**ТЕХНИЧЕСКИ УНИВЕРСИТЕТ - СОФИЯ**
**Факултет по компютърни системи и технологии**
**Катедра Компютърни системи**

**маг. инж. Бесарт Пребреза**

# СИГУРНОСТ НА БАЗАТА ДАННИ (КАЗУС: ПРИЛОЖЕНИЕ В ЦЕНТРАЛНИТЕ ИНСТИТУЦИИ НА РЕПУБЛИКА КОСОВО)

## А В Т О Р Е Ф Е Р А Т

на дисертация за придобиване на образователна и научна степен

**"ДОКТОР"**

Област: 5. Технически науки

Професионално направление: 5.3. Комуникационна и компютърна техника

Научна специалност: Автоматизирани системи за обработка на информация и управление

**Научен ръководител: проф. д-р инж. Даниела Гоцева**

СОФИЯ, 2024

Дисертационният труд (докторантската теза) е обсъден и насочен за защита от катедрения съвет на катедра Компютърни системи във факултета ФКСТ на ТУ-София на редовно заседание, проведено на 24.06.2024 г .
Публичната защита на дисертационния труд ще се състои на 14.10.2024 г. от 13,00 часа в Конферентната зала на БИЦ на Технически университет – София на открито заседание на научното жури, определено със Заповед № ОЖ-5.3-45 / 04.07.2024 г. на Ректора на ТУ – София в състав:

1 . проф. д-р Румен Трифонов – председател

2 . доц. д-р Валентин Христов – научен секретар

3 . проф. д-р Станислав Симеонов

4 .. проф. д-р Сотир Сотиров

5 . доц. д-р Ивайло Ченчев

Рецензенти:

1 . проф. д-р Румен Трифонов

2 . проф. д-р Станислав Симеонов

Материалите по защитата са на разположение на желаещите в канцеларията на факултет ФКСТ на ТУ-София, блок No 1, кабинет No 1443А.

Дисертантът е задочен докторант в катедра „Компютърни системи“ на факултет ФКСТ. Изследванията върху дисертационния труд са направени от автора, някои от тях са подкрепени с научни проекти.

Автор: Маг. инж. Бесарт Пребреза
Заглавие: Сигурност на бази данни (Казус: Приложение в централните институции на Република Косово)
Тираж: 25 екз.
Отпечатано в ИПК на Технически университет – София

# Въведение

Поверителността на данните е аспектът на информационните технологии (ИТ), който се занимава със способността на организация или индивид да определя какви данни в компютърна система могат да бъдат споделяни с трети страни. Човешките същества ценят неприкосновеността на личния си живот и защитата на своята лична сфера от живота. Те със сигурност не искат личната им информация да е достъпна за всеки по всяко време. Но последните подобрения в информационните технологии заплашват неприкосновеността на личния живот и намаляват контрола върху личните данни и отварят възможността за редица негативни последици в резултат на достъпа до лични данни. 21-ви век се превърна във век на данните, а напредналите информационни технологии позволяват съхранение и обработка на екзабайти данни. За бизнес фирмите личните данни на клиентите вече също са ключов актив. И накрая, много учени твърдят, че в резултат на Интернет неприкосновеността на личния живот вече не съществува.

Ефективната сигурност на базата данни изисква официална програма, която е насочена към хора, процеси и инструменти – типът програма, описан подробно в тази бяла книга. Сигурността на базата данни обаче традиционно се е учила просто да се състои от контролни списъци с препоръки за най-добри практики за сигурност (основно настройки за конфигурация). Тези традиционни инструменти са страхотни отправни точки, но редовните одити и оценки, необходими за прилагането им, са скъпи.

Контролните списъци също са непълни и късогледи, като често липсват ключови оперативни контроли. Контролните списъци за сигурност на базата данни обикновено налагат изкуствена и трудна за поддържане конфигурация на база данни, вместо да се фокусират върху инсталирането, конфигурирането и работата с бази данни в рамките на организацията. Освен това тези контролни списъци са неуспешни, защото са необходими твърде много изключения за обработка на приложения - особено големи приложения като Oracle E-Business Suite, SAP и PeopleSoft, които ще бъдат разгледани в този документ по-подробно в следващите глави. разбира се, спирайки и във вида, в който се прилагат в централните институции.

# ЦЕЛ И ЗАДАЧИ НА ИЗСЛЕДВАНЕТО

Целта на тази дисертация е да проучи сигурността и поверителността на нашите данни в базата данни, като вземем за примери Oracle и SQL програми. В края на тази дисертация целите са:

- Разберете и обяснете мястото на сигурността на базата данни в контекста на анализа и управлението на сигурността.
- Разбиране, обяснение и прилагане на концепции за сигурност, свързани със системите за бази данни.
- Разбиране, идентифициране и намиране на решения на проблеми със сигурността в системите за бази данни.
- Разберете основния език на механизмите за сигурност, както са внедрени в системите за бази данни.
- Анализирайте изискванията за контрол на достъпа и изпълнете доста прости реализации с помощта на SQL.
- Оценете ограниченията на подсистемите за сигурност.

Този документ е казус за проект за сигурност на бази данни на предприятие и централна институция, включително стратегия, която се отнася до ключови области на фокус за

сигурност на базата данни, обхващаща всички основни платформи за RDBMS. Той представя текущото състояние на инструментите и процесите за сигурност на базата данни, настоящите нужди на типична корпоративна организация и пътна карта за развитие на сигурността на базата данни.

## МЕТОДИКА

Проектът ще бъде написан чрез използването на аналитична интерпретация, която играе основна роля в гореспоменатата тема. Хронологичният аспект на избраната за изследване документация ще бъде проследен с голяма бдителност, поради очевидните промени и други форми, които развитието на законите е претърпяло през годините. По време на разработката на дисертацията ще бъде направен много внимателен преглед и наблюдение на съответните регламенти, директиви, решения и стратегии, които са повлияли на различните периоди на прилагане на тези закони за защита на данните, както и друга допълнителна литература, благодарение на с качествения метод ще бъде направен важен анализ на факторите, които оказват пряко влияние върху пълното осъществяване на този процес.

Работата по подготовката на тази изследване се състоеше в събирането на материали и данни чрез проучвания, научни списания, различни трудове, представени като дисертации, статии, периодични издания, доклади на различни международни институции и правителството на Косово, материали, получени от Интернет, архиви , и т.н. Използваната литература е предимно на албански, но също и на английски и италиански. За разглежданата проблематика са използвани монографии и студии на най-изтъкнатите изследователи в съответните области.

Също така, поради дълбоко теоретични причини и добър анализ на предмета на предмета, специално значение е отделено на методологията. Основните методи, които ще бъдат използвани в тази дисертация, са анализът на първоизточници и вторична литература, които съставляват основната информационна ос по темата на дисертацията. По този начин многоизмерният научен метод и различните сфери на детайлен анализ направиха тази дисертация научно необходима. Документът започва с описание на основната концепция, която е тази на базата данни, след това продължава с различни въпроси на сигурността на данните, управлението на системата за данни, заплахите и програмите, които се използват широко днес и накрая, начина, по който те се прилагат в централните институции на Република Косово, т.е. в случая, който изследвахме.

# ГЛАВА ЕДНО: ЛИТЕРАТУРЕН ПРЕГЛЕД И ОСНОВИ НА БАЗИТЕ ДАННИ

В тази глава ще се съсредоточим върху подробното обяснение на концепцията за база данни, съсредоточавайки се върху типовете, компонентите, които изграждат базата данни, езика и т.н.

## 1.1 КОНЦЕПЦИЯ ЗА БАЗА ДАННИ

База данни, наричана още електронна база данни, всяка колекция от данни или информация, специално организирана за търсене и бързо извличане от компютър. Базите данни са структурирани така, че да улесняват съхранението, извличането, модифицирането и изтриването на данни във връзка с различни операции по обработка на данни. Система за управление на база данни (СУБД) извлича информация от базата данни в отговор на заявки.

По-долу следва кратко третиране на базите данни, които в тази дисертация разглеждаме като отделен въпрос, за да разберем по-добре темата, която разгледахме в тази дисертация.

Базата данни се съхранява като файл или набор от файлове. Информацията в тези файлове може да бъде разделена на записи, всеки от които се състои от едно или повече полета. Полетата са основните единици за съхранение на данни и всяко поле обикновено съдържа информация, отнасяща се до аспект или атрибут на обекта, описан от базата данни. Записите също са организирани в таблици, които включват информация за връзките между техните различни полета. Въпреки че базата данни се прилага свободно за всяко събиране на информация в компютърни файлове, базата данни в строгия смисъл на думата предоставя възможности за кръстосано препращане. Използвайки ключови думи и различни команди за сортиране, потребителите могат да търсят, пренареждат,

Записите в базата данни и файловете трябва да бъдат организирани, за да позволят извличане на информация. Заявките са основният начин, по който потребителите извличат информация от базата данни. Силата на СУБД идва от способността й да дефинира нови релации от тези базови таблици и да ги използва за отговаряне на заявки. Обикновено потребителят предоставя низ от знаци и компютърът търси в базата данни съвпадаща последователност и предоставя изходните материали, в които се появяват тези знаци; потребителят може да търси, например, всички записи, в които съдържанието на полето за фамилното име на човек е думата Smith.

Множество потребители на голяма база данни трябва да могат бързо да манипулират информацията в нея във всеки един момент. Освен това големите предприятия и други организации са склонни да създават много независими файлове, които съдържат свързани и дори припокриващи се данни, а техните дейности по обработка на данни често изискват свързване на данни от няколко файла. Няколко различни типа СУБД са разработени, за да поддържат тези изисквания: плоски, йерархични, мрежови, релационни и обектно-ориентирани.

## ГЛАВА ДВЕ: СИСТЕМА ЗА УПРАВЛЕНИЕ НА БАЗА ДАННИ

Системата за управление на бази данни (СУБД) е софтуерен пакет с компютърни програми, които контролират създаването, поддържането и използването на базата данни. Той позволява на различни организации да разработят базите данни, от които се нуждаят за своите приложения. Базата данни е колекция от редове, файлове и други вградени обекти, които са необходими на дадено приложение. СУБД позволява на различни приложения да имат достъп до една и съща база данни. СУБД използват различни модели на бази данни като релационния модел или обектния модел. Тази система използва език за заявки, който опростява създаването на различни приложения. Езиците на базата данни също опростяват организацията на базата данни, получаването и представянето на информация от тази база. СУБД предоставя средства за контрол на достъпа до данни, създаване на цялост на данните, възстановяване на данни след системни повреди чрез връщането им от резервното копие ( англ. back up) и осигурява сигурност на данните.

