Aplikácia systému nahlasovania protispoločenskej činnosti s využitím softvérovej podpory

Metodický rámec:

1. SMERNICA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2019/1937 o ochrane osôb, ktoré nahlasujú porušenia práva Únie
2. Zákon č. 54/2019 Z. z. o ochrane oznamovateľov protispoločenskej činnosti a o zmene a doplnení niektorých zákonov
3. ISO 37001:2025 Systémy manažérstva proti korupcii. Požiadavky s usmernením na používanie

Softvérová podpora:

Znalostná softvérová aplikácia ISIT software SK Cybersecurity (IS ISIT KB) s lokalizáciou v slovenskom a v českom jazyku. Modul Manažment výučby je učený pre výučbu riadenia procesov podľa jednotlivých modulov aplikácie.

Moduly IS ISIT KB

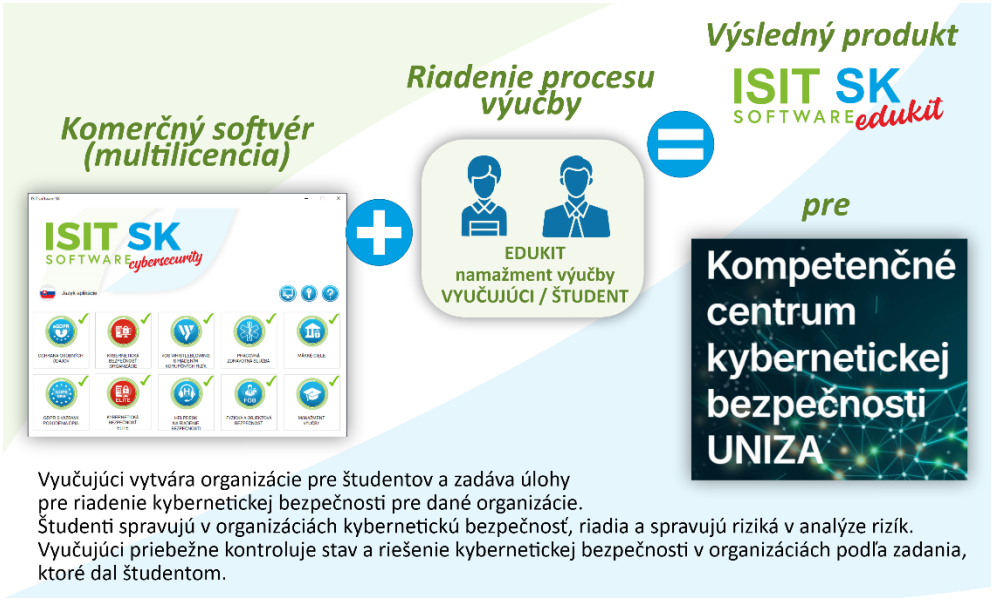
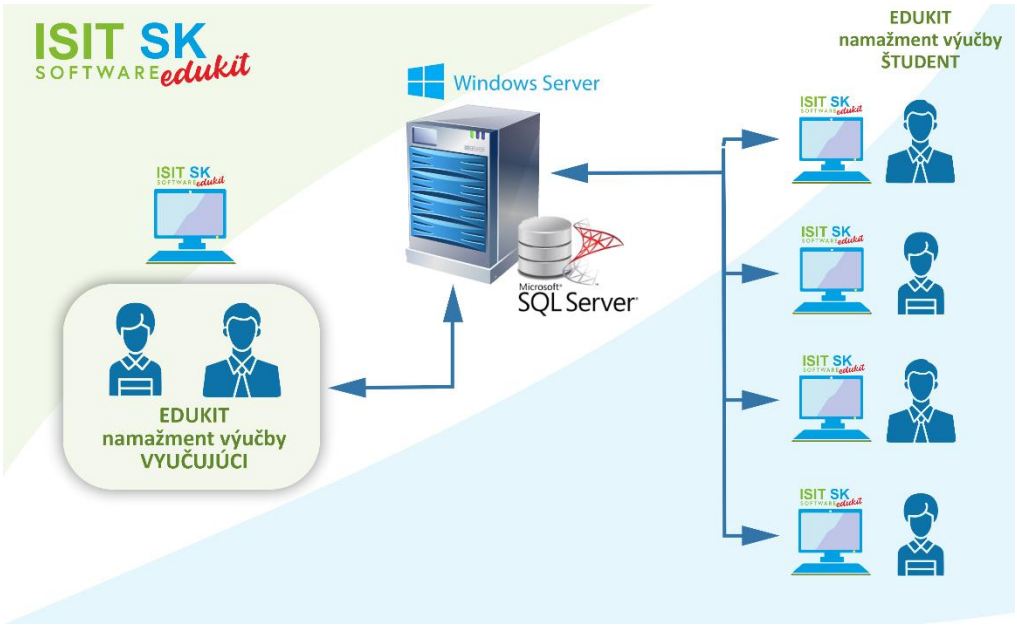


Schéma riešenia IS ISIT KB



Bloková schéma zapojenia IS ISIT GDPR

Zadanie 1: Základná konfigurácia softvéru

Úloha: Oboznámte sa so softvérom SW ISIT modul Whistleblowing a vykonajte jeho základnú konfiguráciu.

Kroky:

- Prihláste sa do administrátorskej konzoly softvéru.

- Vyplňte základné údaje o organizácii (názov, adresa, kontaktné údaje).

- Nastavte prístupové práva pre rôzne úrovne používateľov (Superadmin, Asistent, Audítor).

Cieľ: Naučte sa, ako správne nastaviť softvér pre efektívne spracovanie oznámení a zabezpečiť prevenciu kriminality.

