сигурни механизми за удостоверяване, като гарантират, че чувствителната информация, обменяна по време на сесиите, остава поверителна. Като използват тези инструменти, преподавателите могат да запазят поверителността на комуникациите, докато си сътрудничат с обучаеми или колеги. Това повишава доверието и спазването на разпоредбите за защита на данните.

Инструмент 7:

Тема	**Административни и технологични аспекти на сигурността за защита на данните на учащите се**
Описание на темата	Защитата на данните на учащите се изисква балансиран подход, който съчетава административен надзор с технологични предпазни мерки. В административен план това включва създаване на ясни протоколи за работа с данни, възлагане на отговорности на персонала в зависимост от ролята му и осигуряване на редовно обучение, за да се гарантира, че всеки разбира ролята си в поддържането на сигурността на данните. От технологична гледна точка се прилагат мерки като криптиране, сигурни комуникационни канали и контрол на достъпа, за да се защитят данните от неоторизиран достъп и нарушения. Заедно тези измерения създават съгласувана рамка за защита на информацията за учащите.
Заглавие на инструмента	Софтуер за одит и мониторинг
Връзка към инструмента	• Splunk • SolarWinds
За инструмента	Софтуер за одит и мониторинг като Splunk и SolarWinds следи достъпа до данни и идентифицира потенциални нарушения след сесията. Тези инструменти анализират дневниците и мрежовата активност, за да откриват инциденти със сигурността на ранен етап, което позволява на институциите да предприемат бързи действия за намаляване на щетите. Като използват тези инструменти, преподавателите могат да гарантират, че мерките за сигурност на данните са ефективни и отговарят на регулаторните стандарти. Този проактивен мониторинг помага за поддържане на целостта на образователните системи.

Инструмент 8:

Тема	**Административни и технологични аспекти на сигурността за защита на данните на учащите се**
Описание на темата	Защитата на данните на учащите се изисква балансиран подход, който съчетава административен надзор с технологични предпазни мерки. В административен план това включва създаване на ясни протоколи за работа с данни, възлагане на отговорности на персонала в зависимост от ролята му и осигуряване на редовно обучение, за да се гарантира, че всеки разбира ролята си в поддържането на сигурността на данните. От технологична гледна точка се прилагат мерки като криптиране, сигурни комуникационни канали и контрол на достъпа, за да се защитят данните от неоторизиран достъп и нарушения. Заедно тези измерения създават съгласувана рамка за защита на информацията за учащите.
Заглавие на инструмента	Шаблони за уведомяване за нарушаване на сигурността на данните
Връзка към инструмента	• Съветник по GDPR
За инструмента	Шаблоните за уведомяване за нарушаване на сигурността на данните помагат на институциите да се подготвят за нарушаване на сигурността на данните и да реагират на него, като предоставят структурирани рамки за уведомяване на засегнатите страни и регулаторните органи. Тези шаблони гарантират, че уведомленията са в съответствие с разпоредби като GDPR, като улесняват навременната и прозрачна комуникация в случай на нарушение. Като използват тези шаблони, преподавателите могат бързо да реагират на инциденти, като същевременно поддържат съответствие със законовите изисквания.

Инструмент 9:

Тема	**Административни и технологични аспекти на сигурността за защита на данните на учащите се**
Описание на темата	Защитата на данните на учащите се изисква балансиран подход, който съчетава административен надзор с технологични предпазни мерки. В административен план това включва създаване на ясни протоколи за работа с данни, възлагане на отговорности на персонала в зависимост от ролята му и осигуряване на редовно обучение, за да се гарантира, че всеки разбира ролята си в поддържането на сигурността на данните. От технологична гледна точка се прилагат мерки като криптиране, сигурни комуникационни канали и контрол на достъпа, за да се защитят данните от неоторизиран достъп и нарушения. Заедно тези измерения създават съгласувана рамка за защита на информацията за учащите.
Заглавие на инструмента	Механизми за обратна връзка
Връзка към инструмента	• Формуляри на Google • Mentimeter • Forms.app
За инструмента	Механизми за обратна връзка като формуляри на Google с криптиране или Mentimeter позволяват на преподавателите да събират обратна връзка от обучаемите относно практиките за сигурност на данните по време на курсовете. Тези инструменти осигуряват сигурни платформи за анонимна обратна връзка, като помагат на преподавателите да идентифицират областите за подобрение в процесите на работа с данни. Чрез използването на тези механизми институциите могат да усъвършенстват своите практики за сигурност на данните и да повишат доверието на обучаемите. Този цикъл на обратна връзка е от съществено значение за поддържането на сигурна и отговаряща на нуждите образователна среда.

Инструмент 10:

Тема	**Административни и технологични аспекти на сигурността за защита на данните на учащите се**
Описание на темата	Защитата на данните на учащите се изисква балансиран подход, който съчетава административен надзор с технологични предпазни мерки. В административен план това включва създаване на ясни протоколи за работа с данни, възлагане на отговорности на персонала в зависимост от ролята му и осигуряване на редовно обучение, за да се гарантира, че всеки разбира ролята си в поддържането на сигурността на данните. От технологична гледна точка се прилагат мерки като криптиране, сигурни комуникационни канали и контрол на достъпа, за да се защитят данните от неоторизиран достъп и нарушения. Заедно тези измерения създават съгласувана рамка за защита на информацията за учащите.
Заглавие на инструмента	Механизми за обратна връзка
Връзка към инструмента	• Формуляри на Google • Mentimeter • Forms.app
За инструмента	Механизми за обратна връзка като формуляри на Google с криптиране или Mentimeter позволяват на преподавателите да събират обратна връзка от обучаемите относно практиките за сигурност на данните по време на курсовете. Тези инструменти осигуряват сигурни платформи за анонимна обратна връзка, като помагат на преподавателите да идентифицират областите за подобрение в процесите на работа с данни. Чрез използването на тези механизми институциите могат да усъвършенстват своите практики за сигурност на данните и да повишат доверието на обучаемите. Този цикъл на обратна връзка е от съществено значение за поддържането на сигурна и отговаряща на нуждите образователна среда.