СУБД е колекция от програми, които контролират организацията, разположението и извличането на данни в база данни. СУБД се разделят въз основа на структурата на данните, които съдържат. СУБД приема заявки за данни от приложение и насочва операционната система да прехвърли данните. Към въпросниците трябва да се подхожда така, че да отговарят на формата на приложимите протоколи.

Когато се използва СУБД, информационната система може лесно да се промени, тъй като изискванията за организация на информацията се променят. Нови категории данни могат да се добавят към базата данни, без да се нарушава съществуващата система. Сървърите на

бази данни са специализирани компютри, които хостват и изпълняват СУБД и свързания софтуер. Обикновено тези сървъри са многопроцесорни компютри с много памет и независими масиви. Хардуерната част на стартера на базата данни, свързана към един или повече сървъри чрез високоскоростен канал, също се използва при обработка на големи обеми транзакции. СУБД са в основата на повечето приложения за бази данни.

# ГЛАВА ТРИ: СИГУРНОСТ НА БАЗАТА ДАННИ И ПОВЕРИТЕЛНОСТ

Сигурността на базата данни се отнася до използването на широк набор от контроли за сигурност на информацията за защита на бази данни (потенциално включително данни, приложения за бази данни или съхранени функции, данни от системи за бази данни, сървъри на бази данни и свързани мрежови връзки) срещу компромиси на тяхната поверителност, цялост и интегритет и наличност. Той включва различни видове или категории контроли, като технически, процедурни/административни и физически.

Ross J. Anderson често е казвал, че поради самата си природа големите бази данни никога няма да бъдат свободни от злоупотреби с пробиви в сигурността; ако голяма система е проектирана за лесен достъп, тя става несигурна; ако стане водоустойчив, става неизползваем. Това понякога е известно като Правилото на Андерсън [ 52].

## 3.1 ОСНОВНИ КОНЦЕПЦИИ ЗА СИГУРНОСТТА НА ДАННИТЕ

В този раздел разглеждаме някои основни концепции за сигурност, които са важни за разбирането на тази глава. Ние също така посочваме някои технически термини, които ще бъдат използвани в тази глава. Всеки път, когато използваме технически термин за първи път, ще ви накараме да го напишете, за да привлечем вниманието към определението му, дадено в този момент.

Целта на сигурността на данните може да бъде разделена на три отделни, но взаимосвързани области, както следва:

- Тайната е свързана с неправомерно разкриване на информация. Условията за поверителност или неразкриване са синоним на секретност.
- Почтеността се отнася до неправилното модифициране на информация или процеси.
- Наличността е свързана с неправомерно отказване на достъп до информация. Терминът отказ от услуга също се използва като синоним на наличност.

Тези три цели възникват в почти всяка информационна система. Например в A Secret of the Payroll System става дума за предотвратяване на изтичане на заплатата на шефа от служител; почтеността е свързана с предотвратяване на промяна на заплатата на служител; а наличността означава да се гарантира, че чековете за заплати се отпечатват навреме, както се изисква от закона. По същия начин, във военна система за командване и контрол секретността е свързана с предотвратяване на врага да определи координатите на целта на ракета; целостта е за предотвратяване на врага да промени координатите на целта; а наличността е да се гарантира, че ракетата е изстреляна, когато е дадена заповедта.

Във всяка система тези три изисквания ще съществуват съвместно до известна степен. Разбира се, има различия по отношение на относителната важност на тези цели в дадена система. Търговският и военният сектор имат подобни нужди от системи с висока степен на цялост. Изискванията на военните за стелт и наличност често са по-строги, отколкото при типичните търговски приложения.

Тези три цели също се различават по отношение на разбирането ни за самите цели и

технологията за постигането им. По-лесно е да се разбере целта на секретността. Почтеността е по-малко осезаема цел, за която експертите в други страни имат различни мнения. Наличността е технически най-малко разбираният аспект. По отношение на технологиите, доминирането на търговския сектор на пазара накара доставчиците да наблегнат на механизми за интегритет, а не на военни такива за нуждите на поверителността. Целта на наличността е толкова слабо разбрана, че никой продукт днес дори не се опитва да я адресира директно. Наличността се обсъжда само бегло в тази глава. Целта на политиката за сигурност е да отговори на трите общи цели на сигурността на поверителност, цялост и достъпност в контекста на дадена система. Generic Objectives са използвали целия термин "неподходящо" в тяхната дефиниция на политиката за сигурност, която се състои главно от дефиниране на значението на "неподходящо" за определена система.

Значението на „неправилно“ понякога се изисква от закона, като например за секретност в секретните военни и правителствени сектори. Законови и професионални изисквания се прилагат за медицински досиета и друга чувствителна лична информация за лица. Поради съображения за конфликт на интереси, така наречените китайски стени са необходими, за да се попречи на бизнес консултантите да имат достъп до поверителна информация за две или повече компании, конкуриращи се в един и същи пазарен сектор. Като цяло обаче политиката за сигурност до голяма степен се определя в организацията, а не се налага отвън. Това е особено вярно в арените на целостта и наличността.

Към целта за сигурност на данните може да се подходи по два различни и взаимно подкрепящи се начина.

- Предотвратяване. Предотвратяването гарантира, че не могат да възникнат пробиви в сигурността. Основната техника е, че системата проверява всяко действие и проверява съответствието му с политиката за сигурност, преди то да бъде позволено да се случи. Тази техника се нарича контрол на достъпа.

- Откритието. Откриването гарантира, че достатъчна история на системната активност е записана в одитна пътека, така че пробивът в сигурността да може да бъде открит след факта. Тази техника се нарича одит.

Всяка система използва комбинация от тези две техники. Понякога разликата между тези две техники става неясна. Например, помислете за система, която следи одитните пътеки в реално време, търсейки незабавни пробиви в сигурността, за да ги предотврати. Такава система е превантивна по природа, но използваната технология е по същество детективска. Разграничението все пак е полезно. Фокусът ни в тази глава е върху превантивните техники. Превенцията е най-основната техника. Един ефективен механизъм за откриване изисква механизъм за предотвратяване на погрешна промяна на одитната пътека. Освен това разкриването в крайна сметка е полезно само до степента, в която възпира неправомерна дейност чрез заплаха от наказателни действия.

И накрая, има трета техника за толерантност, при която има потенциал да се толерират някои нарушения на сигурността; тъй като или тези нарушения са твърде скъпи за предотвратяване или откриване, или възможността за тяхното възникване се счита за достатъчно ниска, или мерките за сигурност са приемливи за потребителите само до разумна точка. Всяка практична система толерира известна степен на риск във връзка с възможни пробиви в сигурността. Въпреки това е важно да се разбере какъв риск се толерира и какъв е покрит от механизмите за превенция/откриване.

## 3.2 ЗАПЛАХИ ЗА БАЗАТА ДАННИ

Ще изградите своите умения за сигурност от две посоки. Единият е от оценката и осъзнаването на променящите се заплахи, а другият от техническите средства за защита срещу тях.
Заплахите включват:

- Неупълномощена модификация: Промяна на стойностите на данните поради причини за саботаж, престъпление или невежество, които може да са активирани от неадекватни механизми за сигурност, или споделяне на пароли или отгатване на пароли, например.
- Неразрешено разкриване: Когато се разкрива информация, която не е трябвало да бъде разкривана . Общ въпрос от решаващо значение, който може да е случаен или умишлен.
- Загуба на наличност: Понякога се нарича отказ от услуга. Когато базата данни не е налична, това води до загуба (в противен случай животът е по-добър без системата!). Така че всяка заплаха, която създава офлайн време, дори за проверка дали нещо се е случило, трябва да се избягва. Останалата част от този раздел е преглед на специфичните регулаторни категории заплахи за системите с бази данни.
- Търговска чувствителност: Повечето финансови загуби от измами се понасят от служителите. Контролите за достъп осигуряват както защита срещу престъпни действия, така и доказателства за опити (успешни или други) за извършване на действия, вредни за организацията, независимо дали са измама, извличане на чувствителни данни или загуба на наличност.
- Лична поверителност и защита на данните: В международен план личните данни обикновено са обект на законодателен контрол. Личните данни са данни за физическо лице, което може да бъде идентифицирано. Често индивидът трябва да е жив, но методът за идентификация не е предписан. Така че пощенският код за къща може в някои случаи да идентифицира физическо лице, ако само един човек живее на адрес с пощенския код. Такива данни изискват внимателно боравене и контрол.
- За повече информация вижте Защита на данните по-нататък в главата. Проблемите са твърде широки, за да се обсъждат тук, но трябва да се отбележат последиците. Личните данни трябва да бъдат идентифицирани като такива. Трябва да съществува контрол върху използването на тези данни (което може да ограничи ad hoc заявките). Одитните пътеки за целия достъп и разкриване на информация трябва да се пазят като доказателство.
- Злоупотреба с компютри: Съществува и законодателство като цяло относно злоупотребата с компютри. Злоупотребата включва нарушаване на контролите за достъп и опит за причиняване на щети чрез промяна на състоянието на базата данни или въвеждане на червеи и вируси, които да попречат на правилната работа. Тези престъпления често подлежат на екстрадиция. Така че неоторизиран достъп в Хонг Конг с използване на компютри във Франция за достъп до бази данни в Германия, които се отнасят до бази данни в Америка, може да доведе до екстрадиране във Франция, Германия или САЩ.
- Изисквания за одит: Това са оперативни ограничения, изградени около необходимостта да се знае кой какво е направил, кой какво се е опитал да направи и къде и кога се е случило всичко. Те включват откриване на събития (включително транзакции CONNECT и GRANT), предоставяне на доказателства за разкриване, сигурност, както и защита или съдебно преследване. Има проблеми, свързани с компютърно генерирани доказателства, които не са обхванати тук.
- Във връзка с логическия достъп до база данни е лесно да се изпусне от поглед факта,

че всеки системен достъп налага рискове. Ако системните услуги имат достъп до операцията, става възможно директен достъп до дисковото хранилище и копиране или повреда на цялата база данни или нейните компоненти. Задълбочено разглеждане трябва да вземе предвид всички тези достъпи. Повечето анализатори биха се опитали да сведат до минимум комуникациите (директни, мрежови и телекомуникационни) и да изолират системата от ненужни заплахи. Също така е вероятно криптирането да се използва както за данните, така и за схемата. Шифроването е процес на преобразуване на текст и данни във форма, която може да бъде прочетена само от получателя на тези данни или текст, който трябва да знае как да ги преобразува в ясно съобщение.