Zadanie 2: Simulácia podávania oznámení

Úloha: Simulujte podávanie oznámení prostredníctvom webového formulára.

Kroky:

- Vyplňte oznamovací formulár s rôznymi typmi oznámení (anonymné, chránené).

- Odošlite oznámenie a sledujte proces spracovania.

- Získajte potvrdenie o prijatí oznámenia a pridelenie ID.

Cieľ: Získajte praktické skúsenosti s podávaním oznámení a pochopte, ako systém spracováva tieto podania v kontexte prevencie kriminality.

Zadanie 3: Predbežné posúdenie oznámení

Úloha: Hodnoťte podané oznámenia a vykonajte predbežné posúdenie.

Kroky:

- Pracujte v skupinách a analyzujte rôzne scenáre oznámení, ktoré sa týkajú potenciálnych trestných činov.

- Odpovedzte na štyri kľúčové otázky na určenie rizika a platnosti oznámenia.

- Vygenerujte a zašlite odpoveď oznamovateľovi.

Cieľ: Naučte sa, ako správne posúdiť oznámenia a komunikovať s oznamovateľmi, pričom zohľadnite prevenciu kriminality.

Zadanie 4: Vyšetrovanie oznámení

Úloha: Simulujte proces vyšetrovania platných oznámení.

Kroky:

- Vyplňte záznamy k vyšetrovaniu v aplikácii.

- Navrhnite nápravných opatrenia na základe výsledkov vyšetrovania, ktoré by mohli zabrániť opakovaniu trestnej činnosti.

- Generujte záverečné dokumenty a zašlite ich príslušným orgánom.

Cieľ: Získajte praktické skúsenosti s procesom vyšetrovania a dokumentovaním výsledkov, pričom zohľadnite prevenciu kriminality.

Zadanie 5: Technické požiadavky a implementácia

Úloha: Oboznámte sa s technickými požiadavkami na implementáciu softvéru.

Kroky:

- Diskutujte o technických požiadavkách pre jednorazové a viacorganizácie.

- Navrhnite plán implementácie softvéru v reálnej organizácii, ktorá sa zaoberá prevenciou kriminality.

Cieľ: Pochopte technické aspekty a požiadavky na úspešnú implementáciu systému, ktorý podporuje prevenciu kriminality.

Tieto zadania poskytnú študentom praktické zručnosti a hlboké porozumenie fungovaniu softvéru VOS Whistleblowing v kontexte prevencie kriminality.

Use Case: Implementácia a využitie softvéru ISIT modul Whistleblowing **na Žilinskej univerzite**

Názov: Implementácia systému VOS Whistleblowing pre prevenciu kriminality na Žilinskej univerzite

Účel: Zabezpečiť efektívne a dôverné podávanie oznámení o protiprávnych činnostiach a zlepšiť prevenciu kriminality v akademickom prostredí.

Zainteresované strany:

- **Oznamovatelia**: Študenti, zamestnanci univerzity, ktorí chcú nahlásiť protiprávne činnosti.
- **Administrátori**: Osoby zodpovedné za správu systému a spracovanie oznámení.
- **Audítori**: Osoby, ktoré vykonávajú vyšetrovanie podaných oznámení.
- **Právne oddelenie**: Zabezpečuje dodržiavanie legislatívy a ochranu oznamovateľov.

Predpoklady:

- Softvér VOS Whistleblowing je nainštalovaný a plne funkčný na serveroch univerzity.
- Všetci administrátori a audítori sú vyškolení na používanie systému.

Scenár:

 Podávanie oznámenia:

- Oznamovateľ (študent alebo zamestnanec) navštívi webovú stránku Žilinskej univerzity, kde je umiestnený odkaz na formulár VOS Whistleblowing.
- Oznamovateľ vyplní formulár, pričom si môže zvoliť, či chce oznámenie podať anonymne alebo s ochranou identity.
- Po odoslaní formulára obdrží oznamovateľ potvrdenie o prijatí oznámenia s prideleným ID.

 Spracovanie oznámenia:

- Administrátor sa prihlási do administrátorskej konzoly softvéru.
- Administrátor skontroluje nové oznámenia a priradí ich príslušným audítorom na spracovanie.

- Audítor vykoná predbežné posúdenie oznámenia, odpovedá na štyri kľúčové otázky a určuje, či oznámenie spadá pod legislatívu.

 Vyšetrovanie:

- Ak je oznámenie považované za platné, audítor začne proces vyšetrovania.
- Audítor vyplní záznamy k vyšetrovaniu a navrhne nápravné opatrenia.
- Po ukončení vyšetrovania audítor vygeneruje záverečné dokumenty a zašle ich príslušnému orgánu, ak je to potrebné.

 Komunikácia s oznamovateľom:

- Oznamovateľ je informovaný o výsledku predbežného posúdenia do 7 dní a o výsledku vyšetrovania do 3 mesiacov.
- V prípade, že oznámenie je zamietnuté, oznamovateľ dostane informáciu o dôvodoch zamietnutia.

Výsledok:

- Implementácia systému VOS Whistleblowing na Žilinskej univerzite umožní efektívne a dôverné podávanie oznámení o protiprávnych činnostiach, čím sa zlepší prevencia kriminality a ochrana oznamovateľov v akademickom prostredí.

Záver:

- Tento use case demonštruje, ako môže Žilinská univerzita využiť softvér VOS Whistleblowing na zabezpečenie transparentnosti a ochrany v rámci svojho prostredia, čím sa posilní dôvera medzi študentmi a zamestnancami.