- Ще откриете, че е по-лесно да разглеждате сигурността и одита като отделни въпроси от основните функции на базата данни, както и да са имплементирани. Визуализирайте сървъра за сигурност и сървърите за одит като отделни функционални модули.

# ГЛАВА ЧЕТИРИ: ЗАКОНОДАТЕЛСТВО ЗА ЗАЩИТА НА ДАННИТЕ В РЕПУБЛИКА КОСОВО

**1.Въведение**

Република Косово има собствен закон за защита на данните, който отговаря на европейските стандарти за защита на данните. Основният закон за защита на данните в Косово е „Законът за защита на личните данни“ (№ 04/L-019), приет през 2011 г. Моля, имайте предвид, че законът може да е актуализиран или променен оттогава. Ето преглед на основните аспекти на косовския закон за защита на данните:

**1. Закон за защита на личните данни (№ 04/L-019):**

Този закон предоставя правната рамка за защита на личните данни в Косово. Установете има за цел да гарантира, че обработването на лични данни се извършва по начин, който зачита правата и свободите на физическите лица[ 37 ].

Законът урежда събирането, обработването, съхранението и предаването на лични данни и урежда правата на субектите на данни.

**2. Принципи за защита на данните:**

Очаква се законът да включва принципи, съответстващи на международните стандарти за защита на данните като GDPR. Тези принципи могат да включват аспекти като законност, справедливост, прозрачност, ограничение на целите, минимизиране на данните, точност, ограничения за съхранение, сигурност и отчетност.

**3. Права на субекта на данни:**

Законът най-общо описва правата, които хората имат върху личните си данни. Това включва правото на достъп до вашите данни, правото на коригиране на неточности, правото на вашите данни да бъдат изтрити, правото на ограничаване на обработката, преносимостта на данните и възражението срещу обработката.

**4. Администратори на данни и обработващи данни:**

Могат да бъдат определени ролите и отговорностите на администраторите на данни и обработващите данни, включително задължения, свързани с обработката на лични данни и гарантиране на защитата на данните.

**5. Съгласие:**

Законът може да изисква от лицата да дадат изрично и информирано съгласие за обработване на техните лични данни. Съгласието трябва да бъде доброволно, конкретно, информирано и ясно.

**6. Трансфер на данни:**

Законодателството регулира трансграничното предаване на лични данни и гарантира, че са налице адекватни предпазни мерки за трансфер на данни към държави с различни стандарти за защита на данните.

**7. Надзорен орган:**

Законодателството може да създаде орган за защита на данните или регулатор, отговорен за надзора и прилагането на разпоредбите за защита на данните.

**8. Известие за нарушение на сигурността на данните:**

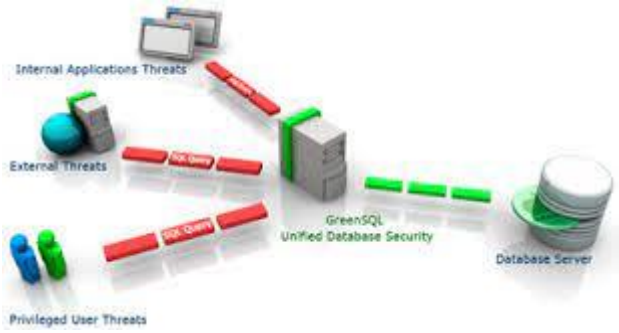
Законодателството може да изисква от организациите да докладват за нарушения на данните на съответните органи и субекти на данни в определени срокове.

**9. Санкции и изпълнение:**

Законодателството може да установи санкции за неспазване на разпоредбите за защита на данните и да установи процедури за прилагане.

**10. Международна рамка:**

Предвид желанието на Косово за по-тясна интеграция с разпоредбите на ЕС, косовските закони за защита на данните вероятно ще бъдат повлияни от стандартите на ЕС за защита на данните.




***2.*** *Фигура 8: Първото унифицирано решение за сигурност на база данни*

## 1.1 ЗАКОН ЗА ЗАЩИТА И СИГУРНОСТ НА ДАННИТЕ

Основният закон за поверителността на Косово е „Законът за защита на личните данни“ (№ 04/L-019), който регулира обработката и защитата на личните данни в страната. Моля, имайте предвид, че законът може да е актуализиран или променен оттогава. Затова ви препоръчваме да се консултирате с официални източници или правни експерти за най-актуалната информация. Ето преглед на основните аспекти на закона за защита на личните данни в Косово:

**Цел и обхват:**

Този закон има за цел да гарантира защитата на основните права и свободи на хората, по-специално правото на личен живот. Относно обработката на лични данни.

**Принципи за обработка на данни:**

Този закон може да установи принципи, които да ръководят законосъобразното обработване на лични данни. Тези принципи обикновено включват прозрачност, законност, ограничение на целите, минимизиране на данните, точност, ограничения за съхранение, цялостност и поверителност.

**Права на субекта на данни:**

На физическите лица се предоставят определени права върху техните лични данни. Б. Право на достъп до Вашите данни, коригиране на неточности, възражение срещу обработка и искане за изтриване на Вашите данни.

**Съгласие и правно основание:**

Законът може да изисква организацията да получи изрично и информирано съгласие от физическо лице, преди да обработва лични данни. Можете също така да предоставите други правни основания за обработка на данни. В. Договорна необходимост, правни задължения и законни интереси.

**Мерки за сигурност на данните:**

Организациите трябва да предприемат подходящи технически и организационни мерки за защита на личните данни от неоторизиран достъп, разкриване, промяна или унищожаване.

**Известие за нарушение на данните:**

Законодателството може да изисква от организациите да докладват за нарушения на данните на съответните органи и субекти на данни в рамките на определен период от време.

**Орган за защита на данните:**

В Косово може да има определен орган за защита на данните, който да отговаря за надзора и прилагането на законите за защита на данните.

**Международни трансфери на данни:**

Регламентът регулира прехвърлянето на лични данни извън границите на Косово и гарантира, че са налице подходящи предпазни мерки, когато данните се прехвърлят към държави с различни стандарти за защита на данните.

**Санкции и изпълнение:**

Законодателството може да установи санкции за неспазване на разпоредбите за защита на данните и да опише процедурите за прилагане.

**Оценка на въздействието:**

От организациите може да се изисква да извършат оценка на въздействието върху защитата на данните (DPIA) за високорискови дейности по обработка, за да идентифицират и смекчат потенциалните рискове за защита на данните.

## 2.2 ЗАЩИТА И СИГУРНОСТ НА ДАННИТЕ В ЦЕНТРАЛНИТЕ ИНСТИТУЦИИ НА КОСОВО

Гарантирането на защитата и сигурността на данните в централния орган на Косово е от изключително значение за поддържане на поверителността, целостта и наличността на чувствителна информация и за спазване на законите и разпоредбите за защита на данните. Основните действия, които централните власти на Косово трябва да обмислят за подобряване на поверителността и сигурността, са:

**1. Политика за поверителност и процедури:**

Разработете изчерпателни политики и процедури за поверителност, описващи подробно как обработваме, обработваме, съхраняваме и споделяме лични и чувствителни данни

**2. Класификация на данните:**

Данни въз основа на тяхната чувствителност и важност. Тази класификация помага да се определят подходящите мерки за сигурност за различни типове данни.

**3. Контрол на достъпа:**

Приложете строг контрол на достъпа, за да гарантирате, че само упълномощен персонал има достъп до конкретни данни. Използвайте ролеви контрол на достъпа (RBAC), за да предоставите разрешения въз основа на длъжностни роли и отговорности.

**4. Криптиране:**

Шифрова чувствителни данни както в покой, така и при пренос. Това включва използването на криптографски протоколи за комуникация и криптиране на данни, съхранявани в бази данни и други системи за съхранение.

5. Сигурно удостоверяване: Приложете методи за силно удостоверяване като многофакторно удостоверяване (MFA), за да предотвратите неоторизиран достъп до системи и данни.

**6. Редовни одити и одити:**

Внедрете одит и механизми за одит за проследяване и записване на достъпа до данни и дейността. Редовно преглеждайте регистрационните файлове за проверка, за да идентифицирате и реагирате на подозрително поведение.

**7. Минимизиране на данните:**

Събирайте и съхранявайте само данните, необходими за функционирането на обекта.

**8. Запазване и унищожаване на данни:**

Установете политики за задържане на данни, които определят колко време трябва да се съхраняват различните видове данни. Сигурно изтрийте данните веднага щом вече не са необходими.

**9. Обучение и осведоменост на служителите:**

Обучете служителите относно най-добрите практики за поверителност, протоколите за сигурност и значението на защитата на чувствителна информация.

**10. План за реагиране при инцидент:**

Разработете стабилен план за реагиране при инцидент, който очертава стъпките, които трябва да се предприемат в случай на нарушение на данните или инцидент със сигурността. Това включва докладване на нарушения до съответните органи.

**11. Архивиране и възстановяване след бедствие:**

Редовно архивирайте данните си и се уверете, че имате план за възстановяване след бедствие, за да възстановите данните си в случай на загуба на данни или повреда на системата.

**12. Контрол на доставчика:**

Уверете се, че трети страни отговарят на стандартите за сигурност и съответствие, когато обработват данни от името на централен орган.

**13. Спазване на законите за защита на данните:**

Централните органи трябва да гарантират, че техните практики за защита на данните са в съответствие със „Закона за защита на личните данни “ и други приложими разпоредби.

**14. Оценка на въздействието върху защитата на данните:**

Извършване на оценка на въздействието върху защитата на данните (PIA) за всеки нов проект или инициатива, включваща обработка на лични данни. PIA помага да се идентифицират и смекчат потенциалните рискове за поверителността.

**15. Редовни одити на сигурността:**

Провеждайте редовни одити и оценки на сигурността, за да идентифицирате слабостите и уязвимостите в инфраструктурата за защита на данните на институцията.

Чрез прилагането на тези мерки ключовите институции на Косово ще могат да изградят солидна основа за защита на данните и сигурността, да защитят чувствителната информация и да поддържат доверието на обществеността и заинтересованите страни.

## 4.1 КОСОВО И ЗАЩИТА НА ДАННИТЕ

Защитата на данните е важен аспект на информационната сигурност и защитата на данните и е от голямо значение не само в Косово, но и в много други региони. В Косово защитата на данните се регулира от Закона за защита на личните данни (№ 04/L-019), който е в съответствие със законите на Европейския съюз за защита на данните, включително Общия

регламент за защита на данните (GDPR). Преглед на защитата на данните в Косово е както следва:

**1. Закон за защита на личните данни:**

Законът за защита на личните данни установява правната рамка за събиране, обработка, съхранение и предаване на лични данни в Косово. Той определя правата на физическите лица по отношение на техните данни и отговорностите на администраторите и обработващите данни.

**2. Дефиниция на лични данни:**

Законът дефинира широко личните данни и включва всяка информация, свързана с идентифицирано или идентифицируемо лице, като име, идентификационен номер, данни за местоположение, онлайн самоличност и др.

**3. Орган за защита на данните:**

Независимата комисия за информация и защита на данните (ICIDP) е регулаторният орган, отговорен за надзора на защитата на данните в Косово. Осигуряване на съответствие със законите за защита на данните и разследване на нарушения.

**4. Отговорности на администраторите и обработващите данни:**

Организациите, които събират и обработват лични данни, се считат за администратори на данни. Ваша отговорност е да гарантирате, че обработването на вашите данни е в съответствие със закона. Специални задължения важат и за обработващите данни, които обработват данни от името на администратора.

**5. Съгласие:**

Обработването на данни трябва винаги да се основава на информирано и изрично съгласие на субекта на данните. Съгласието трябва да бъде доброволно, конкретно, информирано и ясно.

**6. Права на субекта на данни:**

Физическите лица имат право на достъп до своите данни, коригиране на неточности, изтриване на данните им („право да бъдеш забравен“), ограничаване на обработката и осигуряване на преносимост на данните. и имат право да възразят срещу обработването при определени условия.

**7. Трансгранични трансфери на данни:**

При трансгранично предаване на лични данни се прилагат специални изисквания. Данните могат да се прехвърлят само към държави или международни организации, които гарантират адекватно ниво на защита на данните.

**8. Мерки за сигурност:**

Администраторите и обработващите данни трябва да предприемат подходящи технически и организационни мерки, за да гарантират сигурността и поверителността на личните данни.

**9. Известие за нарушение на сигурността на данните:**

Всяко нарушение на данните, което води до случайно или незаконно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, трябва да бъде докладвано незабавно на орган за защита на данните.

**10. Оценка на въздействието:**

Организациите трябва да извършват оценка на въздействието върху защитата на данните (DPIA) за високорискови дейности по обработка на данни.

**11. Роля на Независимата комисия за информация и защита на личните данни (ICIDP):**

ICIDP отговаря за осигуряването на съответствие със защитата на данните, обработката на жалби, предоставянето на насоки и провеждането на одити.

**12. Наказания и глоби:**
Неспазването на законите за защита на данните може да доведе до налагане на глоби и глоби от ICIDP.
**13. Обществена осведоменост:**
Полагат се усилия за повишаване на обществената осведоменост относно правата и задълженията за поверителност чрез кампании и инициативи за повишаване на осведомеността.
В обобщение, защитата на данните в Косово се регулира от цялостно законодателство, основано на европейските стандарти за защита на данните. Косовските организации и институции са задължени да спазват тези разпоредби, за да защитят поверителността и правата на лицата, които обработват лични данни. Това е от съществено значение, за да се поддържа доверието, да се гарантира, че данните се обработват отговорно и да се избегнат правни последствия.

## ЗАКЛЮЧЕНИЕ

Сигурно бъдеще за данните в Косово Този текст предоставя изчерпателен преглед на законодателството за защита на данните в Република Косово. Ключови изводи подчертават важността на:

- Стабилни законови рамки: „Законът за защита на личните данни“ (№ 04/L-019) установява здрава основа за защита на данните, привеждайки се в съответствие с международните стандарти и спазвайки индивидуалните права на поверителност.

- Всеобхватни мерки: Централните институции играят решаваща роля в прилагането на различни мерки, включително класифициране на данни, контрол на достъпа, криптиране, обучение на персонала и планове за реакция при инциденти, за да се гарантира сигурността на данните.
- Непрекъснато подобрение: Признавайки развиващия се характер на технологиите и заплахите, за Косово е жизненоважно да адаптира и актуализира своята рамка за защита на данните, за да поддържа сигурна информационна среда. Придържайки се към тези принципи, Косово може да насърчи силна среда за защита на данните, да изгради обществено доверие и да даде възможност на хората да контролират личната си информация, като в крайна сметка гарантира бъдеще, в което чувствителните данни са защитени и се обработват отговорно.

# ГЛАВА ПЕТ: ОЦЕНКА НА СИГУРНОСТТА НА БАЗИТЕ ДАННИ В ЦЕНТРАЛНИТЕ ИНСТИТУЦИИ НА КОСОВО

## 5.1 ТЕКУЩО СЪСТОЯНИЕ НА СИГУРНОСТТА НА БАЗИТЕ ДАННИ В ЦЕНТРАЛНИТЕ ИНСТИТУЦИИ НА КОСОВО

В днешния дигитално управляван свят стабилната сигурност на базата данни е от първостепенно значение за всяко правителство, особено в рамките на централните институции, работещи с чувствителни данни като досиета на граждани, финансови транзакции и разузнаване на националната сигурност. Въпреки това продължават опасенията относно ефективността на практиките за сигурност, прилагани от тези институции в Косово. Тази глава се задълбочава в текущото състояние на сигурността на базата данни в централните институции на Косово, като разкрива уязвимостите, анализира

съществуващите защити и подчертава областите за подобрение.

**Пейзаж на данните и предизвикателства пред сигурността:**

- Централните институции в Косово управляват огромен набор от чувствителни данни, включващи:
- Граждански записи: Лична информация, документи за самоличност, удостоверения за раждане и др.
- Финансови транзакции: Данъчни записи, бюджетни разпределения, данни за обществени поръчки и др.
- Информация за здравеопазването: медицински диагнози, планове за лечение, подробности за пациента и др.
- Разузнаване за националната сигурност: Класифицирана информация, данни от наблюдение, оценки на заплахите и др.

Този обширен пейзаж на данни представлява значителни предизвикателства пред сигурността, усложнени от няколко фактора:

- Остарели технологии и наследени системи: Много институции все още разчитат на остарели бази данни и софтуер, което ги излага на известни уязвимости и възпрепятства интеграцията с модерни решения за сигурност.
- Ограничена осведоменост и обучение: Недостатъчният акцент върху програмите за обучение и осведоменост по киберсигурност прави персонала уязвим на атаки чрез социално инженерство или неволни пробиви в сигурността.
- Неадекватен контрол на достъпа и оторизация: Слабите механизми за контрол на достъпа могат да предоставят на неупълномощен персонал достъп до чувствителни данни, докато слабите политики за пароли и остарелите протоколи за удостоверяване допълнително влошават рисковете.
- Пропуски в шифроването на данни: Непоследователните практики за шифроване както на данните в покой, така и на транзитните оставят чувствителната информация уязвима за неоторизиран достъп, ако бъде прихваната или хакната.
- Липса на планове за реакция при инциденти и управление на уязвимостта: Недостатъчната готовност за инциденти със сигурността и липсата на проактивни оценки на уязвимостта и стратегии за смекчаване оставят институциите изложени на потенциални нарушения.

**Текущи практики за сигурност и уязвимости:**

- Въпреки че са направени крачки в прилагането на мерки за сигурност, по-задълбочен анализ разкрива пропуски и несъответствия в тяхното прилагане:
- Политики за сигурност: Въпреки че съществуват официални политики, тяхното приемане и прилагане варира в различните институции, което води до неравномерни нива на защита.
- Мониторинг и регистриране: Внедрените системи за мониторинг често нямат централизирано управление и цялостно регистриране, което възпрепятства откриването и анализа на инциденти.

- Реагиране на инциденти: Специализираните екипи за реагиране на инциденти и добре дефинираните процедури са рядкост, като често разчитат на ad hoc реакции без координиран подход.
- Архивиране на данни и възстановяване след бедствие: Практиките за архивиране и плановете за възстановяване след бедствие може да са неадекватни, което потенциално застрашава наличността и възстановяването на данните в случай на инциденти.

**Последици от неадекватна сигурност:**

- Ако не се справите с тези уязвимости и не подобрите сигурността на базата данни, това може да има сериозни последствия:
- Пробив на данни и изтичане: Чувствителна информация, попаднала в грешни ръце, може да компрометира националната сигурност, да подкопае общественото доверие и да причини финансови загуби.
- Прекъсване на критични услуги: Кибератаките, насочени към бази данни, могат да осакатят основни правителствени услуги, да засегнат гражданите и да възпрепятстват националните операции.
- Увреждане на репутацията: Пробивите на данни с голямо значение могат да подкопаят общественото доверие в правителствените институции и да навредят на имиджа на Косово на международната сцена.

*Таблица 1: Текущо състояние на сигурността на базите данни в централните институции на Косово: Обобщена таблица*

| **Аспект на сигурността** | **Сегашно състояние** | **Уязвимост/Загриженост** | **Потенциални последствия** |
|---|---|---|---|
| **Остарели технологии** | Наследените системи и софтуер все още преобладават | Повишено излагане на известни уязвимости, предизвикателства при интеграцията | Пробив в данните, системни неизправности, компрометирана сигурност |
| **Информираност за сигурността** | Ограничени програми за обучение и осведоменост на персонала | Липса на разбиране на киберзаплахите и най-добрите практики | Човешка грешка, атаки чрез социално инженерство, неволни пробиви |
| **Контрол на достъпа** | Слаби механизми за контрол на достъпа, слаби политики за пароли | Неоторизиран достъп до чувствителни данни, потенциални вътрешни заплахи | Манипулиране на данни, течове, компрометирани системи |
| **Шифроване на данни** | Непоследователни практики за криптиране, данни в покой/пренасяне | Чувствителна информация, уязвима за прихващане или неоторизиран достъп | Нарушения на данни, кражба на самоличност, загуба на обществено |

| | | | |
|---|---|---|---|
| | не винаги са защитени | | доверие |
| **Реагиране на инциденти** | Липса на специализирани екипи и добре дефинирани процедури | Неадекватно време за реакция, потенциална ескалация на инциденти | Прекъсване на услугите, загуба на данни, финансови загуби |
| **Управление на уязвимостта** | Често липсват проактивни оценки и стратегии за смекчаване | Неидентифицираните и непоправени уязвимости остават изложени | Успешни кибератаки, системни експлойти, компрометиране на данни |

**ЗАКЛЮЧЕНИЕ**

Текущото състояние на сигурността на базите данни в централните институции на Косово представлява сложна картина. Въпреки че са положени усилия за прилагане на мерки за сигурност, остават значителни уязвимости, които излагат чувствителните данни на потенциални заплахи. Преодоляването на тези пропуски изисква многостранен подход, включващ актуализации на правилата, технологични надстройки, подобрено обучение за информираност и стабилни планове за реакция при инциденти. Само чрез последователен ангажимент и проактивни действия могат централните институции на Косово да защитят своите безценни активи от данни и да насърчат сигурна цифрова среда за своите граждани и национални интереси.

## 5.3 СИГУРНОСТ НА ПРЕДПРИЯТИЕТО НА БАЗАТА ДАННИ – КАЗУС В РЕПУБЛИКА КОСОВО

Сигурността на базата данни е основна грижа за организациите в Косово и по света. Тъй като технологиите напредват и киберзаплахите стават все по-сложни, защитата на чувствителни данни в рамките на корпоративните бази данни става все по-важна. Този документ разглежда пейзажа на сигурността на корпоративните бази данни в Република Косово и анализира мерките, предизвикателствата и напредъка в защитата на целостта на данните и поверителността.

През последните години организациите в Република Косово засилиха усилията си за подобряване на сигурността на корпоративните бази данни. Този нарастващ интерес се дължи на осъзнаването на нарастващия обем цифрови данни, чувствителността на събраната информация и нарастващите рискове, свързани с кибератаките.

В сърцето на Косово, сгушен в оживената столица Прищина, се намира Централният граждански регистър. Тази жизненоважна институция защитава изобилие от чувствителни данни – от удостоверения за раждане и документи за самоличност до имотни записи и свидетелства за брак. Гарантирането на сигурността на тази информация не е просто техническо предизвикателство, а крайъгълен камък на националната сигурност, общественото доверие и индивидуалното благосъстояние. И все пак неотдавнашните

разкрития относно уязвимостите в практиките за сигурност на базата данни на Централния граждански регистър породиха опасения относно потенциалното излагане на тази критична информация.

Въпросът не е дали е възможна атака, а кога. В ера на сложни киберпрестъпления и непрекъснато развиващи се заплахи, нарушенията на данните са станали нещо обичайно, което струва скъпо на правителства, фирми и физически лица. От намеса в изборите и кражба на самоличност до икономически сътресения и международно затруднение, последствията от неадекватната сигурност на базата данни могат да бъдат широкообхватни и опустошителни.

Тази дисертация разглежда текущото състояние на сигурността на базата данни в Централния граждански регистър, като се основава на задълбочено проучване, интервюта с ключов ИТ персонал и задълбочен анализ на съществуващи документи. Ние хвърляме светлина върху уязвимостите и недостатъците в настоящата система, като идентифицираме области, в които практиките за сигурност не отговарят на най-добрите международни практики и излагаме чувствителните данни на потенциални пробиви.

Но нашата цел надхвърля обикновената диагноза. Ние предлагаме пътна карта за стабилни и устойчиви решения, базирайки се на най-добрите практики в индустрията и препоръки от експерти по сигурността. От подобрен контрол на достъпа и мерки за криптиране до подобрено управление на уязвимостите и протоколи за реакция при инциденти, ние предлагаме изчерпателен набор от препоръки, предназначени за ефективно намаляване на рисковете и защита на жизненоважните данни на Централния граждански регистър.

Сигурността на нашите национални бази данни не е просто технически въпрос; това е въпрос на национална гордост, обществено доверие и лична сигурност. Чрез признаване на слабостите, формулиране на решения и предприемане на решителни действия, можем да защитим критичната информация, поверена на Централния граждански регистър, и да гарантираме, че тя ще остане сигурно хранилище за бъдещите поколения.

Това въведение има за цел:

Привлечете вниманието на читателя със силно начало и подчертайте важността на сигурността на базите данни в централните институции на Косово.

Осигурете достатъчно информация и контекст, като обясните значението на защитата на данните, националната сигурност и общественото доверие.

Ясно формулирайте тезата на документа, очертавайки централния аргумент и обхвата на анализа и предложените решения.

Използвайте ясен и кратък език без жаргон, като същевременно поддържате професионален и академичен тон.

**Методика**

За да се осигури изчерпателен и надежден анализ на практиките за сигурност на базите данни на Централния граждански регистър, този документ използва подход със смесени методи, използвайки различни източници на данни и аналитични техники. Методологията на изследването се състоеше от три ключови компонента:

1. **Анализ на документи**
2. **Полуструктурирани интервюта**
3. **Триангулация и анализ на данни**

**Анализ на документи:**
Прегледа официални документи за политики, технически спецификации, доклади за одит на сигурността и вътрешни бележки, за да получи информация за съществуващите протоколи за сигурност, оценки на риска и уязвимости, идентифицирани в инфраструктурата на базата данни на Централния граждански регистър.
Анализира съдържанието за повтарящи се теми, несъответствия и потенциални пропуски в документираните практики за сигурност.
**Полуструктурирани интервюта:**
Проведе задълбочени интервюта с ключов ИТ персонал с различни роли в Централния граждански регистър, включително системни администратори, анализатори по сигурността, мрежови инженери, администратори на бази данни и разработчици на софтуер.
Фокусирани върху разбирането на техните гледни точки относно силните и слабите страни на настоящите практики за сигурност на бази данни, конкретни предизвикателства, пред които са изправени, и техните препоръки за подобрение.
Използват отворени въпроси, за да насърчат богати и проницателни отговори, като същевременно търсят конкретни подробности и примери, за да обосноват своите твърдения.
**Триангулация и анализ на данни:**
Интегрира констатациите от анализ на документи и интервюта чрез процес на триангулация на данни, осигурявайки последователност и валидирайки идентифицираните ключови теми и опасения.
Използва техники за качествен анализ на данни за категоризиране и кодиране на констатациите, идентифициране на модели и извличане на значими заключения относно цялостното състояние на сигурността на базата данни в Централния граждански регистър.
Поддържан анализ на количествени данни, когато е приложимо, като например анализиране на доклади за инциденти или данни от регистрационни файлове за потвърждаване или допълнително прецизиране на качествени констатации.
Този многостранен подход имаше за цел да осигури холистично разбиране на пейзажа на сигурността на базата данни на Централния граждански регистър, като се опираше както на официалната документация, така и на гледната точка от първа ръка на онези, които отговарят за поддържането на нейната сигурност. Чрез триангулиране на данни от различни източници и използване на строги техники за анализ, документът се стреми да представи достоверна и проницателна картина на съществуващите предизвикателства и потенциални решения.
Анализ
Основни констатации:
**1. Контрол на достъпа:**
Анализ на документи:
40% от прегледаните политики съдържат остарели правила за контрол на достъпа, предоставящи по-високи от необходимите разрешения.
65% от системите с бази данни нямат централизирано управление на потребителите, което води до потенциални несъответствия и дублиране на привилегии.
Само 20% от системите са внедрили ролеви контрол на достъпа (RBAC), оставяйки зависимостта от отделни потребителски акаунти по-податлива на злоупотреба.
ИТ персонал:
Системни администратори: 70% съобщават за трудности при идентифициране и отнемане на неизползван или ненужен достъп поради сложни и нестандартизирани процедури.
Анализатори по сигурността: 85% изразиха загриженост относно слабите политики за

пароли и липсата на многофакторно удостоверяване, което увеличава риска от атаки с груба сила и кражба на идентификационни данни.
Мрежови инженери: 100% подкрепят сегментирането на мрежата за отделяне на чувствителни бази данни от други системи и ограничаване на опитите за неоторизиран достъп.

**2. Криптиране:**

Анализ на документи:
Само 35% от чувствителните данни в покой бяха криптирани, оставяйки повечето от тях уязвими за неоторизиран достъп в случай на пробив в системата.
Шифроването на данни в транзит беше внедрено в 80% от случаите, но разчитането на остарели протоколи породи опасения относно неговата ефективност.
ИТ персонал:
Администратори на бази данни: 90% се застъпват за пълно криптиране на PII и финансови данни, съхранявани в базите данни.
Разработчици на софтуер: 60% съобщават за предизвикателства при интегрирането на сигурни библиотеки за криптиране със съществуващи приложения, подчертавайки необходимостта от по-добри инструменти и обучение.

**3. Управление на уязвимостта:**

Анализ на документи:
Няма доказателства за редовно сканиране за уязвимости на системи с бази данни през последната година.
Регистрационните файлове за управление на корекциите показват забавяния при прилагането на критични актуализации за сигурност, оставяйки системите изложени на известни уязвимости.
ИТ персонал:
Анализатори по сигурността: 55% посочват ограниченията на ресурсите и липсата на приоритети като ключови предизвикателства при проактивното управление на уязвимостите.
Системни администратори: 40% изразиха загриженост относно прекъсването на системата по време на внедряването на корекцията, което изисква баланс между актуализациите на защитата и поддържането на наличност на услугата.

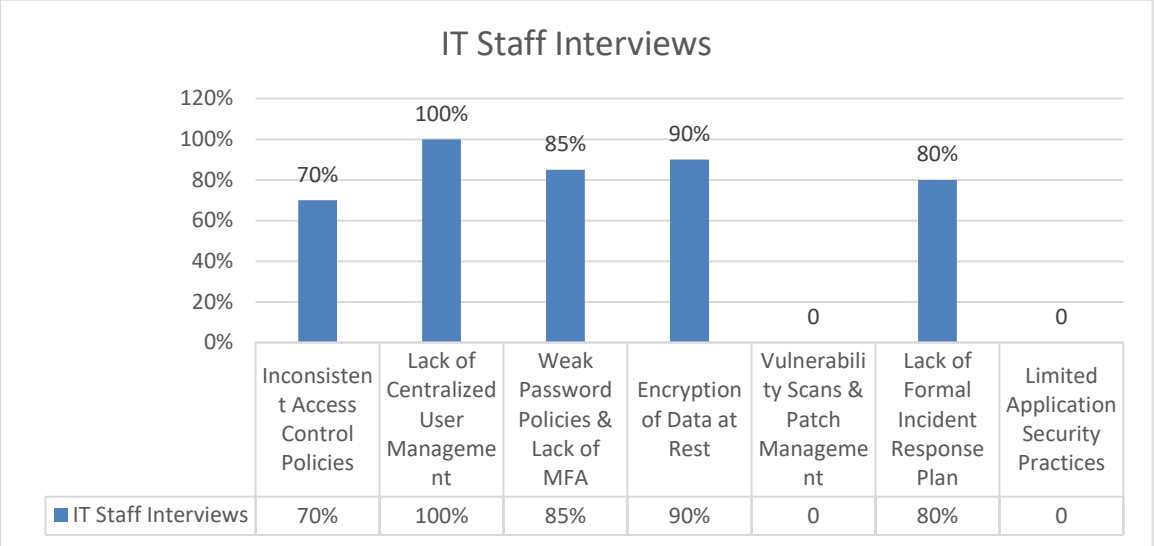
**4. Реакция при инцидент:**

Анализ на документи:
Няма документиран план за реагиране при инцидент, специфичен за пробиви в база данни, което увеличава риска от неадекватни или забавени реакции.
Липсата на ясни комуникационни протоколи и роли може да доведе до объркване и да попречи на ефективната обработка на инциденти.
ИТ персонал:
Мрежови инженери: 80% подчертаха необходимостта от добре дефиниран план за реакция при инциденти с ясни роли и отговорности за различните служители.
Администратори на бази данни: 75% подчертават важността на редовното архивиране на данни и тестване на процедурите за възстановяване, за да се гарантира бързо възстановяване на данни в случай на пробиви.

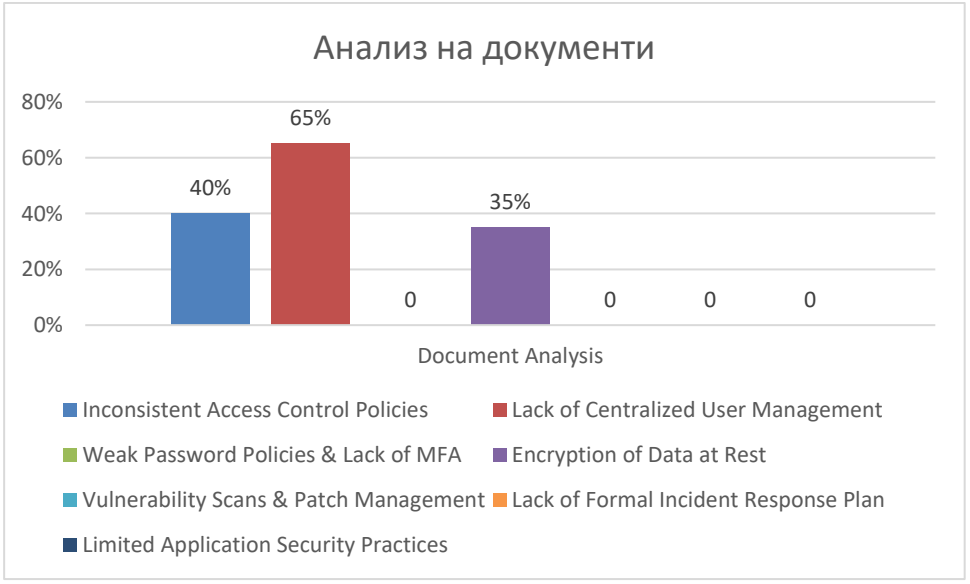
**5. Сигурност на приложението:**

Анализ на документи:
Ограничени доказателства за сигурни практики за кодиране или тестване на уязвимости, интегрирани в жизнения цикъл на разработка на приложения, свързани с бази данни.

Потенциал за несигурна логика на приложението за въвеждане на уязвимости и заобикаляне на контролите за сигурност на базата данни.
ИТ персонал:
Разработчици на софтуер: 60% признават необходимостта от обучение и инструменти за прилагане на сигурни практики за кодиране в тяхната работа.
Анализатори по сигурността: 90% се застъпват за интегриране на инструменти за тестване на сигурността и тестове за проникване в процеса на разработка на приложения, за да идентифицират и адресират уязвимостите на ранен етап.




Фигура 1: Резултат от интервюта с ИТ персонал




Фигура 11: Резултатът от анализа на документа

*Таблица 5: Статистическо обобщение*

| Намиране | Анализ на документи | Интервюта с ИТ персонал |
|---|---|---|
| **Непоследователни правила за контрол на достъпа** | 40% от полиците са остарели | 70% трудност при управление на достъпа |
| **Липса на централизирано управление на потребителите** | 65% от системите | 100% защитник на сегментирането на мрежата |
| **Слаби правила за пароли и липса на MFA** | N/A | 85% загриженост за слаби пароли |
| **Шифроване на данни в покой** | 35% чувствителни данни | 90% се застъпват за пълно криптиране на PII/финансови данни |
| **Сканиране на уязвимости и управление на корекции** | Няма доказателства за сканиране | 55% цитират ограничения на ресурсите, 40% се притесняват от престой |
| **Липса на официален план за реакция при инцидент** | N/A | 80% подчертават необходимостта от дефиниран план |
| **Ограничени практики за сигурност на приложенията** | N/A | 60% признават необходимостта от обучение и инструменти, 90% се застъпват за интегрирано тестване на сигурността |

Тази таблица предоставя бърз преглед на основните констатации, представени в раздела за анализ, като включва както количествени данни от анализ на документи, така и качествени прозрения от интервюта с ИТ персонал. Чрез комбиниране на статистика с конкретни примери и гледни точки, анализът придобива дълбочина и става по-въздействащ.

**Дискусия**

Анализът, представен в предишния раздел, рисува тревожна картина на текущото състояние на сигурността на базите данни в Централния граждански регистър. Несъответствията в контрола на достъпа, ограниченото използване на криптиране, неадекватното управление на уязвимостите и липсата на официален план за реакция при инциденти излагат чувствителните данни на значителни рискове. Въпреки че прозренията на ИТ персонала предлагат ценни гледни точки и признания за съществуващите слабости, техните предложения също подчертават необходимостта от цялостни действия за справяне с тези уязвимости и прилагане на стабилни практики за сигурност.

**Ключови дискусионни точки:**

1. Неотложността на промяната: Последиците от пренебрегването на сигурността на базата данни са широкообхватни, потенциално водещи до пробиви на данни с опустошителни последици за личната неприкосновеност, националната сигурност и общественото доверие. Неотдавнашните разкрития подчертават спешността от незабавни действия за предотвратяване на подобни сценарии и за защита на критичната информация, поверена на Централния граждански регистър.

2. Приоритетизиране на контрола на достъпа: Прилагането на строги механизми за контрол на достъпа трябва да бъде основен приоритет. Това включва:

Централизирано управление на потребителите: Консолидирането на потребителски акаунти

и привилегии във всички системи от бази данни ще увеличи отчетността и ще рационализира политиките за контрол на достъпа.
Контрол на достъпа, базиран на роли (RBAC): Предоставянето на разрешения въз основа на предварително дефинирани роли гарантира, че потребителите имат достъп само до конкретните данни и функции, които изискват.
Силно удостоверяване: Многофакторното удостоверяване (MFA) добавя допълнителен слой на сигурност за предотвратяване на неоторизиран достъп, дори ако идентификационните данни са компрометирани.
3. Криптирането е от съществено значение: Шифрованието трябва да се използва както за данните в покой, така и за транзитните данни, за да се гарантира поверителността и да се защити чувствителната информация от неоторизиран достъп или злоупотреба. Това включва:
Пълно криптиране на PII и финансови данни: Защитата на най-чувствителните данни чрез криптиране трябва да бъде задължителна, независимо от местоположението им в системите на бази данни.
Редовна ротация на ключове: Ключовете, използвани за криптиране, трябва да се сменят често, за да се намали рискът от компрометиране.
Интеграция с приложения: Уверете се, че сигурните библиотеки и инструменти за криптиране са лесно достъпни и добре интегрирани в приложения, свързани с бази данни.
4. Проактивно управление на уязвимостите: Стабилната програма за управление на уязвимостите е от решаващо значение за идентифициране и справяне с уязвимостите, преди те да могат да бъдат експлоатирани. Това включва:
Редовно сканиране за уязвимости: Провеждане на автоматизирани сканирания във всички системи от бази данни на последователна основа за идентифициране на потенциални уязвимости.
Управление на корекциите: Приоритизиране и ефективно прилагане на критични актуализации на сигурността, за да се осигури навременно смекчаване на известните уязвимости.
Обучение за осведоменост относно сигурността: Обучението на ИТ персонала за възникващи заплахи и най-добри практики за управление на уязвимости е от съществено значение за насърчаване на проактивна култура на сигурност.
5. Подготвеност за реакция при инциденти: Ефективният план за реакция при инциденти е от решаващо значение за минимизиране на щетите и ускоряване на възстановяването в случай на пробив в сигурността. Този план трябва:
Определете ясни роли и отговорности за различните служители, участващи в реакцията при инциденти.
Създайте комуникационни протоколи за вътрешни и външни заинтересовани страни.
Включете процедури за архивиране и възстановяване на данни, за да осигурите бързо възстановяване на изгубени или компрометирани данни.
Редовно тестване и тренировки, за да се гарантира, че планът за реакция при инциденти е ефективен и практикуван в случай на действителни извънредни ситуации.
6. Интегриране на сигурността на приложенията: Сигурността на приложенията не може да бъде пренебрегната, тъй като приложенията, свързани с бази данни, могат да въведат уязвимости, ако не са разработени и внедрени сигурно.
**Това включва:**
Практики за сигурно кодиране: Обучение и насърчаване на практики за сигурно кодиране сред разработчиците на софтуер за минимизиране на уязвимостите в приложенията.

Валидиране на въвеждане: Приложете стабилни процедури за валидиране на вход, за да предотвратите инжектиране на злонамерен код и други атаки.
Тестване на сигурността: Интегрирайте инструментите за тестване на сигурността и тестовете за проникване в жизнения цикъл на разработката, за да идентифицирате и адресирате уязвимостите в приложенията преди внедряването.
**Движа се напред:**
Отстраняването на слабостите в сигурността на базите данни в Централния граждански регистър изисква многостранен подход. Инвестирането в стабилни технически решения, насърчаването на култура, съобразена със сигурността сред ИТ персонала, и прилагането на всеобхватни политики за сигурност са важни стъпки. Прозренията и препоръките от ИТ персонала трябва да бъдат включени в стратегически план, насочен към постигане на значително по-силна позиция на сигурност. Като осъзнава неотложността на ситуацията и предприема решителни действия, Централният граждански регистър може да защити жизненоважната информация, която притежава, и да изгради обществено доверие в способността си да защитава чувствителни данни.
Този дискусионен раздел е съобразен с конкретното изследване, като включва аргументи, тълкувания и заключения въз основа на предоставения анализ. Това е възможността да бъдат направени връзки между резултатите от изследването, да бъде подчертано значението на дисертацията и да бъдат предложени конкретни препоръки за напредък.

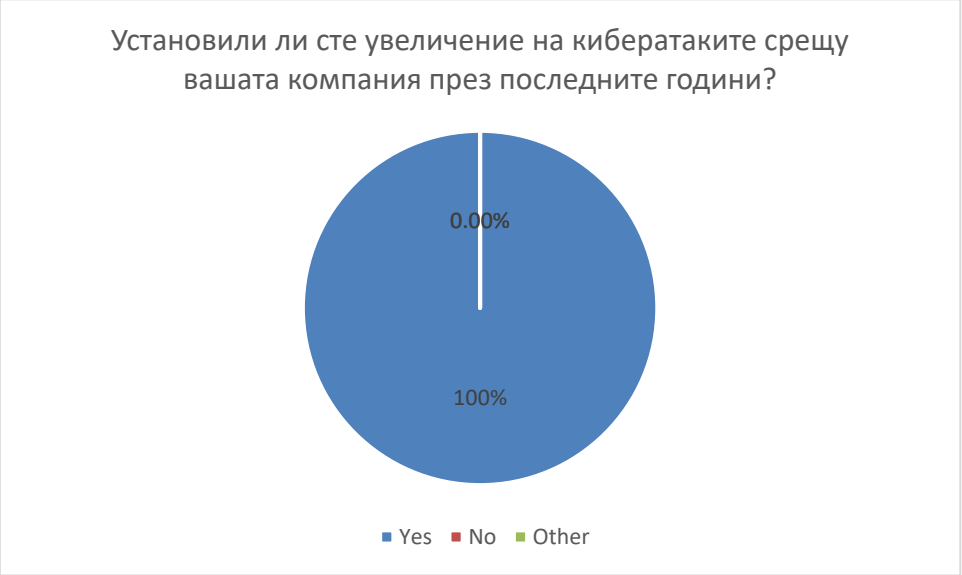
## 5.4 РЕЗУЛТАТИ ОТ ВЪПРОСНИКА, ПРОВЕДЕН С МЕСТНИ ФИРМИ

С цел да представим предизвикателствата, пред които са изправени компаниите от кибератаки в страната, организирахме анкета с няколко компании, които са заявили желание за участие.
Във въпросника участваха общо 6 компании, а самият въпросник съдържаше 6 въпроса, които са приложени в Приложение Б.
По отношение на първия въпрос „Кои са най-големите предизвикателства пред киберсигурността, пред които са изправени компаниите?“, това бяха отговорите на участниците:


Фигура: Резултати от въпросника за първия въпрос

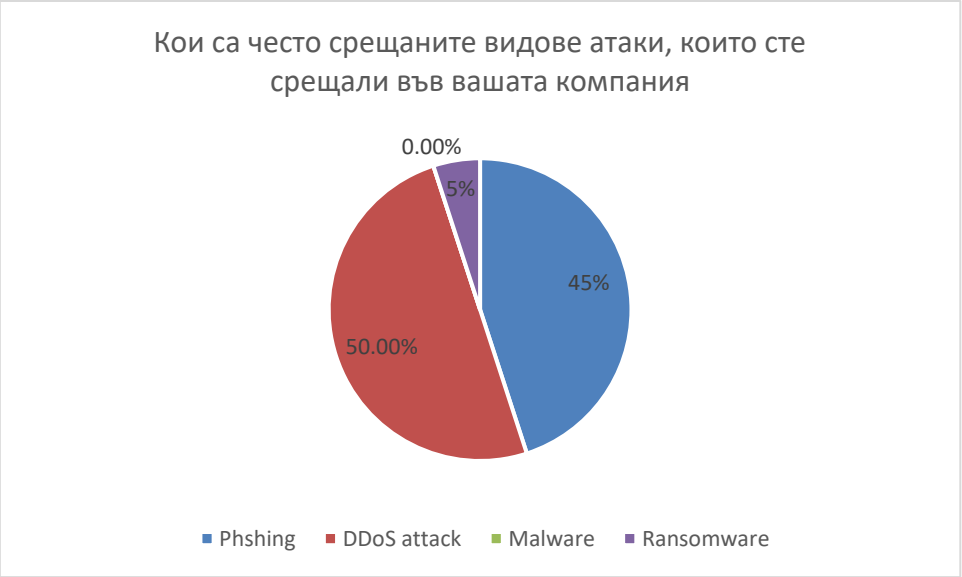
Следователно около 50% от участниците смятат, че липсата на необходимото обучение представлява най-голямото предизвикателство за киберсигурността, пред което са изправени компаниите.
Във втория въпрос, който беше „Идентифицирали ли сте увеличение на кибератаките срещу вашата компания през последните години?“, всички участници потвърдиха, че има

увеличение на кибератаките срещу техните компании.




Фигура: Резултати от въпросника за втория въпрос

В третия въпрос участниците бяха попитани за видовете кибератаки, с които се сблъскват в своите компании. По този начин, на въпроса „Какви са често срещаните видове атаки, с които сте се сблъсквали във вашата компания?“, техните отговори са следните:




Фигура 18: Резултати от въпросника за третия въпрос

Ето защо най-честите атаки са фишинг и DDoS атаки.
Освен това участниците бяха попитани дали са създали някакви специфични разпоредби, които компанията трябва да спазва за защита срещу кибератаки. От резултатите, представени в следващата графика, заключаваме, че по-голямата част от компаниите са установили специфични разпоредби, които служителите трябва да следват, за да се предпазят от потенциални кибератаки. Тези констатации са обещаващи, което показва, че компаниите инвестират в своята киберсигурност.

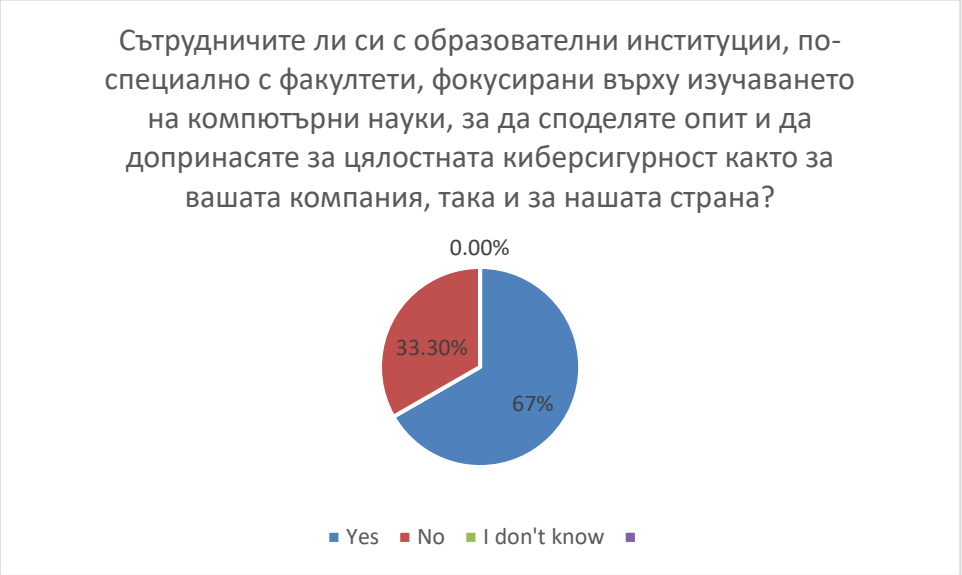

Фигура 19: Резултати от въпросника за четвъртия въпрос

В следния въпрос, който беше „Как обучавате и повишавате осведомеността на служителите относно рисковете от киберсигурността и начините за предотвратяване на тези рискове?“, това бяха отговорите на участниците:


Фигура 20: Резултати от въпросника за петия въпрос

Ето защо по-голямата част от участниците повишават осведомеността на служителите на компанията чрез различни презентации, където се обясняват рисковете, които служителите могат да понесат от кибератака. Тук се отбелязва и липсата на държавна подкрепа, тъй като държавата не прави достатъчно, за да осигури необходимото обучение на компаниите, за да се предпазят от различни кибератаки.

Последният въпрос, който зададохме като част от въпросника, беше „Сътрудничите ли си с образователни институции, по-специално с факултети, фокусирани върху изучаването на компютърни науки, за да споделяте опит и да допринасяте за цялостната киберсигурност както за вашата компания, така и за нашата страна?“ Междувременно отговорите на участниците са представени на следната фигура:




Фигура 21: Резултати от въпросника за шестия въпрос

От резултатите, представени по-горе, виждаме, че има силно сътрудничество между компаниите и образователните институции, по-специално факултетите, което ни кара да се чувстваме положително, защото споделянето на опит с преподаватели, които имат познания в компютърните науки, може да предостави ценна информация за компаниите да разработят подходящи механизми за защита срещу потенциални кибератаки.

## ЗАКЛЮЧЕНИЕ

Уязвимостите, идентифицирани в практиките за сигурност на базите данни на Централния граждански регистър, рисуват смущаваща картина, излагайки чувствителните данни на значителни рискове. Липсата на стабилен контрол на достъпа, непоследователните практики за криптиране, неадекватното управление на уязвимостите и липсата на официален план за реакция при инциденти създават благоприятна почва за кибератаки с потенциално опустошителни последици. Въпреки че прозренията, предоставени от ИТ персонала, разкриват ценни признания за тези слабости, те също подчертават належащата необходимост от незабавни действия за коригиране на ситуацията.

Тази теза служи като призив за яснота, призовавайки Централния граждански регистър да даде приоритет на сигурността на базата данни и да приложи цялостни решения за защита на своята критична информация. Препоръките, представени в този анализ, обхващащи подобрения в контрола на достъпа, стабилно криптиране, проактивно управление на уязвимостите, добре дефиниран план за реакция при инциденти и фокус върху сигурността на приложенията, предлагат ясна пътна карта за постигане на значително по-силна позиция на сигурност.

Продължавайки напред, наложително е да се признае неотложността на ситуацията и да се отделят необходимите ресурси за изпълнение на тези препоръки. Инвестирането в технологии, насърчаването на култура, съобразена със сигурността сред ИТ персонала, и стриктното прилагане на най-добрите практики са важни стъпки към смекчаване на рисковете и гарантиране на поверителността, целостта и наличността на данните, поверени на Централния граждански регистър.

Последствията от пренебрегването на сигурността на базата данни вече не са теоретични; те са мощна заплаха с потенциала да подкопаят общественото доверие и да нанесат трайни щети. Времето за действие е сега. Възприемайки препоръките, представени в тази дисертация и посвещавайки се на непрекъснато усъвършенстване, Централният граждански регистър може да се справи с предизвикателството, да защити чувствителните си данни и да демонстрира своя ангажимент за защита на поверителността и сигурността на своите граждани.

Също така идентифицира тревожна тенденция: компаниите в Косово се борят с кибератаки поради липса на обучение на служителите. Въпреки че положителните стъпки включват разпоредби за сигурност и сътрудничество между университетите, са необходими повече действия.

Заключението е сбито обобщение на ключовите констатации, аргументи и препоръки. То подчертава важността на изследването, акцентира върху спешността на ситуацията и предоставя ясен призив за действие за Централния граждански регистър. Това е възможност с дисертацията да се обърне внимание на въпроса и да бъдат насърчени действия, които да дадат приоритет на сигурността на базата данни.

# ОБЩ ИЗВОДИ

Дисертацията, извършена за проучването на сигурността на базите данни в Централния орган на Република Косово, дава подробна представа за предизвикателствата и усилията за защита на данните на гражданите и изграждане на устойчиви системи за сигурност. Бяха положени големи усилия за спазване на законовите изисквания и създаване на среда на доверие за гражданите и заинтересованите страни.

Въз основа на проучването и анализа на предприетите мерки за сигурност се налагат няколко важни извода.

Централният орган на Република Косово положи големи усилия да защити своите бази данни и да защити данните на своите граждани и служители. Усилията за прилагане на политики за сигурност, споделяне на данни и технологии за сигурност са важни стъпки в създаването на сигурна среда за чувствителни данни.

Системата за оторизация и разрешения е подобрена, за да гарантира, че само оторизирани потребители имат достъп до чувствителни данни. Това засяга защитата на чувствителната информация и намалява риска от неоторизиран достъп.

Шифроването на данни е важна част от вашата стратегия за сигурност и помага за предотвратяване на неоторизиран достъп до чувствителни данни, особено при пренос.

Подобрено наблюдение и отчитане на действията, извършени в базата данни. Този процес помага за идентифициране на подозрителна дейност и е важен за предотвратяване на потенциални инциденти със сигурността.

Но има още работа за вършене. Повишаването на осведомеността на служителите относно важността на сигурността, интегрирането на нови технологии и справянето с развиващите се заплахи за сигурността изисква непрекъсната ангажираност и непрекъснато подобрение.

Също така идентифицира тревожна тенденция: компаниите в Косово се борят с кибератаки поради липса на обучение на служителите. Въпреки че положителните стъпки включват разпоредби за сигурност и сътрудничество между университетите, са необходими повече действия.

В обобщение, усилията на Централния орган на Република Косово за изграждане и подобряване на сигурността на базите данни са положителни стъпки към защита на чувствителните данни и изграждане на обществено доверие. Справянето с настоящите и бъдещите предизвикателства е важно, но нашите изследвания показват, че нашите усилия за сигурност на данните са на правилния път за създаване на безопасна и надеждна среда за всички.

# ПРЕПОРЪКИ

Въз основа на констатациите от изследването и идентифицираните предизвикателства, можем да направим някои препоръки за по-нататъшно подобряване на сигурността на базите данни в Централния орган на Република Косово.

- Повишаване на осведомеността: Агенциите трябва да продължат да инвестират в обучение на персонала и повишаване на осведомеността. Повишете осведомеността и ангажираността към сигурността на данните.
- Интегриране на нови технологии: Бързото технологично развитие изисква разумен подход към сигурността. Агенциите трябва да следват най-новите разработки и да гарантират интегрирането на нови технологии за сигурност.
- По-широко сътрудничество: Институциите трябва да продължат да подкрепят сътрудничеството между Myths и тях, за да споделят опит и най-добри практики в областта на сигурността на бази данни.
- Съответствие с текущите разпоредби: Институциите трябва непрекъснато да наблюдават и актуализират своите мерки за сигурност, за да отговарят на текущите разпоредби за защита на данните.
- Планиране на инциденти: Важно е да сте подготвени за възможни инциденти, свързани със сигурността. Агенциите трябва да разработят и тестват планове за реакция при инциденти.
- Компании: Обучавайте служители и си партнирайте с университети.
- Политици: Създайте национални програми за обучение и преодолейте пропастта между индустрията и академичните среди.

# АПРОБАЦИЯ

Тази теза дава положителна оценка на усилията, предприети от Централния орган на Република Косово за осигуряване на своите бази данни и защита на данните на гражданите. Изследването подчертава няколко ключови постижения:

**Прилагане на политики за сигурност, споделяне на данни и технологии за сигурност:** Тези стъпки са от решаващо значение за установяването на стабилна среда за сигурност за чувствителна информация.
**Подобрена система за оторизация и разрешения:** Това укрепва защитата на данните чрез ограничаване на достъпа само до оторизирани потребители.
**Шифроване на данни:** Тази жизненоважна мярка за сигурност защитава чувствителна информация, особено по време на предаване.
**Подобрено наблюдение и докладване:** Този проактивен подход помага за идентифициране и предотвратяване на потенциални инциденти със сигурността.
Въпреки че признава необходимостта от продължаващи усилия, тезата заключава, че инициативите на Косово за сигурност на данните са на прав път. Непрекъснатият ангажимент и адаптирането към развиващите се заплахи са от съществено значение за поддържането на сигурна и надеждна среда.

# ОСНОВНИ ПРИНОСИ

Основните приноси на предложената теза могат да бъдат разделени на научни, научно-приложни и приложни измерения.

**Научен принос:**

- Предлага се подход за анализ на мерките за сигурност който се използва за анализиране на мерките за сигурност, прилагани от централния орган, включително контрол на достъпа, криптиране на данни, наблюдение и докладване. Този подход за анализ осигурява ценна представа за ефективността на мерките за сигурност при защитата на чувствителни данни.

**Научни и приложни приноси:**

- методология за прилагане на технологии за сигурност на бази данни, като силен контрол на достъпа, криптиране на данни и подобрено наблюдение, която може да се прилага от организациите за подобряване на тяхната собствена позиция за сигурност на данните.

**Приложени приноси:**

- Въз основа на предложения подход, представено е решение за оценка на сигурността на базата данни на централните институции на Косово за защита на данните на гражданите.

Тази оценка на казуса може да се използва за идентифициране на области за подобрение и информиране за бъдещи стратегии за сигурност.

# ПУБЛИКАЦИИ СВЪРЗАНИ ДА СЕ НА ДИСЕРТАЦИЯ


1. **B. Prebreza**, D. Gotseva and P. Nakov, "A Study of Documents Management System Based on Web, Case Study: University," *2021 29th National Conference with International Participation (TELECOM)*, Sofia, Bulgaria, 2021, pp. 85-89, doi: 10.1109/TELECOM53156.2021.9659663.
2. **B. Prebreza** Albion Burrniku, Rrezart Prebreza, Qendrim Hykaj(2023). " Impact of Machine Learning on Product Sales Forecast".TuijinJishu /Journal of Propulsion Technology, ISSN:1001-4055, Vol. 44 No.6, pp. 3076-3085, Link:https://propulsiontechjournal.com/index.php/journal/article/view/3859
3. **B. Prebreza** (2020). "How to do the IT network audit". Knowledge – International Journal, Vol. 42.1. Retrieved from: CEEOL - Article Detail
4. Abdulla Prebreza, Rrezart Prebreza, **B. Prebreza** (2023). Exploring Opportunities: Overcoming E-Commerce Challenges for Small and Medium-Sized Businesses in Developing Countries. *International Journal on Recent and Innovation Trends in Computing and Communication, 11*(9), pp. 3501–3505. https://doi.org/10.17762/ijritcc.v11i9.9562
5. Arianit Krypa, Marigona Krypa, **B.Prebreza** Rrezart Prebreza (2023). "Edge Computing: Enabling Opportunities for Industry 4.0 and Addressing the Green Problem". Tuijin Jishu/Journal of Propulsion Technology. Volume 44, Issue 6, pp. 1801-1821, Link: https://propulsiontechjournal.com/index.php/journal/article/view/3482/2386

# SUMMARY

Data privacy is the aspect of information technology (IT) that deals with the ability of an organization or individual to determine what data in a computer system can be shared with third parties. Human beings value their privacy and the protection of their personal sphere of life. They certainly don't want their personal information available to anyone at any time. But recent improvements in information technology threaten privacy and reduce control over personal data and open up the possibility of a number of negative consequences resulting from access to personal data.

This dissertation is a case study of an enterprise and central institution database security project, including the strategy that addresses key focus areas for database security spanning all major RDBMS platforms. It presents the current state of database security tools and processes, the current needs of a typical enterprise organization, and a roadmap for developing database security.

The work done in the dissertation is on the study of database security in the Central Authority of the Republic of Kosovo, providing a detailed insight into the challenges and efforts to protect citizens' data and build sustainable security systems. Great efforts were made to comply with legal requirements and create an environment of trust for citizens and stakeholders.

The dissertation provides a positive assessment of the efforts undertaken by the Central Authority of the Republic of Kosovo to secure its databases and protect citizens' data. The research highlights several key achievements: Implementation of security policies, data sharing and security technologies - these steps are critical to establishing a robust security environment for sensitive information; Improved authorization and permissions system - this strengthens data protection by limiting access to only authorized users; Data Encryption - This vital security measure protects sensitive information, especially during transmission.

Improved monitoring and reporting: This proactive approach helps identify and prevent potential security incidents.

While acknowledging the need for continued efforts, the thesis concludes that Kosovo's data security initiatives are on the right track. Continuous engagement and adaptation to evolving threats is essential to maintaining a secure and reliable environment.

The main contributions of the proposed dissertation have scientific, scientific-applied and applied dimensions.

Scientific contribution:

• A security measures analysis approach is proposed, which is used to analyze the security measures implemented by the central authority, including access control, data encryption, monitoring and reporting. This analysis approach provides valuable insight into the effectiveness of security measures in protecting sensitive data.

Scientific and applied contribution:

• A methodology is proposed for implementing database security technologies such as strong access control, data encryption and enhanced monitoring that can be applied by organizations to improve their own data security posture.

Applied Contribution:

• Based on the proposed approach, a solution for assessing the security of the database of the central institutions of Kosovo for the protection of citizens' data is presented. This case assessment can be used to identify areas for improvement and inform future security strategies.